International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1171

(02/2009)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services – Networked ID security

Threats and requirements for protection of personally identifiable information in applications using tag-based identification

Recommendation ITU-T X.1171

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	**X.1170–X.1179**
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1171

Threats and requirements for protection of personally identifiable information in applications using tag-based identification

Summary

The widespread deployment of identification tags, including radio frequency identification (RFID) tags can give rise to concerns of privacy infringement because of the abilities of RFID technology to automatically collect (and process) data, with the possible disclosure of such data to the public (deliberately or accidentally).

For applications using tag-based identification and relying on a personalized identification tag in personalized after-sale management applications, healthcare-related applications, etc., the privacy issue is becoming an increasingly serious problem. This Recommendation describes a number of personally identifiable information (PII) infringements for applications using tag-based identification, and requirements for PII protection. In addition, this Recommendation provides a basic structure of PII protection based on PII policy profile.

Source

Recommendation ITU-T X.1171 was approved on 20 February 2009 by ITU-T Study Group 17 (2009-2012) under the WTSA Resolution 1 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Recommendation ITU-T X.1171[1]

Threats and requirements for protection of personally identifiable information in applications using tag-based identification

1 Scope

The scope of this Recommendation covers the following objectives including threats and requirements for protection of personally identifiable information (PII) in applications using tag-based identification as described below:

– To describe PII threats in a business-to-customer (B2C)-based environment of applications using tag-based identification;

– To identify requirements for PII protection in a B2C-based environment of applications using tag-based identification.

The following objectives are not covered by the scope of this Recommendation:

– to analyse the general security threats and requirements of applications using tag-based identification;

– to analyse the PII threats and requirements between an identification (ID) tag and an ID terminal;

– to analyse the PII threats and requirements depending on the specific ID tagging and reading method, e.g., radio frequency identification (RFID) tag and ID terminal;

– to define and develop the message formats and mechanism for protection of PII based on the user PII policy profile of an application using tag-based identification.

NOTE 1 – Further work will be necessary to define such formats, which may not be restricted to the sole protection of PII of tag-based identification use, but perhaps with a more general (privacy) approach.

In this Recommendation, the ID tag user has the capability for controlling the ID tag itself, and therefore it is assumed that the ID tag user is responsible for the behaviour of the ID tag.

NOTE 2 – In some cases, the ID tag user cannot have any capability for controlling the ID tag. For example, someone buys a tagged product and the manufacturer requires the ID tag to remain active for warranty purposes. In this scenario, the ID tag user may be just a person carrying and using the tagged product. Hence, this Recommendation cannot be applied to solve the above problem for this case. This scenario involves some legislation and policy issues (see [b-OECD]) and this issue can be addressed in another Recommendation.

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.

[ITU-T X.1121] Recommendation ITU-T X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.

[1] This Recommendation may not be applicable in Germany due to German legislation.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 application server [ITU-T X.1121]: An entity that connects to an open network for data communication with mobile terminals.

3.1.3 application service provider (ASP) [ITU-T X.1121]: An entity (person or group) which provides application service(s) to mobile users through an application server.

3.1.4 authentication [b-ITU-T X.811]: The provision of assurance of the claimed identity of an entity.

NOTE – The usage of the word identity is made with the understanding that in the context of telecommunications it is an identifier or set of identifiers that is trusted, meaning it is considered to be reliable for the purposes of a particular situation to represent a network element, network terminal equipment, or user, after the completion of a validation process. As the term is used here, one cannot conclude that trusted identifiers constitute positive validation of a person.

3.1.5 identifier [b-ITU-T F.771]: A series of digits, characters and symbols or any other form of data used to identify a real-world entity. It is used to represent the relationship between the real-world entity and its information/attributes in computers. This relationship enables users to access the information/attributes of the entity stored in computers via users' ID terminals.

3.1.6 ID tag [b-ITU-T F.771]: A tiny physical object which stores a small amount of information which is an identifier or includes an identifier with other additional application data such as name, title, price, and address.

3.1.7 ID terminal [b-ITU-T F.771]: A device with a capability to capture data from ID tags, and other capabilities such as communication capability and multimedia information presentation capability. The data capture capability may include a function to obtain identifier from ID tags even with no communication capability such as barcodes and 2D barcodes. Examples of equipment that use data capture techniques are digital camera, optical scanners, RF transponders, IrDA, galvanic wire-lines, etc.

3.1.8 mobile network [ITU-T X.1121]: A network that provides wireless network access points to mobile terminals.

3.1.9 mobile terminal [ITU-T X.1121]: An entity that has a wireless network access function and connects a mobile network for data communication with application servers or other mobile terminals.

3.1.10 mobile user [ITU-T X.1121]: An entity (person) that uses and operates the mobile terminal for receiving various services from application service providers.

3.1.11 personally identifiable information (PII) [b-ITU-T Y.2720]: 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).

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 applications using tag-based identification: Applications which involve at least the elements: identifier, ID terminal, ID tag and network(s). In this application, the identifier is stored on an ID tag and all information associated to the identifier is provided on the network side.

