INTERNATIONAL STANDARD

ISO 18185-4

First edition
2007-05-01

Freight containers — Electronic seals —

Part 4: Data protection

Conteneurs pour le transport de marchandises — Scellés électroniques —

Partie 4: Protection des données

Reference number
ISO 18185-4:2007(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) 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 18185-4 was prepared by Technical Committee ISO/TC 104, *Freight containers*, Subcommittee SC 4, *Identification and communication*.

ISO 18185 consists of the following parts, under the general title *Freight containers — Electronic seals*:

— *Part 1: Communication protocol*

— *Part 2: Application requirements*

— *Part 3: Environmental characteristics*

— *Part 4: Data protection*

— *Part 5: Physical layer*

Introduction

This part of ISO 18185 was prepared by ISO Technical Committee 104/Subcommittee 4/Working Group 2, using the drafting conventions of ISO/IEC Directives, Part 2.

In early 2005, an extensive Vulnerability Assessment took place to analyse the use cases and potential data integrity threats posed to devices based on the ISO/IEC 18185 series as written. Based on learnings from that assessment, spoofing and cloning were identified as potential data integrity risks to electronic seals. Device authentication became the highest priority solution to mitigate those identified risks, and the scope of the electronic seal standard-setting work was expanded to meet that objective.

Three aspects are discussed in this part of ISO 18185: data protection, device authentication and conformance.

Data protection addresses the confidentiality and integrity of transmitted data. ISO TC 104/SC 4/WG 2 decided that for this part of ISO 18185, all seal information has been deemed to be public information, and as such, can be transmitted in clear text. Data confidentiality and integrity requirements are presented in this part of ISO 18185 for both fixed data (e.g. data items created during the seal manufacturing process) and variable data (e.g. event information generated by and stored within the seal during use).

Device authenticity addresses the capability to identify the seal as a valid device. This first-generation specification outlines methods for physical authentication.

Conformance addresses the requirement for electronic seals claiming compliance with ISO 18185 to also contain the physical properties of high security mechanical seals in ISO/PAS 17712, and identifies best practices for electronic seal manufacturers.

This part of ISO 18185 defines the first-generation specifications for device authentication and data protection. Further generations of this part of ISO 18185 may be created upon further review of the potential benefits for these electronic seal devices using additional device authentication and data protection methods.

Freight containers — Electronic seals —

Part 4: Data protection

1 Scope

This part of ISO 18185 specifies requirements for the data protection, device authentication and conformance capabilities of electronic seals for communication to and from a seal and its associated reader. These capabilities include the accessibility, confidentiality, data integrity, authentication and non-repudiation of stored data.

The protection of this information is provided through a radio-communications interface providing seal identification and a method to determine whether a freight container's seal has been opened.

This part of ISO 18185 specifies a freight container seal identification system, with an associated system for verifying the accuracy of use, having:

— a seal status identification system;

— a battery status indicator;

— a unique Seal Identifier including the identification of the manufacturer;

— a seal (tag) type.

This part of ISO 18185 is intended for use in conjunction with the other parts of ISO 18185.

This part of ISO 18185 is designed to facilitate electronic device authentication. For mechanical seals, the seal manufacturer is able to determine the authenticity of the device if and when necessary, e.g. to determine the unauthorized opening of the seal. There are electronic authentication methods which can provide similar validation without visual inspection. This part of ISO 18185 provides only the guidelines for those methods.

This part of ISO 18185 applies to all electronic seals used on freight containers covered by International Standards ISO 668, ISO 1496-1 to ISO 1496-5 and ISO 8323 and should, wherever appropriate and practicable, also be applied to freight containers other than those covered by these International Standards.

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 17025, *General requirements for the competence of testing and calibration laboratories*

ISO/PAS 17712, *Freight containers — Mechanical seals*

ISO 18185-3, *Freight containers — Electronic seals — Part 3: Environmental characteristics*

3 Terms and definitions

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

3.1
AEI
Automatic Equipment Identification

3.2
authentication
method to verify the validity of a transmitted message and its originator

3.3
asset
anything an individual or a company owns which has value

NOTE In the container environment, an asset could be a container, the container's contents, or information pertaining to the container.

3.4
electronic seal
read-only, non-reusable freight container seal conforming to the high security seal defined in ISO/PAS 17712 and conforming to this part of ISO 18185 that electronically evidences tampering or intrusion though the container doors

3.5
reader
wireless RFID communication device which interacts with RFID tags and electronic seals

3.6
Radio Frequency Identification
RFID
electrical transponder which stores information that can then be used to identify an item to which the transponder is attached, similar to the way in which a bar code on a label stores information that can be used to identify the item to which the label is attached

3.7
system
complete end-to-end RFID tracking solution of seal-to-reader-to-network-to-application-to-user

3.8
threat
potential abuse of an asset created by exploiting a vulnerability in order to impair the value of an asset

3.9
validation
process by which the integrity and correctness of data are established

3.10
vulnerability
potential flaw or weakness in system security procedures, design, or implementation that could be exercised (accidentally triggered or intentionally exploited) and result in harm done to a system

4 Data protection

4.1 General

Data protection addresses the concern about the confidentiality and integrity of the data presented by the electronic seal.

4.2 Confidential information

Under the terms of this first-generation part of ISO 18185, the current communication with the electronic seal is performed in clear text and does not include any confidential information. Consequently, there are no requirements regarding confidential information at this time.

4.3 Public information

All current information communicated by the electronic seal has been determined to be public information, and as such, shall be communicated in clear text format. While it is not necessary to transmit public information using confidentiality methods, there is a need to prevent the accidental or fraudulent alteration of the data contained within the electronic seal.

4.3.1 Fixed data

Fixed data is defined as all seal information which will not change after the time of manufacture. This includes the manufacturer ID, the tag ID (serial number), the protocol ID, the model number, the product version, the seal tag type and the protocol version.

Fixed data shall be protected against erasure or alteration during the manufacturing process such that it cannot be modified or deleted by an outside entity. The technical details of how fixed data protection is performed are beyond the scope of this part of ISO 18185 and are left to the individual electronic seal manufacturer.

4.3.2 Variable data

Variable data is defined as all seal event information which, after the time of manufacture, can and most probably will change throughout the life of the seal. This includes the time of seal closure, the time of seal opening and the battery status.

Event information shall be added to the seal's memory upon each status change. Once written into the event log, this information shall become a permanent record within the seal and shall not be modified or erased by either the seal or an outside entity.

Variable data shall be protected against erasure or alteration within the device throughout the lifetime of the seal. The technical details of how variable data protection is performed are beyond the scope of this part of ISO 18185 and are left to the individual electronic seal manufacturer.

5 Device authentication

5.1 General

In addition to the integrity of the data communicated, this part of ISO 18185 requires the capability to verify the authenticity of the electronic seal.