

Freight containers — Electronic seals — Part 1: Communication protocol

Warning

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

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

Document type: International Standard
Document subtype:
Document stage: (30) Committee
Document language: E

Copyright notice

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

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

[Indicate the full address, telephone number, fax number, telex number, and electronic mail address, as appropriate, of the Copyright Manger of the ISO member body responsible for the secretariat of the TC or SC within the framework of which the working document has been prepared.]

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

Violators may be prosecuted.

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Common requirements	2
5 Seal data	2
6 Data link layer protocol for electronic seal	4
6.1 Data link layer packet structure	4
6.2 Anti-collision algorithm Collection algorithm	7
6.3 Command codes and parameters	9
6.4 Command code	9
6.5 Seal model and version	11
Bibliography	18

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 & 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: Sensor interface requirements (under request for withdrawal)*
- *Part 6: Message sets for transfer between seal reader and host computer*
- *Part 7: Physical Layer.*

Introduction

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

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.

ISO 18185 is an International Standard in multiple 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: Sensor interface requirements (under request for withdrawal)

Part 6: Message sets for transfer between Seal reader and host computer

Part 7: Physical layer.

Freight containers — Electronic seals — Part 1: Communication protocol

1 Scope

This International Standard provides a system for the identification and presentation of information about freight container electronic Seal s. The identification system provides an unambiguous 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 to determine whether a freight container's Seal has been opened.

This International Standard specifies a freight container Seal identification system, with an associated system for verifying the accuracy of use, having:

- A Seal status identification system;
- A battery status indicator;
- A unique Seal Identifier including the identification of the manufacturer.

This International Standard applies to all electronic Seal s used on:

Freight containers covered by International Standards ISO 668, parts 1 to 5 of ISO 1496, ISO 8323 and should, wherever appropriate and practicable, also be applied to freight containers other than those covered by these International Standards.

2 Normative references

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

ISO 646, *Information processing - ISO 7-bit coded character set for information interchange*

ISO 668, *Series 1 freight containers - Classification, dimensions and ratings*

ISO 830, *Freight containers - Vocabulary*

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

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

ISO/IEC 19762, *Information technology AIDC techniques - Harmonized vocabulary*

ISO/IEC 15963, *Automatic identification - Radio frequency identification for item management - Unique identification for RF tag*

ISO 17712, *Freight containers - Mechanical seals.*

3 Terms and definitions

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

3.1 electronic seal
a 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
unique identification of each manufactured Seal incorporating all necessary information such as serial number (i.e., Tag ID), and manufacturer ID. This combination shall be called Seal ID. The Seal unique identification shall conform to the UCC.EAN format specified in ISO/IEC 15963.

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

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 standard.

5 Seal data

5.1 The electronic Seal mandatory data includes Seal status, Seal tag Id and manufacturer ID (that combined to make up the Seal ID), date/time for Sealing and opening, Seal status, low battery status, protocol ID, model ID, product version, and protocol version.

The Seal status occupies 2 bits, as follows:

- Open and unsealed
- Closed and sealed
- Opened

The following are definitions of the Seal states:

- 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).

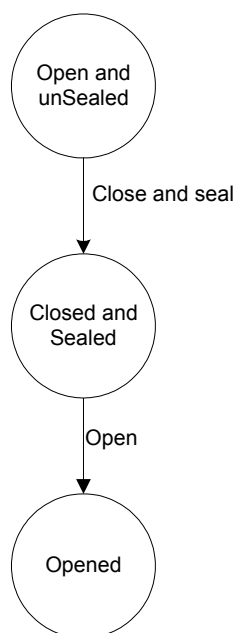


Figure 1 — Seal states

5.2 The low battery Status occupies 1-bit. For low battery Status; “0” indicates battery state is above threshold. “1” indicates battery state at or below 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 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 14816:2000. The RF Component Manufacturer ID of the Seal is programmed by the RF Component Manufacturer.