NOTE – The identifier is stored on a ID tag (or in an ID tag, depending on the kind of ID tag) and an ID terminal reads or writes the identifier from/to the ID tag via an optical scanner (read only), camera (read only), IrDA (read/write), RF technique (read/write) or other similar methods.

3.2.2 business-to-consumer (B2C): A business relationship between businesses and consumers where the service providers provide valuable and useful services to the consumers and the consumers use them.

3.2.3 default PII policy profile: A formatted set of the PII protection rules and policies of an application using tag-based identification.

3.2.4 identification (ID): The procedure of specifically identifying an object from a large class of objects through the reading of identifiers of ID tags.

3.2.5 ID tag user: A person who purchases and carries or uses an ID tag-enabled object.

3.2.6 ID terminal user: A person who uses and operates an ID terminal. A typical example of an ID terminal user could be a mobile user with an ID terminal.

3.2.7 personalized ID tag: An ID tag that contains an identifier that enables the possible identification of an individual rather than an anonymous object.

3.2.8 PII protection service (PPS): A security service that provides protection of PII for ID tag and/or ID terminal users of an application using tag-based identification. PPS manages (i.e., creates/updates/deletes/applies) a (ID tag and/or ID terminal) user's PII policy profile on the network on which an application using tag-based identification is running.

3.2.9 PII policy profile: A formatted set of PII protection rules and policies.

3.2.10 user-defined PII policy profile: A formatted set of the PII protection rules and policies as defined by the (ID tag and/or ID terminal) user.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ASP	Application Service Provider
B2C	Business-to-Customer
ID	Identification
IrDA	Infrared Data Association
OECD	Organization for Economic Cooperation and Development
PII	Personally Identifiable Information
PPS	PII Protection Service
RF	Radio Frequency
RFID	Radio Frequency Identification
SCM	Supply Chain Management

5 Conventions

None.

6 Overview

The widespread deployment of identification tags (including RFID tags) can give rise to concerns of privacy infringement because of the abilities of RFID technology to automatically collect (and process) data, with the possible disclosure of such data to the public (deliberately or accidentally).

For applications using tag-based identification and relying on a personalized identification tag in personalized after-sale management services, healthcare-related services, etc., the privacy issue is becoming an increasingly serious problem.

In the academia and industry, most of the efforts toward the PII protection mechanism have focused on authentication protocols between the ID tag and the ID terminal. Note, however, that these efforts cannot be applied to the actual environment, particularly to applications using tag-based identification, the environment where meaningful information of the identifier exists on the server in the network domain. Therefore, coming up with the proper PII protection mechanism in the environment of applications using tag-based identification is essential. A profile-based PII protection mechanism can be one of the many possible solutions for such an environment.

This Recommendation describes the PII infringements in the environment of applications using tag-based identification, requirements for PII protection, and the basic structure of PII protection based on the user-defined PII policy profile.

7 B2C applications using tag-based identification

An application using tag-based identification is defined as an expanded and more general identification application used to communicate with a series of networks, inter-networks and globally distributed application systems. In other words, an application using tag-based identification is a global network-based application triggered by an ID tag (including RFID).

Applications using tag-based identification have already been adopted widely in the industries such as supply chain management (SCM) and warehouse management, and in anti-counterfeit measures in the supply chain of medicines. The application of tag-based identification is now extended to the end-user application region (e.g., information content delivery of products triggered by ID tag, after-sale management of the physical object, patient records, toll control, etc.), and industrial applications.

B2C applications using tag-based identification can be classified into three types:

a) ID terminal user as the customer: For example, in the information content delivery service, the customer retrieves the information by using the ID terminal he/she owns. In this type of service, most application service providers may assume that the ID terminal has a mobile telecommunication capability and multimedia information presentation capability. Figure 1 shows a basic model of this type of application using tag-based identification. It consists of two basic network operations: ID resolution and content retrieval. ID resolution is the procedure of translating or resolving an identifier into an address [b-ITU-T Y.2213]. The mobile terminal equipped with an ID terminal first resolves an Identifier as received from the ID tag via the directory service and performs a content retrieval afterwards.

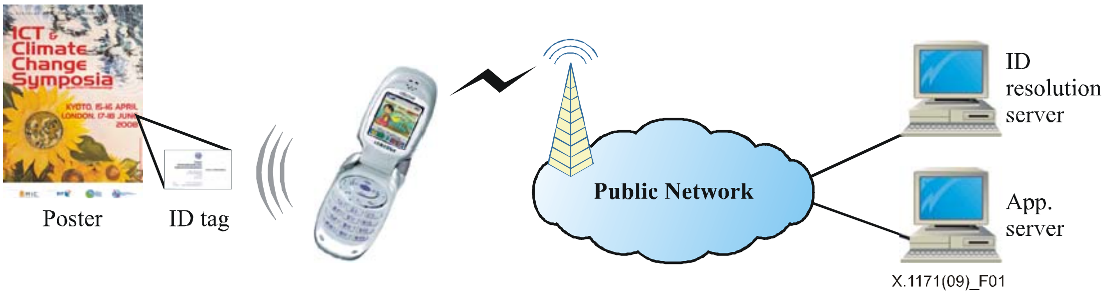

Figure 1 – Basic model of a B2C application using tag-based identification

b) ID tag user as the customer: A typical example of this B2C application using tag-based identification deals with access control and/or authentication, e.g., entrance check, passport, license, after-sale management service, etc. In this type of application model, ID terminals are of the fixed terminal type and/or mobile terminal type; the customer may not need his/her own ID terminal.

