

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/>.

© ITU 2009

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

CONTENTS

Page

1	Scope	1
2	References.....	1
3	Definitions	2
3.1	Terms defined elsewhere	2
3.2	Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	3
5	Conventions	3
6	Overview	3
7	B2C applications using tag-based identification	4
8	Reference model for B2C applications using tag-based identification	5
9	PII infringement in B2C applications using tag-based identification.....	5
9.1	Leakage of information associated with the identifier	6
9.2	Leakage of the historical context data	6
9.3	Relationship between PII infringements and the reference model.....	7
10	PII protection requirements for B2C applications using tag-based identification.....	7
10.1	Control of PII by ID tag user and/or ID terminal user	8
10.2	Authentication for ID tag user and/or ID terminal user	8
10.3	Access control to the PII of an ID tag user in an application server	8
10.4	Data confidentiality of information associated to an ID tag.....	8
10.5	Consent for collection of PII	8
10.6	Technical safeguards for the application servers.....	8
10.7	Relationship between requirements and PII infringements.....	8
	Annex A – Basic principles of national application	10
	Annex B – Basic principles of international application: free flow and legitimate restrictions	11
	Appendix I – Location tracking by the identifier in RFID services.....	12
	Appendix II – PII protection service (PPS) for applications using tag-based identification ...	13
II.1	PII protection service (PPS) for applications using tag-based identification.....	13
II.2	Service entities of the PPS for applications using tag-based identification ...	13
II.3	General service scenario for the PPS.....	13
II.4	Functions of the PPS	14
	Bibliography.....	18

Copyright International Telecommunication Union/ITU Telecommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS

Recommendation ITU-T X.1171¹

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.