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)

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.

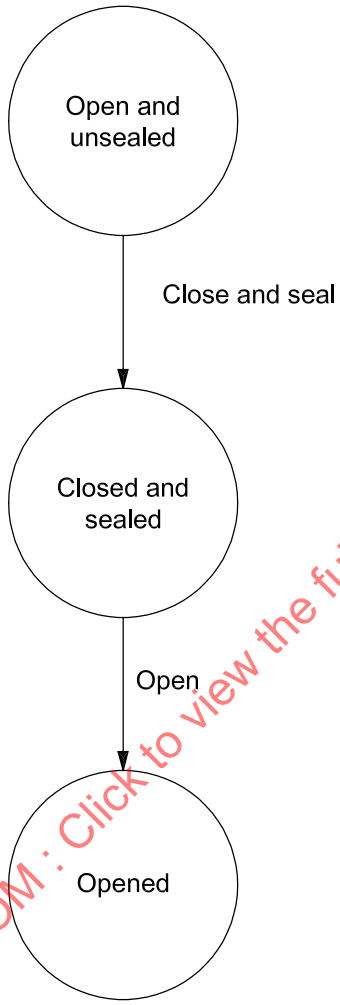

Figure 1 — Seal states

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.