INTERNATIONAL STANDARD

ISO 18185-1

First edition
2007-05-01

Freight containers — Electronic seals —

Part 1: **Communication protocol**

Conteneurs pour le transport de marchandises — Scellés électroniques —

Partie 1: Protocole de communication

Reference number
ISO 18185-1:2007(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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

Publié en Suisse

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 18185-1 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

The communication protocol for an electronic seal for freight containers has been developed by the committee to provide for the data link requirements related to the unambiguous interrogation and maintenance of the integrity of a freight container seal from point of sealing to point of opening.

Freight containers — Electronic seals —

Part 1: **Communication protocol**

1 Scope

This part of ISO 18185 provides a system for the identification and presentation of information about freight container electronic seals. The identification system provides an unambiguous and unique identification of the container seal, its status and related information.

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

This part of ISO 18185 specifies a read-only, non-reusable 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,
- the seal (tag) type.

This part of ISO 18185 is used in conjunction with the other parts of ISO 18185.

It applies to all electronic seals used on freight containers covered by ISO 668, ISO 1496-1 to ISO 1496-5, and ISO 8323. Wherever appropriate and practicable, it also applies 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/TS 14816, *Road transport and traffic telematics — Automatic vehicle and equipment identification — Numbering and data structure*

ISO 17712, Freight containers — Mechanical seals

ISO 18185-2, *Freight containers — Electronic seals — Part 2: Application requirements*

ISO 18185-5, *Freight containers — Electronic seals — Part 5: Sensor interface*

ISO/IEC 18000-7, *Information technology — Radio frequency identification for item management — Part 7: Parameters for active air interface communications at 433 MHz*

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

ISO/IEC 19762-2, *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary — Part 2: Optically readable media (ORM)*

ISO/IEC 24730-2, *Information technology — Real-time locating systems (RTLS) — Part 2: 2,4 GHz air interface protocol*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762-1, ISO/IEC 19762-2, ISO 17712 and the following apply.

3.1
electronic seal
eSeal
read-only, non-reusable freight container seal conforming to the high-security seal defined in ISO 17712 and conforming to ISO 18185 or revision thereof that electronically evidences tampering or intrusion through the container doors

3.2
seal identification
Seal ID
unique identification of each manufactured seal incorporating serial number (i.e. Tag ID) and manufacturer ID

3.3
interrogator identification
Interrogator ID
code used to identify the source address during every communication session originated by the interrogator

3.4
low frequency transmitter
LF transmitter
device that emits a short range magnetically coupled signal

3.5
Short Range Link
SRL
low frequency link using the low frequency magnetically coupled signalling

3.6
Long Range Link
LRL
radio frequency link using 433,92 MHz or 2,4 GHz signalling

3.7
localization
capability in any operational scenario to associate an eSeal to the container onto which it is affixed

4 Common requirements

The seal shall be uniquely identified by the tag manufacturer ID and the tag ID (serial number) combination. This combination shall be called seal ID and shall be used in all point-to-point communication to uniquely identify a source (seal to interrogator) and destination address (interrogator to seal).

The seal ID is permanently programmed into the seal during manufacturing and cannot be modified.

The interrogator ID is a user configurable parameter and their assignment is not regulated by this International Standard.

The LF transmitter ID is a user configurable parameter.

The seal shall be verified by uniquely identifying the location of that specific seal during the communication exchange with the seal as defined in ISO 18185-2.

5 Seal data

5.1 The electronic seal mandatory data includes seal tag ID and manufacturer ID (which combine to make up the seal ID), date/time for sealing and opening, seal status, low battery status, protocol ID, and protocol version. Model ID and product version are optional data.

The seal status occupies two bits as follows:

- open and unsealed;
- closed and sealed;
- opened.

The following are definitions of the seal states (see Figure 1):

- open and unsealed: the initial state of the seal when the container is open and seal is still unsealed;
- closed and sealed: physically closed and sealed (cable connected, bolt inserted, etc.);
- opened: physically open and seal broken (cable disconnected, bolt removed).

5.2 The low battery status occupies one bit. For low battery status, “0” indicates that the battery state is above the threshold; “1” indicates a battery state at or below the threshold. For battery-less seals, this field is fixed to a value of “0”. The battery low state is defined to indicate that the battery left is insufficient for another trip as defined in ISO 18185-2.

5.3 The seal tag ID occupies 32 bits. This is the identification number (serial number) that the manufacturer assigned to the seal.

5.4 The tag manufacturer ID occupies 16 bits. This is the identification of the tag component manufacturer. This identification is assigned in accordance with ISO/TS 14816. The RF component manufacturer ID of the seal is programmed by the RF component manufacturer.

5.5 Date/time sealed occupies 32 bits. The eSeal will record the time of sealing from a real-time clock based on UTC time.

5.6 Date/time opened occupies 32 bits. The eSeal will record the time of opening from a real-time clock based on UTC time.

5.7 The protocol ID occupies eight bits. It indicates the protocol type.

5.8 The model ID occupies 16 bits. It indicates the manufacturer’s model number.

5.9 Product version occupies 16 bits. It indicates the version of the product (firmware version). The high byte is the major version number and the low byte is the minor version.

5.10 Protocol version occupies 16 bits. It indicates the version of the standard protocol (this International Standard) to which the seal adheres. The high byte is the major version number and the low byte is the minor version. For this version of the International Standard, this parameter shall be 0x0100 (i.e. version 1.0).

5.11 LF transmitter ID occupies 16 bits. It indicates the LF transmitter identification.

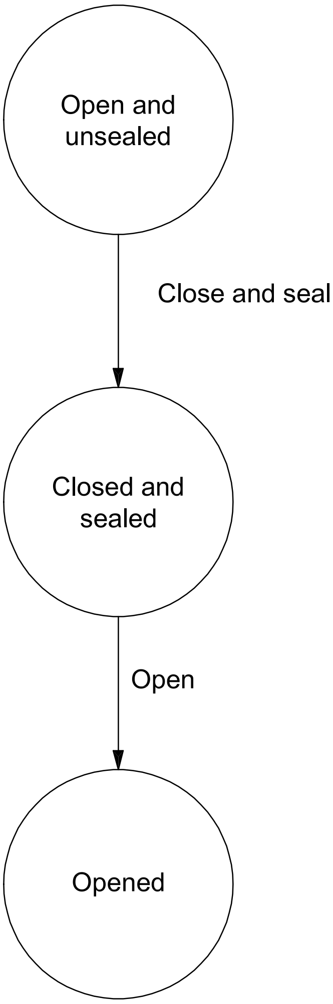


Figure 1 — Seal states

6 Data link layer protocol for electronic seal

There are two types of physical layers. Type A physical layer is the 433 MHz long range link and LF short range link. Type B physical layer is the 2,4 GHz long range link and FSK short range link. The eSeal shall support all the data link protocols. The data link protocols are different for each physical layer. Interrogators and reader devices may support one or both of the physical layers.

The eSeal shall be capable of communicating on both operational mode types A and B. The protocol for these type A long range links at 433 MHz is specified in 6.1. The protocol for the type A short range links using OOK is specified in 6.2. The protocol for these type B long range links at 2,4 GHz is specified in 6.3. The protocol for the type B short range links using FSK is specified in 6.4. Data may be transmitted from the LF transmitter to the eSeal(s) without acknowledgment (one-way link only).

6.1 433 MHz long range data link layer protocol for type A systems

This clause specifies the long range data link layer packet structure for 433 MHz communications.

6.1.1 Packet fields format and definition

6.1.1.1 Protocol ID

The Protocol ID field identifies the data link layers packet structures as defined by this International Standard. The protocol ID that complies with this International Standard is 0x80.

6.1.1.2 Argument Length

The Argument Length field represents the total number of argument bytes in the packet.

6.1.1.3 Min Command Duration

The Min Command Duration field represents the minimum duration in milliseconds from the end of the command to the following command. This field is optional and, if not specified, it is considered to be 0. When a seal is awake and receives this command, but realizes the command is not addressed to it, it may switch to Sleep mode for the duration specified by this field.

NOTE This field can be used for saving power consumption in scenarios where an interrogator must send a sequence of point-to-point commands to several tags. This way, each seal can be in Sleep mode between each command that is not addressed to it.

6.1.1.4 Max Command Duration

The Max Command Duration field represents the maximum duration in milliseconds from the end of the command to the following command. This field is optional and, if not specified, it is considered to be 30 000 ms (30 s). When a seal receives this command and the command is directed to it, it may switch to Sleep mode after this interval if it does not receive another command.

NOTE This field can be used for saving power consumption in scenarios where an interrogator does not have to send more commands to the seal.

6.1.1.5 Packet Options

The Packet Options field is defined as follows.

Table 1 — Packet Options field

Bit	Value = 0	Value = 1	Description
0	Reserved	Reserved	
1	Broadcast (Tag ID and manufacturer ID not present)	Point to Point (Tag ID and Manufacturer ID field present)	The command is either broadcast to all tags or only to the seal whose ID is present in the packet.
2	Min Command Duration not present	Min Command Duration present	
3	Max Command Duration not present	Max Command Duration present	
4	Reserved		
5 – 6	Reserved		
7	Reserved		

6.1.2 Protocol identification and field synchronization

In this subclause, the packet structure for the data link layer is defined. In the data link layer packet structure, the packet shall start with protocol identification. To comply with this International Standard, the protocol ID shall be 0x80.

Some of the data fields within the packet structure may use different length/fields depending on the commands. In the forward link (interrogator to seal), field synchronization is accomplished through the use of the Packet Options field. The Packet Options field is defined in 6.1.1. In the reverse link (seal to interrogator), field synchronization is accomplished through the use of the Mode field defined within the seal status word. The Mode field defines the type of the packet being received as specified within the given Protocol ID packet structure. The seal status word is defined in 6.1.3. The Mode field is defined in 6.1.3.

The Protocol ID specifies general packet structure as defined by this International Standard.

Table 2 — Interrogator to Seal Command Format (Point to Point)

Protocol ID	Packet Options	Tag Manu-facturer ID	Tag ID	Interrogator ID	Command Code	Min Command Duration[a]	Max Command Duration[a]	Argument Length	Command Arguments	CRC
1 byte 0x80	1 byte (8 bits)	2 bytes	4 bytes	2 bytes	1 byte	2 bytes	2 bytes	1 byte	N bytes	2 bytes

[a] This field is command-dependent; some commands may or may not need this field.

Table 3 — Seal to Interrogator Response Format (Point to Point)

Protocol ID	Seal Status	Packet Length	Interrogator ID	Tag Manu-facturer ID	Tag ID	Command Code	Data[a]	CRC
0x80	2 bytes	1 byte	2 bytes	2 bytes	4 bytes	1 byte	N bytes	2 bytes

[a] This field is command-dependent; some commands may or may not need this field.

Table 4 — Interrogators to Seal Command Format (Broadcast)

Protocol ID	Packet Options	Interrogator ID	Command Code	Argument Length	Command Arguments	CRC
0x80	8 bits	2 bytes	1 byte	1 byte	N bytes	2 bytes

Table 5 — Seal to Interrogator Response Format (Broadcast)

Protocol ID	Seal Status	Packet Length	Interrogator ID	Tag Manufacturer ID	Tag ID	Data[a]	CRC
0x80	2 bytes	1 byte	2 bytes	2 bytes	4 bytes	0 – N bytes	2 bytes

[a] This field is command-dependent; some commands may or may not need this field.

Table 6 — Seal to Interrogator Alert Message Format

Protocol ID	Seal Status	Packet Length	Tag Manufacturer ID	Tag ID	Event Code	Event Date & Time	Event Data[a]	CRC
0x80	2 bytes	1 byte	2 bytes	4 bytes	1 Byte	4 Bytes	0 – N Bytes	2 bytes

[a] This field is command-dependent; some commands may or may not need this field.

6.1.3 Seal Status

The Seal Status field, which is included in all seal to interrogator messages, shall consist of the information in Table 7.

