INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

STUDY GROUP 17

Ref. TD 0913

English only

Original: English

Question(s): 10/17 Geneva, 7-16 April 2010

TEMPORARY DOCUMENT

Source: Editor of Rec. X.1275

Title: Draft Recommendation ITU-T X.1275, Guideline on protection of personally identifiable information in the application of RFID technology

Draft Recommendation ITU-T X.1275 (X.rfpg)

Guideline on protection of personally identifiable information in the application of RFID technology

Summary

Recommendation ITU-T X.1275 recognizes that RFID technology renders information pertaining specifically to the merchandise worn or carried by individuals open to abuse even as it greatly facilitates access to and distribution of such information for useful purpose. The abuse can be manifest as tracking the location of the individual or invasion of his or her privacy in another malfeasant manner. For this reason the Recommendation provides guidelines regarding the RFID procedures that can be used to enjoy the benefits of RFID while attempting to protect personally identifiable information.

Keywords

Protection of personally identifiable information, RFID application

Contact: Hyangjin Lee Tel: +82 2 405 6626

Korea Internet & Security Agency Fax: +82 2 405 5419

Korea (Republic of) Email: jiinii@kisa.or.kr

Table of Contents

Guidelines on protection of personally identifiable information in the application of RFID technology

1 Scope

This Recommendation provides guidance to RFID users and vendors (including RFID service providers and manufacturers) in protecting personally identifiable information for the privacy of individuals in the context of RFID technology.
These guidelines can be applied to cases wherein the RFID system may be used to invade individual privacy; e.g., personally identifiable information is recorded in an RFID tag and subsequently collected, or the object information collected by means of RFID is linked to personally identifiable information. However it does not apply to such cases where the object information is collected and used without any risk of disclosure of personally identifiable information and invasion of privacy.
These guidelines seek to protect personally identifiable information for the privacy of individuals potentially affected by an RFID system and to promote a safe environment for RFID use. These guidelines are intended to provide the basic rules for the RFID service provider and guidance to the RFID service provider, manufacturers and user with regard to privacy in RFID and are subject to local and national laws.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ISO/IEC 18000] ISO/IEC 18000-6C (2004), *Information technology -- Radio frequency identification for item management -- Part 6: Parameters for air interface communications at 860 MHz to 960 MHz*

[ISO/IEC 19762-3] ISO/IEC 19762-3 (2005), *Information technology – Automatic identification and data capture (AIDC) techniques-Harmonized vocabulary--Part3: Radio frequency identification (RFID)*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 personally identifiable information (PII) [ITU-T X.1171]**:** The information pertaining to any living person, which makes it possible to identify such individual (including the information capable of identifying a person when combined with other information even if the information does not clearly identify the person).

3.1.2 RFID system [ISO/IEC 19762-3]: Automatic identification system and data capture system comprising one or more RFID readers/interrogators and one or more RFID tags wherein data transfer is achieved by means of suitably modulated inductive or radiating electromagnetic carriers

3.1.3 RFID tag [ISO/IEC 19762-3]: Any transponder plus the information storage mechanism attached to the object

3.2 Terms defined in this Recommendation

3.2.1 consent: Provision of opt-in or opt-out agreement for a data controller to collect, transfer, use, store, archive, or dispose (of) particular PII, meaning individual, limited agreement.

3.2.2 data controller: An entity linking the object information recorded in the RFID tag to PII, or recording PII in the RFID tag or collecting PII recorded in the RFID tag

3.2.3 data subject: An entity who can be identified by one or more pieces of data related to his or her physical, physiological, mental, financial, cultural, or social attributes

3.2.4 personal data: See personally identifiable information. It is synonymous of personal identifiable information

3.2.5 opt-in: An individual's explicit consent for a PII controller to collect, transfer, use, store, archive, or dispose (of) particular PII for a specific purpose

3.2.6 opt-out: An individual's exercise of choice through a request that a particular collection, transfer, usage, storage, archiving, or disposal of data does not occur

3.2.7 RFID manufacturer: Any entity manufacturing and selling RFID chips/tags or manufacturing (including processing or packaging) and selling objects with built-in attached RFID tags

3.2.8 RFID service provider: Any entity offering a service based on objects that have built-in or attached RFID tags

3.2.8 user: A person who purchases an object with built-in or attached RFID tags or makes use of the service based on an object with built-in or attached RFID tag

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

– PDA: Personal Digital Assistant

– PIA: Privacy Impact Assessment

– PII: Personally identifiable information

– RFID: Radio frequency identification

5 Conventions

None.

6 Privacy principles

The guidelines described in this Recommendation are based on the privacy principles contained in the following document : [b-Council Of Europe], [b-EC1], [b-EC2], [b-OECD], [b-UNHCR]. Those principles include in particular;

– Collection limitation: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, appropriate, with the knowledge or consent of the data subject.
– Data quality: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
– Purpose specification: The purposes for which personal data are collected should be specified not later than at the time of data collection, and the subsequent use limited to the fulfillment of those purposes, or others that are not incompatible with those purposes and as are specified on each occasion of change of purpose.
– Use limitation: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the specified purpose.
– Security safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
– Openness: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
– Individual participation: An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him or her;
b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

– Accountability: A data controller should be accountable for complying with measures that give effect to the principles stated above.

7 Threats and infringements of PII in RFID

Threats and infringements of PII in RFID can be attributable to the characteristics of contact-less RFID technology, vulnerabilities of wireless communication, and possibility of a third party's collection of information via an RFID reader. Appendix II describes the characteristics of RFID technology in detail.

In addition, there is increasing possibility of PII violation due to the introduction of RFID, since the information obtained by a data controller from the RFID tag can be used throughout the entire network, instead of being used in accordance to national and regional laws, regulations and policies, it can also be modified to derive PII. The following section describes the major threats and infringement of PII posed by RFID technology.

Note, however, that including some security mechanisms inside the current RFID tag may be difficult, because of the resources that can be used by a tag, such as electronic power, processing time, storage space, etc. Appendix II and Appendix III describe the restriction of RFID technology and technical measures for protection in the RFID system.

7.1 Invisibility of data collection

Data collection can take place without the knowledge of the data subject, due to the particular characteristics of RFID technology. Data in an RFID tag can be read without any direct line-of-sight because radio waves penetrate obstacles such as bags or clothes, and anybody with a reader can read the data in the RFID tag. Moreover, the size of both an RFID tag and a reader can be very small, and there may be no signs of their operation. This feature can be one of the causes of infringement of PII of RFID technology.

7.2 Profiling

Access to RFID tag information in an object owned or carried by a data subject can reveal the private aspects of his or her preferences. In particular, the profiles and inferences that could be drawn from a cluster of RFID tags carried by a data subject could reveal sensitive information. Moreover, more sensitive information such as nationality, biometric information or medical records could also be revealed in RFID applications such as e-passport and healthcare using RFID technology, and could be directly used to draw up profiles and inferences regarding the data subject.

