

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1275

(12/2010)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cyberspace security – Identity management

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

Recommendation ITU-T X.1275

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
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

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

Recommendation ITU-T X.1275

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

Summary

Recommendation ITU-T X.1275 recognizes that radio frequency identification (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 manifest as tracking the location of the individual or invasion of his or her privacy in another malfeasant manner. For this reason, this Recommendation provides guidelines regarding the RFID procedures that can be used to enjoy the benefits of RFID while attempting to protect personally identifiable information.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1275	2010-12-17	17

Keywords

Protection of personally identifiable information, RFID application.

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/>.

© ITU 2011

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms	2
5 Conventions	2
6 Privacy principles	3
7 Threats and infringements of PII in RFID.....	3
7.1 Invisibility of data collection.....	4
7.2 Profiling.....	4
7.3 Tracking.....	4
8 RFID applications.....	4
8.1 Supply-chain management	5
8.2 Transportation and logistics	6
8.3 Healthcare and medical application.....	7
8.4 e-government.....	8
8.5 Information service.....	9
9 Guidelines on protection for personally identifiable information	10
9.1 Policies and procedures	10
9.2 Restriction on recording PII	11
9.3 Information, consent, right of access, rectification, right to oppose	11
9.4 Restriction on collecting and linking PII.....	12
9.5 Deactivation of the RFID tag once the purpose is fulfilled.....	13
9.6 Information about service providers and data controllers	13
9.7 Organizational and technical measures for protecting PII	13
9.8 Assessment of the privacy impact of the RFID system.....	14
9.9 Appointment of a data protection official	15
Appendix I – Characteristics and restrictions of RFID tag.....	16
I.1 Classification and characteristics of RFID tags.....	16
I.2 Restrictions of passive tags	16
Appendix II – Technical measures for protecting PII in the RFID system.....	18
II.1 Kill tag using password	18
II.2 Privacy protection using physical technology	18
II.3 Privacy protection using cryptographic technology	19
Bibliography.....	22

Recommendation ITU-T X.1275

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

1 Scope

This Recommendation provides guidance to radio frequency identification (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 18000-6 (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 – Part 3: 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 radio frequency identification (RFID) system [ISO/IEC 19762-3]: Automatic identification system and data capture system comprising one or more reader/interrogators and one or more transponders in which data transfer is achieved by means of suitably modulated inductive or radiating electromagnetic carriers.

3.1.3 radio frequency identification (RFID) tag [ISO/IEC 19762-3]: Any transponder plus the information storage mechanism attached to the object.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

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 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.

3.2.5 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.

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

3.2.7 radio frequency identification (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 radio frequency identification (RFID) service provider: Any entity offering a service based on objects that have built-in or attached RFID tags.

3.2.9 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 and acronyms:

AES	Advanced Encryption Standard
NFC	Near Field Communication
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 documents: [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, as 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 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 contactless 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 with national and regional laws, regulations and policies. This information can also be modified to derive PII. The following clause describes the major threats and infringement of PII posed by RFID technology.

Copyright International Telecommunication Union/ITU Telecommunication Sector

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. Appendices I and II 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