Table 7 — Seal Status field

Bit							
15	**14**	**13**	**12**	**11**	**10**	**9**	**8**
Mode field				01 – Unsealed and open 10 – Sealed and closed 11 – Open 00 – Reserved		Reserved	Ack 1 = NAK 0 = ACK

Bit							
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**
Reserved		Seal type			Reserved	Reserved	Battery 1 = low 0 = good

The Mode field indicates response data format from the seal (Broadcast, Point to Point, Alert). It is defined as in Table 8.

Table 8 — Mode field

Mode Field	Mode Format Code (Bit 15-12)
Broadcast	0000
Alert	0001
Point to point	0010

The Seal Type field indicates whether the seal is a high-security seal as defined in ISO 17712 and the generation of electronics within. See Table 9.

The Acknowledgment flag indicates whether the received packet complies with the standard and all parameters are within the specified range. The seal shall not respond if the received packet does not comply with this protocol format or has a Cyclic Redundancy Check (CRC) error. The seal shall respond with a NAK flag if the received packet complies with this protocol format and has a valid CRC, but with an unknown command code. The Opened flag indicates the current status of the seal. The Acknowledgment flag, which is contained in every response, is used to indicate packet error other than CRC. If the CRC is invalid, the seal will reject the packet and will not respond.

The Battery Low flag indicates that the eSeal does not have enough time left for the next trip, based on the trip length defined in ISO 18185-2.

Table 9 — Seal Type field

Seal Type Field	Seal Type Code (Bit 5-3)
Extensibility	111
High Security – First Generation Electronics	101
Reserved	000, 001, 010, 011, 100, 110

6.1.3.1 Command Arguments

The Command Argument field is needed for some commands. This field varies with each command. Some commands may not have this field.

6.1.4 Communication errors (error detection, retries, ACK, NAK)

A CRC checksum is calculated as a 16-bit value over all data bytes according to the CCITT polynomial ($x^{16} + x^{12} + x^5 +1$). The CRC is appended to the data as two bytes.

All interrogators to seal packets and seal to interrogator responses (broadcast, point-to-point commands) use CRC polynomial initialized with all zeros. All seal initiated packets (alert packets) use CRC polynomial initialized with all ones. This feature provides the interrogator with an additional error-checking mechanism where several solicited and unsolicited seal packets are being received by the interrogator.

6.1.5 Collection algorithm

The purpose of the collision arbitration sequence during tag collection is to perform an efficient and orderly collection of the tags placed within the interrogator communication range and to receive information on the tag capabilities and data contents in a single sequence. The information that the tag shall return is specified by the command code set in the command from the interrogator. The interrogator is the master of the communication with one or multiple tags. The detailed timing for the collection algorithm is specified in the physical layer specification. It is the intent of this part of ISO 18185 that the collection algorithms shall be identical for ISO 18185-1, ISO 18185-5, and ISO 18000-7. The definitive document shall be the current version of ISO 18000-7.

6.1.6 Command codes and parameters

Summary of all command codes defined by this protocol is in Table 10.

Table 10 — Command code summary

Command Code	Command Name	Command Type	Description
‘0x10’	Collection	Broadcast	Collect all seal IDs within interrogator RF communication range.
’0x15’	Sleep	Point to Point	Put seal to sleep.
’0x0C’	Product Version	Point to Point	Set by manufacturer.
’0x0E’	Model ID	Point to Point	Set by manufacturer.
‘0x1B’	Read RTC	Point to Point	Reads the current time from the real-time clock (number of seconds elapsed since 1990/01/01, 00:00:00 (GMT)).
‘0x3C’	Read Seal Product Parameter	Point to Point	Reads one of the seal parameters that identify the seal, its manufacturer, product and operational parameters.
‘0x14’	Collect seal IDs with Event Record	Broadcast	Performs a collection round and receives an Event Record from each seal.
‘0x1C’	Standby	Point to Point	Tells a seal not to respond in the next collection round.
‘0x16’	Sleep All But	Broadcast	Tells all the receiving seals except one to return to Sleep mode.
’0x1A’	Read Event Records	Point to Point	Reads one or more Event Records from a seal.
‘0x19’	Get Seal Status	Point to Point	Get the seal status such as sealed or opened.
0x32/B2	Turn on/off beacon for transmitter type	Point to Point	Turns on/off the beacon at 433 MHz, 2,4 GHz.
0x70 – 0x7F	(Reserved for future use)		Reserved
NOTE The seal will ignore the unrecognized commands.			

In the following subclauses, each command is described along with the structure of its parameter and the response structure.

6.1.7 Command and Response Format

6.1.7.1 Collection

The Collection command shall be used to perform a collection round and receive only the seal ID from each seal that meets a specified criterion.

Table 11 — Collection command format

Command Code	Command Arguments	
‘10’	Window Size	Collection criteria
	2 bytes	1 byte

Table 12 — Seal collect arguments

Argument Name	Size	Description
Window Size	2 bytes	The Window Size parameter indicates the time an interrogator will listen for tag responses during a current collection round. The unit of each slot is in milliseconds.
Collection criteria	1 byte	The criteria for the seals that should respond. See below for more details.

The collection criteria argument determines which seal or seals should respond to the command according to the following codes:

- All seals – 0x00;
- Sealed seals – 0x02;
- Opened seals– 0x04;
- Specific seal type – NNNX0000b.

The bit 4, denoted with X, indicates that the Seal Type field is included as part of the collection criteria. If bit 4 is cleared, then the three most significant bits are ignored by the seal and only the four lower bits are used during collection.

Note that these codes or conditions are inclusive.

6.1.7.1.1 Seal response

The seal response shall have no data.

6.1.7.2 Sleep

Table 13 — Sleep command format

Command Code	Command Arguments
‘15’	None

6.1.7.2.1 Description

The Sleep command shall be used to direct a specific seal to enter the Sleep mode. The seal shall not respond to this command nor to any subsequent command until the seal is awakened again by the Wakeup signal.

6.1.7.2.2 Arguments

This command has no arguments.

6.1.7.2.3 Seal Response

The seal shall not respond to this command.

Table 14 — Sleep

None

Sleep operation is used to put a specific seal in the Sleep state, which prevents the seal from participating in the subsequent collection rounds during the collection process.

In this state, the seal will ignore any command from the interrogator until it receives a Wakeup signal.

If the seal does not receive a Sleep command, it will automatically resume the Sleep state 30 s after it has been woken up or after the Max Command Duration field of the last frame has been passed.

6.1.7.3 Sleep All But

Table 15 — Sleep All But

Command Code	Command Arguments	
‘16’	Tag Manufacturer ID	Tag ID
	2 bytes	4 bytes

6.1.7.3.1 Description

The Sleep All But command may be used to tell all the seals except a specified one to return to Sleep mode. In the Sleep state, all seals will ignore any command from the interrogator until it receives a Wakeup signal.

6.1.7.3.2 Seal Response

The seal shall not respond to this command.

6.1.7.3.3 Response

Table 16 — Sleep All But

None

6.1.7.4 Seal model and version

The following two commands are optional for compliance with this part of ISO 18185.

6.1.7.5 Product Version

Table 17 — Product Version command format (read)

Command Code
’0C’

6.1.7.5.1 Read Response

Table 18 — Product Version command format (read response)

Command Code	Product Version
‘0C’	2 bytes

The Product Version indicates seal firmware version.

6.1.7.6 Model ID

6.1.7.6.1 Read

Table 19 — Model ID command format

Command Code
‘0E’

6.1.7.6.2 Read Response

Table 20 — Model ID command format (read response)

Command Code	Model ID
‘0E’	2 bytes

The Model ID indicates seal model number.

6.1.7.7 Read Seal Product Parameter

6.1.7.7.1 Description

The Read Seal Product Parameter command may be used to read one of the parameters that identify the seal, e.g. manufacturer, operational parameters, etc. The full list of Seal Product Parameters is given in Table 23.

6.1.7.7.2 Command Code: 0x3C

Arguments are included in Table 21.

Table 21 — Read seal product parameter arguments

Argument Name	Size	Description
Seal Parameter Code	1 byte	The code of the seal parameter that will be read, according to Table 23.

6.1.7.7.3 Response

The seal response is according to the Seal Parameter Code argument, as in Table 23. If the seal does not recognize the Parameter Code (e.g. 0x0F), it returns no data and the “NAK” flag in the response should be on.

If the seal does recognize the Parameter Code (e.g. 0x07), it returns the response with data of the format in Table 22.

Table 22 — Data field format for read seal product parameters response

Parameter Code	Parameter
1 byte	N as specified in Table 23
Seal Parameter Code according to Table 23	The content of the parameters

Table 23 — Seal product parameters

Parameter Name	Parameter Code	Size	Description
Reserved	0x00	-	Reserved.
Seal Tag ID	0x01	4 bytes	The seal tag identifier (serial number).
Manufacturer ID	0x02	2 bytes	An ID number that is assigned to each manufacturer.
Model ID	0x03	2 bytes	An ID that is assigned by the manufacturer for each eSeal model.
Product Version	0x04	2 bytes	The ID of the version of the product (firmware version). The high byte is the major version number and the low byte is the minor version number.
Protocol Version	0x05	2 bytes	The version of the standard protocol (this part of ISO 18185) to which the seal adheres. The high byte is the major version number and the low byte is the minor version number. For this version of the standard, this parameter shall be 0x0100. (i.e. version 1.0).
Number of Events	0x06	1 byte	Returns the number of Event Records currently written in the seal's Event Memory.
Collection Mode Timeout	0x07	1 byte	Number of seconds for seal timeout in Collection mode (valid value=16 s - 32 s).
Point-to-Point Mode Timeout	0x08	1 byte	Number of seconds for seal timeout in Point-to-Point mode (valid value=2 s - 32 s).
(Reserved for future use)	0x09-0x7F		Reserved for future use.
(Reserved for manufacturer specific use)	0x80 – 0xFF		Reserved for future use (not to be standardized).

6.1.7.8 Collect Seal IDs with Event Record

6.1.7.8.1 Description

Performs a collection round and receives one Event Record from each seal (see Table 24).

6.1.7.8.2 Command Code: 0x14

6.1.7.8.2.1 Arguments

The Window Size parameter represents the number of time slots.

Table 24 — Collect Seal ID with Event Record

Argument Name	Size	Description
Window Size	2 bytes	The number of time slots in the collection round. Each slot is defined in the air interface standard.
Event Record Offset	2 bytes	The offset of the Event Record that is being requested.

6.1.7.8.2.2 Response

The seal response contains the requested Event Record as in the Read Event command.

6.1.7.9 Standby

6.1.7.9.1 Description

The Standby command shall be used to tell a seal not to respond in the next collection round.

6.1.7.9.2 Command Code: 0x1C

6.1.7.9.2.1 Arguments

This command has no arguments.

6.1.7.9.2.2 Response

The seal shall not respond to this command.

Table 25 — Standby — Command

Command Code
0x10

Table 26 — Standby — Response

None

Standby operation is used to put specific seals in Standby state, which prevents these seals from participating in the subsequent collection rounds during the collection process.

In this state, a seal will ignore any broadcast command from the interrogator and will only respond to the point-to-point command received by the interrogator that initially set the seal in the Standby mode.

If the seal does not receive the point-to-point command it will automatically resume Sleep state 30 s after it has been woken up, or after the Max Command Duration field of the last frame has been passed.

6.1.7.10 Get Seal Status

Until the seal is closed and sealed it will not respond.

6.1.7.10.1 Description

Table 27 — Get Seal Status — Read

Command Code
0x19

Table 28 — Get Seal Status — Response

Command Code	Seal Status
0x19	1 byte

This command code reads current seal status with following status codes:

- Sealed — 0x01;
- Opened — 0x04.

6.1.7.11 Read Event Records

6.1.7.11.1 Event Log Codes Description

Reads one or more Event Records from a seal.

6.1.7.11.2 Command Code: 0x1A

6.1.7.11.2.1 Arguments

Table 29 — Read Event Records arguments

Argument Name	Size	Description
Starting Event Offset (N)	2 bytes	The index of the first Event Record requested. The most recent Event Record is 0.
Number of Events to Read (M)	1 byte	The number of Event Records requested.