7.3 Tracking

Data subjects carrying an RFID tag could be tracked, since a unique identifier is assigned to an RFID tag. Tracking is enabled by the collection or processing of location and time data and can be performed either post hoc - with data already stored in a database, or in real time.

8 RFID Applications

RFID technology is widely used for a variety of applications such as healthcare, transportation and logistics, e-government, and information services in support of the retail and supply chain. Table 1 shows the possible threats to PII existing in typical applications using RFID technology

Table 1 – Typical RFID applications and possible threats to PII

Field	Typical applications	Information in RFID tag	Possible privacy threats
Supply chain	Inventory management	Product	Tracking, profiling of persons performing of inventory
	Retail (e.g., Supermarket)	Product	Tracking, profiling (after purchasing good)
Transportation and logistics	Public transportation ticket	User's ID, charging, etc.	Tracking, profiling
	Highway toll	User's ID, charging, etc.	Tracking, profiling
	Vehicle tracking	Product	Tracking, profiling
	Fleet / container management	Product	Tracking, profiling of persons handling of containers
Healthcare	Tracking patients	Patient's ID, medical history, etc	Tracking, profiling, invisibility(ex. VeriChip)
	Preventing medication errors,	Patient's ID, Medical history, prescription, etc.	Tracking, Profiling
	Blood or medicines tracking for anti-counterfeiting	Product	×
e-Government	ePassport	People's ID, nationality, biometric	Tracking, profiling, counterfeiting PII
Information services	Smart poster	Product	×

As shown in Table 1, not all RFID applications give rise to PII infringement concerns (nor do they give rise to possible problems). If the RFID application does not include the user, for example, in some supply chain applications, concerns over the infringement of PII are not likely to be raised
However, if workers are handling containers for instance in other cases of supply chain applications, the activity of those workers can be controlled using the RFID tags.
Following sub-clauses present some application examples with service scenarios which PII infringement may raise concerns.

The combination of RFID readers and other (e.g., mobile) applications enable a variety of communication relationships which could result in enhanced capabilities for tracking and profiling.

8.1 Supply-chain management

RFID technology has been widely used for supply-chain management for a long time now. Key business applications in supply-chain management using RFID include inventory/asset management, retail application, etc. Retail provides the most representative RFID application service. Figure 1 gives an example of RFID use in a retail application, illustrating how an RFID tag is distributed.
RFID retail applications are enabled by a manufacturer that makes an RFID tag, writes the object information to the RFID tag, and attaches the tag to the object. In this example, the retailer in question is an RFID service provider selling an object affixed with an RFID tag to a user. Passive tags have been generally used for the RFID system in supply-chain management and using kill password, etc., to protect for the data subject's PII. In some cases such as applications for individual articles, supply-chain management often requires passive tags with a long communication range even for individual articles.

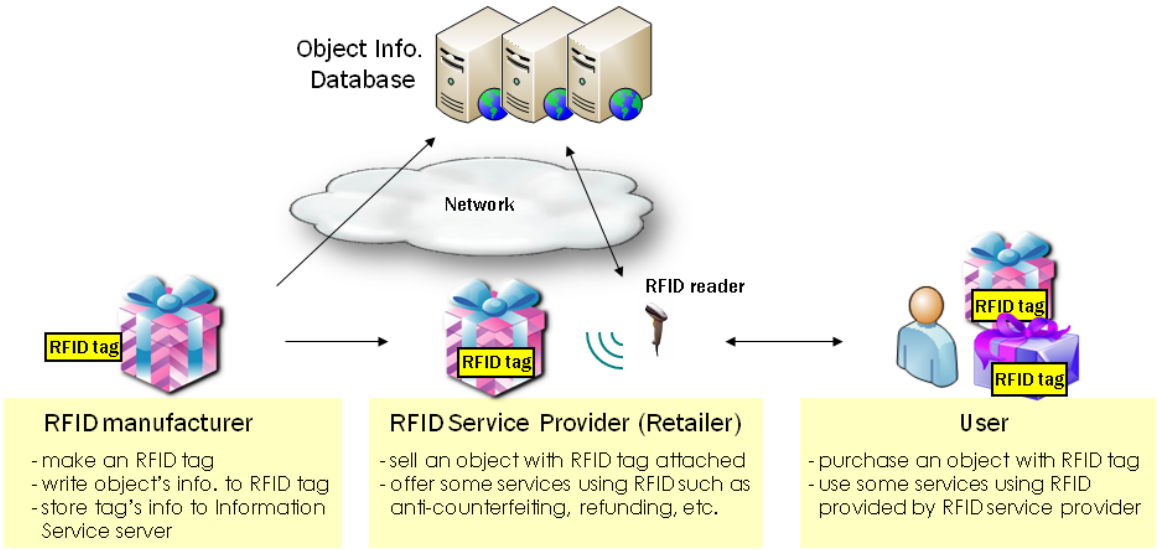

Figure 1 – Example of RFID use in retail applications

Concerns over PII infringement with regard to retail application are mainly raised after a user purchases an object to which an RFID tag is attached, since the participation of the user occurs at the point of sale only during this process. When a user purchases an object affixed with an RFID tag, the retailer can identify such user's preferences by linking the object information stored in the RFID tag with the user's payment information or loyalty card, and by continuously observing and analyzing the user's purchase pattern. In this case, the RFID service provider becomes the data controller, and the user becomes the data subject. And the RFID tag may be read by anybody with a reader, unless the tag is removed or destroyed.

8.2 Transportation and logistics

RFID systems are well suited to certain transportation and logistics applications. Given the appropriate distribution of RFID readers, vehicles equipped with a tag can be tracked in a small area such as a storehouse or a factory. Public transportation tickets and highway toll collection systems such as those described in [b-E-ZPass] are applications that can give rise to privacy concerns in the transportation and logistics sectors.

There are several applications of RFID in transport and logistics. In particular, many public transportation tickets and highway toll systems are already based on RFID technology. Figure 2 gives an example of a transportation application, illustrating how an RFID tag is used for the identification and tracking of a vehicle in the highway toll system.
The RFID manufacturer in a highway toll application simply makes an RFID tag and sells it to the RFID service provider. The RFID service provider offering and managing a highway toll service can write a user's payment information to an RFID tag in some specific cases. The user's payment information stored in an RFID tag is PII that can be used to identify the user conveniently.
If the user's payment information is associated with the movement track information of the user as recorded by the highway toll system, however, such information can seriously threaten the user's privacy. In this case, the RFID service provider -- the highway toll system -- becomes the data controller, and the user becomes the data subject.

Passive tags have been generally used for the RFID system in transportation and logistics. In transportation lightweight cryptographic schemes (based on symmetric encryption scheme) are often used for authentication between the tag and the reader and to secure further data transmission.

