INTERNATIONAL STANDARD

ISO
18186

First edition
2011-12-01

Freight containers — RFID cargo shipment tag system

Conteneurs pour le transport de marchandises — Système d'étiquettes RFID d'expédition de fret

Reference number
ISO 18186:2011(E)

© ISO 2011

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 18186:2011
https://standards.iteh.ai/catalog/standards/sist/9dc6a4f5-8c2f-4f9f-9e26-
9cea4d7ef630/iso-18186-2011

COPYRIGHT PROTECTED DOCUMENT

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 18186:2011
https://standards.iteh.ai/catalog/standards/sist/9dc6a4f5-8e2f-4f9f-9e26-
xxxxxxxxxxxx/iso-18186-2011

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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

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

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

ISO 18186 was prepared by Technical Committee ISO/TC 104, *Freight containers*, Subcommittee SC 4, *Identification and communication*.

This first edition of ISO 18186 cancels and replaces the first edition of ISO/PAS 18186:2010.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 18186:2011
https://standards.iteh.ai/catalog/standards/sist/9dc6a4f5-8c2f-4f9f-9e26-
9cea4d7ef630/iso-18186-2011

Introduction

This International Standard describes the composition, application requirements and operational procedures of an RFID cargo shipment tag and its relevant system used for improving transparency of the freight container transportation process. It identifies data content and format as well as operational characteristics of an RFID cargo shipment tag. It also provides a solution for electronic transfer of relevant information between an RFID cargo shipment tag and its associated information system platform.

The overall purpose of this International Standard is to improve freight container logistic transparency and efficiency by using an RFID cargo shipment tag and an associated, Internet-based information management system.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 18186:2011
https://standards.iteh.ai/catalog/standards/sist/9dc6a4f5-8c2f-4f9f-9e26-
9cea4d7ef630/iso-18186-2011

ISO 18186:2011
https://standards.iteh.ai/catalog/standards/sist/9dc6a4f5-8c2f-4f9f-9e26-
9cea4d7ef630/iso-18186-2011

Freight containers — RFID cargo shipment tag system

1 Scope

This International Standard is applicable to freight containers as defined in ISO 668 as well as other associated containers and transport equipment.

This International Standard defines how freight container logistic transparency and efficiency can be improved through use of an RFID cargo shipment tag system and an Internet-based software package. Such an RFID cargo shipment tag system can co-exist with, but is separate from, a container security and identification RFID framework using container "license plate" tags, described in ISO 10374 and ISO/TS 10891, and electronic seals ("e-seals"), described in ISO 18185 (all parts). In all cases, operation of and information from ISO/TS 10891 and ISO 18185 devices is independent from the operation and information of the cargo shipment tag and information from these devices is passed in discrete messages that are not routed via the RFID cargo shipment tag.

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 668, *Series 1 freight containers — Classification, dimensions and ratings*

ISO 6346, *Freight containers — Coding, identification and marking*

ISO 10374, *Freight containers — Automatic identification*

ISO/TS 10891, *Freight containers — Radio frequency identification (RFID) — Licence plate tag*

ISO 18185 (all parts), *Freight containers — Electronic seals*

IEC 60068-2 (multiple sub-parts), *Environmental testing*

IEC CISPR/TR 28, *Industrial, scientific and medical equipment (ISM)-Guidelines for emission levels within the bands designated by the ITU*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
RFID cargo shipment tag
read-write tag into which data specific to a containerized cargo shipment can be stored and the tag and the data uploaded in it are the responsibility of the shipper

NOTE   The tag can be affixed to the container by the shipper or, as per the shipper's instructions, by the party that physically performs the loading ("stuffing") of the container. Data capabilities are flexible and can, at the shipper's discretion, include destination, routing, conveyance or other transportation information, time and location of the interrogation, cargo information (including hazardous material information, where applicable) or other trip-specific information. The tag must perform reliably from the point of stuffing of the container to delivery destination, and is to be removed by the consignee upon final delivery. The tag is reusable.

3.2
reader
device that can exchange information with RFID cargo shipment tags by wireless communication methods and move information to and from an internet-based information system

3.3
network platform
information processing system through which data from an RFID cargo shipment tag is communicated, processed and viewed

NOTE   It is a subset within/of the cargo shipment tag system. The network platform system includes a wireless radio network, a server, terminal(s), database, middleware, etc. Information from the cargo shipment tag system is accessible, according to pre-determined access criteria, to authorized users through a dedicated internet website.