6.1.7.11.2.2 Response

The seal response is a concatenation of the requested Event Records, starting from the newest to the oldest. The Event Records have a fixed length and a format as specified in Table 32.

Table 30 — Event Log Data Command — Read

Command Code	Starting Event Offset (N)	Number of Events to Read (M)
0x1A	2 byte	1 byte

Table 31 — Event Log Data Command — Response

Command Code	Event Records (M)
0x1A	

This reads M events starting with offset event N. Offset 0 is the most recent event.

The Event Record has a fixed length and a format as specified in Table 32.

Table 32 — Event Record Parameter Format

Event Field Name	Length	Description
Event Record Length	1 byte	Number of bytes in this Event Record.
Event Number	1 byte	Sequence ID that increments for each newly recorded event.
Date & Time	4 bytes	Number of seconds since midnight 1990/01/01 UTC.
Event Category	1 byte	Defines the category of Event.
Event Code	1 byte	See Event Code table.
Event Data	8 bytes	Event Data (specific to each Event Code).

6.1.7.12 Event Categories

Table 33 — Event Categories

Event Category Name	Event Category Code	Description
Seal Events	0x0002	Events as defined in Table 32.
Reserved for future use	0x1, 0x3-0xF	Reserved.

6.1.7.13 Seal Events

Table 34 — Event Codes for Seal Events

Event Name	Event Code	Event Data	Event Data Length	Description
(Reserved)	0x00			
Sealed	0x01	Time Stamp	8 bytes	Written when a sealing operation has been completed successfully. Unique integer number generated by the seal during the seal operation.
Seal open	0x03	Time Stamp	8 bytes	Written when an open operation has been completed successfully. Unique integer number generated by the seal during the open operation.
Battery low flag raised	0x14	Time Stamp	8 bytes	Written when the Battery Low flag is raised. Unique integer number generated by the seal when the Battery Low flag is raised.
SRL wake up	0x15	SRL transmitter ID & timestamp	10 bytes	Written when a SRL Wakeup command was received.
(Reserved for future use)	0x04-0x13, -0x7F		N	
(Reserved for manufacturer use)	0x80 – 0xFF		N	

Where Event Data is defined as follows.

Table 35 — Event Data for Seal Events

Name	Length	Note
Event Date and Time	4 bytes	Date and Time recorded when event occurred.

6.1.7.14 Read RTC

Command Code: 0x1B (Read)

Date and Time counter is a 32-bit integer that increments every second. This is programmed to the number of seconds elapsed since midnight 1990/01/01, UTC. This is initialized at the time of manufacture and unchangeable thereafter. Accuracy of time is within ± 5 s per day.

The seal response is as specified in Table 37.

Table 36 — Read RTC Command

Command Code
0x1B

Table 37 — Read RTC Response

Command Code	Date and Time Counter
0x1B	4 bytes

6.1.7.15 Set/Get Beacon TX period

Write the following.

Table 38 — Set Beacon TX period

Operation Code	Transmission Type	Transmission Rate
0xB2	1 byte	2 bytes

Table 39 — Get Beacon TX period

Operation Code
0x32

Table 40 — Get Beacon TX period Response

Operation Code	Transmission Type	Transmission Period
0x32	1 byte	2 bytes

The tag can be configured to transmit a beacon/alert packet periodically. The Transmission Type parameter selects the type of the transmission: 433 MHz and/or 2,4 GHz. The least significant bit 0, when set (i.e. bit 0 value is 1), selects 433 MHz alert transmission type while setting the bit 1 (i.e. bit 1 value is 1) will select 2,4 GHz alert transmission type. The Transmission Period parameter defines transmission period in seconds for the selected Transmission Type: 433 MHz or 2,4 GHz. Alternatively, the application can choose to set the same period for both types by setting both bits “0” and “1” of the Transmission Type parameter. The transmission period shall be no less than 10 s. Default value is 0x00, which means the beaconing is disabled.

6.2 SRL data link layer definition for type A systems

6.2.1 System Operation Description for localization

To help eSeal Localization, communication with the eSeal will be done using two types of communication links: the Long Range Link (LRL) and a low frequency (LF) channel called the Short Range Link (SRL).

The main building block for the eSeal localization is the system's ability to detect the crossing or presence of a defined eSeal in the vicinity of an SRL transmitter. The eSeal vicinity detection is done as follows:

- The SRL transmitter broadcasts an SRL Wakeup message to any eSeal within its short communication range. The transmission can be cyclic or initialized by any kind of container/vehicle presence detection.

- The eSeal, upon reception of the SRL Wakeup, does not ACK to the SRL transmitter. Upon detection of a valid wake-up signal on LF the tag should exit sleep mode, and listen for SRL Wakeup on LF or a Collect on UHF.

- The eSeal receives the LF transmitter ID and will send a message with LF transmitter ID, eSeal ID, and eSeal status via UHF communication link.

- The eSeal uses the LRL Alert message to initiate the transfer to the LRL Reader. The alert transmission shall be synchronized with the SRL transmitter and use a random slot selection as collision prevention algorithm. The eSeal will repeat the Alert message until it receives a Sleep command from the LRL reader or send a maximum of 20 times before it receives a command addressed to it or goes to sleep. Upon receiving the alert message from the eSeal, the LRL Reader shall ACK the alert and send the eSeal to sleep.

As a result of each of these possible processes, the LRL Reader shall receive the ID of all the SRL transmitters near a specific eSeal.

6.2.2 SRL transmitter Message structure

The SRL transmitter to eSeal communication protocol uses a byte-oriented, packet-based message structure utilizing a 16-bit CRC error detection mechanism for reliable communication. The protocol utilizes an 8-bit Packet Option field that defines the message structure and optimizes the packet size sent to the eSeal.

6.2.3 SRL data link layer packet structure

The data link layer for the SRL shall have the same data structure as the LRL Interrogator to Seal broadcast message. The interpretation of bytes will be the same as for the LRL.

Table 41 — Broadcast collection command format

Sync Frame	Protocol ID	Mode Options	SRL Transmitter ID	CRC
0x96	0x80	0x00	2 bytes	2 bytes

6.2.3.1 SRL transmitter Packet Option field

6.2.3.1.1 Sync Frame

The Sync Frame field signals the start of the packet. The SRL Sync Frame that complies with this standard is 0x96.

6.2.3.1.2 Protocol ID

The Protocol ID field identifies the SRL data link layers packet structures as defined by this protocol standard. The SRL protocol ID that complies with this part of ISO 18185 is 0x80.

Mode options indicate potential different packet options. The mode options value that complies with this standard is 0x00. When the tag receives this command from SRL transmitter, it shall wake up.

The eSeal shall ignore any packets that do not conform to this format.

6.2.3.1.3 SRL transmitter ID

This is the unique ID index of the SRL transmitter within the sight.

6.3 2,4 GHz LRL layer data protocol for type B systems

The data link layer protocol for the 2,4 GHz physical layer utilizes beacon-based architecture for most communications as defined in ISO/IEC 24730-2. The eSeal may transmit beacons at a pre-programmed rate. The beacon rate shall be set to blink only when stimulated be the LF field from the FSK SRL link. The eSeal shall be programmed to blink at a 5-s blink rate with 8 sub-blinks for 20 s after leaving the SRL field. The 2,4 GHz eSeal protocol shall be in accordance with the specifications as set forth in draft ISO/IEC 24730-2. The protocol specified within this document is in addition to the parameters specified in ISO/IEC 24730-2 and is intended as an application layer that shall specify the parameters specific to eSeal function. The terms “exciter” used in ISO/IEC 24730-2 and “LF transmitter” used in this part of ISO 18185 refer to the same physical device.

Specified within this subclause is a protocol that transmits all the data that is available via the 433 MHz link. Therefore, infrastructure can be compliant with either ISO/IEC 18000-7 or ISO/IEC 24730-2 and have access to the same data.

6.3.1 Data link layer packet structure

The following subclauses specify the data link layer packet structure for 2,4 GHz communications.

6.3.1.1 Packet fields format and definition

There are four packet structures specified whose formats are shown in Tables 42-45.

Table 42 — Message 1 Format

Preamble	Seal Status	Seal ID	Message Type Identifier	Mfg ID	Seal Time	Current Time	Payload CRC	Message CRC
0x01	4 bits	32 bits	0x10	16 bits	32 bits	32 bits	8 bits	12 bits

Table 43 — Message 2 Format

Preamble	Seal Status	Seal ID	Message Type Identifier	Mfg ID	Seal Type	Protocol Version	Protocol ID	Battery Time	Payload CRC	Message CRC
0x01	4 bits	32 bits	0x11	16 bits	8 bits	16 bits	0x80	32 bits	8 bits	12 bits

Table 44 — Message 3 Format

Preamble	Seal Status	Seal ID	Message Type Identifier	Mfg ID	Seal Type	Protocol Version	Protocol ID	Open Time	Payload CRC	Message CRC
0x01	4 bits	32 bits	0x12	16 bits	8 bits	16 bits	0x80	32 bits	8 bits	12 bits

Table 45 — Message 4 Format (Optional)

Preamble	Seal Status	Seal ID	Message type Identifier	Mfg ID	Model ID	Product Version	Battery Time	Payload CRC	Message CRC
0x01	4 bits	32 bits	0x13	16 bits	16 bits	16 bits	32 bits	8 bits	12 bits

The field definitions are shown below.

6.3.1.1.1 Tag status

The Tag Status field is a 4-bit field that includes the 2-bit seal open/close status and the 1-bit battery status.

6.3.1.1.2 Seal Tag ID

The Seal Tag ID is the unique 32-bit ID of the seal for each manufacturer. The combination of the Seal Tag ID and Manufacturer ID shall uniquely identify every seal.

6.3.1.1.3 Message type identifier

The message type identifier specifies the data link layer packet structure.

All tags, whether opened or sealed, shall transmit message type identifier 0x10 containing current time and seal time stamp. Sealed tags shall also transmit message type identifier 0x11, which contains seal type, protocol version, protocol ID and battery alarm time. Open tags shall also transmit message type identifier 0x12, which contains seal type, protocol version, protocol ID, and open time stamp. Seals should also transmit optional command type 0x13, which contains model ID, product version and battery alarm time stamp.

6.3.1.1.4 Protocol ID

The protocol ID identifies the data link layers packet structure as defined by this protocol standard. The protocol ID that complies with this part of ISO 18185 is 0x80.

6.3.1.1.5 Manufacturer ID

The Manufacturer ID is a unique 16-bit ID assigned to the seal manufacturer.

6.3.1.1.6 Seal Time

The Seal Time is a 32-bit value representing the number of seconds since midnight 1990/01/01 during which the seal was closed.

6.3.1.1.7 Open Time

The Open Time is a 32-bit value representing the number of seconds since midnight 1990/01/01 during which the seal was opened.

6.3.1.1.8 Current Time

The Current Time is a 32-bit value representing the number of seconds since midnight 1990/01/01 to the present time.

6.3.1.1.9 Battery time

The Battery Time is a 32-bit value representing the number of seconds since midnight 1990/01/01 during which the battery alarm was raised. This field shall be set to 0x00000000 if the battery is good.

6.3.1.1.10 Model ID (optional)

The Model ID is a 16-bit value that identifies the model number of the seal. The high byte is the major model type and the low byte is the model variation type.

6.3.1.1.11 Product Version (optional)

The Product Version is a 16-bit value that identifies the firmware version of the seal. The high byte is the major version and the low byte is the minor version.

6.3.1.1.12 Seal Status

The Seal Status is a 16-bit status including the 2-bit seal open/closed status, the seal type and 1-bit battery status.

6.3.1.1.13 Protocol Version

The Protocol Version is a 16-bit value that identifies the version of the standard to which the seal adheres. The high byte is the major version and the low byte is the minor version. For this version of this part of ISO 18185, the parameter shall be 0x0100 (i.e. version 1.0).