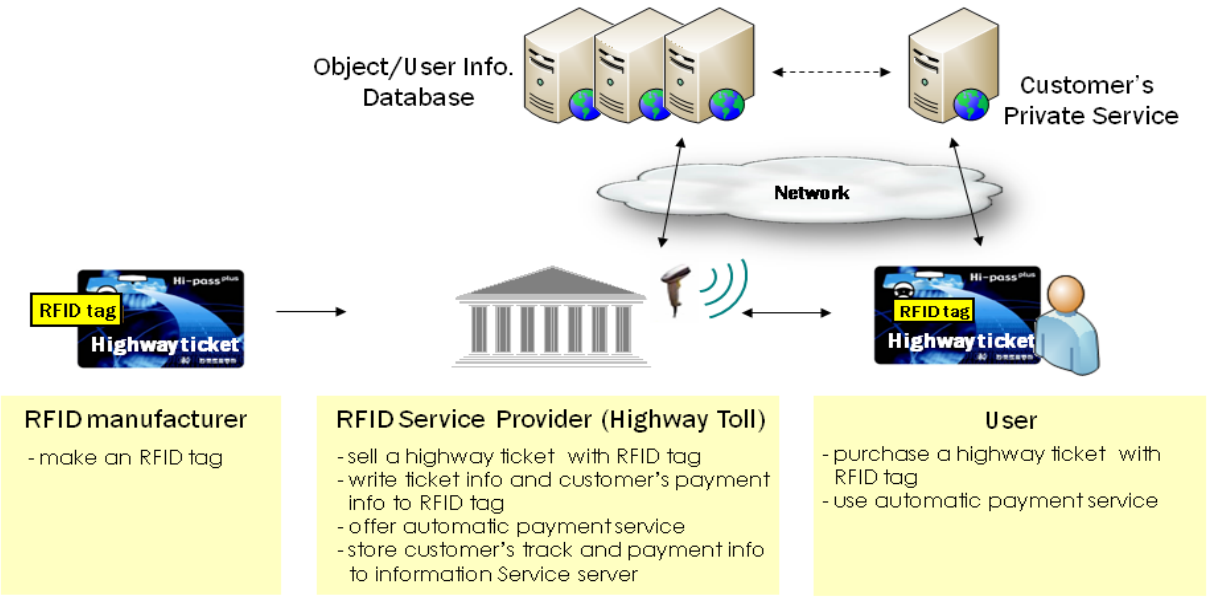

Figure 2 – Example of RFID use in transportation and logistics

For transportation tickets, a contact-less smart card fabricated with RFID chip communicating at 13.56 MHz and having a short communication range is frequently used. In the case of a short read range tag as in this case, using conventional secure cryptographic schemes (even asymmetric schemes) are, at least technically, possible -- which can partially mitigate the risk of leaking the data subject's PII. Note however, that existing protocols in use today can only prevent copying a tag (and so prevent usurpation of the user). The tag ID is still revealed in clear text at the beginning of the transaction between the tag and the reader. As such it can still be read by anybody, with the associated PII infringement concerns. In any case, the data collected in the database when the user interacts with the system should be anonymised as soon as possible in order to reduce the threats to users' privacy. .

8.3 Healthcare and medical application

There are several applications of RFID in healthcare. However, the RFID use in healthcare application can give rise PII infringement concerns owing to the privacy sensitive nature of healthcare data. Various applications of RFID in healthcare include tracking patients for security and safety reason, medicines for anti-counterfeiting measures, patient prescription compliance, and blood tracking. RFID systems are already used in the pharmaceutical industry to facilitate the tracking of medicines and to prevent counterfeiting and loss resulting from theft during transport. Figure 3 gives an example of RFID use in healthcare applications, illustrating how an RFID tag is used.
The RFID manufacturer in patient prescription compliance simply makes an RFID tag and sells it. The RFID service provider, i.e., doctors and nurses in the hospital can become data controllers who write and manage the medical information of the patient.

In the application shown in Figure 2, doctors or nurses in the hospital can check the treatment history and prescriptions of the patient by reading the RFID tag information carried by the patient, and subsequently take the appropriate action based on such. Conversely, in the medicine tacking application, the tag information of the person holding the tagged medicine outside the hospital or the pharmacy store can be easily disclosed; the name of the patient's disease can also be inferred directly from the RFID tag's information. Consequently, the risk of disclosing the data subject's personal information may be higher than that in the application described in Figure 2. Therefore, if the patient's medical information, as stored in an RFID tag or a backend database is not properly managed and protected, such can pose a direct threat to the data subject's PII.

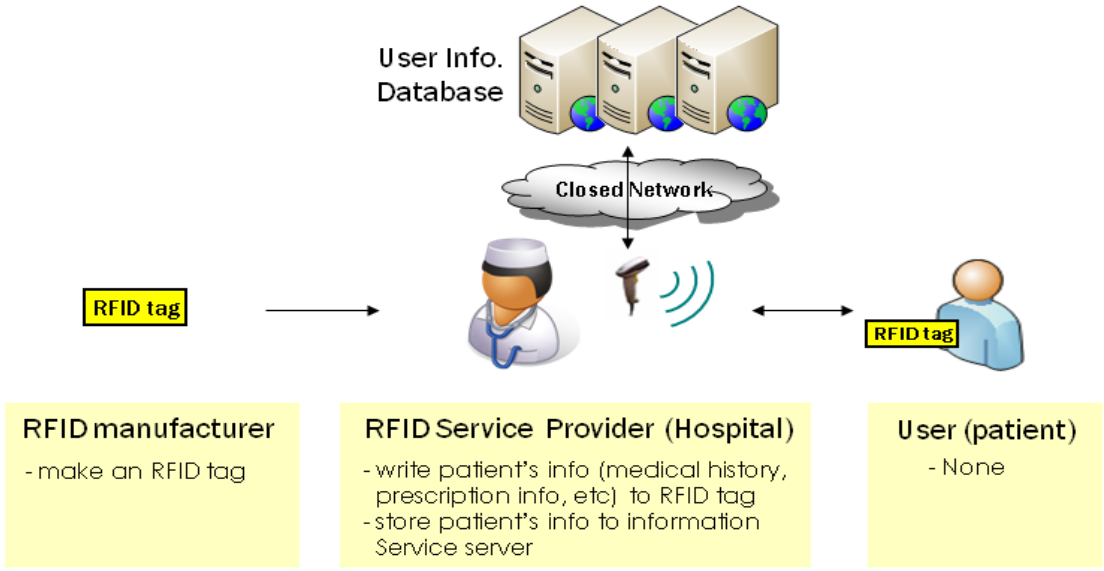

Figure 3 – Example of RFID use in healthcare and medical applications

Active tags with long communication range have not been generally used for the RFID system in healthcare medical applications. However, that there are some cases where active tag with long communication range may be preferred, such as homecare for monitoring an invalid's condition.

