

IEEE Standard for Message Sets for Vehicle/Roadside Communications

Sponsor

**Rail Transit Vehicle Interface Standards Committee
of the
IEEE Vehicular Technology Society**

Reaffirmed 7 June 2006

Approved 26 June 1999

IEEE-SA Standards Board

Abstract: Those characteristics of a dedicated short-range communications (DSRC) system that are independent of the Physical and Data Link Layers (ISO model Layers 1 and 2) are specified. The required and optional features of the roadside equipment (RSE) and the onboard equipment (OBE) are specified. In addition, the Applications Layer (ISO model Layer 7) services and protocols, the RSE resource manager, the corresponding OBE command interpreter, and the application-specific messages are all specified. Standard supports and guidelines are provided for implementing secure DSRC systems.

Keywords: access control, application layer, automatic vehicle identification, AVI, beacon, Commercial Vehicle Operations, CVO, data authentication, data privacy, data security, dedicated short-range communications, DSRC, electronic toll collection, ETC, Layer 7, Mailbox, reader, resource manager, smart card, tag, transponder, vehicle to roadside communications, VRC

The Institute of Electrical and Electronics Engineers, Inc.
345 East 47th Street, New York, NY 10017-2394, USA

Copyright © 1999 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 20 September 1999. Printed in the United States of America.

Print: ISBN 0-7381-1769-2 SH94768
PDF: ISBN 0-7381-1770-6 SS94768

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. Members of the committees serve voluntarily and without compensation. They are not necessarily members of the Institute. The standards developed within IEEE represent a consensus of the broad expertise on the subject within the Institute as well as those activities outside of IEEE that have expressed an interest in participating in the development of the standard.

Use of an IEEE Standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of all concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration.

Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; (978) 750-8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Introduction

(This introduction is not part of IEEE Std 1455-1999, IEEE Standard for Message Sets for Vehicle/Roadside Communications.)

The electronic toll and traffic management (ETTM) field is rapidly evolving, and ETTM systems across North America use a variety of incompatible dedicated short-range communications (DSRC) products. Several mainline screening systems for commercial vehicle operations (CVOs) are now in operation and likewise use incompatible data definitions. In addition, the acceptance of the ASTM Standard for DSRC Layers 1 and 2 will create the potential for significant interference between radio frequency (RF) compatible systems.

The lack of standard message sets, lower layer protocols, and transponder resource definition threatens to postpone the deployment of DSRC systems, a technology critical to the intelligent transportation systems (ITS) marketplace. This standard consolidates and builds upon previous application-specific data definitions to support CVO, ETTM, and private DSRC usage. The open nature of this standard ensures that it is extensible to other DSRC areas, such as CVO credential information exchange, preclearance screening, fleet management, and vehicle condition monitoring.

While this standard has been developed to ensure efficient operation when used in conjunction with the ASTM Layer 1 and Layer 2 standards, it is not limited to that application. This standard may be use in conjunction with a variety of lower layer protocols, including both RF and other communications media.

At the time this standard was developed, the Working Group on Dedicated Short-Range Communications Applications for Intelligent Transportation Systems had the following membership:

Peter B. Houser, *Chair*

Frederico Alvarez
Lee Armstrong
Charles Gary Belda
Hamed Benouar
Broady Cash
Alex Castro
Amos Chenoweth
Stan Ciszewski
Clayton Collier
Ken Cook
Roy Courtney

Joe Crabtree
Ronald F. Cunningham
Ron DeLeon
Neil Gray
Ed Grose
Martha Harrell
George Herndon
Chuck Johnson
David Martin
Russell McCarty
Irwin Morse

David Newman
Roger J. O'Conner
Mike Onder
Satoshi Oyama
Tom Rieflin
Lewis Sabounghi
Ove Salomousson
Richard Schnacke
Bo Strickland
Robert Tiernay
Ray Yuan

The following members of the balloting committee voted on this standard:

Robert Barrett
James Bartol
Charles Gary Belda
Hamed Benouar
Amos Chenoweth

Clayton Collier
Roy Courtney
Joe Crabtree
Ronald F. Cunningham
Richard W. Doering
Peter B. Houser

Russell McCarty
Roger J. O'Connor
Lewis Sabounghi
Richard Schnacke
Ray Yuan

When the IEEE-SA Standards Board approved this standard on 26 June 1999, it had the following membership:

Richard J. Holleman, *Chair*

Donald N. Heirman, *Vice Chair*

Judith Gorman, *Secretary*

Satish K. Aggarwal
Dennis Bodson
Mark D. Bowman
James T. Carlo
Gary R. Engmann
Harold E. Epstein
Jay Forster*
Ruben D. Garzon