6.3.1.1.14 Payload CRC/parity

The Payload CRC/Parity is a 7-bit CRC and a 1-bit parity computed over all fields except the preamble, tag status and message CRC. The CRC polynomial is x^7 + x^6 + x^3 + x^1 + 1 and the initial seed value is 0x01. The parity bit starts with 0 and toggles with every 1 bit in the message (including the payload CRC)

6.3.1.1.15 Message CRC

The message CRC is a 12-bit CRC with seed value of 0x001 and a polynomial of 0x80F. The CRC is calculated on all message bits except the preamble.

6.4 SRL data link layer definition for type B systems

6.4.1 FSK Packet fields format and definition for 2,4 GHz Systems

The following describes the packet fields format of the frequency shift keyed (FSK) low frequency (LF) protocol, as described in ISO/IEC 24730-2, as well as the seal response. The LF Transmitter message is repeated without any time gap between messages. The start sync of one message begins immediately after the stop sync of the previous message.

Table 46 — Low Frequency FSK LF Transmitter to Seal Message

Start Sync	Opcode	LF Transmitter ID	Message CRC	Stop Sync
6 Manchester periods	1111	16 bits	8 bits	6 Manchester periods

The seal response shall be identical 2,4 GHz transmissions at a five-second interval. The data included in the blink provides the seal status, seal ID, manufacturer ID, LF Transmitter ID, seal type, last event type, and last event time stamp.

Table 47 — Seal Response to FSK LF transmitter Message

Preamble	Seal Status	Seal ID	Command Type	Mfg ID	LF Transmitter ID	Seal Type	Seal Event Type	Last Event Time	Payload CRC	Message CRC
0x01	4 bits	32 bits	0xFD	16 bits	16 bits	8 bits	8 bits	32 bits	8 bits	12 bits

Bibliography

[1] ISO 646, *Information processing — ISO 7-bit coded character set for information interchange*

[2] ISO 668, *Series 1 freight containers — Classification, dimensions and ratings*

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

[4] ISO 1496-2, *Series 1 freight containers — Specification and testing — Part 2: Thermal containers*

[5] ISO 1496-3, *Series 1 freight containers — Specification and testing — Part 3: Tank containers for liquids, gases and pressurized dry bulk*

[6] ISO 1496-4, *Series 1 freight containers — Specification and testing — Part 4: Non-pressurized containers for dry bulk*

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

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

[9] ISO 10374:—[1], *Freight containers — Radio-frequency automatic identification*

[10] ISO/IEC 15963, *Information technology — Radio frequency identification for item management — Unique identification for RF tag*

[11] ISO 17363, *Supply chain application for RFID — Freight containers*

[12] ETSI EN 300 220, *Radio equipment and systems (RES); short range devices (SRDs); Technical characteristics and test methods for radio equipment to be used in the 25 MHz to 1000 MHz frequency range with power levels ranging up to 500 mW*

[13] BS 7480, *Specifications for security seals*

[14] ANSI INCITS 256 Part 4.2, *Radio Frequency Identification (RFID) — UHF RFID Protocols*

[15] USA, Code of Federal Regulations, Federal Communications Commission, 47 CFR, Part 15 — *Radio frequency devices*

[1] Under preparation. (Technical revision of ISO 10374:1991.)

ICS 55.180.10

Price based on 23 pages

INTERNATIONAL STANDARD

ISO 18185-2

First edition
2007-04-15

Freight containers — Electronic seals —

Part 2: Application requirements

Conteneurs pour le transport de marchandises — Scellés électroniques —

Partie 2: Exigences d'applications

Reference number
ISO 18185-2:2007(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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

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 18185-2 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.

This part of ISO 18185 provides a system for the identification and presentation of information about freight container electronic seals. The identification system provides an unambiguous unique identification of the container seal and its status.

The presentation 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.

Freight containers — Electronic seals —

Part 2:
Application requirements

1 Scope

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 used in conjunction with the other parts of ISO 18185.

It applies to all electronic seals used on freight containers covered by ISO 668, ISO 1496-1 to ISO 1496-5, and ISO 8323. Wherever appropriate and practicable, it also applies 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 8601, *Data elements and interchange formats — Information interchange — Representation of dates and times*

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

ISO 17712, *Freight containers — Mechanical seals*

ISO 18185-1, *Freight containers — Electronic seals — Part 1: Communication protocol*

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

ISO 18185-5, *Freight containers — Electronic seals — Part 5: Sensor interface*

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)*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762-1, ISO/IEC 19762-3, ISO 17712 and the following apply.

3.1
electronic seal
e-seal
read-only, non-reusable freight container seal conforming to the high security seal defined in ISO 17712 that electronically evidences tampering or intrusion through the container doors

NOTE The electronic seal is read-only in all aspects except being able to electronically record date and time of sealing (as described in 4.2), and date and time of opening (as described in 4.3).

3.2
seal identification
seal ID
unique identification of each manufactured seal incorporating serial number (i.e. tag ID) and manufacturer ID, the combination of which is called seal ID

3.3
interrogator identification
interrogator ID
code used to identify the source address during every communication session originated by the interrogator

3.4
localization
capability in any operational scenario to associate an e-seal to the container on to which it is affixed

4 Seal application requirements

The seal shall be uniquely identified by the tag manufacturer ID and the tag ID (serial number) combination. This combination shall be called seal ID and shall be used in all point-to-point communication to uniquely identify a source (seal to interrogator) and destination address (interrogator to seal).

4.1 Data description

Unique identification of each manufactured seal tag incorporating all necessary information such as seal tag ID, manufacturer ID and seal tag type includes:

— Seal ID: This is permanently programmed into the seal during manufacturing and cannot be modified.

— Seal tag ID: This is the ID field (serial number) for the seal. The seal number is assigned by the user or the manufacturer and is programmed by the manufacturer. Also, the ID shall be marked on the exterior (casing) of the seal. Until the seal is closed and sealed, it will not respond.

— Seal tag type: The manufacturer is responsible for determination of seal tag type, in compliance with the high security seal requirements in ISO 17712, and programming (see also 4.7). Also, the seal tag type shall be permanently programmed into the seal and marked on the exterior (casing) of the seal. Reading of the seal tag type shall be remotely possible under the same conditions and parameters as reading of the seal ID.

— Battery life: The battery in the seal shall have a minimum life sufficient to remain in inventory for a period of two years, followed by a trip of up to 60 days' duration. The seal shall provide an indication of whether there is sufficient battery power to last for a trip of duration of 60 days with a minimum of 1000 interrogations per trip. Additionally, the manufacturer shall, according to user's specifications, provide for the visual identification of the seal's "use by date" (represented in numeric ISO format, as defined in ISO 8601).

- The seal status bit: This is the status bit that indicates the seal having been opened or sealed.
- The seal tag manufacturer ID: This is the manufacturer identification of the tag. This identification shall be assigned in accordance with ISO/TS 14816.
- The seal tag manufacturer ID of the seal is programmed by the RF Component Manufacturer.

4.2 Date and time of sealing

The seal shall give indication of the date and time when it was sealed in the format CCYYMMDDHHMM (UTC), as defined in ISO 8601. The accuracy of the time compared to actual UTC shall be no worse than ±5 seconds per day, as defined in ISO 18185-1.

4.3 Date and time of opening

The seal shall give indication of the date and time when it was opened in the format CCYYMMDDHHMM (UTC), as defined in ISO 8601. The accuracy of the time compared to actual UTC shall be no worse than ±5 seconds per day, as defined in ISO 18185-1.

4.4 RF regulations

The device shall work according to the local radio regulations and ISO 18185-5.

4.5 Reading devices

The seals shall have the ability to be interrogated by an international standards based reading device.

4.6 Environmental characteristics

The seals shall perform reliably in operating environments as defined in ISO 18185-3.

4.7 Mechanical characteristics

The seals shall have minimum mechanical characteristics in accordance with the high security provisions of ISO 17712.

4.8 Reading reliability and accuracy

The reliability and accuracy of reading the seals shall in any operational scenario be no less than 99,99% and 99,998% respectively.

4.9 Localization and seal verification scenarios

Performance requirements for electronic seals will be presented in the context of seal verification scenarios. Each scenario will motivate technical requirements such as read ranges, travel speeds and others. Container terminals, container stuffing locations, border crossings and other facilities are expected to utilize combinations of the described scenarios based on their specific local needs.

All scenarios are assumed to share a common three-step process for seal verification:

1) Determination of the container’s identity;

2) Determination of identity, type and status of the electronic seal on that container;

3) Determination whether the seal on that container is the correct seal.

Steps 1 and 3 describe functions that are outside of the scope of this International Standard. Regarding step 2, current technology does not support localization in all the below described scenarios. In situations where localization is not possible, a reading confirming that the e-seals have not been tampered with or are missing shall be sufficient. If the reading detects that one or more seals have been tampered with or are missing, those e-seals and the containers on which they are affixed will be subject to exception management as established by the user of the technology.

4.9.1 Container handling and moving equipment scenarios

This set of scenarios deals with electronic seal verification while containers are being handled. Handling equipment covered by this scenario includes top loaders, side loaders, reach stackers, straddle carriers (collectively known as “mobile equipment”), as well as rubber-tired gantry cranes (RTG), rail-mounted gantry cranes (RMGC) and quay cranes. The minimum container travel speed for seal verification for all container handling scenarios is 0 km/h (0 mph). Upcoming generations of quay cranes are anticipated to move containers at speeds of up to 12 m/s. The maximum container travel speed while seal verification takes place is consequently defined as 12 m/s (44 km/h, 27 mph).

Automatic identification devices and/or antennas may be mounted on spreaders on both mobile equipment and cranes. However, in those situations where such devices, instead of being mounted on spreaders, are mounted on the equipment itself, the read distance requirements will differ between mobile equipment and cranes. These latter scenarios are described in more detail in 4.9.1.2 and 4.9.1.3.

4.9.1.1 With spreader-mounted devices

Where feasible, automatic identification devices or antennas may be mounted on spreaders (or other components that directly connect to the container) and must be sufficiently fabricated and/or installed for appropriate levels of water resistance and ongoing shock and vibration.

4.9.1.2 Without spreader-mounted devices — Cranes

On quay cranes or gantry cranes, where the mounting of automatic identification devices or antennas on spreaders (or other components that directly connect to the container) is not feasible or deemed undesirable, the devices may instead be mounted on the crane legs. In these situations, the system level coverage will depend on user requirements and shall be capable of a minimum of 35 m (115 ft).

4.9.1.3 Without spreader-mounted devices — Mobile equipment

In the case of mobile equipment, where the mounting of automatic identification devices or antennas on spreaders (or other components that directly connect to the container) is not feasible or deemed undesirable, the devices may instead be mounted on the equipment itself. In these situations, the system level coverage will depend on user requirements and shall be capable of a minimum of 10 m (33 ft).

4.9.1.4 Moves with multiple containers simultaneously

Container handling equipment that moves single 40-ft containers or two 20-ft containers is often capable of moving more than one 40-ft or two 20-ft containers simultaneously. Any combination of container orientations is possible (e.g., doors left, right, both doors out or butted together).

Such multiple container moves are defined as having the same minimum and maximum speeds as discussed in 4.9.1. Read distances would be dependent upon whether the container handling equipment has spreader mounted devices or not as discussed in 4.9.1.1, 4.9.1.2 and 4.9.1.3.

4.9.2 Restricted lane scenarios

This set of scenarios deals with electronic seal verification while containers travel in restricted lanes. Containers could be pulled by road or yard trucks or travel on rail cars. Some kind of physical restriction assures movement in only one direction (e.g. forwards/backwards but not sideways) within a confined or defined space (e.g. lane or rail track).

4.9.2.1 Single-lane gates or portals

This scenario covers all situations where container traffic is reduced to a single lane. This includes truck gates, structured pre-gates, OCR portals and yard portals. Structures on either or both sides of the lane exist to restrict movement and for permanent installation of automatic identification devices or antennas.

Lanes are assumed to be 3 m to 6 m wide and containers are assumed to travel at speeds ranging from 0 km/h (0 mph) to 50 km/h (31 mph).

4.9.2.2 Multiple-lane gates or portals

This scenario covers all situations where containers travel in multiple parallel lanes. This includes truck gates, structured pre-gates, OCR portals and yard portals. Structures between lanes exist to restrict movement and for permanent installation of antennas or automatic identification devices. Containers in adjacent lanes may travel in opposite directions.