8.4 e-government

e-passport is the most typical application in e-government. The RFID chip embedded into the e-passport usually has lots of the data subject's PII such as passport number, name, nationality, picture, biometric information, etc.; thus possibly giving rise to major PII infringement concerns.

It is essential that the RFID tag integrates appropriate security measures to mitigate the risks of capturing or cloning of data in e-passport, since data in e-passport is the most important and critical among PIIs. Figure 4 gives an example of RFID use in the e-passport system, illustrating how an RFID chip is used.

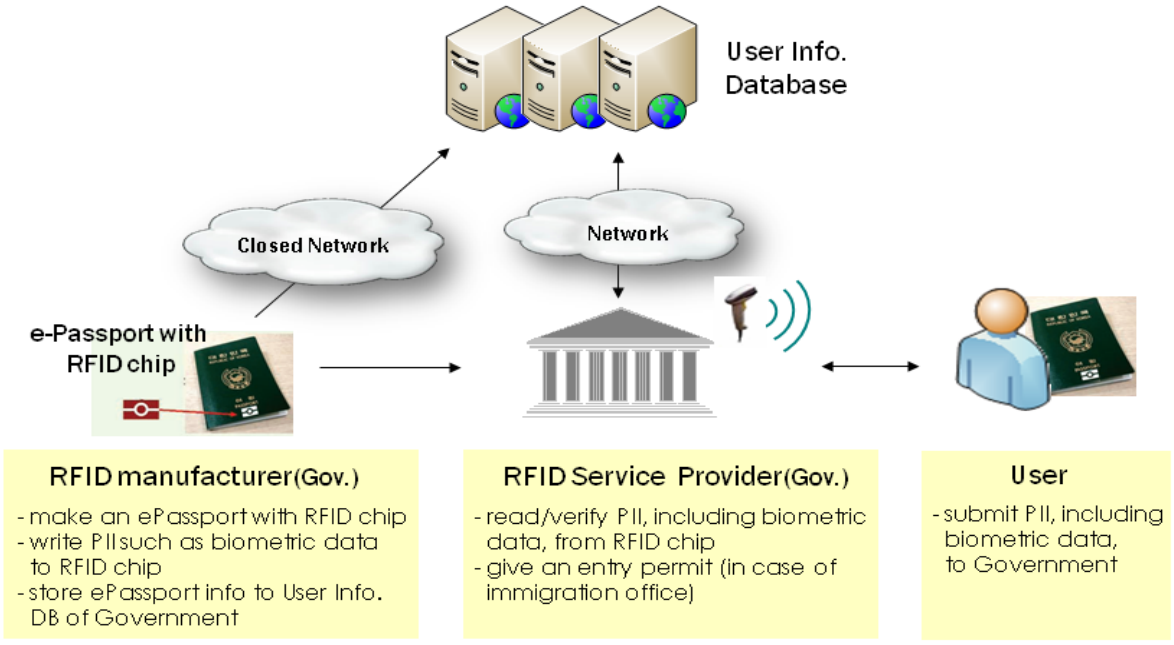

Figure 4 – Example of RFID use in e-passport applications

Any user wishing to get a biometric e-passport submits PII including biometric data to government ministries, which can be the RFID manufacturer in e-passport application. They make an e-passport with RFID chip and write the user's PII including biometric data to the RFID chip. The RFID service provider

such as immigration office reads PII from the RFID chip and verifies such. Biometric data stored in the RFID chip of e-passport is one of the most sensitive PIIs; it can be used to authenticate or identify the user. If disclosed or modified, such biometric data would seriously threaten the user's privacy. In this application, both the RFID manufacturer and RFID service provider can be the data controller; the user is the data subject. Passive tags with short communication range have been generally used in this application. e-passport shall support cryptography.

But the security protocols described in standards such as [b-ICAO] are sometimes optional, or badly used. Therefore, there are still great privacy concerns in e-passport applications.

8.5 Information service

Smart poster is one of the typical information service applications. In the case of smart poster, an RFID reader is usually equipped in a mobile device and an RFID tag resides at a fixed location. Figure 5 gives an example of RFID use in smart poster application, illustrating how an RFID tag and reader are used.

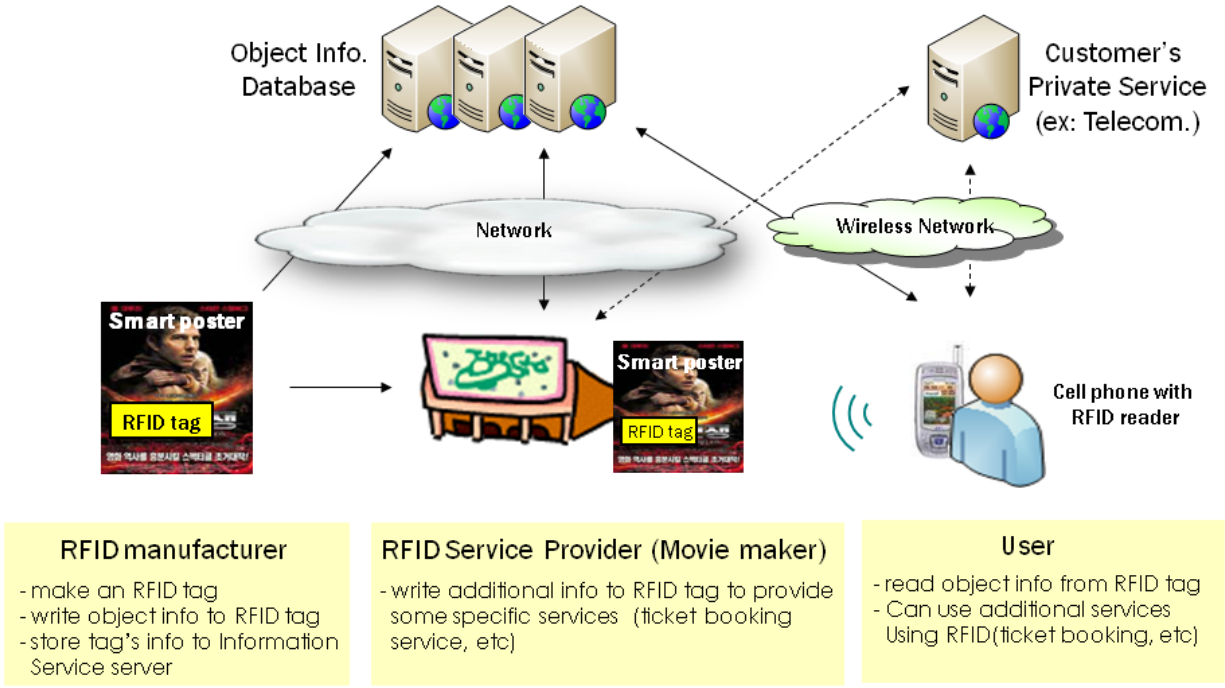

Figure 5 – Flow of RFID use in smart poster application

The RFID manufacturer of a smart poster simply makes an RFID chip and sells it to the RFID service provider. The movie maker or theater is an RFID service provider writing information about the movie to the RFID tag embedded into the smart poster. In other examples of information services, road guidance is a service that gives information to the user as to how to find a route easily. These kinds of applications actually do not give rise to any privacy concerns because they do not use any private or sensitive information. Note, however, that the mobility and read range of the RFID reader embedded into mobile device can be one factor threatening the privacy of users.

