

Date: 2006-10-21

**ISO/FDIS 18185-4**

ISO/TC 104/SC 4

TC104 Secretariat: ANSI

## **Freight containers – Identification and communication, Electronic seals – Part 4: Data protection**

*Réceptier de fret - identification et transmission, joints électroniques - partie 4: Protection de données*

### **Warning**

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

### Copyright notice

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

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.ch](mailto:copyright@iso.ch)  
Web [www.iso.ch](http://www.iso.ch)

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

**Contents**

Page

|  |           |
|--|-----------|
| <b>Foreword</b> .....  | <b>iv</b> |
| <b>Introduction</b> .....  | <b>v</b>  |
| <b>1 Scope</b> .....   | <b>1</b>  |
| <b>2 Normative references</b> .....  | <b>1</b>  |
| <b>3 Terms, definitions, and abbreviated terms</b> .....                                   | <b>2</b>  |
| <b>4 Data protection</b> .....   | <b>3</b>  |
| <b>4.1 General</b> .....   | <b>3</b>  |
| <b>4.2 Confidential information</b> .....  | <b>3</b>  |
| <b>4.3 Public information</b> .....  | <b>3</b>  |
| <b>5 Device authentication</b> .....   | <b>4</b>  |
| <b>6 Conformance</b> .....   | <b>4</b>  |
| <b>Annex A (normative) Electronic seal manufacturers' security-related practices</b> ..... | <b>5</b>  |
| <b>Bibliography</b> .....  | <b>11</b> |

## 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 Technical Committee ISO/TC 104, Freight containers, Subcommittee SC 4, Identification and Communication, Working Group WG2, Automatic Equipment Identification (AEI) for containers and container related equipment prepared ISO 18185-4.

This document sets out first generation requirements for data protection and authentication for electronic seals. It focuses on the physical device authentication of the seals. Future generations of this document may be created, that, upon further analysis and review of issues including but not limited to a) cost considerations, b) the relative significance of potential threats to data integrity compared to other container security vulnerabilities, and c) operational characteristics and challenges in the intermodal freight container industry, may include further requirements for additional device authentication by electronic methods and also for data protection.

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 6: Message sets for transfer between seal reader and host computer*
- *Part 7: Physical layer*

## Introduction

This International Standard 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 analyze the use cases and potential data integrity threats posed to devices based on the 18185 standard 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.

There are three parts to this standard: 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 standard, 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 standard 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 17712 and identifies best practices for electronic seal manufacturers.

This standard defines the first generation specifications for device authentication and data protection. Further generations of this standard 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 — Identification and communication; Electronic seals — Part 4: Data protection

## 1 Scope

This International Standard 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 International Standard 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;

This standard is designed to facilitate electronic device authentication. For mechanical seals, the seal manufacturer must be 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 first standard provides only the guidelines for those methods.

This International Standard applies to all electronic seals used on:

Freight containers covered by International Standards ISO 668, parts 1 to 5 of ISO 1496, 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 668, *Series 1 freight containers — Classification, dimensions and ratings*

ISO 1496-1, *Series 1 freight containers — Specification and testing — Part 1: General cargo containers for general purposes*

ISO 1496-5, *Series 1 freight containers — Specification and testing — Part 5: Platform and platform-based containers*

ISO 8323, *Freight containers — Air/surface (intermodal) general purpose containers — Specification and tests*

ISO 9001, *Quality management systems — Requirements*

ISO/TS 14816, *Road transport and traffic telematics — Automatic vehicle and equipment identification — Numbering and data structure*

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

ISO 17712, *Freight containers — Mechanical seals*

### **3 Terms, definitions, and abbreviated terms**

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 ISO 18185 or revision thereof that electronically evidences tampering or intrusion through the container doors

#### **3.5**

##### **reader**

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

#### **3.6**

##### **RFID**

##### **Radio Frequency Identification**

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 1<sup>st</sup> generation standard, 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 standard and 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 standard and left to the individual electronic seal manufacturer.

## **5 Device authentication**

### **5.1 General**

In addition to the integrity of the data communicated, this standard requires a capability to be able to verify the authenticity of the electronic seal.

### **5.2 Physical authentication**

The ability for forensic authentication is necessary for both the mechanical and the electronic components of a seal. The seal manufacturer must be able to identify and authenticate the seal as a valid seal based on proprietary information, its unique manufacturing characteristics, and the fixed data defined in provision 4.3.1.

Presented with the physical device, the seal manufacturer shall be able to validate the authenticity of the mechanical and electronic components of the seal. The technical details of how physical device authentication is performed are beyond the scope of this standard and left to the individual electronic seal manufacturer.