Lanes are assumed to be 3 m to 6 m wide and containers are assumed to travel at speeds ranging from 0 km/h (0 mph) to 50 km/h (31 mph).

4.9.2.3 Single-track train gates or portals

This scenario covers single-track rail gates. Structures on either side, both sides, or above the track exist or can be created for permanent installation of antennas or automatic identification devices. Containers on rail cars travel at speeds of up to 50 km/h (31 mph) and can be stacked up to two containers high. Lanes are assumed to be 3 m to 6 m wide.

4.9.2.4 Multiple-track train gates or portals

This scenario covers rail gates with multiple parallel tracks. Structures on either side, between or above tracks exist or can be created for permanent installation of antennas or automatic identification devices.

Containers on rail cars travel at speeds of up to 50 km/h (31 mph) and can be stacked up to two containers high. Lanes are assumed to be 3 m to 6 m wide.

4.9.2.5 Containers on rail cars

Containers can be stacked up to two high on rail cars but only the bottom containers can be 20-ft containers (e.g. four 20-ft containers shall not be loaded onto a single rail car).

Table 1 — Containers stacked on rail cars

<table>
<tr><td>40 ft – 53 ft</td></tr>
<tr><td>40 ft – 53 ft</td></tr>
</table>

<table>
<tr><td colspan="3">40 ft – 53 ft</td></tr>
<tr><td>20 ft</td><td></td><td>20 ft</td></tr>
</table>

(View from the side)

In the case well cars are used to transport containers, the bottom 2,04 m of the bottom containers may be covered by the steel of the well car. The well car steel cover can reach as high as 2,04 m on the left and right sides of the rail car.

4.9.3 Short-range hand-held scenarios

In addition to automated seal verification with fixed equipment as described in the previous scenarios, seal verification may be done with hand-held devices. Examples for the use of hand-held devices are exception handling as well as locations that lack fixed infrastructure.

The short-range hand-held scenario assumes a person is able to walk up very close to the container door(s) to which the seal(s) are affixed. The hand-held device shall be ergonomically viable and seal verification shall support situations where the person stands still or is walking at speeds of up to 5 km/h (3 mph). The hand-held device shall read electronic seals at a range of 3 m (10 ft) or less.

4.9.4 Long-range hand-held scenarios

Situations may arise where seal verification must be done using a hand-held device over long distances. In this case, the long-range hand-held scenario assumes a person is unable to be close to the container door. An example for the use of long-range hand-held devices is the use by crane operators for containers under the hook. The hand-held device shall be ergonomically viable and seal identification shall support situations where the container stands still or moves at speed of up to 12 m/s (44 km/h, 27 mph). The distance between the hand-held device and the container is limited to no more than 50 m (164 ft).

Bibliography

[1] ISO 10374:—[1], *Freight containers — RF automatic identification*

[2] ISO/IEC 2382-26, *Information technology — Vocabulary — Part 26: Open systems interconnection*

[3] ISO/IEC 18000-7, *Information technology — Radio frequency identification for item management — Part 7: Parameters for active air interface communications at 433 MHz*

[4] ISO 17363, *Supply chain applications of RFID — Freight containers*

[5] ISO 18185-4, *Freight containers — Electronic seals — Part 4: Data protection*

[1] To be published (technical revision of ISO 10374:1991).

ICS 55.180.10

Price based on 7 pages

INTERNATIONAL STANDARD

ISO 18185-3

First edition
2006-06-01

Freight containers — Electronic seals —

Part 3: **Environmental characteristics**

Conteneurs pour le transport de marchandises — Scellés électroniques —

Partie 3: Caractéristiques environnementales

Reference number
ISO 18185-3:2006(E)

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 18185-3 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 7: Physical layer*

The following parts are under preparation:

— *Part 4: Data protection*

— *Part 6: Message sets for transfer between seal reader and host computer*

Introduction

This part of ISO 18185 defines the environmental characteristics for compliant electronic seals.

blank

Freight containers — Electronic seals —

Part 3: Environmental characteristics

1 Scope

This part of ISO 18185 specifies the minimum environmental characteristics for electronic seals.

This part of ISO 18185 describes the environmental requirements for the ISO 18185 series, for ISO 10374 (*Freight containers — RF automatic identification*) and for ISO 17363 (*Supply chain applications of RFID — Freight containers*), since it is expected that the implementation of these International Standards will face the same environmental conditions. However, each of these International Standards has its own unique requirements other than environmental conditions.

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 830, *Freight containers — Vocabulary*

ISO 17712, *Freight containers — Mechanical seals*

ISO 18185-1:—[1], *Freight containers — Electronic seals — Part 1: Communication protocol*

ISO 18185-2:—[2], *Freight containers — Electronic seals — Part 2: Application requirements*

ISO 18185-7:—[3], *Freight containers — Electronic seals — Part 7: Physical layer*

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)*

IEC 60068-2-1, *Environmental testing — Part 2: Tests. Tests A: Cold*

IEC 60068-2-2, *Environmental testing — Part 2: Tests. Tests B: Dry heat*

IEC 60068-2-11, *Environmental testing — Part 2: Tests. Test Ka: Salt mist*

[1] To be published.

[2] To be published.

[3] To be published.

IEC 60068-2-18, *Environmental testing — Part 2-18: Tests — Test R and guidance: Water*

IEC 60068-2-27, *Environmental testing — Part 2: Tests. Test Ea and guidance: Shock*

IEC 60068-2-31, *Environmental testing — Part 2: Tests. Test Ec: Drop and topple, primarily for equipment-type specimens*

IEC 60068-2-32, *Environmental testing — Part 2: Tests. Test Ed: Free fall*

IEC 60068-2-38, *Environmental testing — Part 2: Tests. Test Z/AD: Composite temperature/humidity cyclic test*

IEC 60068-2-53, *Environmental testing — Part 2: Tests. Guidance to Tests Z/AFc and Z/BFc: Combined temperature (cold and dry heat) and vibration (sinusoidal) tests*

IEC 60068-2-68, *Environmental testing — Part 2: Tests — Test L: Dust and sand*

MIL-STD-810F, *Department of Defense test method standard for environmental engineering considerations and laboratory tests*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 830, ISO/IEC 19762-1, ISO/IEC 19762-3, ISO 17712, and the following apply.

3.1
electronic seal
eSeal
read-only, non-reusable freight container seal, conforming to the high-security seal defined in ISO 17712 and to ISO 18185, that electronically provides evidence of tampering or intrusion through the container doors

3.2
seal identification
seal ID
unique code used to identify each manufactured seal, incorporating a combination of the serial number (i.e. Tag ID) and the manufacturer ID

3.3
interrogator identification
interrogator ID
code used to identify the source address during every communication session originated by the interrogator

4 Environmental characteristics

4.1 General

This part of ISO 18185 shall be used in conjunction with the other parts of ISO 18185.

This part of ISO 18185 applies to all electronic seals used on freight containers covered by the following International Standards: ISO 668, ISO 1496-1, ISO 1496-2, ISO 1496-3, ISO 1496-4, ISO 1496-5 and ISO 830. This part of ISO 18185 should also, wherever appropriate and practicable, be applied to freight containers other than those covered by the aforementioned International Standards.

Container seals are typically subjected to the harsh environments of the marine, rail and road transportation industries. Sand and dust, salt spray, grease, snow, ice and grime can be expected to coat the tag and sensing equipment. Physical shock and vibration are commonly encountered as a result of handling and transport operations.

Substantial temperature variations are common in worldwide container operations, as well as prolonged exposure to sunlight, including ultraviolet rays. The electronic seal shall operate satisfactorily at seal surface temperatures between -40 °C and $+70$ °C and shall maintain the integrity of stored data at temperatures from -51 °C to $+85$ °C. The electronic seal shall survive and maintain the integrity of stored data under (as a minimum) the severest of the environmental conditions covered by the test methods specified below.

The system shall be capable of full operation in the electromagnetic environment typically found at transportation facilities. The electronic seal shall survive and maintain the integrity of stored data in a maximum peak field strength of 50 V/m for 60 s, as may be encountered from any radio-frequency source such as a shipborne radar under normal operation or other such devices.

4.2 Low temperature

Electronic seals shall fully operate at a minimum low temperature of -40 °C. Electronic seals shall fully operate at such minimum temperatures after having been stored at a minimum low temperature of -51 °C with an exposure time of 24 h per day for a period of up to 60 days. Testing will be accomplished in accordance with IEC 60068-2-1 (MIL-STD-810F, Method 502.4).

4.3 High temperature

Electronic seals shall fully operate after having been cycled between $+70$ °C and $+38$ °C, as specified in 3.1. Electronic seals shall fully operate at such temperature extremes after having been stored at a minimum high temperature of $+85$ °C with an exposure time of 12 h to 15 h per day for a period of up to 60 days (which is the minimum electronic seal life time required for electronic seals compliant with ISO 18185-2). Testing will be accomplished in accordance with IEC 60068-2-2 (MIL-STD-810F, Method 501.4).

4.4 Mechanical shock

Electronic seals shall fully operate during and after having been subjected to a mechanical shock of 30 g for 11 ms, using a half-sine pulse. Testing will be accomplished in accordance with IEC 60068-2-27 (MIL-STD-810F, Method 516.5).

4.5 Random vibration

Electronic seals shall fully operate during and after having been subjected to a random vibration of a duration of 2 h, on all axes up to 3 g between -40 °C and $+70$ °C. Testing will be accomplished in accordance with IEC 60068-2-53 (MIL-STD-810F, Method 514.5).

4.6 Humidity

Electronic seals shall fully operate during and after having been subjected to humidity of up to 95 % non-condensing. Testing will be accomplished in accordance with IEC 60068-2-38 (MIL-STD-810F, Method 507.4).

4.7 Rain/snow

Electronic seals shall fully operate during and after having been subjected to rain and snow, as well as surviving submersion under 1 m of salt water. Testing will be accomplished in accordance with IEC 60068-2-18 (MIL-STD-810F, Method 506.4/512.4).

4.8 Salt fog

Electronic seals shall fully operate during and after having been subjected to salt fog. Testing will be accomplished in accordance with IEC 60068-2-11 (MIL-STD-810F, Method 509.4).

4.9 Drop shock

Electronic seals shall fully operate during and after having been subjected to a drop shock from a height of 3,3 m onto an impact surface of concrete or steel. Testing will be accomplished in accordance with IEC 60068-2-31 and IEC 60068-2-32 (MIL-STD-810F, Method 516.5), although the distance and impact surface will be as defined in this subclause.

4.10 Sand and dust

Electronic seals shall fully operate during and after having been subjected to exposure of sand and dust. Testing will be accomplished in accordance with IEC 60068-2-68 (MIL-STD-810F, Method 510.4).

4.11 Electromagnetic environment

Electronic seals shall survive and maintain the integrity of stored data under a maximum peak field strength of 50 V/m for 60 s. Such electronic seals shall further survive and maintain the integrity of stored data after having been subjected to a 25 kV electrostatic discharge.

Bibliography

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

[2] ISO 1496-2, *Series 1 freight containers — Specification and testing — Part 2: Thermal containers*

[3] ISO 1496-3, *Series 1 freight containers — Specification and testing — Part 3: Tank containers for liquids, gases and pressurized dry bulk*

[4] ISO 1496-4, *Series 1 freight containers — Specification and testing — Part 4: Non-pressurized containers for dry bulk*

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

[6] ISO 6346, *Freight containers — Coding, identification and marking*

[7] ISO 10374, *Freight containers — RF automatic identification*

[8] ISO 17363, *Supply chain applications of RFID — Freight containers*

[9] ISO 18185-4, *Freight containers — Electronic seals — Part 4: Data protection*

[10] ISO 18185-6, *Freight containers — Electronic seals — Part 6: Message sets for transfer between seal reader and host computer*

[11] European Union, ERC Recommendation 70-03, *Relating to the use of Short Range Devices (SRD), Annex 1 Non Specific Short Range Devices*

[12] European Union, ETSI EN 300 220, *Radio Equipment and Systems (RES); Short Range Devices; Technical Characteristics and Test Methods for Radio Equipment to Be Used in the 25 MHz to 1 000 MHz Frequency Range with Power Levels Ranging up to 500 mW*

[13] ANS INCITS 256 Part 4.2, *Radio Frequency Identification (RFID) — UHF RFID Protocols — 433.92 MHz UHF Narrowband Active Tag Interface*

[14] USA, 47 CFR, Part 15, *Code or Federal Regulations, Federal Communications Commission, 47 CFR, — Part 15 Radio frequency devices*

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)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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

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.