9 Guidelines on protection for personally identifiable information

Since technologies for privacy and security related to RFID are in the early stage, even as they are being developed, and there is no "fit-all" solution as the context of use and the technical characteristics of the RFID tags greatly differ from one application to another, applying them to the entire RFID service would be a premature move. Therefore, these guidelines mainly focus on the general managerial measures for protecting the data subject's PII rather than on technical measures. Nonetheless, technical measures should not be ignored: during the conception of an RFID-based application, designers are encouraged to consider the adoption of state-of-the-art technical solutions that may improve privacy protection

9.1 Policies and procedures

Data controllers in the RFID service should formulate policies and procedures governing the RFID system particularly on the appropriate use of PII and publish them in advance. Roles and responsibilities related to managing and using PII should be assigned in such policies and procedures. Moreover, the data controller should assign more responsibilities to a person managing and using PII directly in contrast to others.

9.2 Restriction on recording PII

Data controllers should comply with the collection limitation principle. Therefore, the controller shall only process data which are relevant for the purpose for which the system was designed and PII may not be stored for longer than necessary.
In particular, data controllers in the RFID service shall not normally record PII on the RFID tag except where recording of PII is stipulated by law or by an explicit written consent from the data subject.
All PII recorded on RFID tags are required to be encrypted, if data controllers have to record PII on the RFID tag. When data controllers need the data subject's consent, opt-in should be preferred. Data controllers must notify the data subject in advance of the purpose for recording and the potential use of PII.

Data controllers in the RFID service need to get individual, specific consent for each recorded item of PII and should inform data subjects of the purpose of recording or using PII.

9.3 Information, consent, right of access, rectification, right to oppose

Data controllers should comply with the individual participation principle. Therefore, data controllers in the RFID service are required to take appropriate measures to provide the user information about the recorded PII and consent, right of access, rectification, right to oppose of data subject's PII without costs for the user. This is applicable for PII that is encoded on the RFID tags as well as for PII which is linked with information stored in the RFID tags.

9.3.1 Information

Data subject should be notified by the data controllers of indication of the attached RFID tag and installation of the RFID reader, third parties to whom the data have been disclosed of any rectification, erasure of blocking, unless this proves impossible or involves a disproportionate effort.

9.3.1.1 Indication of the attached RFID tag

For a built-in or attached RFID tag, even after the user purchased or received the object, data controllers in the RFID service shall explain the following to the user in advance, before he purchases the object, or indicate the information on the object or use some easily noticeable means:

- The fact that an RFID tag is attached and its location
- Nature and function of the RFID tag
- Type of information recorded in the RFID tag
- Purpose or use of the information recorded in the RFID tag
- Contact information of a data protection official in accordance with clause 9.9

Note that if the tag is not meant to be used by the data subject once he has purchased the object, it should be deactivated by the RFID service or data controllers at the moment when the user purchases the tagged object, unless the user decides to keep the tag in operation.

9.3.1.2 Indication of installation of the RFID reader

Anybody installing a reader capable of reading the information on an object with a built-in or attached RFID tag (or PII recorded in the RFID tag and delivered to data subjects) shall indicate where and why a reader is installed on the place such as checkout that data subjects can easily notice it. The notice shall include at least the identity of the operator and a point of contact for individuals to obtain the information policy for the service

If an RFID reader is embedded into a personal PDA or cell phone, the read range of the reader must be restricted to limit the acquisition of PII through the RFID tag.

9.3.2 Consent

Data controllers are required to obtain the data subject's consent in advance. In cases of retail and logistics when the principle is deactivation by default, data controllers can obtain the data subject's consent by getting specific written agreement, user registration form, email and etc. In other case such as biometric e-passport application, user consent is not required because there is a legal obligation to collect PIIs and store them in the tag.

9.3.3 Rights of access, rectification and right to oppose

Data subject should be able to obtain from the data controller, without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to the data subject are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
- communication to the data subject in an intelligible form of the data undergoing processing and of any available information as to their source,
- knowledge of the logic involved in any automatic processing of data concerning the data subject at least in the case of the automated decisions

Moreover, data subject should be able obtain from the data controller as appropriate the rectification, erasure or blocking data, in particular because of the incomplete or inaccurate of the data.

Data controllers are required to immediately destroy the information after they have accomplished the purpose of processing PII, unless there are special regulations requiring retention of PII once the purpose for which data were originally processed has been accomplished.

In particular, if the tag is of no use for the data subject (e.g., in the retail sector, when a user purchases a tagged item), data controllers are required to kill or destroy the tag unless the data subjects requests that such tag should remain in operation.

9.4 Restriction on collecting and linking PII

Data controllers in the RFID service should notify the relevant data subject when they collect the PII recorded in the tag or stored in a database by linking with object information in the tag. If RFID service providers need to use PII for purposes other than the intended one or offer such information to a third party, they are required to obtain the data subject's written specific and informed consent in advance.

9.4.1 PII recorded in RFID tag

Data controllers in the RFID service are required to notify the relevant data subject accordingly or indicate in an easily noticeable manner that they can collect the PII recorded in the RFID tag, and get in advance user's specific and informed consent.

When data controllers collect PII, they shall take some certification measures for the RFID reader and tag, such as an authentication protocol between the RFID tag and reader. Certification measures also concern tags and not only the backend database. Here, "certification measure" refers to the cryptographic scheme for the backend database storing the RFID tag identifier and PII used to identify and authenticate the RFID reader and data controller.
From the PII protection point of view, however, it should be noted that existing authentication protocols between the tag and the reader are only efficient if the tag stores more information than the ID of the tag, as, with existing RFID transmission protocols, the tag ID itself is not protected.

9.4.2 PII linked object information in the RFID tag

If data controllers want to link the object information recorded in the RFID tag to PII, they shall, normally before providing the tag, notify the data subject concerned in advance, indicate such in an easily noticeable manner and get the specific and informed consent. When data controllers link the object information in the RFID tag to PII, they should take some certification measures for the RFID reader such as password or authentication protocol between the RFID reader and tag.

If PII was not supposed to be linked to object information when it was collected but needs to be linked later, data controllers should notify the user of its purpose and obtain additional specific and informed consent to comply with legal requirements.