### **5.3 Electronic authentication**

Under the terms of this first generation standard, there are no requirements for the ability to electronically authenticate a seal through data transmissions.

## **6 Conformance**

Electronic seals claiming compliance with ISO 18185 must have the high security mechanical seal physical properties defined in ISO 17712.

## Annex A (normative)

### Electronic seal manufacturers' security-related practices

#### A.1 Introduction

This normative annex addresses security-related practices relevant to the manufacture and distribution of electronic security seals (electronic seals) and related equipment that conform to the parts of ISO 18185.

Since electronic seals require interrogators (reader/writers) for communication, this annex also addresses security-related practices related to the manufacture and distribution of such related equipment.

The annex is similar to the normative annex to ISO 17712 with modifications appropriate to electronic seals and related equipment.

The structure of this document reflects the six stages in the life of a freight container electronic seal, as shown in the table below. Since this document is about the security-related practices of electronic seal/device manufacturers, the focus within each stage is on the actions within the purview of those manufacturers.

“Manufacturer,” as used in this annex, refers to the entity responsible for the design and sale of the product. While that entity usually owns and operates the producing factory, this is not always the case since firms may subcontract the actual production. In the case of subcontract production, “manufacturer” refers to the firm that drives the process and brings the product to market, not to the operator/owner of the xyz factory.

**Table A.1 – Six stages in the life of a freight container electronic seal**

| Stage Number | Stage Name                               | Role of electronic seal/Device manufacturers   |
|--------------|--|--|
| 1            | Electronic seal/equipment design process | Total responsibility   |
| 2            | Manufacturing                            | Total responsibility   |
| 3            | Distribution                             | Must set standards and expectations of distributors and re-sellers.<br><br>Must help educate distributors and re-sellers.  |
| 4            | User knowledge and discipline            | Must help educate users in correct use and maintenance of electronic seal readers and related equipment.<br><br>Must help educate users in the care of electronic seals prior to their application to containers, trailers, or other receptacles.<br><br>Must help educate users in correct use of electronic seals.   |
| 5            | In-transit management                    | May help users and regulators educate supply chain personnel.  |
| 6            | After-life                               | Total responsibility for maintaining data on production, sales, and ID numbers of electronic seals, readers and related equipment.<br><br>Must help educate distributors and re-sellers about maintaining historical data on their electronic seal inventories and sales.<br><br>Have no role in maintaining chain-of-custody information on completed cargo shipments |

## **A.2 Manufacturer security-related practices in Stage 1, Electronic seal/equipment design process**

- A.2.1 Manufacturers will design and classify the physical performance characteristics of electronic seal products in accordance with ISO/PAS 17712, or its successor International Standard. It establishes uniform procedures for classification of mechanical seals for freight containers. The specification defines physical parameters for different levels of an electronic seal's physical performance—indicative electronic seals, security electronic seals, and high security electronic seals.
- A.2.2 Physical design of electronic seal readers and related equipment shall respect the environmental characteristics covered in ISO 18185-3.
- A.2.3 Although this international standard is designed for marine containers, electronic seals that conform to it are suitable for other applications, such as bulk railcars or truck trailers used in cross-border and domestic operations.
- A.2.4 Manufacturers will endeavour to 'design-in' effective tamper resistance and tamper evidence for all their electronic seal products.

## **A.3 Manufacturer security-related practices in Stage 2, Manufacturing**

This section describes the security-related practices to be applied by electronic seal/device manufacturers during Stage 2. As with the other stages, not every point applies in every situation. If a manufacturer elects not to apply a point because it does not apply to a particular facility, then the manufacturer shall document the rationale for this action and keep it on file for review by certification and regulatory authorities.