5.5 Date/Time sealed: the eSeal will record the time of sealing from real-time clock based on UTC time.

5.6 Date/Time opened: the eSeal will record the time of opening from real-time clock based on UTC time.

5.7 The Protocol ID indicates the protocol type.

5.8 The Model ID indicates the manufacturer’s model number.

5.9 Product Version 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 indicates the version of the standard protocol (this document) that the Seal adheres to. The high byte is the major version number and the low byte is the minor version. For this version of the standard this parameter must be 0x0100. (I.e. version 1.0).

6 Data link layer protocol for electronic seal

6.1 Data link layer packet structure

6.1.1 Protocol identification and field synchronization

In this section, 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 specification, 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 packet options field. The packet options field is defined in 6.1.2. In the reverse link (Seal to Interrogator), field synchronization is accomplished through the use of 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 6.1.2. The mode field is defined in 6.1.2.

The Protocol ID specifies general packet structure as defined by this protocol standard.

Table 1 — Interrogator for seal command format (point to point)

Protocol ID	Packet Options	Tag Manufacture 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 2 — Seal to interrogator response format (point to point)

Protocol ID	Seal Status	Packet Length	Interrogator ID	Tag Manufacture 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 3 — 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 4 — Seal to interrogator response format (Broadcast)

Protocol ID	Seal Status	Packet Length	Interrogator ID	Tag Manufacture 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 5 — Seal to interrogator alert message format

Protocol ID	Seal Status	Packet Length	Tag Manufacture 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.								

6.1.2 Packet fields format and definition

6.1.2.1 Protocol ID

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

6.1.2.2 Argument Length

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

6.1.2.3 Min. command duration

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 realize the command is not addressed to it; it may switch to sleep mode for duration of specified by this field.

NOTE This field can be used for saving power consumption in scenarios where an Interrogator has to send a sequence of Point-to-Point commands to several Tags. This way each Seal can be in sleep mode between all the commands that are not addressed to it.

6.1.2.4 Max. command duration

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 seconds). When a Seal receives this command and the command is directed to it, it may switch to sleep mode after this interval if it doesn't 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.

6.1.2.5 Packet options

Packet Options field is defined as follows:

Table 6 — Packet option field

Bit	Value = 0	Value = 1	Description
0	Reserved	Reserved	
1	Broadcast (Tag ID and manufacture ID not present)	Point to Point (Tag ID and manufacture ID field present)	The command is either broadcast to all Tags or only to the Seal who's 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		

6.1.3 Seal status

6.1.3.1 General

The Seal Status field, which is included in all Seal to Interrogator messages, shall consist of the following information:

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 = Nack 0 = Ack

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

Mode field indicates response data format from the Seal (Broadcast, Point to Point, Alert). It is defined as follows.

Table 8 — Mode field

Mode field	Mode format code (Bit 15 - 12)
Broadcast	0000
Alert	0001
Point to point	0010

Seal Type indicates specific Seal Tag type as defined by each manufacturer.

Acknowledgment flag indicates whether received packet complies with the standard and all parameters are within the specified range. Seal shall not respond if received packet does not comply with this protocol format or has CRC error. Seal shall respond with a Nak flag if the received packet comply with this protocol format and has a valid CRC, but with an unknown command code. *Opened* flag indicates current status of the Seal. 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.

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

6.1.3.2 Command arguments

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 Cyclic Redundancy Check (CRC) is appended to the data as 2 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 Interrogator with an additional error checking mechanism where several solicited and unsolicited Seal packets are being received by the Interrogator.

6.2 Anti-collision algorithm Collection algorithm

6.2.1 General

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.

6.2.2 Algorithm

The collision arbitration uses a mechanism, which allocates tag transmissions into slots within specified collection round (or so called window size). 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 specific type and amount of data to be transmitted by the tag within 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:

- 1) The Interrogator does not receive a response because either no tag has selected current slot or Interrogator did not detect a tag response. Once no tag is detected in any slot, the Interrogator then terminates current collection round. This process will be repeated for 3 rounds before the collection process is terminated.
- 2) 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 collision and continue, "listening" for a new tag in the subsequent slot.
- 3) 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 command to all tags collected during the previous collection round. The tags that receive Sleep command 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 being detected during three subsequent collection rounds.