9.5 Deactivation of the RFID tag once the purpose is fulfilled

Built-in or attached RFID tags, shall be removed, destroyed or permanently deactivated by the RFID service provider or data controllers at the moment when the user purchases or receives the tagged object (point of sale), unless the user decides to keep the tag in operation or it is required by law or regulation that the tag needs to be kept active. Even though the user decides to keep the tag in operation, data controllers should provide measures to remove, destroy or permanently deactivate the tags at a later stage on data subject's request. And the user should be notified about consequences of the deactivation.

Deactivation is required to be the normal case, but it can be not an appropriate solution for every applications. For example, if the tag which is employed to access the patient's treatment history and prescription information in the healthcare application – is deactivated, then continuous treatment of the patient may become more difficult. Deactivation can be mandatory in applications in supply chain management, whereas it can be user's option in applications in transportation and logistics. In case of applications in healthcare and e-Government, deactivation is not applicable, for public health or by law. The RFID manufacturer or data controller in the RFID service can use some technical measures for deactivating the RFID tag, such as kill password, RFID Zapper, etc. If deactivating an RFID tag impairs the user's interest or public interest, however, data controllers should explain the reason to the user or indicate it on the object or use easily noticeable means.

9.6 Information about service providers and data controllers

Service providers and data controllers should develop and publish a concise, accurate and easy to understand information policy for each of their applications. The policy should at least include:

- the identity and address of the controllers,
- the purpose of the RFID system,
- what data are to be processed by the system, in particular if personal data will be processed, and whether the location of tags will be monitored,
- a summary of the privacy and data protection impact assessment,
- the likely privacy risks, if any, relating to the use of tags in the application and the measures that individuals can take to mitigate these risks.

9.7 Organizational and technical measures for protecting PII

- When data controllers in the RFID service use the RFID system to record and collect PII or link the object information of the RFID tag to PII, they should take organizational and technical security measures to protect PII of the RFID system lest the relevant PII be lost, stolen, leaked, altered or impaired. Organizational and operational measures for protecting PII include the following:
  - Internal security management plan
  - Risk analysis, privacy threat analysis and privacy impact assessment
  - Education on privacy in the RFID service, etc.
- Technical measures for protecting PII include the following:
  - Access control and audit for backend database
  - Access control to prevent any reader from accessing the information stored in the tag
  - Encryption for PII stored on the tag and backend database
  - Use of any feasible protocol between the reader and the tag to protect PII transmission, such as cryptography protocols or any technique which may be pertinent
  - Use of tags implementing random tag identifiers, to reduce tracking risks
  - Certification of valid RFID reader
  - Deactivating the RFID tag such as, Kill password, RFID Zapper, etc
  - Restricting the ability of the reader and the tag such as Active jamming, RFID sensor detection, clipped tag, blocker tag, etc [b-Juels]

- Security measures to mitigate the privacy risks derived from the PIA.

Note that organizational and technical measures listed above are part of all measures for protecting PII. New measures may emerge in the future because the research in this area is in progress.

9.8 Assessment of the privacy impact of the RFID system

When RFID service providers and data controllers use the RFID system to record and collect PII, or link the object information of the RFID tag to PII, they should make efforts to ensure that PII is not infringed by analyzing and assessing any PII leak possibility or threats to PII accompanying the use of the RFID system before the RFID system is introduced, ideally at the design stage.
Owing to the wide variety of technical configuration and use scenarios, there is no solution that fits all various RFID applications. Therefore, a privacy impact assessment could help determine the implications for privacy (according to different points of view such as legal, and technical aspects) and to aid in finding the best strategies for mitigating them. The following describes a possible PIA (privacy impact analysis) process. The PIA should cover the entire RFID system.

- Step 1: Project initiation
  This step determines the scope of business executing PIA organizes the PIA execution team, and applies the PIA tools to reflect the defined scope.
- Step 2: Data flow analysis
  The purpose of this step seeks to draw a diagram or a flowchart of the personally identifiable information so that the target of the risk analysis can be checked by identifying the personally identifiable information handled by the impact evaluation target service and information assets containing such information.

  Specifically, this step identifies which PII is collected, used, stored, disposed of, or provided to a third party by using what method in a diagram or a flowchart. In addition, this step describes the role and responsibility of the person in charge of each step (collection, use, storage, and disposal) of handling PII.
- Step 3: Analysis of personally identifiable information infringement factors and risk
  This step identifies the threats and vulnerabilities against personally identifiable information assets, and performs risk analysis on such.
- Step 4: Improvement plan and risk management planning
  This step determines the level of risk that requires management among the various risks identified during risk analysis with regard to personally identifiable information, and prepares various control methods for each risk to be mitigated and managed.
- Step 5: Reporting the PIA result
  As one of the most critical steps of the PIA process, this step involves composing and submitting reports on the PIA process and result.

  The PIA reports should include the result of the contents discussed in all PIA processes, from the PIA result to the control and risk management method for the identified risk with regard to personally identifiable information.

Note that the described PIA process above is only an illustration and actual PIA process can be adapted to specific needs or based on other existing external PIA process

9.9 Appointment of a data protection official

Data controllers should appoint a data protection official in charge of in particular for keeping a register containing detailed information on the processing operations carried out by the data controller, including information the privacy impact assessments and security measures of the RFID applications, and for promptly processing users' complaints or requests to exercise their rights.

Appendix I. Characteristics and restrictions of RFID tag

(This Appendix does not form an integral part of this Recommendation)

I.1 Classification and characteristics of RFID tags

This section explains the characteristics of RFID tag classification, as well as why security techniques cannot be applied to a passive tag easily. RFID tags can usually be classified into passive and active tags. Table I.1 shows the classification of the tags.

Table I.1 – Classification and characteristics of RFID tags

Characteristics	Passive tags	Active tags
Power source	Power transferred from the reader	Internal battery
Communication range	3m or less	100m or more
Life time	Unlimited	Limited by the battery life
Data storage	Small read/write data storage (Bytes)	Large read/write data storage (KBytes)
Typical applications	Inventory management, Retail, Luggage/Pallet control, Security cards, etc.	Complex applications with tracking person, etc. (Healthcare or Area monitoring, Highway toll, etc)

Passive tags do not have an internal source of power; they use the power transferred from the RFID reader, to send a signal to the reader. The communications range of passive tags is about 3 m or less. In the case of 13.56 MHz, the communications range is around 4~10 cm, but can be extended with a large-scale antenna The UHF tag has a longer communication range is about 3 m~7 m.

In contrast to passive tags, active tags have their own source of power which enables them to send a signal to the reader by themselves. The communication range of active tags is about 100 m or more, but their life time is limited to that of their batteries. Furthermore, active tags are larger and more expensive than passive tags.

Usually, a system operating in the low frequency (125/135 kHz) or high frequency (13.56 MHz) band is a passive system. Systems operating in the ultra high frequency (433/900 MHz, 2.45 GHz) and microwave frequency bands can be either passive or active systems.