### A.3.1 Electronic seal/device manufacturer certification

- A.3.1.1 Manufacturer shall maintain ISO 9001 or equivalent certification on all company-owned manufacturing facilities.
- A.3.1.2 When purchasing contract production services for market-ready electronic seal products, manufacturer shall purchase from ISO 9001 (or equivalent) certified plants.
- A.3.1.3 If a manufacturer's facility or outside production facility for market-ready electronic seal products loses its ISO 9001 or equivalent certification, notification shall be sent to the appropriate customs administrations if de-certification impacts the use of that company's specific product in international trade.
- A.3.1.4 The security practices referenced herein shall be implemented in accordance with this document.
- A.3.1.5 Manufacturer shall accept random and unannounced inspections of facilities and documentation for conformance with this document; inspections are to be accomplished by appropriate third-party certification bodies.<sup>1</sup>
- A.3.1.6 Manufacturer shall conduct an initial security risk assessment of its facilities, and periodic update reviews, and implement countermeasures and/or policies to overcome potential vulnerabilities or threats.
- A.3.1.7 Manufacturer shall assign responsibility for security and product integrity to knowledgeable individual(s), with a principal point of contact.
- A.3.1.8 Manufacturer shall agree to cooperate with relevant law enforcement officials.
- A.3.1.9 Manufacturer shall cooperate with regulatory or certification bodies in responding to questions or issues regarding compliance, irregularities, copying, etc.<sup>2</sup>
- A.3.1.10 Manufacturer shall develop and maintain a crisis management strategy to prepare for and respond to tampering and other malicious, criminal, or terrorist actions; the strategy shall provide guidelines to segregating and securing affected product.
- A.3.1.11 Manufacturer shall promote electronic seal/reader security awareness among all staff. Security awareness includes identification of whom in management they should alert about potential security problems (24-hour contacts).
- A.3.1.12 Manufacturer shall require background checks on all employees to the extent allowed under local law or regulation.

---

<sup>1</sup> The "certification bodies" will be governmental agencies or accredited independent organizations. Nothing in this document implies that industry certifying or regulatory bodies would reveal trade secrets or proprietary information among competitors.

<sup>2</sup> See note 1 above.

### A.3.2 Electronic seal/reader product certification

- A.3.2.1 Manufacturer shall, on an annual basis, submit samples of all relevant products to an independent third party testing laboratory to insure the product complies with this document and ISO 17712 or its successor international standard. The testing lab must be certified according to the standards outlined in ISO/IEC 17025, General requirements for the competence of testing and calibration laboratories.
- A.3.2.2 Manufacturer shall mark electronic seals and readers with its company identity. (Note: the manufacturer's identity is part of the electronic seal data structure in ISO 18185-1)
- A.3.2.3 Manufacturer shall produce electronic seals with unique physical and electronic numbers or identifiers. (Note: the electronic seal ID is addressed in ISO 18185-2). The seal manufacturer ID, a component of the seal ID, is addressed in ISO/TS 14816.
- A.3.2.4 Manufacturer shall produce electronic seal readers and related equipment with unique physical serial numbers or identifiers. There will also be an electronic two-byte field set aside for a logical reader identifier which shall be assigned as part of the reader field installation process, able to be tailored to the needs of each installation. (Note: This logical reader identifier will be used by the terminal or area management system to associate the reader with a given location).
- A.3.2.5 Manufacturer shall track the physical and electronic identifiers of all electronic seals and related products that it produces or has produced for it. Manufacturers shall record, by electronic seal/device type, the number/identifier, date of finished production, date of order, date electronic seals were shipped, and names of consignee(s). Manufacturer shall retain this information for a period of at least seven (7) years in a manner that makes it readily available upon request by a regulatory or certification body.
- A.3.2.6 Manufacturer shall segregate and render non-functional any incidental production of scrap electronic seal product before disposal.
- A.3.2.7 Manufacturer shall control access to production and storage areas and loading docks and stores electronic seals and related equipment in secure areas.
- A.3.2.8 Manufacturer shall lock all loaded trailers or containers on the premises.
- A.3.2.9 Manufacturer shall "inspect what it expects," by verifying driver identification, if applicable, and verifying the load and count of inbound electronic seal components.
- A.3.2.10 Manufacturer shall implement a policy for off-hour deliveries to ensure prior notice of these deliveries. The policy will require the presence of an authorized individual to receive these shipments. Advance notification, by phone, fax, or e-mail, should be required from all vendors/suppliers for incoming deliveries.

#### A.4 Manufacturer security-related practices in Stage 3, Distribution

Sales organizations such as distributors or resellers can enhance or undermine even the best manufacturer's security program. The manufacturer/responsible party shall help educate their distributors and resellers about the importance, mutual advantage, and specifics of effective electronic seal security programs.