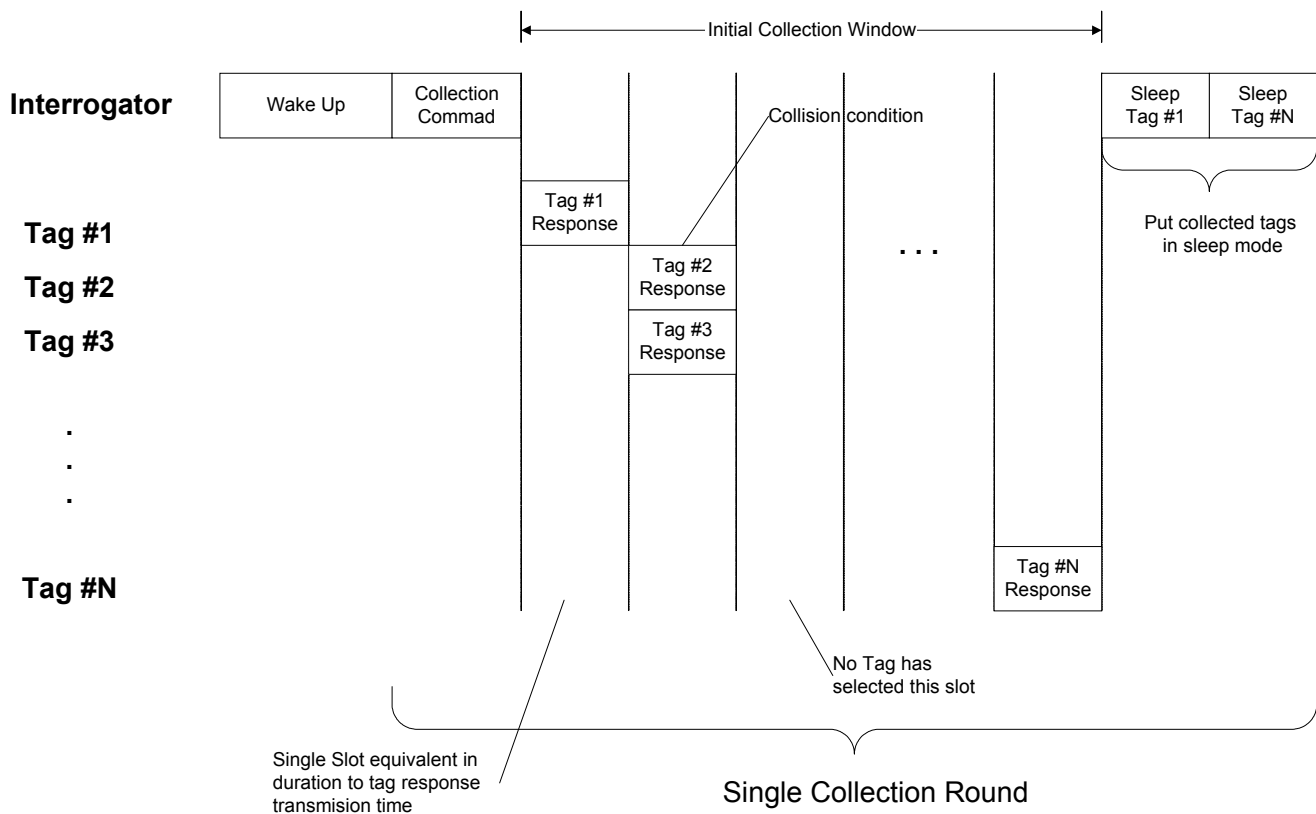


Figure 2 — Collection process example

6.3 Command codes and parameters

Summary of all Command codes defined by this protocol per Table 9:

Table 9 — 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	Read the current time from the real-time clock. (Number of seconds elapsed since Jan 1 st , 1990, 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	Tell all the receiving Seals except of 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
0x 70 – 0x7F	(Reserved for future use)		Reserved
NOTE The seal will ignore the unrecognized commands			

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

6.4 Command code

6.4.1 Collection

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

Table 10 — Collection command format

Command Code	Command Arguments	
'10'	Windows size	Collection criteria
	2 bytes	1 byte

Table 11 — Seal collect arguments

Argument name	Size	Description
Window Size	2 bytes	The number of time slots in the collection round. Each slot is TBD ms.
Collection Criteria	1 byte	The criteria for the Seal s that should respond. See below for more details.