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 shall 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 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 part of ISO 18185 and are left to the individual electronic seal manufacturer.

5.3 Electronic authentication

Under the terms of this first-generation part of ISO 18185, there are no requirements for the ability to electronically authenticate a seal through data transmissions.

6 Conformance

Electronic seals claiming compliance with this part of ISO 18185 shall have the high security mechanical seal physical properties defined in ISO/PAS 17712. They shall further comply with the electronic seal manufacturers' security-related practices identified in Annex A.

Annex A
(normative)

Electronic seal manufacturers’ security-related practices

A.1 Introduction

This annex addresses security-related practices relevant to the manufacture and distribution of electronic security seals (electronic seals) and related equipment that conform to all 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/PAS 17712 with modifications appropriate to electronic seals and related equipment.

The structure of this part of ISO 18185 reflects the six stages in the life of a freight container electronic seal, as shown in Table A.1. Since this part of ISO 18185 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 subcontracted 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	Shall set standards and expectations of distributors and resellers. Shall help educate distributors and resellers.
4	User knowledge and discipline	Shall help educate users in correct use and maintenance of electronic seal readers and related equipment. Shall help educate users in the care of electronic seals prior to their application to containers, trailers, or other receptacles. Shall 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. Shall help educate distributors and resellers about maintaining historical data on their electronic seal inventories and sales. 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

Manufacturers shall 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.

Physical design of electronic seal readers and related equipment shall respect the environmental characteristics covered in ISO 18185-3.

Although this part of ISO 18185 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.

Manufacturers shall 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 clause 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

The manufacturer shall maintain ISO 9001 (or equivalent) certification on all company-owned manufacturing facilities.

When purchasing contract production services for market-ready electronic seal products, the manufacturer shall purchase from ISO 9001 (or equivalent) certified plants.

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 decertification impacts the use of that company's specific product in international trade.

The security practices referenced herein shall be implemented in accordance with this part of ISO 18185.

The manufacturer shall accept random and unannounced inspections of facilities and documentation for conformance with this document; inspections shall be accomplished by appropriate third-party certification bodies. The "certification bodies" shall be governmental agencies or accredited independent organizations. Nothing in this part of ISO 18185 implies that industry certifying or regulatory bodies would reveal trade secrets or proprietary information among competitors.

The manufacturer shall conduct an initial security risk assessment of its facilities and periodic update reviews, and shall implement countermeasures and/or policies to overcome potential vulnerabilities or threats.

The manufacturer shall assign responsibility for security and product integrity to knowledgeable individual(s), with a principal point of contact.

The manufacturer shall agree to cooperate with relevant law enforcement officials.

The manufacturer shall cooperate with regulatory or certification bodies in responding to questions or issues regarding compliance, irregularities, copying, etc. The "certification bodies" shall be governmental agencies or accredited independent organizations. Nothing in this part of ISO 18185 implies that industry certifying or regulatory bodies would reveal trade secrets or proprietary information among competitors.

The 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 products.

The 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).

The manufacturer shall require background checks on all employees to the extent allowed under local law or regulation.

A.3.2 Electronic seal/reader product certification

The manufacturer shall, on an annual basis, submit samples of all relevant products to an independent third party testing laboratory to ensure the product complies with this part of ISO 18185 and ISO/PAS 17712 or its successor International Standard. The testing lab shall be certified according to the standards outlined in ISO/IEC 17025.

The manufacturer shall mark electronic seals and readers with its company identity.

NOTE 1 The manufacturer's identity is part of the electronic seal data structure in ISO 18185-1.

The manufacturer shall produce electronic seals with unique physical and electronic numbers or identifiers. The seal manufacturer ID, a component of the seal ID, is addressed in ISO/TS 14816.

NOTE 2 The electronic seal ID is addressed in ISO 18185-2.

The manufacturer shall produce electronic seal readers and related equipment with unique physical serial numbers or identifiers. There shall 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 3 This logical reader identifier is used by the terminal or area management system to associate the reader with a given location.

The 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). The 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.

The manufacturer shall segregate and render non-functional any incidental production of scrap electronic seal products before disposal.

The manufacturer shall control access to production and storage areas and loading docks and stores electronic seals and related equipment in secure areas.

The manufacturer shall lock all loaded trailers or containers on the premises.

The manufacturer shall "inspect what it expects", by verifying driver identification, if applicable, and verifying the load and count of inbound electronic seal components.

The manufacturer shall implement a policy for off-hour deliveries to ensure prior notice of these deliveries. The policy shall 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.

The distributor/reseller shall permit the manufacturer to review its security procedures.

The 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.

The distributor/reseller shall not sell electronic seals or related equipment without the manufacturer (responsible party's) identity marked on the devices.

The 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. The 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.

The distributor/reseller shall conduct an initial security risk assessment of its facilities and implement countermeasures and/or policies to overcome potential vulnerabilities or threats.

The distributor/reseller shall control access to storage areas and loading docks, and store electronic seals and related equipment in secure areas.

The distributor/reseller shall lock all loaded trailers or containers on the premises.

The distributor/reseller shall "inspect what it expects", by verifying driver identification, if applicable, and verifying the load and count of inbound electronic seal components.

The 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 e-mail, 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.

Manufacturers will help educate users in the importance of proper control of, and record-keeping about, electronic seals prior to their application and use.

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:

- total responsibility for maintaining the manufacturer's data on electronic seal/reader production, sales, and unique numbers and identifiers; and

- responsibility to educate distributors and resellers 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 646, *Information processing — ISO 7-bit coded character set for information interchange*

[2] ISO 668, *Series 1 freight containers — Classification, dimensions and ratings*

[3] ISO 690, *Documentation — Bibliographic references — Content, form and structure*

[4] ISO 690-2, *Information and documentation — Bibliographic references — Part 2: Electronic documents or parts thereof*

[5] ISO 830, *Freight containers — Vocabulary*

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

[7] ISO 1496-2, *Series 1 freight containers — Specification and testing — Part 2: Thermal containers*

[8] ISO 1496-3, *Series 1 freight containers — Specification and testing — Part 3: Tank containers for liquids, gases and pressurized dry bulk*

[9] ISO 1496-4, *Series 1 freight containers — Specification and testing — Part 4: Non-pressurized containers for dry bulk*

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

[11] ISO 6346, *Freight containers — Coding, identification and marking*

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

[13] ISO 9001, *Quality management systems — Requirements*

[14] ISO/IEC TR 10000-1, *Information technology — Framework and taxonomy of International Standardized Profiles — Part 1: General principles and documentation framework*

[15] ISO 10241, *International terminology standards — Preparation and layout*

[16] ISO 10374, *Freight containers — Automatic identification*

[17] ISO 14816, *Road transport and traffic telematics — Automatic vehicle and equipment identification — Numbering and data structure*

[18] ISO 17363, *Supply chain applications of RFID — Freight containers*

[19] ISO 18185-1, *Freight containers — Electronic seals — Part 1: Communication protocol*

[20] ISO 18185-2, *Freight containers — Electronic seals — Part 2: Application requirements*

[21] IEC 60027 (all parts), *Letter symbols to be used in electrical technology*

ICS 55.180.10

Price based on 10 pages

INTERNATIONAL STANDARD

ISO 18185-5

First edition
2007-05-01

Freight containers — Electronic seals —

Part 5: **Physical layer**

Conteneurs pour le transport de marchandises — Scellés électroniques —

Partie 5: Couche physique

Reference number
ISO 18185-5:2007(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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 18185-5 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 defines the physical layer for compliant electronic seals.

It has been created to ensure global adoption of ISO 18185, providing a standardized physical layer as developed in the RFID standards of ISO/IEC 18000 and ISO/IEC 24730.

Freight containers — Electronic seals —

Part 5: **Physical layer**

1 Scope

This part of ISO 18185 specifies the air interface between electronic container seals and Reader/Interrogators of those seals.

It is to be used in conjunction with the other parts of ISO 18185.

This part of ISO 18185 describes the physical layer for supply chain applications of RFID for freight containers in accordance with the ISO 18185 series and ISO 17363, since it is expected that the implementation of these standards will face the same international conditions. However, each of these standards has its own unique requirements other than the physical layer. It is expected that RFID Freight Container Identification (as specified in ISO 10374 and ISO 17363), and electronic seals (as specified in the ISO 18185 series) will be able to use the same infrastructure, while recognizing that that there may be requirements for different frequencies for passive devices as opposed to the active devices identified in this part of ISO 18185.

This part of ISO 18185 is applicable to all electronic seals used on freight containers covered by ISO 668, ISO 1496 (parts 1 to 5) and ISO 830 and should, wherever appropriate and practicable, be applied to freight containers other than those covered by the aforementioned 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/PAS 17712, *Freight containers — Mechanical seals*

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

ISO/IEC 18000-7:—[1], *Information technology — Radio frequency identification for item management — Part 7: Parameters for active air interface communications at 433 MHz*

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)*

ISO/IEC 2382-26, *Information technology — Vocabulary — Part 26: Open systems interconnection*

ISO/IEC 24730-2:2006, *Information technology — Real-time locating systems (RTLS) — Part 2: 2,4 GHz air interface protocol*

[1] To be published. (Revision of ISO/IEC 18000-7:2004)

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 17712, ISO/IEC 19762-1, ISO/IEC 19762-3 and the following apply.

3.1
electronic seal
eSeal
read-only, non-reusable freight container seal conforming to the high security seal defined in ISO 17712 and conforming to ISO 18185 (or revision thereof) that electronically evidences tampering or intrusion through the container doors

3.2
seal identification
seal ID
unique identification of each manufactured seal incorporating serial number (i.e. Tag ID) and manufacturer ID

NOTE The combination is called the seal ID.

3.3
Interrogator identification
Interrogator ID
code used to identify the source address during every communication session originated by the Interrogator

3.4
physical layer
in the Open Systems Interconnection reference model, the layer that provides the mechanical, electrical, functional, and procedural means to establish, maintain and release physical connections for transfer of bits over a transmission medium

[ISO/IEC 2382-26]

3.5
LF transmitter ID
code used to identify the LF transmitter

4 Physical layer for electronic seals

4.1 General

The ISO 18185 system consists of the three distinct components: eSeal, LF transmitter, and Reader. The main feature of the system is its dual frequency operation.

There are two types of physical layers:

- type A physical layer is the 433 MHz long-range Link and OOK LF short-range link;

- type B physical layer is the 2,4 GHz long-range link and FSK short-range link.

The eSeal shall support both types of air interfaces. The data link protocols are different for each physical layer. Interrogators and Reader devices may support one or both types of physical layers.

The eSeal shall be capable of communicating on two long-range RF links. The protocol for these two links is specified in 4.2.1 and 4.3.1. The e-seal shall also be capable of receiving LF magnetically coupled transmissions as specified in 4.2.2.1 and 4.3.2. Data may be transmitted from the LF transmitter to the eSeal(s) without acknowledgment (one-way link only).

A short-range, low-frequency link between LF transmitter and eSeal(s) is used to localize eSeal(s) inside the magnetically coupled transmitter antenna field of an LF transmitter. Data are transmitted from the LF transmitter to the eSeal(s) without LF acknowledgment. All eSeal(s) in the field of an LF transmitter receive the LF transmitter's data simultaneously; i.e. the LF transmitter takes the same amount of time to transmit its data to any number of eSeals.

The long range links (433,92 MHz or 2,4 GHz) are used by eSeal(s) to reply to the Reader with the location (i.e. LF transmitter ID), its own identification (eSeal ID), and eSeal Status data are transmitted from the eSeal(s) to the Reader(s).