The low-frequency tag is mostly used for security, asset management, and checking of the authenticity of a product due to its short tag-scanning range; whereas, the high-frequency tag is used for railway services, logistics, and distribution, due to its scanning range of 30 m+. In particular, 13.56 MHz is incorporated and used by credit cards or transportation fee payment cards. e-passport and near field communication (NFC) are other examples of applications using 13.56 MHz.

I.2 Restrictions of passive tags

Many experts working in the RFID sector point out that the RFID tag price should be lower than 5 cents in order to promote the RFID market. This requirement for the RFID tag price limits the resources that can be used by a tag, such as electric power, processing time, storage space, and the number of gates.

For a tag to be priced at less than 5 cents, RFID tags can only store hundreds of bits, have 5-10 K logic gates, and a maximum communication range of a few meters. Within this gate counting, only somewhere between 250 and 3000 gates can be devoted to security functions. Additionally, power restrictions should be taken into account, since most of the RFID tags currently in use are passive.
Legislation often limits the radiation power of the readers and, as such, powering the tag is limited. With today's technology, even without the cost restriction, the use of secure standard cryptography with passive tags is limited to short range tags. In tags with a range of several meters, the power radiated by the reader is not enough to power the many gates needed to implement secure cryptographic functions.

According to [b-CRYPTREC], 6~13 K gates are required to implement an asymmetric encryption algorithm, and a similar number of gates is also required to implement a hash function. For example, 20~30 K gates are required for a standard implementation of the Advanced Encryption Standard (AES). Currently, a lightweight encryption algorithm is being developed for application to an RFID tag. Still the implementation of an encryption algorithm within a tag has not yet been enabled fully due to these limitations on the resources.

Appendix II. Technical measures for protecting PII in the RFID system
(This Appendix does not form an integral part of this Recommendation)

Various PII protection technologies are being developed to minimize the threat of privacy invasion in RFID application services. In particular, the new technologies described below are being developed, since the existing encryption and authentication technology designed to protect privacy cannot be applied owing to resource limitation within RFID tags.

II.1 Kill tag using password

As the most common method of protecting the user's privacy, this technique makes use of the fact that an RFID tag can have a "kill" or an "active" stage. When required, the reader sends a "Kill" command including a password (32 bits) to deactivate the tag function. However, the Kill tag can only be used in some applications, since the automatic identification function that is the strength of RFID technology, cannot be used once the Kill command has been applied. For example, if the tag function of the item attached with an RFID tag is disabled upon purchase, return or refund may be impossible since the history of the product in question cannot be retrieved. Moreover, the Kill tag is not secure enough to protect PII because it has only a 32-bits password and the kill functionality may also be vulnerable to a denial-of-service attack wherein an attacker kills all tags around the attacker.

II.2 Privacy protection using physical technology

II.2.1 Faraday cage

A Faraday cage is a technology that prevents the illegal RFID reader from scanning the tag information by disturbing a reader's wireless signal transmission, using a container made of a special material that blocks radio emissions. A metallic coil is used to block the wireless signal. Even though it has useful applications in some areas, however, the use of the Faraday cage is relatively limited, since the privacy protection function is lost when the item is removed from the container.

Figure II.1 – Faraday cage Passport Wallet

II.2.2 Blocker tag

The blocker tag is a technology developed by the RSA in 2003. This special RFID tag prevents the leak of tag information caused by an illegal reader's attempts to disturb the communication of neighboring tags by generating a meaningless signal. For example, an RFID tag contains a special bit assigned as "public" or "private". For medical supply item attached with this tag, the special bit is set to "public" before its sale but changed to "private" at the counter upon purchase. When medical supply item with a "private" tag is inserted into a container using a blocker tag, the tag information set to "private" by a blocker tag cannot be read by others; thus protecting the privacy of the purchaser.

II.2.3 Active jamming

Active jamming disturbs the operation of all RFID readers located close to the device, using a device that emits a strong jamming wave. This way, this technology prevents personal information leakage by blocking the RFID tag information.

Note that blocker tag and active jamming are simple technology which may easily be used for denial of service attacks. Furthermore it is possible solutions only at the user level and not solutions which can be integrated in the RFID service.

II.2.4 Clipped tag

The clipped tag was developed by IBM to supplement the shortcomings of the Kill command, by shortening the communication distance of a tag by cutting off some of the antenna connection line located inside a tag. It can minimize the possibility of privacy violation through location tracing from a remote site, by reducing the information distance considerably while keeping the information storage function of a tag unchanged.

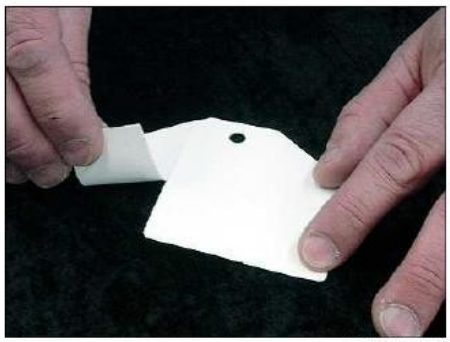

Figure II.2 – Clipped Tag

II.2.5 RFID Zapper

The RFID Zapper was presented on the Chaos Communication Congress 2005. It is an electronic device which can permanently deactivate passive RFID tags. The RFID zapper is designed to not damage any device the RFID tag may be attached in contrast to other methods such as active jamming and clipped tag.

II.3 Privacy protection using cryptographic technology

The following are solutions using light weight cryptography protocols to provide better security and privacy protection at the tag level. The proposed solutions are not mature enough to be used efficiently in an actual application, but a lot of academic research in this area is underway. Even though they are non applicable today, the proposed solutions give a good insight of what a mature solution may look like in the future. Note that there is a good chance that these protocols will require changes to currently standardized radio protocols (ISO/IEC 14443, ISO/IEC 18000 or EPCGlobal)."

II.3.1 Hash lock

As one of the representative methods using cryptographic technology, the hash lock transmits the tag information to the authorized reader and the backend database only based on the difficulty of computing a reversed function of a one-way hash function. As described in detail in Figure II.3, only metaID is provided in response to the reader's tag information request, which is then transmitted to a reader after checking the authentication information legally obtained by the reader from the backend database. However, that this method entails a problem, i.e., the user can be traced, since a metaID is static value and could have been used as a tag identifier.