The Collection Criteria argument determines which Seal/s should respond to the command according to the following codes:

- All Seals – 0x00
- Sealed Seals – 0x02
- Opened Seals– 0x04
- Specific Seal type – NNX0000b.

The bit 4, denoted with X, indicates that Seal type field is included as part of collection criteria. If bit 4 is cleared than 3 most significant bits are ignored by Seal and only lower 4 bits are used during collection.

Note that these codes or conditions are inclusive OR-ed.

6.4.1.1 Seal response

The Seal response shall have no data.

6.4.2 Sleep

Table 12 — Sleep command format

Command code	Command Arguments
'15'	None

6.4.2.1 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 awoken again by Wake Up signal.

6.4.2.2 Arguments

This command has no arguments.

6.4.2.3 Seal response

The Seal shall not respond to this command.

Table 13 — Seal Response to Sleep

None

Sleep operation is used to put a specific Seal in 'Sleep' state, which prevents the Seal to participate in the subsequent collection rounds during the collection process.

In this state the Seal will ignore any command from the Interrogator until it receives "Wake up" signal.

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

6.4.3 Sleep all but

Table 14 — Sleep all but

Command code	Command arguments	
'16'	Tag Manufacture ID	Tag ID
	2 bytes	4 bytes

6.4.3.1 Description

The Sleep all but command may be used to tell all the Seal s except of a specified one to return to Sleep mode. In the sleep state all Seal s will ignore any command from the Interrogator until it receive "Wake up" signal.

6.4.3.2 Seal response

Seal shall not respond to this command.

Table 15 — Sleep all but - Response

None

6.5 Seal model and version

Following two commands are optional for compliance with this part of ISO 18185:

6.5.1 Product version

The Product Version indicates Seal firmware version.

Table 16 — Product version command format - read

Command code
'0C'

Table 17 — Product version command format - response

Command code	Firmware version
'0C'	1 byte

6.5.2 Model ID

The Model ID indicates Seal Model number.

Table 18 — Model ID command format - read

Command code
'0E'

Table 19 — Model ID command format - response

Command code	Model ID
'0E'	2 bytes

6.5.3 Read seal product parameter

6.5.3.1 Description

“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 in Table 22.

Command Code: **0x3C**

6.5.3.2 Arguments

Table 20 — 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 22

6.5.3.3 Response

The Seal response is according to the Seal Parameter Code argument, as in Table 22. If the Seal does not recognize the Parameter Code (e.g. 0x0F) it returns no data, and the “Nack” 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 following format:

Table 21 — Data field format for read seal product parameters response

Parameter Code	Parameter
1 byte	N as specified in Table 22
Seal Parameter Code according to Table 22	The content of the parameters

Table 22 — 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 byte	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.
Protocol Version	0x05	2 bytes	The version of the standard protocol (this document) that the Seal adheres to. The high byte is the major version number and the low byte is the minor version. For this version of the standard this parameter must 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=16-32 seconds)
Point-to-Point Mode Timeout	0x08	1 byte	Number of seconds for Seal timeout in Point-to-Point mode (valid value=2-32 seconds)
(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).

6.5.4 Collect seal IDs with event record

6.5.4.1 Description

Performs a collection round and receives one Event Record from each Seal.

Command Code: 0x14

6.5.4.2 Arguments

The Window size parameter represents number of time slots.

Table 23 — 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.

6.5.4.3 Response

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

6.5.5 Stand by

6.5.5.1 Description

The “Stand By” command shall be used to tell a Seal not to respond to in the next collection round.

Command **Code**: 0x1C.

6.5.5.2 Arguments

This command has no arguments.

6.5.5.3 Response

The Seal shall not respond to this command.

Table 24 — Stands by - command

Command code
0x10

Table 25 — Stands by - response

None

Stand By operation is used to put specific Seal s in ‘Stand By’ 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 Interrogator that initially set the Seal in the Stand By mode.