c) Customer as both an ID tag user and an ID terminal user: In the product information retrieval service (basic type of the B2C application using tag-based identification), the customer also becomes a tag user upon purchasing the tagged product after browsing the product information contents from his/her mobile terminal. In another example, a healthcare-related service triggered by an ID tag-enabled patient card can be considered. In this application, there are many kinds of customers, e.g., patient, doctor, nurse, etc., as the ID tag user. The ID tag user can browse his/her own patient records through the mobile terminal with an ID terminal by reading his/her ID tag-enabled patient card.

Since many applications using tag-based identification are expanded into B2C applications, consumers are very concerned about PII leakage by ID tags. In this Recommendation, we are focusing mainly on the model of B2C applications using tag-based identification.

8 Reference model for B2C applications using tag-based identification

Figure 2 shows a reference model for B2C applications using tag-based identification.

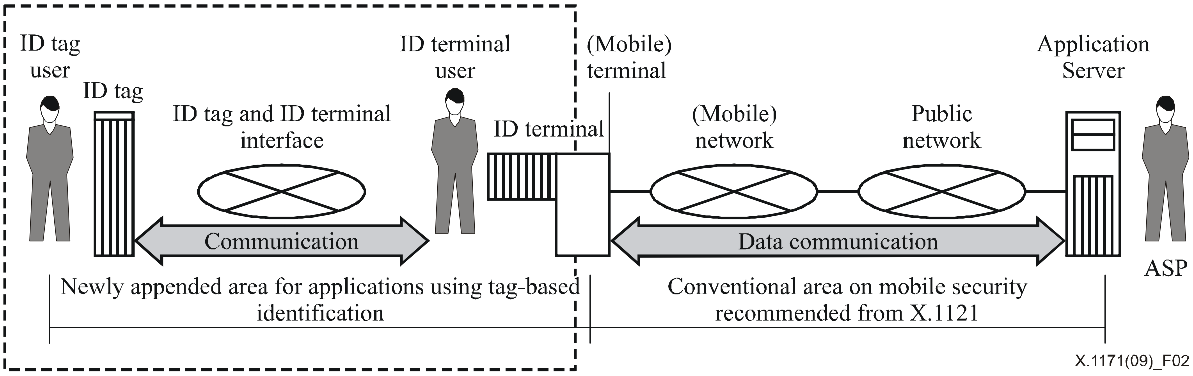
ID tag user
ID tag
ID tag and ID terminal interface
ID terminal user
ID terminal
(Mobile) terminal
(Mobile) network
Public network
Application Server
ASP
Communication
Data communication
Newly appended area for applications using tag-based identification
Conventional area on mobile security recommended from X.1121
X.1171(09)_F02

Figure 2 – Reference model for B2C applications using tag-based identification

This reference model is an augmented model of the mobile end-to-end data communication in [ITU-T X.1121]. Newly appended entities include an ID tag, ID tag user, ID tag and ID terminal interface, and ID terminal. In this model, the (mobile) terminal can be a wired stationary terminal as well as a wireless mobile terminal, and can be considered an ID terminal.

9 PII infringement in B2C applications using tag-based identification

In the environment of applications using tag-based identification, major PII infringements occur in cases where ownership of a product or a document equipped with an ID tag is transferred to a private person.

In the environment of applications using tag-based identification, there are several identifier storing/reading methods such as (2-dimensional) bar code and optical scanner (or camera), near field passive RFID tag and reader, far field passive RFID tag and reader. This clause only describes the generic PII leakages in a B2C-based environment of applications using tag-based identification. More precisely, the following threats are not covered by the scope of this Recommendation:

- General security threats in the applications using tag-based identification: This clause only focuses on PII-related threats in the applications using tag-based identification.
- Identifier storing/reading method-specific threats: For example, in the case of an RFID tag, an attacker can trace the location of the ID tag user of the RFID-tagged product through the identifier of the RFID tag. Appendix I provides a detailed explanation on such location tracking in the RFID environment.
- Threats between an ID tag and an ID terminal: This clause only focuses on the network-side PII threats.

9.1 Leakage of information associated with the identifier

The attacker can read information from the ID tag without the knowledge of the ID tag user of the tagged product. First, the attacker reads an identifier from an ID tag carried by the user. Afterwards, he/she resolves the identifier and queries the information location from the directory service. Finally, the attacker requests for information associated with the ID tag. Furthermore, if the information is related to the PII such as credit card information or medical history, etc., then it may mean more serious infringement of the ID tag user's PII. Figure 3 depicts PII violation through information leakage. In this situation, the attacker can collect some dynamic information (time and location of purchasing the tagged product, tracking information of the product, etc.) as well as static information such as product name and description.