The manufacturer/responsible party shall set guidelines and should undertake to ensure that their distributors and resellers comply with the following security-related guidelines:

- A.4.1 Distributor/reseller shall permit manufacturer to review its security procedures.
- A.4.2 Manufacturer, if it becomes aware of a gap in distributor/reseller security practices, shall identify that gap and recommend needed changes that will provide electronic seals and related equipment with the necessary oversight and accountability.
- A.4.3 Distributor/reseller shall not sell electronic seals or related equipment without the manufacturer (responsible party's) identity marked on the devices.
- A.4.4 Distributor/reseller shall record all aspects of an electronic seal and/or related equipment shipment, including source, electronic seal numbers and identifiers, description and the name and address of the individual placing the order and the consignee for the order. Distributor/reseller shall retain such records for a period of at least seven (7) years. Upon request from a government regulatory agency, the distributor/reseller shall make the necessary records available to assist the agency in the investigation of a cargo shipment incident.
- A.4.5 Distributor/reseller shall conduct an initial security risk assessment of its facilities and implement countermeasures and/or policies to overcome potential vulnerabilities or threats.
- A.4.6 Distributor/reseller shall control access to storage areas and loading docks, and store electronic seals and related equipment in secure areas.
- A.4.7 Distributor/reseller shall lock all loaded trailers or containers on the premises.
- A.4.8 Distributor/reseller shall "inspect what it expects," by verifying driver identification, if applicable, and verifying the load and count of inbound electronic seal components.
- A.4.9 Distributor/reseller shall implement a policy for off-hour deliveries to ensure prior notice of these deliveries. The policy will require the presence of an authorized individual to receive these shipments. Advance notification, by telephone, facsimile transmission, or email, should be required from all vendors/suppliers for incoming deliveries.

### **A.5 Manufacturer security-related practices in Stage 4, User knowledge and discipline**

This stage focuses upon the security-related practices of *bona fide* users, including government agencies, such as Customs administrations that might apply electronic seals to a container shipment. The influence and responsibility of electronic seal/device manufacturers in Stage 4 is limited to education.

Security-related practices, in this instance, can be enhanced by the electronic seal/device manufacturers through the inclusion of educational information about electronic seals and readers on product cartons, product literature, the Internet, and on-site training when appropriate.

- A.5.1 Manufacturers will help educate users in the importance of proper control of and record-keeping about electronic seals prior to their application and use.
- A.5.2 Manufacturers will help educate users in correct and most effective use of electronic seals and readers, including conformance with applicable standards and regulations.

### **A.6 Manufacturer security-related practices in Stage 5, In-transit management**

In-transit shipment chain-of-custody falls beyond the responsibility of the electronic seal/device manufacturer. However, manufacturers may help users and regulators educate supply chain personnel.

Such education involves the application of chain-of-custody principles. Such principles may include assuring that readers are functioning, that the electronic seal is the right type, that its number has been documented and verified, that its application is correct, and that an audit trail is established. In addition, the principles may include an electronic seal anomaly policy, such as procedures to follow if tampering is noted during a shipment.

### **A.7 Manufacturer security-related practices in Stage 6, After-life**

Most of the post-shipment stage in the life cycle of an electronic seal relates to maintaining chain-of-custody information about the shipment of goods itself. Electronic seal manufacturers have no role in maintaining chain-of-custody information on completed cargo shipments.

Manufacturers' responsibilities and best practices relate to data about the electronic seals and related equipment themselves. These responsibilities and practices are covered in Stages 2, 3 and, to a lesser extent, 4. Manufacturers' retain:

- A.7.1 Total responsibility for maintaining the manufacturer's data on electronic seal/reader production, sales, and unique numbers and identifiers.
- A.7.2 Responsibility to educate distributors and re-sellers about maintaining historical data on their electronic seal inventories and sales, and to educate users about maintaining historical data on their electronic seal inventories.

## Bibliography

- [1] ISO/IEC Directives, Part 2, *Rules for the structure and drafting of International Standards*, 2004
- [2] ISO 31 (all parts), *Quantities and units*
- [3] ISO 646, *Information processing — ISO 7-bit coded character set for information interchange*
- [4] ISO 690, *Documentation — Bibliographic references — Content, form and structure*
- [5] ISO 690-2, *Information and documentation — Bibliographic references — Part 2: Electronic documents or parts thereof*
- [6] ISO 830, *Freight containers — Vocabulary*
- [7] ISO 1000, *SI units and recommendations for the use of their multiples and of certain other units*
- [8] ISO 6346, *Freight containers — Coding, identification and marking*
- [9] ISO/IEC TR 10000-1, *Information technology — Framework and taxonomy of International Standardized Profiles — Part 1: General principles and documentation framework*
- [10] ISO 10241, *International terminology standards — Preparation and layout*
- [11] ISO 10374, *Freight containers — Automatic Identification*
- [12] ISO 17363, *Supply chain applications of RFID — Freight containers*
- [13] IEC 60027 (all parts), *Letter symbols to be used in electrical technology*