If the Seal does not receive Point to point command it will automatically resume ‘Sleep’ state 30 sec. after it has been woken up. Or after the Max Command Duration field of the last frame has been passed.

6.5.6 Seal status

6.5.6.1 Description

Table 26 — Seal status - read

Command code
0x19

Table 27 — 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

6.5.7 Read event record

6.5.7.1 Event Log Codes Description

Reads one or more Event Records from a Seal.

Command Code: 0x1A

6.5.7.2 Arguments

Table 28 — 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.

6.5.7.3 Response

The Seal response is a concatenation of the requested Event Records, starting from the newest to the oldest. The Event Records have fixed length and their format is according to Table 32.

Table 29 — Event log data - read

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

Table 30 — Event log data - 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 fixed length and has the following parameters:

Table 31 — Event record parameters 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	No. Of seconds since midnight January 1 st , 1990 UTC.
Event Category	1 byte	Defines the category of Event
Event Code	1 byte	See Event Code table
Seal set key	8 bytes	Event Data (specific to each Event Code).

6.5.7.4 Event Categories

Table 32 — Event categories

Event Category Name	Event Category Code	Description
Seal Events	0x0002	Events as defined in Table 33
Reserved for future use	0x1, 0x3-0xF	Reserved

6.5.7.5 Seal Events

Table 33 — Event codes for seal events

Event name	Event Code	Event Data	Event Data Length	Description
(Reserved)	0x00			
Sealed	0x01	Time Stamp	8 bytes Seal Set Key	Written when a sealing operation has been completed successfully.
				Unique integer number generated by the Seal during the Sealing process.
Seal open	0x03	Time Stamp	8 bytes Seal Set Key	Written when an open operation has been completed successfully.
Battery low flag raised	0x14	Time Stamp	8 bytes Seal Set Key	Written when the battery low flag is raised
(Reserved for future use)	0x04- 0x13, 0x15--0x7F		N	
(Reserved for manufacturer use)	0x80 – 0xFF		N	

Where Event Data is defined as follows:

Table 34 — Event data for seal events

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

6.5.8 Date and time

Command Code: 0x1B (Read)

Date and Time counter is a 32-bit integer that increments every second. This is programmed to number of seconds elapsed since midnight January 1st, 1990, UTC. This is initialized at time of manufacture and unchangeable thereafter. Accuracy of time is within +/-5 seconds per day.

The Seal response is per Table 4.

Table 35 — Get Date and Time - read

Command code
0x1B

Table 36 — Get Date and Time - response

Command code	Date and Time counter
0x1B	4 bytes

Bibliography

[1] The following standards contain provisions, which may assist in the understanding of this International Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on International Standards are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of ISO maintain registers of current valid International Standards.

[2] [1] ISO 1496-1, *Series 1 freight containers - Specification and testing - Part 1: General cargo containers for general purposes*

[3] [2] ISO 1496-2, *Series 1 freight containers - Specification and testing - Part 2: Thermal containers*

[4] [3] ISO 1496-3, *Series 1 freight containers - Specification and testing - Part 3: Tank containers for liquids, gases and pressurized dry bulk*

[5] [4] ISO 1496-4, *Series 1 freight containers ó Specification and testing - Part 4: Non-pressurized containers for dry bulk*

[6] [5] ISO 1496-5, *Series 1 freight containers ó Specification and testing - Part 5: Platform and platform-based containers*

[7] [6] ISO 10374, *Freight containers - Automatic Identification*

[8] [7] ETSI EN 300 220, *Radio equipment and systems; short range devices; 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*

[9] [8] BS 7480, *Specifications for security Seals*

[10][9] ANSI INCITS 256 Part 4.2, *Radio Frequency Identification (RFID) - UHF RFID Protocols*

[11][10] USA, 47 CFR, Part 15, *Code of Federal Regulations, Federal Communications Commission, 47 CFR, Part 15 - Radio frequency devices*

[12][11] ISO 17363, *Supply chain application for RFID -- Freight containers*