This kind of PII violation is prevented by removing the ID tag or disabling the ID tag functionality. In many applications using tag-based identification such as personalized after-sale management service, healthcare-related service, etc., however, preserving the ID tag and its functionality is essential.

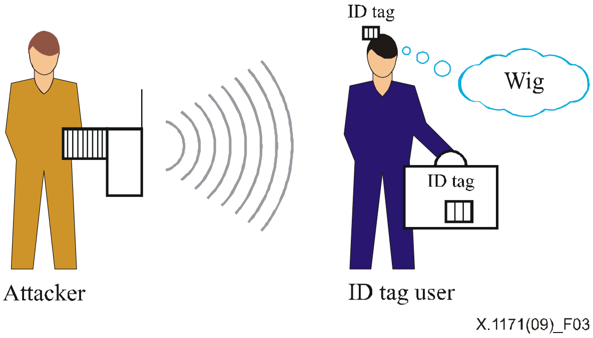

Figure 3 – PII infringement through information leakage

9.2 Leakage of the historical context data

The attacker can extract the user's meaningful data such as preferences, habits, areas of interest, etc., from the historical context data associated with the ID tag. Moreover, the attacker may use such data for illegal or commercial purposes without the user's consent. In such infringement situation, the user refers to the ID terminal user. The ID terminal user reads the identifier from tagged products or documents using his/her ID terminal and obtains useful information from the application server in applications using tag-based identification. At this moment, the various context log data (date of renting of the DVD movie, date and place of purchase of the object, location of reading the movie poster, etc.) can be collected by the network of applications using tag-based identification; this data can be linked with the user (see Figure 4).

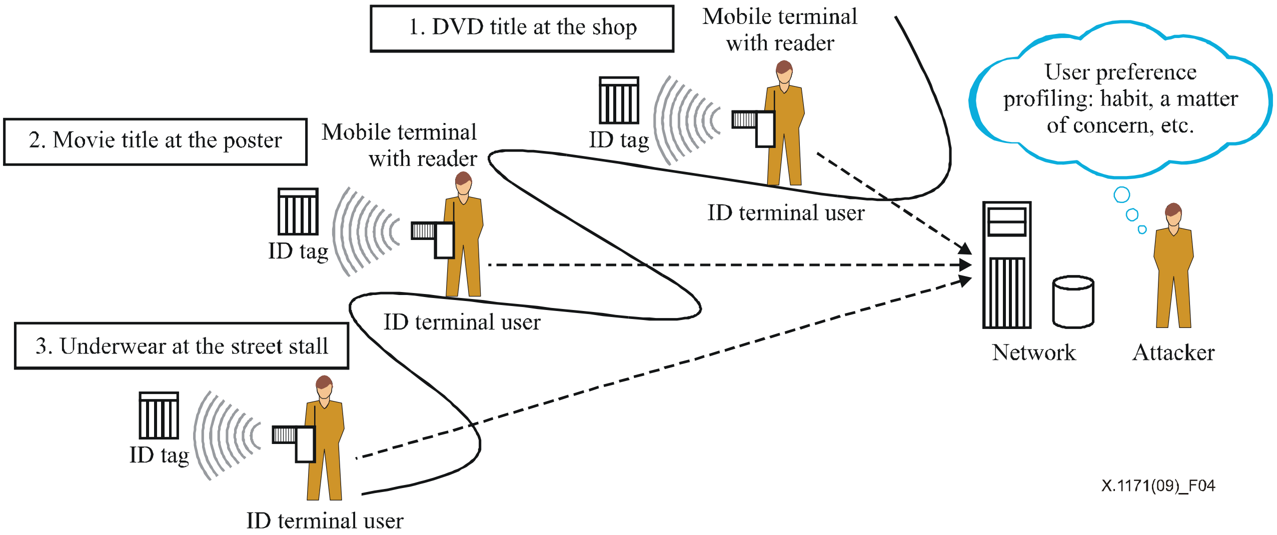
1. DVD title at the shop
Mobile terminal with reader
ID tag
ID terminal user
User preference profiling: habit, a matter of concern, etc.
2. Movie title at the poster
Mobile terminal with reader
ID tag
ID terminal user
3. Underwear at the street stall
ID tag
ID terminal user
Network
Attacker
X.1171(09)_F04

Figure 4 – PII infringement through the collection of historical context data

9.3 Relationship between PII infringements and the reference model

The relationship between PII infringements and entities in the model shown in Figure 2 is summarized in Table 1. In the table, cells marked with "X" mean that a PII infringement in the row is related to an entity or relationship between entities in the column.