To avoid collisions during UHF transmission, in type A operation mode, the eSeal operates according to the anti-collision algorithm specified in 4.2; in type B operation mode, the eSeals do not require an anti-collision protocol.

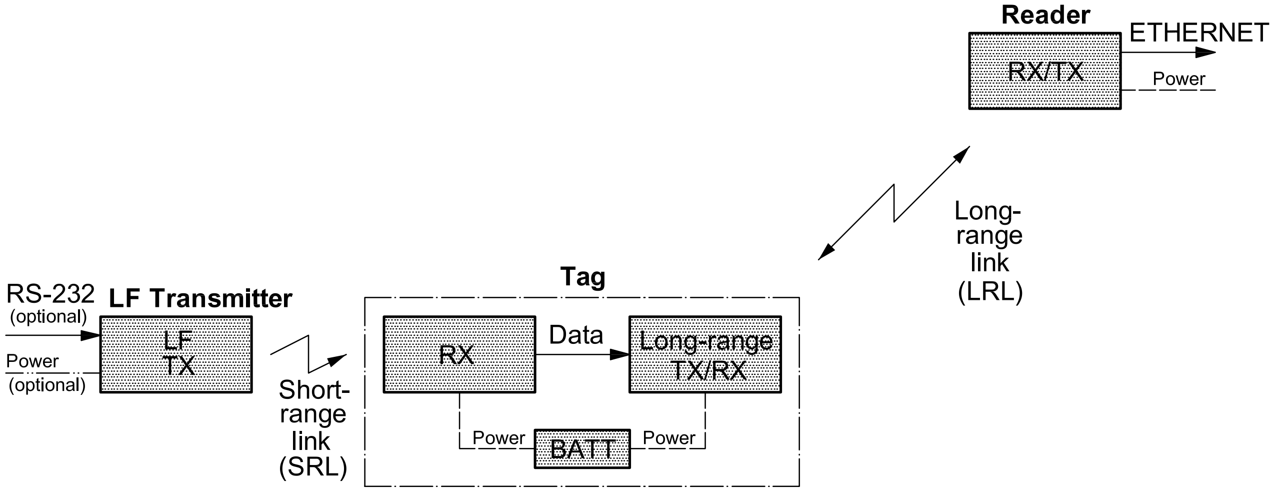


Figure 1 — System components

4.2 Type A physical layer protocol

4.2.1 433 MHz long-range link physical layer protocol

4.2.1.1 General

The collision arbitration uses a mechanism that allocates tag transmissions into slots within a specified collection round (or so-called window size). The window size parameter indicates the time an Interrogator will listen for tag responses during a current collection round. A collection round consists of a number of slots. Each slot has a duration long enough for the Interrogator to receive a tag response. The actual duration of a slot is determined by the Interrogator collection command type and is a function of the tag transmission time.

The Interrogator initiates a tag collection process by sending a Collection command. Tags receiving a Collection command randomly select a slot in which to respond, but do not immediately start transmitting. The number of slots in a current collection round is determined by the required field size based on the type of Collection command. Each Collection command requires a specific type and amount of data to be transmitted by the tag within a single slot time. Therefore, the size of each slot is determined by the length of time needed for a tag to provide the designated response indicated by the specific command. The number of available slots will be determined by dividing the window size by the time required for an individual tag response. During the subsequent collision arbitration process, the Interrogator dynamically chooses an optimum window size for the next collection round based on the number of collisions in the round. The number of collisions is a function of the number of tags present within the Interrogator communication range that participate in the current collection round.

On receiving a Collection command, tags select a slot in which to respond. The selection is determined by a pseudo-random number generator. When a tag selects a slot number, it will wait for a pseudo-random time delay equal to a time of slot number multiplied by slot delay before it responds. The number of slots is determined by the current window size, indicated through the Interrogator collection command type and a tag transmission time.

After the Interrogator has sent the Collection command, there are three possible outcomes:

a) The Interrogator does not receive a response because either no tag has selected a current slot or the Interrogator did not detect a tag response. Once no tag is detected in any slot, the Interrogator then terminates the current collection round. This process will be repeated for three rounds before the collection process is terminated.

b) The Interrogator detects a collision between two or more tag responses. Collisions may be detected either as contention from the multiple transmissions or by detecting an invalid CRC. The Interrogator records the collision and continues “listening” for a new tag in the subsequent slot.

c) The Interrogator receives a tag response without error, i.e. with a valid CRC. The Interrogator records the tag data and continues to listen for a new tag in the subsequent slot.

The collection round continues until all slots within the round have been explored.

When the collection round is completed, the Interrogator starts transmitting Sleep commands to all tags collected during the previous collection round. The tags that receive Sleep commands move to “sleep” mode and will not participate in collection in the subsequent collection rounds.

The Interrogator immediately starts the next collection round by transmitting the collection command.

This process continues until no more tags are detected during three subsequent collection rounds.

ISO 18185-1 defines the communications protocol beyond the physical layer.

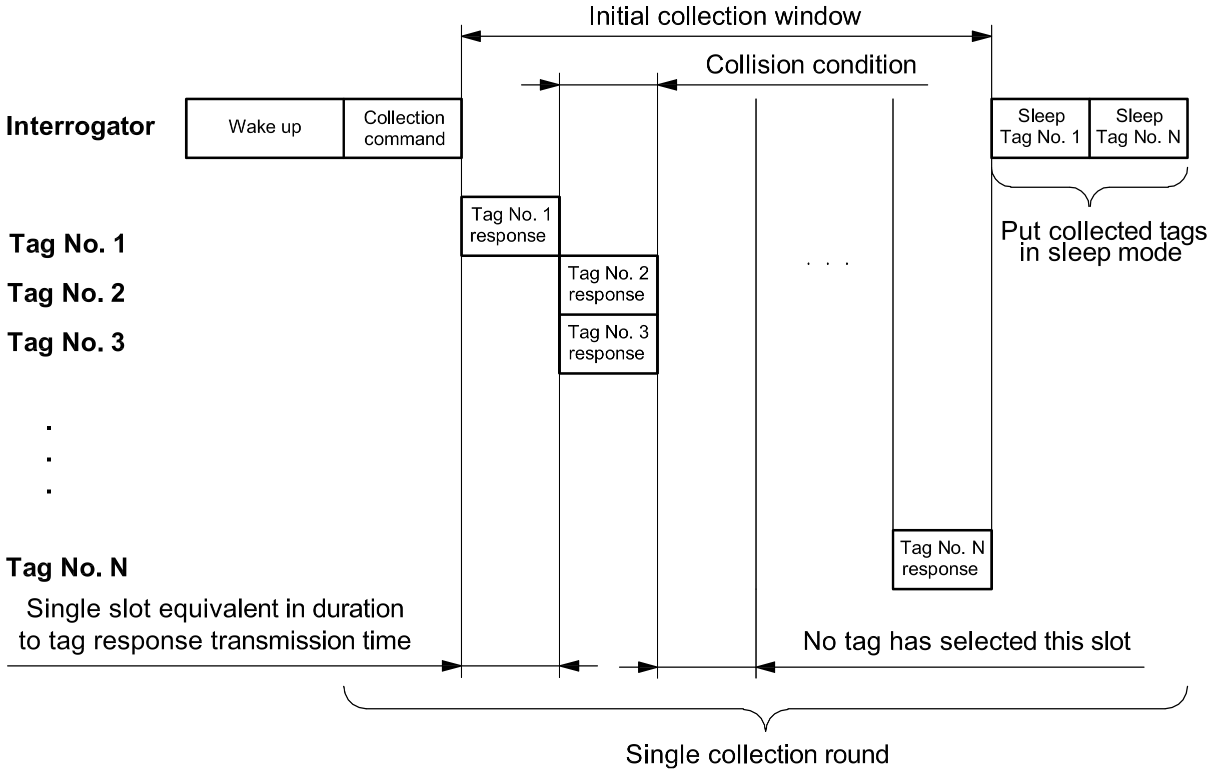


Figure 2 — Collection process example

4.2.1.2 Compliance to air interface standards

The physical layer of an electronic seal compliant with this part of ISO 18185 shall be in accordance with ISO/IEC 18000-7:—, 6.1, 6.2.2, 6.2.3, 6.2.5, 6.3.1 and 6.3.2.

4.2.2 OOK LF physical layer protocol

4.2.2.1 General

The LF transmitter to eSeal communication utilizes low frequency (123 kHz to 125 kHz) OOK modulation schemes and operates at short range. Data are repeatedly transmitted (or when triggered by the external sensor) from the LF transmitter to the eSeal without acknowledgment.

4.2.2.2 Data modulation and coding

4.2.2.2.1 Data modulation

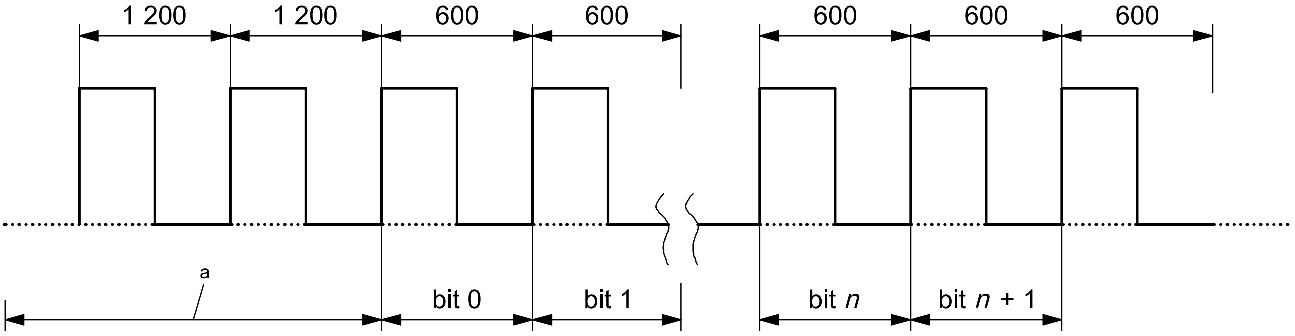
Data transmitted between the LF transmitter and the eSeal utilizes OOK.

4.2.2.2.2 Data encoding

Manchester encoding is used for data with the same symbol encoding as defined in 4.2.1.2 for LRL.

4.2.2.2.3 Data rate

The data rate is approximately 1 600 bps.



[a] Preamble.

NOTE The first data bit always starts with transmission from low to high.

Figure 3 — OOK LF packet structure

As each packet sent from the LF transmitter to the eSeal might have a different length, the start of every packet is indicated by a preamble. The end of a packet is indicated by a final period of at least 1 200 µs of continuous “off” modulation transmission (i.e. no transmission) for each packet after the CRC bytes.

The preamble is defined as at least eight subsequent pulse intervals of 1 200 µs. If multiple packets are sent one after another, a preamble of at least two 1 200 µs intervals is used between two subsequent packets.

4.3 Type B physical layer protocol

4.3.1 2,4 GHz long-range link physical layer protocol

The physical layer conforming to this part of ISO 18185 shall be in accordance with subclause 5.5, Table 1 and Clause 6 of ISO/IEC 24730-2:2006 and, with the exception of the location function of ISO/IEC 24730-2, shall be completely compatible with that standard.

4.3.2 2,4 GHz physical link parameters

For the purposes of this part of ISO 18185, the parameter definitions given in Table 1 apply. These parameters are referenced by parameter name. These operating parameters shall be defined for the temperature range and shall be amended with the parameters in ISO 18185-3.

