TECHNICAL REPORT

ISO/IEC TR 24729-4

First edition
2009-03-15

Information technology — Radio frequency identification for item management — Implementation guidelines —

Part 4: Tag data security

Technologies de l'information — Identification de radiofréquences pour la gestion d'items — Lignes directrices pour la mise en œuvre —

Partie 4: Sécurité des données de repère

Reference number
ISO/IEC TR 24729-4:2009(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, the joint technical committee may propose the publication of a Technical Report of one of the following types:

— type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

— type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

— type 3, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 24729-4, which is a Technical Report of type 2, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

ISO/IEC TR 24279 consists of the following parts, under the general title *Information technology — Radio frequency identification for item management — Implementation guidelines*:

— *Part 1: RFID-enabled labels and packaging supporting ISO/IEC 18000-6C*

— *Part 2: Recycling and RFID tags*

— *Part 3: Implementation and operation of UHF RFID Interrogator systems in logistics applications*

— *Part 4: Tag data security*

Introduction

This Technical Report has its genesis as *Guidance from AIM Global's RFID Expert Group, RFID — Guidelines on data access security*. It looks at systemic solutions that prevent unauthorized or inadvertent access to data on an RFID tag and in an RFID system. It is intended to provide guidance to users and systems designers on potential threats to data security and countermeasures available to provide RFID data security.

Determining the appropriate approach to RFID data security is highly dependent on the type(s) of possible threat(s), the intended use of the tag, and the type of data on the tag for a particular application. Therefore, this Technical Report cannot provide specific recommendations but, rather, offers sufficient guidance to enable users or developers to assess potential risks and determine appropriate techniques to mitigate these risks.

An RFID system is divided into modules, each having its own security elements. These modules are tag, tag-to-reader, reader, reader-to-host, host (back-end enterprise) system, and data throughout the tag, reader, host and communications. This Technical Report addresses the RFID components of a system: tag and tag-to-reader (or tag-to-tag) communications. Other components of the system are more typical "system" security issues and are covered by a variety of other best practice documents.

This Technical Report is divided into three sections:

— possible threats to data access security ranging from unauthorized access to data to denial of service;

— a methodology for assessing the various possible threats in order to determine the relative risk level of a specific application and whether security measures are required;

— countermeasures to effectively address specific possible threats.

The thorough review of possible threats should not be construed to mean that RFID itself is inherently vulnerable but, rather, like any technology, it will be subject to attempts to exploit or subvert it by unscrupulous individuals or by those merely wishing to demonstrate their technical prowess. This information is provided to help technical personnel anticipate and prevent successful attacks on RFID systems.

Potential threats must also be taken in context. Technologies or methodologies currently being used for some of the applications discussed may have greater risk factors.

Implemented with appropriate countermeasures and forethought, RFID systems can be secure, beneficial and cost-effective.

Information technology — Radio frequency identification for item management — Implementation guidelines —

Part 4:
Tag data security

1 Scope

This Technical Report provides guidance to systems designers to help them determine potential threats to data security of the tag and tag-to-reader communication in an RFID system, and appropriate countermeasures to provide data security (identified as 1 through 2 in Figure 1). Although important, it is beyond the scope of this Technical Report to address security aspects of the reader-to-host and back-end enterprise modules (identified as 4 through 7 in Figure 1).[1)]

This Technical Report is not intended to specifically address consumer privacy concerns; however, since data and personal privacy depend on the use of appropriate security measures, privacy is addressed in general terms. Data access security provides a measure of personal privacy protection by mitigating the potential for unauthorized reading of data on a tag. However, not all data access security countermeasures provide the same level of protection.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15963, *Information technology — Radio frequency identification for item management — Unique identification for RF tags*

ISO/IEC 19762-1, *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary — Part 1: General terms relating to AIDC*

ISO/IEC 19762-3, *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary — Part 3: Radio frequency identification (RFID)*

1) "Privacy Best Practices for Deployment of RFID Technology" released by The Center for Democracy in Technology (CDT) provides more information on elements 4 through 7 in Figure 1:

http://www.cdt.org/privacy/20060501rfid-best-practices.php

Users are also encouraged to become familiar with ISO/IEC 27002, which is a comprehensive set of controls comprising best practices in information security.