3.4
operators of network platform
network operator
neutral entity/organization/party that operates the network platform of the RFID cargo shipment tag system

NOTE   This entity operates/maintains the web server, database server and/or the middleware.

3.5
RFID cargo shipment tag system
system consisting of RFID cargo shipment tag, its associated reader(s) and the network platform

4   RFID cargo shipment tag system

4.1   System composition

The RFID cargo shipment tag system is composed of the following basic elements: RFID cargo shipment tag, reader(s) and network platform (including database, operational system and related system software). The system is open and distributed, which can achieve management efficiencies in different geographical areas. Components of the RFID cargo shipment tag system operate in a manner described later in this International Standard.

4.2   System operator

The shipper, or its authorized representative, is the only one who may affix and remove the RFID cargo shipment tag. The shipper is responsible for the supply, placement and ultimate removal of the physical tag as well as all operations using it, including uploading, maintaining, altering, deleting and reading cargo shipment tag data.

4.3   System authorization

The shipper may, at its discretion and in accordance with 5.1, write any relevant container transport and shipping data onto the cargo shipment tag. The shipper shall enter into an agreement with the network operator of the cargo shipment tag system before dispatching the shipment. As part of this agreement, the network operator shall provide access credentials which allow the shipper to upload tag, cargo and other information to the network platform and query the network platform for journey information as needed.

4.4   System functions

Reading from and writing to the RFID cargo shipment tag may only be done by the shipper, or its authorized representative, using access credentials supplied by the network operator. Each shipper, or its authorized representative, shall only have access to data on its own shipment tags.

Container transport and shipping data, or any other allowed information, can be transferred by the shipper between network memory locations, including the RFID cargo shipment tags themselves. Use of access credentials, and/or other security measures, shall prevent one shipper from accessing the tag information or network information of another shipper.

Search capabilities are available to the shipper, or an authorized party identified by it, through the network platform using access credentials supplied by the network operator. A shipper shall only have the ability to search through its own information and its own tags.

4.5   System internal data transmission

Except for wireless transmissions between cargo shipment tags and readers, all internal EDI data transmissions through the network platform should use HTTP protocol, data format to be described by XML. For more detailed data, refer to Annex A.

4.6   System safeguard measures

A shipper, using its unique access credentials, shall set up the reading and writing authority levels of RFID cargo shipment tags through the network platform according to its own requirements.

A shipper, using its unique access credentials, shall set up the inquiry and search authority levels for shipment information through the network platform according to its own requirements.

Information within the RFID cargo shipment tag shall be encrypted or otherwise secured at the point and time when it is first written into the tag and during any subsequent modifications, alterations, changes and/or erasures. The tag shall be capable of having encrypted or otherwise secure data written to it and read from it without interference from the tag design or structure. Further, the system shall not write to the tag cargo shipment-specific data that is not encrypted or otherwise secured.

All parts of the cargo shipment tag system, especially the network platform and associated information systems, shall implement suitable disaster tolerance and protections from hostile attacks, including hacking, viruses and denial of service.

5   RFID cargo shipment tag

5.1   General requirements

The RFID cargo shipment tag shall have its own unique tag identification number in permanent memory. The container serial number (see ISO 6346), as well as any other desired container transport and shipping data, may be programmed into the volatile memory of the tag.

Information written to the RFID cargo shipment tag shall be encoded using formats defined in Annex A for transmission between tags and readers.

A clock chip shall be built into each RFID cargo shipment tag and it shall be set to UTC time. The RFID cargo shipment tag system shall automatically record all interrogation events, including each trip's initial activation and deactivation of the tag, including the date and time of these events. The time error shall be less than 5 seconds per day.

The RFID cargo shipment tag system shall automatically receive and record the geographical location information from each reader interrogating it. The geographical location information refers to the reader position when it reads the tag.

The RFID cargo shipment tag shall be capable of carrying any cargo shipment and/or logistic information as desired by the shipper and described in Annex A.

The RFID cargo shipment tag data shall be protected as described in 4.6.

The RFID cargo shipment tag may be either a one-time-use or a reusable device. In either case, the tag shall be removed by the consignee after final delivery. Prior to re-use, it is the shipper's responsibility to make sure that a reusable tag has had its user memory cleared. Return and recycling of reusable tags is also the sole responsibility of the shipper.

An RFID cargo shipment tag shall support data capturing, amendment and deletion events for one full trip from the container's origin to final destination, as per the shipper's requirements.