Table 1 – Relationship between PII infringements and the reference model

Entities and relationships between entities	Infringements	
	Leakage of information provided by application(s) using tag-based identification	**Leakage of historical context data stored in application server(s)**
Relationship between the ID tag and ID terminal user		X
Relationship between the (mobile) terminal and application server	X	X
Relationship between the ID tag user and application server	X	
Relationship between the ID tag and application server	X	
Application server	X	X

10 PII protection requirements for B2C applications using tag-based identification

This clause mainly focuses on the technical requirements against two PII infringements that are analysed in clause 9. More general guidelines for RFID users and vendors regarding PII protection in the context of RFID technology are dealt with in other Recommendations. The requirements are partially based on the principles from the OECD privacy guidelines [b-OECD]. Annex A describes the principles of [b-OECD] considered in this clause and Annex B describes further principles of [b-OECD]. The following requirements are drawn from the PII infringements in B2C applications using tag-based identification:

– control of PII by ID tag user and/or ID terminal user;

– authentication for ID tag user and/or ID terminal user;

– access control to the PII of an ID tag user in an application server;

– data confidentiality of information associated to an ID tag;

– consent for collection of PII;

– technical safeguards for the application servers.

10.1 Control of PII by ID tag user and/or ID terminal user

The ID tag user and/or ID terminal user is required to be able to manage or update PII associated with his/her ID tag and/or ID terminal on the network. In this way, the user can determine which PII should be deleted or retained in the application using tag-based identification. Furthermore, the user can determine a time limit for his/her PII in the application using tag-based identification.

10.2 Authentication for ID tag user and/or ID terminal user

The application server of an application using tag-based identification is required to provide an authentication procedure for the ID tag user, and the application server may provide an authentication procedure of the ID terminal user if it is necessary (some applications using tag-based identification are not required to authenticate the user).

10.3 Access control to the PII of an ID tag user in an application server

Access to the PII of ID tag users stored by an application server should be secured, and limited to authorized information requestors and to the relevant information needed by each requestor.

10.4 Data confidentiality of information associated to an ID tag

The application server for an application using tag-based identification is required to provide data confidentiality to ensure that the information associated with an ID tag cannot be read by unauthorized users.

10.5 Consent for collection of PII

The application server for an application using tag-based identification is required to provide a consent procedure for the collection of PII, including ID terminal user-related log data. The application using tag-based identification provides technical solution to keep PII as accurate and up-to-date as necessary for the identified purpose and limited to the relevant information needed. In the consent process, the application should provide the purpose of the PII collection. Another consent of the user is needed if the previously collected PII is to be used for another use not included in the initial purpose.

10.6 Technical safeguards for the application servers

The ASP of an application using tag-based identification in charge of processing PII is required to adopt technical security measures for the application servers, including the PII.

10.7 Relationship between requirements and PII infringements

Table 2 summarizes the relationship between the PII protection requirements and PII infringements. In the table, cells marked with "X" mean that a PII infringement in the column is related to a PII protection requirement in the row.

Table 2 – Relationship between the requirements and PII infringements

Requirements	Infringements	
	Leakage of information associated with the identifier	Leakage of historical context data
Control of PII by ID tag user and/or ID terminal user	X	
Authentication for ID tag user and/or ID terminal user	X	X
Access control to the PII of an ID tag user in an application server	X	
Data confidentiality of information associated to an ID tag	X	X
Consent for collection of PII		X
Technical safeguards for the application servers	X	X

Annex A

Basic principles of national application[2]

(This annex forms an integral part of this Recommendation)

- 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 fulfilment of those purposes or such others as 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 for 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;
  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 points 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 which give effect to the principles stated above.

[2] These principles have been extracted from Part II of "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", OECD, 1980.

Annex B[3]

Basic principles of international application: free flow and legitimate restrictions

(This annex forms an integral part of this Recommendation)

- Member States should take into consideration the implications for other Member States of domestic processing and re-export of personal data.
- Member States should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member State, are uninterrupted and secure.
- A Member State should refrain from restricting transborder flows of personal data between itself and another Member State except where the latter does not yet substantially observe these guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member State may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member State provides no equivalent protection.
- Member States should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

[3] These principles have been extracted from part III of "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", OECD, 1980.

Appendix I

Location tracking by the identifier in RFID services

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

The attacker can trace the location of the ID tag user of the tagged product through the identifier of the RFID tag. This kind of security violation enables tracking or monitoring of a specified tag identifier using an invisible, rogue RFID reader. Since the attacker can use the tag's identifier as a personal identifier, he/she can easily trace the user's location, as shown in Figure I.1.

