Date: 2006-10-31

ISO/FDIS 18185-1

ISO/TC 104/SC 4

TC 104 Secretariat: ANSI

TC 104/SC 4 Secretariat: DIN

Freight containers – Electronic seals – Part 1: Communication protocol

Récipients de fret - Joints électroniques - Partie 1: Protocole de transmission

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: if applicable
Document stage: (50) Approval
Document language: E

H:\Abteilungs Archiv\Geschichtsakte FAKRA-Normen\Normen_15001-20000\18185\Part 1\FDIS\FDIS_18185-1_2006_10_31.doc Basic template BASICEN3 2002-06-01

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.

International Standard ISO 18185, which is a standard in multiple parts, was prepared by Technical Committee 104, Freight Containers, Subcommittee SC4, Identification and communication, Working Group WG2, Automatic Identification Equipment (AEI) for containers and container related equipment.

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

— *Part 1: Communication protocol*

— *Part 2: Application requirements*

— *Part 3: Environmental characteristics*

— *Part 4: Data protection*

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

— *Part 7: Physical layer*

Introduction

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 International Standard 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, 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 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;
- Seal (tag) type.

This International Standard shall be used in conjunction with the other Parts of ISO 18185.

This International Standard applies to all electronic seals used on:

Freight containers covered by International Standards ISO 668, parts 1 to 5 of ISO 1496, 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 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 17712, *Freight containers – Mechanical seals*

ISO/IEC 18000–7, *Information Technology, Automatic Identification and Data Capture Techniques – Radio Frequency Identification (RFID) for Item Management – Air Interface Part 7: Parameters for an Active RFID Air Interface Communications at 433 MHz*

ISO/IEC 24730, *Information technology - Automatic Identification and Data Capture Techniques - 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, Parts 1 and 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 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; the combination of which shall be 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
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 signaling.

3.6
Long Range Link (LRL)
radio frequency link using 433.92MHz or 2.4GHz signaling.

3.7
localization
capability in any operational scenario to associate an e-seal to the container on to 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 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 (that combined 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 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)

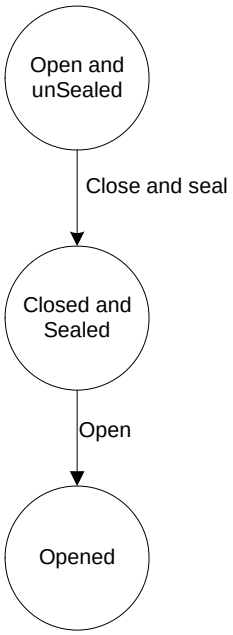

Figure 1 – Seal states

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. 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 real-time clock based on UTC time.

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

5.7 The Protocol ID occupies 8-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 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)

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

6 Data Link layer protocol for electronic seal

There are two types of physical layers as specified in ISO 18185 Part 7. Type A physical layer is the 433MHz as long range Link and ook LF short range link. Type B physical layer is the 2.4GHz 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 E-seal shall be capable of communicating on both operational mode type A and type B. The protocol for these type A long range links at 433MHz is specified in sections 6.1. The protocol for the type A short range links using OOK is specified in sections 6.2. The protocol for these type B long range links at 2.4GHz is specified in sections 6.3. The protocol for the type B short range links using FSK is specified in sections 6.4. Data may be transmitted from the LF transmitter to the E-seal(s) without acknowledgment (one-way link only).

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

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

6.1.1 Packet fields format and definition

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.

Argument Length

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

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.

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 30000 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 doesn't have to send more commands to the seal.

Packet Options

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 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		

6.1.2 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 Clause 6.1.1. 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 Clause 6.1.3. The Mode field is defined in Clause 6.1.3.

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

Table 2 – Interrogator to seal Command Format (Point to Point)

Protocol ID	Packet Options	Tag Manufacture ID	Tag ID	Interrogator ID	Command Code	Min Command Duration*	Max Command Duration*	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

* 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 Manufacture ID	Tag ID	Command Code	Data*	CRC
0x80	2 bytes	1 byte	2 bytes	2 bytes	4 bytes	1 byte	N bytes	2 bytes

* 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 Manufacture ID	Tag ID	Data*	CRC
0x80	2 bytes	1 byte	2 bytes	2 bytes	4 bytes	0 – N bytes	2 bytes

* 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 Manufacture ID	Tag ID	Event Code	Event Date & Time	Event Data*	CRC
0x80	2 bytes	1 byte	2 bytes	4 bytes	1 Byte	4 Bytes	0 – N Bytes	2 bytes

* 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 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 = NAK 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 whether the seal is a high security seal as defined in ISO 17712 and the generation of electronics within. See Table below.

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

Table 9 – Seal type field

Seal type field	Seal type code (Bit 5-3)
Extensibility	111
High Security – 1st Generation Electronics	101
Reserved	000, 001, 010, 011, 100, 110

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.

6.1.5 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 standard that the collection algorithms shall be identical for 18185-1, 18185-7, and 18000-7. The definitive document shall be the current version of 18000-7.

6.1.6 Command codes and Parameters

Summary of all Command codes defined by this protocol is in the following table:

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	Read the current time from the real-time clock. (Number of seconds elapsed since Jan 1st, 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

0x32/B2	Turn on/off beacon for transmitter type	Point to Point	Turn on/off the beacon at 433MHz, 2.4GHz
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.