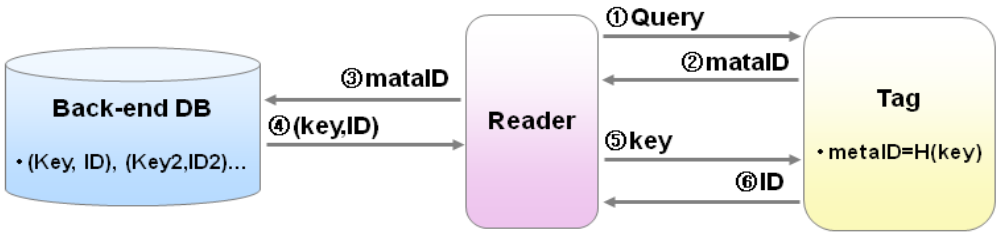

Figure II.3 – Hash lock

The randomized hash lock technique is one of the methods suggested to resolve the problem of user traceability in the existing hash lock technique. As described in detail in Figure II.4, this technique can prevent tracing by making a tag generate a different value whenever the tag information is accessed, using a random number generator with a hash function. Various other techniques based on a hash function - such as hash chain – have been proposed, however, they were deemed impractical [b-Weis].

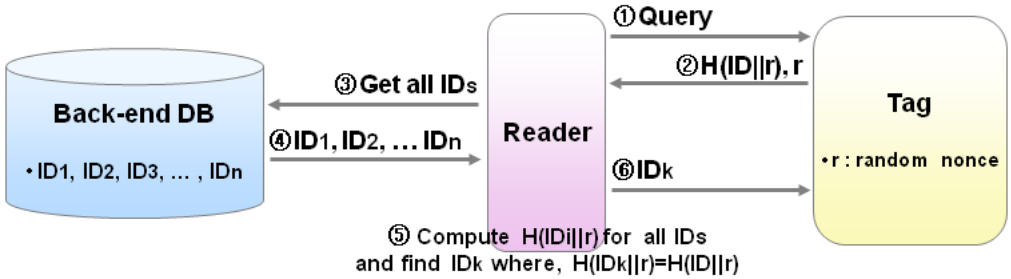

Figure II.4 – Randomized hash lock

II.3.2 Re-encryption

The re-encryption method allows only the backend database or reader with the backend database's public key to collect the tag information, since the legal backend database or reader encrypts the tag ID periodically with the public key and saves the generated information in a tag. The protocol of re-encryption is based on ElGamal and consists of two steps. Initially, backend database generates C using its public key and random number, and saves C in a tag. Second step is described in detail in Figure II.5.

This method can be applied to a high-value note. Once this method is employed, periodic encryption prevents the tracing of the RFID tag information. Nonetheless, the threat of information leak by wire-tapping during public key transmission exists, since a public key encryption method is used. In addition, the methods based on public key encryption such as re-encryption cannot be applied to a low-priced passive tag using the currently available technology.

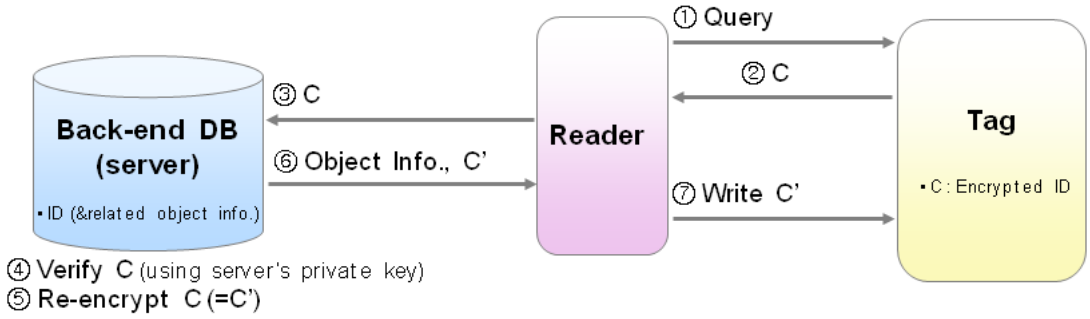

Figure II.5 – Re-encryption

Bibliography

[b-CouncilofEurope] Councile of Europe, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", 1981 http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm

[b-CRYPTREC] Information-technology Promotion Agency of Japan, "CRYPTREC Report2002", March 2003

[b-DSTI/ICCP] OECD DSTI/ICCP, "RFID, OECD Policy Guidance, A Focus on Information Security and Privacy, Applications, Impacts and Country Initiatives", June 2008

[b-EC1] Directive 95/46/EC of the european parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

[b-EC2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

[b-EPIC] Electronic Privacy Information Center, "Guidelines on Commercial Use of RFID Technology", July 2004.

[b-E-Zpass] http://www.ezpass.com/static/info/howit.shtml

[b-ICAO] ICAO, Machine Readable Travel Documents, Doc 9303 Part1 Volume 2, 6th edition 2006

[b-IPC] Information and Privacy Commissioner/Ontario, "Privacy Guidelines for RFID information Systems", June 2006

[b-Isamu Y] Isamu Y., Shinichi S., Akira I. and Satoshi I., "Secure Active RFID tag System", 7th International Conference on Ubiquitous Computing, September 2005.

[b- Japan] MIC (Ministry of Internal Affairs and Communications), METI(Ministry of Economy, Trade and Industry) of Japan, "Guidelines for Privacy Protection with Regard to RFID Tags", July 2004.

[b-Juels] Juels, A., Rivest, R.L., and Szydlo, M., "The Blocker tag: Selective Blocking of RFID Tags for Consumer Privacy", ACM Conference on Computer and Communications Security, 2003.

[b-Junichiro] Junichiro Saito, Jae-Cheol Ryou, and Kouichi Sakurai, "Enhancing Privacy of Universal Re-encryption Scheme for RFID tags", Embedded and Ubiquitous Computing 2004.

[b-Korea] MIC (Ministry of Information and Communication) of Korea, "RFID Privacy Protection Guideline", July 2005

[b-NIST] NIST SP 800-98, "Guidance for Securing Radio Frequency Identification (RFID) Systems", September 2007

[b-OECD] OECD, "Guideline on the Protection of Privacy and Transborder Flows of Personal Data", 1980

[b-Peris-Lopez] Pedro Peris-Lopez et al, "M^2 AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags", 3rd International Conference on Ubiquitous Intelligence and Computing, September 2006

[b-PIA Canada] Treasury Board of Canada Secretariat, "Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks", http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld2-eng.asp

[b-ISO 22307] ISO 22307:2008, "Financial services – Privacy Impact Assessment", August 2008

[b-PIA Korea] MIC (Ministry of Information and Communication) of Korea, "Privacy Impact Assessment Guideline for Private Sector", December 2005

[b-Simon L1] Simson L. Garfinkel, Ari Juels and Ravi Pappu, "RFID Privacy: An Overview of Problems and Proposed Solutions", IEEE Security and Privacy, 2005.

[b-Simon L2] Simson L. Garfinkel and Beth Rosenberg, "RFID: Applications, Security, and Privacy", Addison-Wesley Professional, July 2005

[b-UNHCR] UN General Assembly, “Guidelines for the Regulation of Computerized Personal Data Files”, 1990 http://www.unhcr.org/refworld/publisher,UNGA,THEMGUIDE,,3ddcafaac,0.html

[b-Weis] S. Weis et al., “Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems”, Security and Pervasive Computing 2003

_____