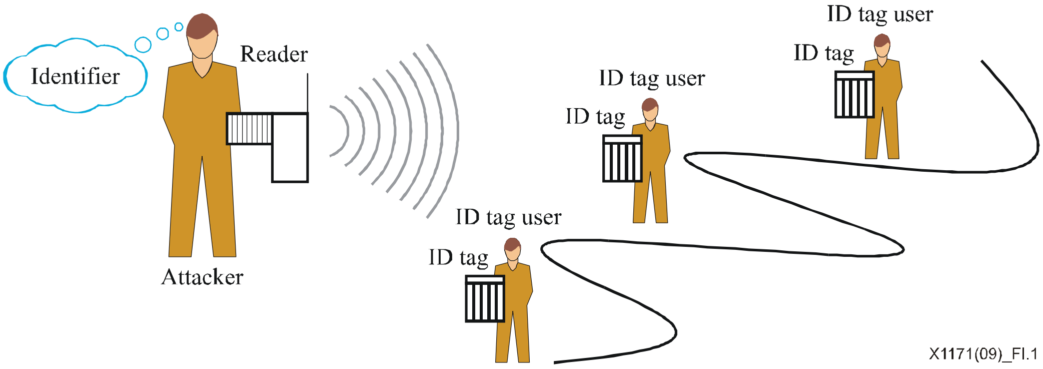

Figure I.1 – Security threat through location tracking for a person

To protect traceability for the identifier, an authentication method may be used between the RFID tag and reader. The RFID tag gives the reader its identifier only if the reader is authenticated by the RFID tag. In other words, the attacker cannot obtain the tag's identifier without the authentication procedure. However if the RFID tag does not have enough power to do computationally intensive operations, such as cryptographic computation, this authentication method may not be a realistic solution.

Another solution may be the identifier recoding technique. Identifier recoding involves recoding the RFID tag's identifier periodically with a pseudo-identifier (or meta-identifier); thus reducing the connectivity of the ID tag's identifier and the ID tag user. Note, however, that this identifier recoding method is not applicable if the RFID tag has no re-writable functionality or if the ID tag makes use of a particular identifier format (such as the EPC code ([b-EPCglobal])). Furthermore, the usefulness of this technique is limited to services which require frequent reading of the RFID tag, and may introduce a lot of complexity on the server side.

Appendix II

PII protection service (PPS) for applications using tag-based identification

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

II.1 PII protection service (PPS) for applications using tag-based identification

The PPS is one example of a PII protection service based on the user's PII policy profile.

Clause II.3 shows a general service scenario of the PPS for an application using tag-based identification. For the PPS, the ID tag or ID terminal user being served a specific application using tag-based identification creates his/her PII protection policies for such an application and sends it to a trusted third party system (PPS system). This system then creates the user's PII policy profile and sends it to the application servers (Service-side systems). At this time, the application servers can control access to the PII information associated with the ID tag and/or ID terminal user.

II.2 Service entities of the PPS for applications using tag-based identification

The PPS has three service entities as follows (see Figure II.1):

– PPS system: As an entity with the management function for the user's PII policy, this entity creates the user-defined PII policy profile for the user's PII policy and provides the PII policy profile to the service-side system(s).

  NOTE – In the case of a centralized PPS system which is responsible for many applications using tag-based identification, appropriate counter-measures against a single point of failure should be provided. However, depending on the use case, there may be only one PPS system for an application using tag-based identification.

– Service-side system: An entity that provides information related to the identifier of an ID tag, i.e., that can be regarded as an application server in an application using tag-based identification. Therefore many service-side systems can exist for an application using tag-based identification. This entity provides an access-control function using the user-defined PII policy profile or default PII policy profile.

– User-side system: An entity with the wireless (or wired) network access function and identifier capturing function if necessary, this entity could be a mobile terminal with ID terminal. The ID tag and/or ID terminal user can access the service-side and PPS systems via such a user-side system. Using the user-side system, the user controls his/her PII protection policy for a specific application using tag-based identification.

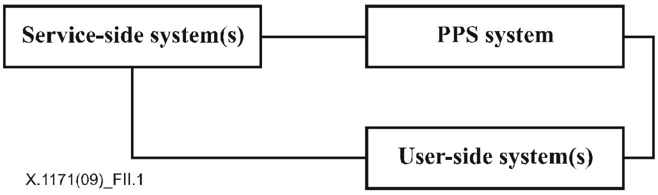

Figure II.1 – Service entities of the PPS for applications using tag-based identification

II.3 General service scenario for the PPS

The service scenario for the PPS generally arises from a tag personalizing procedure such as tagged product purchase. Figure II.2 illustrates the general PPS flow of the application using tag-based identification.