Table 1 — eSeal transmitter link parameters

Parameter name	Description
Operating frequency range	2 400 MHz to 2 483,50 MHz
Operating frequency accuracy	± 25 ppm maximum
Centre frequency	2 441,750 MHz
Occupied channel bandwidth	60 MHz
Transmit power	Class 1:.. 10 dBm EIRP max. Class 2:.. Maximum in accordance with local regulations.
Spurious emission, out of band	The device shall transmit in conformance with spurious emissions requirements defined by the country's regulatory authority within which the system is operated.
Modulation	BPSK Direct Sequence Spread Spectrum (DSSS)
Data encoding	Differentially encoded
Data bit rate	59,7 kb/s
Bit error rate	0,001 %
PN chip rate	30,521875 MHz ± 25 ppm
PN code length	511
PN spread code	0x1CB
Data packet lengths	152 bits
Message CRC polynomial	$G(x) = X^{12} + X^{11} + X^3 + X^2 + X + 1$
CRC polynomial initialized value	0×001
Blink interval	Programmable, 5 s minimum
Blink interval randomization	± 638 ms maximum
Number of sub-blinks	Programmable, 1 - 8
Sub-blink interval randomization	125 ms ±16 ms maximum
Maximum frequency drift	< ± 2 ppm over the duration of the entire message
Phase accuracy	< 0,50 radians within any 33 μs period
Phase noise	< 15 degrees when the noise is integrated from 100 Hz to 100 kHz

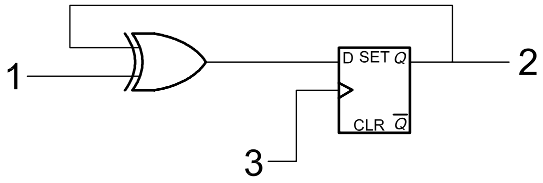
4.3.3 System description

4.3.3.1 General

The 2,4 GHz transmitter module in an eSeal is a compact internally powered radio frequency device that is a component of the eSeal system (hereinafter referred to as the transmitter). Each transmission is a pulse of direct sequence spread spectrum radio signal. The Reader infrastructure receives these signals or blinks. The blink is a short ID-only message or a longer telemetry message also containing the transmitter's ID. Each transmission also contains a status data word that provides information on the transmitter configuration, battery status and other data. The transmitter's ID, status data word, and location are provided to the host by the Reader Infrastructure. Multiple transmitters may be present in typical installations allowing a large number of items to be tracked and located in real time.

Anti-collision synchronization protocols are not required. Each "blink" comprises multiple sub-blinks. The sub-blinks are part of a multiple-level anti-interference system: time diversity, spatial diversity, processing gain. The combination of these multiple sub-blinks, multiple receiving antennas and spread spectrum correlation also allows multiple transmitters to blink simultaneously and still be received.

The transmitter data shall be binary encoded with the MSB (Most Significant Bit) transmitted first in all messages. It is differentially encoded using the example circuit of Figure 4. The output of the encoder shall be initialized to "1". It shall be exclusively OR'd with the output of the PN (Pseudo Noise) generator, modulated using a BPSK (Bi-Phase Shift Keyed) format and upconverted using a single sideband upconverter. The signal is then amplified and transmitted to the Reader infrastructure.



Key

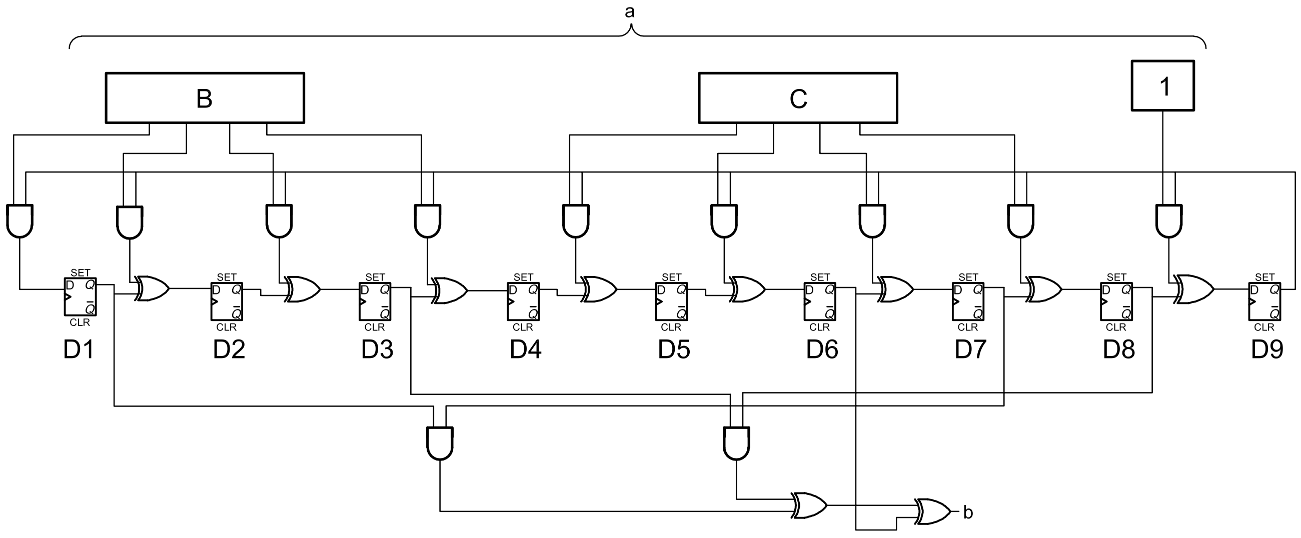
1 data in

2 data out

3 clock

Figure 4 — Example of differential encoding circuit

An example of the eSeal transmitter PN generator is shown in Figure 5.



[a] PN code.

[b] PN generator output.

Figure 5 — eSeal transmitter PN generator

The data encoding and transmission process is shown in Figure 6

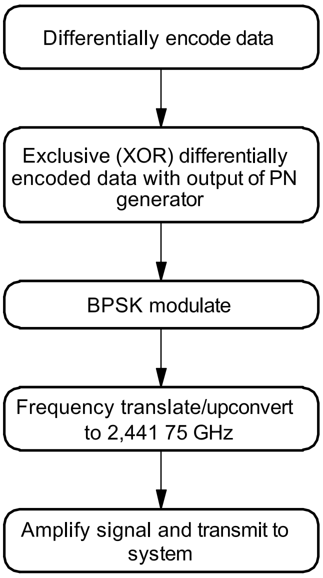
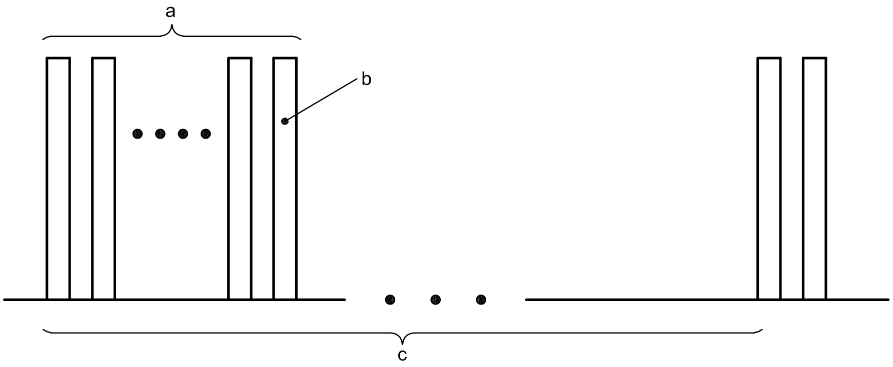

Differentially encode data
Exclusive (XOR) differentially encoded data with output of PN generator
BPSK modulate
Frequency translate/upconvert to 2,441 75 GHz
Amplify signal and transmit to system

Figure 6 — Transmitter data encoding and transmission process

The format of the Direct Sequence Spread Spectrum (DSSS) transmission from the transmitter is shown in Figure 7. Each DSSS transmission from the transmitter contains a "blink" packet containing N sub-blinks. All sub-blinks within a "blink" shall be identical to provide time diversity. Each sub-blink includes the fields defined in the 2,4 GHz protocol specified in ISO 18185-1. The "blink" packet occurs at the beginning of the blink interval. Sub-blinks shall be separated by an interval, which is not user configurable. The number of sub-blinks per blink and the blink interval may be configurable.

The DSSS carrier frequency is fixed at 2 441,75 MHz and the chip rate shall be fixed at 30,521 875 MHz.



[a] Blink containing N sub-blinks.

[b] Sub-blink.

[c] Blink interval.

Figure 7 — DSSS air interface

4.3.3.2 Transmitter radiated power

Two classes of transmitters exist with respect to the output power level they are capable of delivering. The Equivalent Isotropically Radiated Power (EIRP) of a Class 1 transmitter is less than 10 mW (10 dBm). Class 1 transmitters are intended for applications with moderate to dense infrastructures and minimal obstructions.

The EIRP of a Class 2 transmitter is greater than 10 mW (10 dBm) and less than the maximum allowed by local radio regulations. Class 2 transmitters are intended for sparse infrastructures where Readers may be located greater than 300 m from the transmitter or environments with major obstructions.

4.3.3.3 DSSS message encoding

The PN Spreading Code shall be 0x1CB. The PN generator is initialized with “1” in register D9 and “0” in all other registers.

The beginning of the blink interval shall be randomized by a maximum of ±638 ms to avoid repeatedly colliding with blinks from other transmitters. The beginning of each successive sub-blink shall also be randomized. The interval between each sub-blink shall be 125 ms randomized by a maximum of ±16 ms from the beginning of the previous sub-blink.

4.3.4 FSK short-range link physical layer protocol

4.3.4.1 Physical link specifications

Table 2 lists the physical link specifications from the LF transmitter to the eSeal.

Table 2 — Magnetic physical link specifications

Item	Parameter	Value
M 1	Signaling frequencies	114,688 kHz and 126,976 kHz
M 2	Field strength	Regulatory/application dependent
M 3	Bit data rate	2,048 kb/s
M 4	Symbol period	244,14 µs
M 5	Data error rate	0,001 %
M 6	Start sync	3 symbol periods @ 114,688 kHz followed by 3 symbol periods @ 126,976 kHz
M 7	End sync	3 symbol periods @ 126,976 kHz followed by 3 symbol periods @ 114,688 kHz
M 8	Data bit “0”	1 symbol period @ 126,976 kHz followed by 1 symbol period @ 114,688 kHz
M 9	Data bit “1”	1 symbol period @ 114,688 kHz followed by 1 symbol period @ 126,976 kHz

4.3.4.2 LF transmitter air interface

The LF transmitter is a device that shall repetitively transmit, without gap, 28-bit or 44-bit magnetic messages designed to stimulate responses from RTLS transmitters. The LF transmitter shall be a transmit-only device and shall not have an air interface receiver. The transmitter configuration shall change to the parameters specified in the 44-bit message.

The LF transmitter shall communicate via a FSK magnetic link. The magnetic FSK frequencies shall be 114,688 kHz and 126,976 kHz. The LF transmitter shall use Manchester Encoding.

Bibliography

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

[2] ISO 830, *Freight containers — Vocabulary*

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

[4] ISO 1496-2, *Series 1 freight containers — Specification and testing — Part 2: Thermal containers*

[5] ISO 1496-3, *Series 1 freight containers — Specification and testing — Part 3: Tank containers for liquids, gases and pressurized dry bulk*

[6] ISO 1496-4, *Series 1 freight containers — Specification and testing — Part 4: Non-pressurized containers for dry bulk*

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

[8] ISO 10374, *Freight containers — RF automatic identification*[2]

[9] ISO 17363, *Supply chain applications of RFID — Freight containers*

[10] ISO 18185-1, *Freight containers — Electronic seals — Part 1: Communication protocol*

[11] European Union, ERC Recommendation 70-03, *Relating to the use of Short Range Devices (SRD), Annex 1 Non-specific Short Range Devices*

[12] European Union, ETSI EN 300 220, *Radio equipment and systems (RES); short range devices (SRDs); Technical characteristics and test methods for radio equipment to be used in the 25 MHz to 1 000 MHz frequency range with power levels ranging up to 500 mW*

[13] ANS INCITS 256 Part 4.2, *Radio Frequency Identification (RFID) — UHF RFID Protocols — 433,92 MHz UHF narrowband active tag interface*

[14] USA, 47 CFR, Part 15, Code of Federal Regulations, Federal Communications Commission, 47 CFR, Part 15: *Radio frequency devices*

[2] To be published. (Revision of ISO 10374:1991)

ICS 55.180.10

Price based on 10 pages