6.1.7 Command and Response Format

6.1.7.1 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 11 – Collection command forma

Command Code	Command Arguments	
'10'	Windows 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 ms and defined in the collection algorithm in Part 7.
Collection Criteria	1 Byte	The criteria for the seals 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 – NNNX0000b

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.

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

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 awaken again by Wake Up signal.

Arguments:

This command has no arguments.

Seal Response:

The seal shall not respond to this command.

Table 14 – Sleeps

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.

6.1.7.3 Sleep All But

Table 15 – Sleep All But

Command code	Command Arguments	
'16'	Tag Manufacture ID	Tag ID
	2 Bytes	4 Bytes

Description:

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

Seal Response

Seal shall not respond to this command.

Response

Table 16 – Sleep All But

None

6.1.7.4 Seal model and version

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’

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

Read

Table 19 – Model ID command format

Command code
‘0E’

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

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 23

Command Code: 0x3C

Arguments:

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 Seal Product Parameters

Response:

The seal response is according to the seal Parameter Code argument, as in Table 23 Seal Product Parameters. 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 following format:

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 Seal Product Parameters	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 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 Bytes	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).

6.1.7.8 Collect seal IDs with Event Record

Description:

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

Command Code: 0x14

Arguments:

The Window size parameter represents 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 byte	The offset of the Event Record that is being requested.

Response:

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

6.1.7.9 Standby

Description:

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

Command Code: 0x1C

Arguments:

This command has no arguments.

Response:

The seal shall not respond to this command.

Table 25 – Stands By - Command

Command code
0x10

Table 26 – Stands By - 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 interrogator that initially set the seal in the Standby 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.

6.1.7.10 Get Seal Status

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

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

Event Log Codes Description:

Reads one or more Event Records from a seal.

Command Code: 0x1A

Arguments:

Table 29 – Read Event Records arguments

Argument Name	Size	Description
Starting Event Offset (N)	2 byte	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.

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 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 fixed length and has the following parameters:

Table 32 – 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 1st, 1990 UTC.
Event Category	1 byte	Defines the category of Event
Event Code	1 byte	See Event Code table
Event Data	8bytes	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
SRLwake 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 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 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

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 type of the transmission: 433MHz and/or 2.4GHz. The least significant bit 0 when set (i.e, bit 0 value is 1) selects 433MHz alert transmission type while setting the bit1 (i.e, bit 1 value is 1) will select 2.4GHz alert

transmission type. The Transmission Period parameters defines transmission period in seconds for the selected Transmission Type: 433MHz or 2.4GHz. Alternatively application can choose to set the same period for both types by setting both bits '0' and '1' of Transmission Type parameter. The transmission period must be no less than10 seconds. 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 LRL (Long Range Link) and a LF (Low Frequency) channel to be called SRL (Short Range Link).

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

- The SRL transmitter will broadcast a "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 Wake-Up on LF or a Collect on UHF
- The eSeal will receive the LF transmitter ID and will send the a message with LF transmitter ID, eSeal ID, and eSeal status via UHF communication link.
    - The eSeal will use 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 till it receives a "sleep" command from LRL reader or send a maximum 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 will 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 byte oriented, packet based message structure utilizing 16-bit CRC error detection mechanism for reliable communication. The protocol utilizes 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 will 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 transmiss ter ID	CRC
0x96	0x80	0x00	2 bytes	2 bytes

6.2.3.1 SRL transmitter Packet option field

Sync Frame

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

Protocol ID

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 standard is 0x80.

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

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

SRL transmitter ID

unique ID index of the SRL transmitter within the sight.

6.3 2.4 GHz long range link 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 e-seal 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 blink at a 5 second blink rate with 8 sub-blinks for 20 seconds after leaving the SRL field.. The 2.4 GHz e-seal protocol shall be in accordance with the specifications as set forth in draft ISO/IEC 24730-2. The protocol specified within this document are in addition to the parameters specified in 24730-2 and are intended as an application layer that shall specify the parameters specific to e-seal function. The term "exciter" used in ISO/IEC 24730-2, and "LF transmitter" used in this document refer to the same physical device.

Specified within this sub-section 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 the draft ISO/IEC 24730-2 DSSS RTLS standard and have access to the same data.

6.3.1 Data Link layer packet structure

The following clauses 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, and their format is shown in tables 38-41.

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 a 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 standard 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 January 1, 1990 that the seal was closed.

6.3.1.1.7 Open time

The seal time is a 32-bit value representing the number of seconds since midnight January 1, 1990 that 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 January 1, 1990 to the present time.

6.3.1.1.9 Battery time

The seal time is a 32-bit value representing the number of seconds since midnight January 1, 1990 that 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 model ID 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 the the seal adheres to. The high byte is the major version and the low byte is the minor version. For this version of the standard, the parameter must 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 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

6.4.1.1 FSK Packet fields format and definition for 2.4GHz Systems

The follow describes the packet fields format of the frequency shift keyed (FSK) low frequency (LF) protocol, as described in ISO-24730, 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 1496-1, *Series 1 freight containers - Specification and testing - Part 1: General cargo containers for general purposes*

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

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

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

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

[7] ISO 10374, *Freight containers – Radio-frequency automatic identification*

[8] ISO/IEC 15963, *Automatic identification – Radio frequency identification for item management – Unique identification for RF tag*

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

[10] ISO TRxxxxx, *Freight containers – Concept of operations for RF and freight containers*

[11] 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*

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

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

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