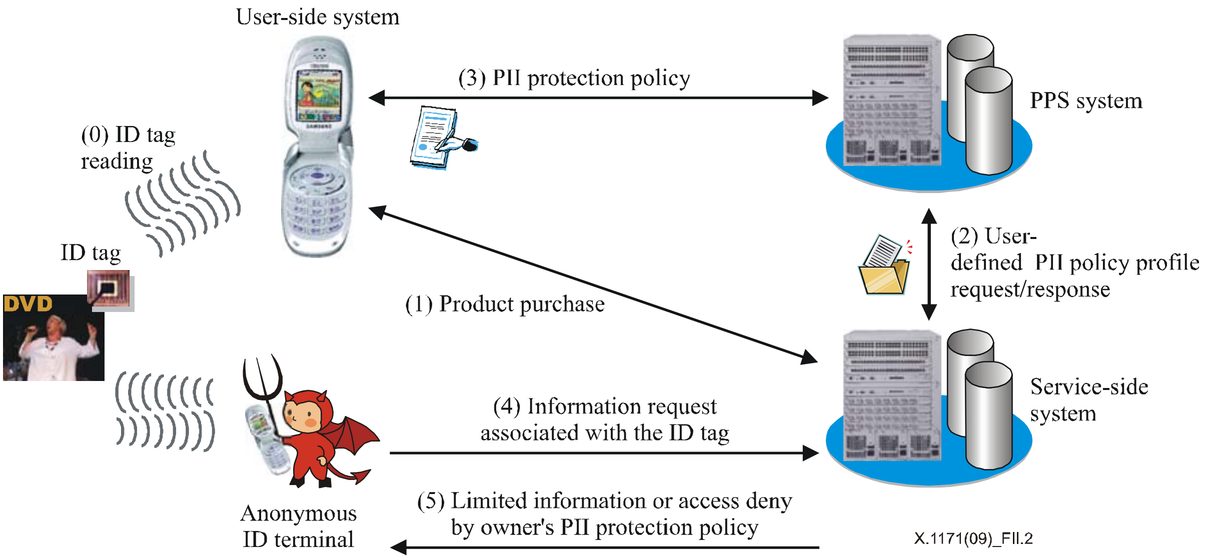
User-side system
(3) PII protection policy
PPS system
(0) ID tag reading
ID tag
DVD
(2) User-defined PII policy profile request/response
(1) Product purchase
Service-side system
(4) Information request associated with the ID tag
Anonymous ID terminal
(5) Limited information or access deny by owner's PII protection policy
X.1171(09)_FII.2

Figure II.2 – General PPS flow

0) A consumer reads the identifier from the tagged product using his/her mobile terminal equipped with an ID terminal.

1) The consumer browses the product-related information from the application service network and subsequently purchases the product using one of various payment methods. At this moment, the consumer becomes the ID tag user.

2) The application using tag-based identification then requests for the user-defined PII policy profile from the PPS system, which then responds with the user-defined PII profile to the application.

3) The PPS system receives the user's PII protection policy for this application.

4) Anyone may request the information associated with this ID tag from the service-side system.

5) The requestor can browse all information provided by the service-side system if the requestor is the ID tag user. Otherwise, either the requestor obtains limited information or he/she cannot access any information.

NOTE – Further work will be necessary to study various use case scenarios of the PPS for applications using tag-based identification, which may describe the advantages of the PPS.

II.4 Functions of the PPS

To satisfy the requirements for the PII protection of applications using tag-based identification, the PPS have the following functions:

- PII policy profile management.
- Access control.
- Registration.
- PII policy profile transmission.
- PII policy profile refreshing.

II.4.1 PII policy profile management

PII policy profile management is a core function of the PPS. The PPS system manages two kinds of PII policy profiles as follows:

- Default PII policy profile: This refers to a formatted set of PII protection rules and policies of an application using tag-based identification. Such rules can be based on fair information practices such as those described in the OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data ([b-OECD]).
- User-defined PII policy profile: This pertains to a formatted set of the PII protection rules and policies as defined by the ID tag and/or ID terminal user.

The PPS system carries out the establishment and management of the user-defined (or default) PII policy profile. Specifically, the PPS system should create and manage the default PII policy profile for an application using tag-based identification and the user-defined PII profile from the user's PII protection policy as provided by the registration procedure. Thus, this PII policy profile can be sent to the service-side system(s). Basically, it can contain the following items:

- Disclosure policy for information resources (including PII)
- Expiration policy for information resources
- Event log collection policy

The service-side system then controls access to information resources using such PII policy profile for each information requestor.

II.4.2 Access control

The access control function of the PPS system is used to authenticate the identity of the user or ASP and authorize access to the user's information resources, which are mainly the owner's PII protection policies.

NOTE – The word identity is used with the understanding that in the context of telecommunications it is an identifier or set of identifiers that is trusted, meaning that it is considered to be reliable for the purposes of a particular situation to represent a network element, network terminal equipment, or user, after the completion of a validation process. As the term is used here, one cannot conclude that trusted identifiers constitute positive validation of a person.

On the other hand, the access control function of the service-side system is an essential component of the PPS, since the service-side system should control access to all information resources, and provide PII based on the user-defined PII policy profile (or default PII policy profile in the absence of a user-defined PII policy profile). The service-side system is required to be able to deduce if a requestor has access to a certain user's PII based on the owner-defined PII policy profile.

II.4.3 Registration

The service-side system and the user-side system have a registration procedure with the PPS system. In the registration procedure, the registration information provided by the service-side and user-side systems is as follows:

- Service-side system: Identity information (including authentication information such as password) and information type (i.e., price information, purchase method, etc.) provided by the application server using tag-based identification to a user-side system.
- User-side system: Identity information (including authentication information such as password) and user's own PII protection policies and consent to the application using tag-based identification.

The PPS system should create the default PII policy profile for the service-side system and provide the default PII policy profile to the service-side system (see Figure II.3). The default PII policy profile can be created through the PII profile management functionality.

On the other hand, the PPS system should create the user-defined PII policy profile based on the user's PII protection polices. Figure II.3 shows the registration procedure of the PPS.

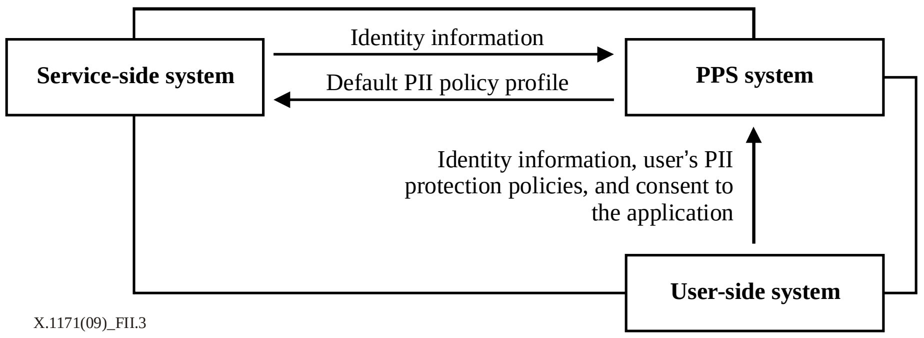
Service-side system
Identity information
Default PII policy profile
PPS system
Identity information, user's PII protection policies, and consent to the application
User-side system
X.1171(09)_FII.3

Figure II.3 – Registration procedure

II.4.4 PII policy profile transmission

The PII policy profile transmission procedure is triggered by the service-side system. Figure II.4 shows the PII profile transmission procedure.

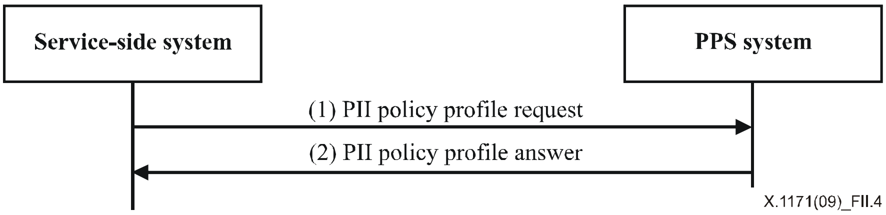

Figure II.4 – PII policy profile transmission procedure

1) PII policy profile request: The service-side system requests for the user-defined PII policy profile with the user's identity.

2) PII policy profile answer: The PPS system checks for the user-defined PII policy profile for this user and sends the user-defined PII policy profile.

NOTE – The word identity is used with the understanding that in the context of telecommunications it is an identifier or set of identifiers that is trusted, meaning that it is considered to be reliable for the purposes of a particular situation to represent a network element, network terminal equipment, or user, after the completion of a validation process. As the term is used here, one cannot conclude that trusted identifiers constitute positive validation of a person.

II.4.5 PII policy profile refreshing

The PII policy profile refreshing procedure is triggered by the PPS system. When the user changes his/her own PII protection policies, the PPS system regenerates the user-defined PII policy profile. The PPS system then sends the PII policy profile refreshing message to all service-side systems that are registered in the PPS system. Afterwards, each service-side system updates the user-defined PII policy profile and sends the PII policy profile refreshing answer message. Figure II.5 shows the PII policy profile refreshing procedure.

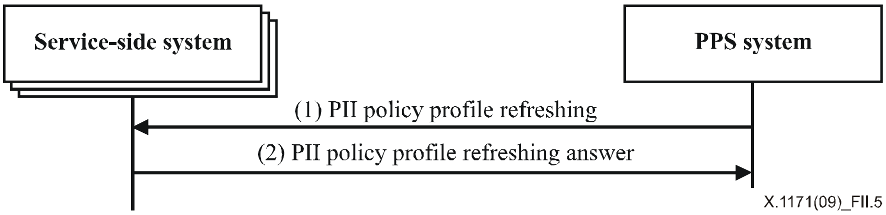
Service-side system
PPS system
(1) PII policy profile refreshing
(2) PII policy profile refreshing answer
X.1171(09)_FII.5

Figure II.5 – PII policy profile refreshing procedure

1) PII policy profile refreshing: The PPS system sends the updated user-defined PII profile to each service-side system.

2) PII policy profile refreshing answer: Each service-side system sends the refreshing answer message to the PPS system.

Bibliography

[b-ITU-T F.771] Recommendation ITU-T F.771 (2008), *Service description and requirements for multimedia information access triggered by tag-based identification*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework.*

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2008), *Terms and definitions for Next Generation Networks*.

[b-ITU-T Y.2213] Recommendation ITU-T Y.2213 (2008), *NGN service requirements and capabilities for network aspects of applications and services using tag-based identification*.

[b-ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework*.

[b-EPCglobal] EPCglobal standard (2008), EPCglobal Tag Data Standards Version 1.4.
<http://www.epcglobalinc.org/standards/tds/tds_1_4-standard-20080611.pdf>

[b-OECD] OECD (1980), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.
<http://www.oecdbookshop.org/oecd/display.asp?CID=&LANG=EN&SF1=DI&ST1=5LMQCR2K94S8>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2009