James H. Gurney
Lowell G. Johnson
Robert J. Kennelly
E. G. "Al" Kiener
Joseph L. Koepfinger*
L. Bruce McClung
Daleep C. Mohla
Robert F. Munzner

Louis-François Pau
Ronald C. Petersen
Gerald H. Peterson
John B. Posey
Gary S. Robinson
Akio Tojo
Hans E. Weinrich
Donald W. Zipse

*Member Emeritus

Also included is the following nonvoting IEEE-SA Standards Board liaison:

Robert E. Hebner

Contents

1.	Overview.....	1
1.1	Scope.....	1
1.2	Purpose.....	1
1.3	Standards maintenance.....	2
1.4	Interoperability and noninterference.....	3
1.5	Precedence of data representation.....	3
2.	References.....	3
3.	Definitions, abbreviations, and acronyms.....	4
3.1	Definitions.....	5
3.2	Abbreviations and acronyms.....	7
4.	Architecture and communications flow summary	8
4.1	DSRC context and processing flow	8
4.2	Access control flow summary.....	10
5.	Transponder resources	11
5.1	Transponder resources definition.....	11
5.2	Read-only memory definition	15
5.3	Interoperability requirements.....	20
6.	Transponder commands and memory access.....	21
6.1	Basic concepts.....	21
6.2	Command set template.....	21
6.3	Command information flow.....	24
6.4	Command definitions.....	25
6.5	Standard command responses	40
6.6	Interoperability requirements.....	43
6.7	Error detection and processing.....	44
7.	Resource manager.....	45
7.1	Resource manager processing summary	46
7.2	BOA interface	46
7.3	Beacon interface (nonmandatory).....	48
7.4	Memory page management.....	49
7.5	UI management.....	50
8.	ITS application messages.....	51
8.1	Message concepts.....	51
8.2	Message headers	51
8.3	Message data elements.....	57
8.4	Electronic Toll Collection (ETC) message set.....	57
8.5	Commercial Vehicle Operations (CVO) Border Clearance message set.....	62

8.6	CVO Electronic Screening message set.....	70
8.7	Common utility message set	77
8.8	Private message set	83
8.9	Message error detection and processing	83
9.	Application layer.....	84
9.1	Scope.....	84
9.2	DSRC application domain assumptions.....	85
9.3	Architecture.....	86
9.4	T-KE	91
9.5	I-KE.....	97
9.6	B-KE	105
9.7	Session suspend and resume	107
Annex A	(normative)ASN.1 definitions.....	109
Annex B	(normative) ASN.1 considerations.....	119
Annex C	(normative) Communications data flows.....	121
Annex D	(normative) ASN.1 PER encoding for a sample BST and VST	125
Annex E	(normative) Transponder identifier values.....	128

IEEE Standard for Message Sets for Vehicle/Roadside Communications

1. Overview

1.1 Scope

This standard is applicable to dedicated short-range communications (DSRC). Within the overall context of DSRC operations (illustrated in Figure 1), this standard governs the communications protocols above the open systems interconnection (OSI) data link layer for the DSRC wireless interface. This standard does not specify the interface between the transponder and other pieces of onboard equipment (OBE) (identified as “5” in Figure 1), nor does it specify the interface between the roadside equipment (RSE) and the back office equipment (BOE) that hosts an intelligent transportation systems (ITS) back office application (BOA) (identified as “1” in Figure 1). However, to obtain desirable levels of DSRC performance, it is essential that those interfaces be defined in a manner that is consistent with this standard.

Interface 2 in many systems may be the interface between the application layer and lower layer service. Nothing precludes combining a vehicle-to-roadside communication (VRC) controller, a reader, and an antenna into a single piece of equipment.

These communications protocols have been specified by defining the message set and data dictionary, the low-level commands used to control transponder resources and thereby access such messages, and the OSI application layer services used to connect the upper interface elements with the OSI data link layer elements. This standard also specifies the resources that may be present on a transponder and the means by which the RSE shall control those resources.

Product compliance with this standard shall be verified based upon tests of Interfaces 1 and 4 shown in Figure 1. Internal interfaces such as 2 are at the discretion of the equipment vendor and shall not be considered when determining product compliance.

1.2 Purpose

This standard is intended to be used in several ways by various DSRC equipment stakeholders:

- The standard specifies the internal resources that shall be provided within and commands that shall be recognized by compliant transponders. This information will be used by transponder manufacturers when developing compliant transponders. This information will also be used by RSE manufacturers when developing equipment that communicates with such transponders.

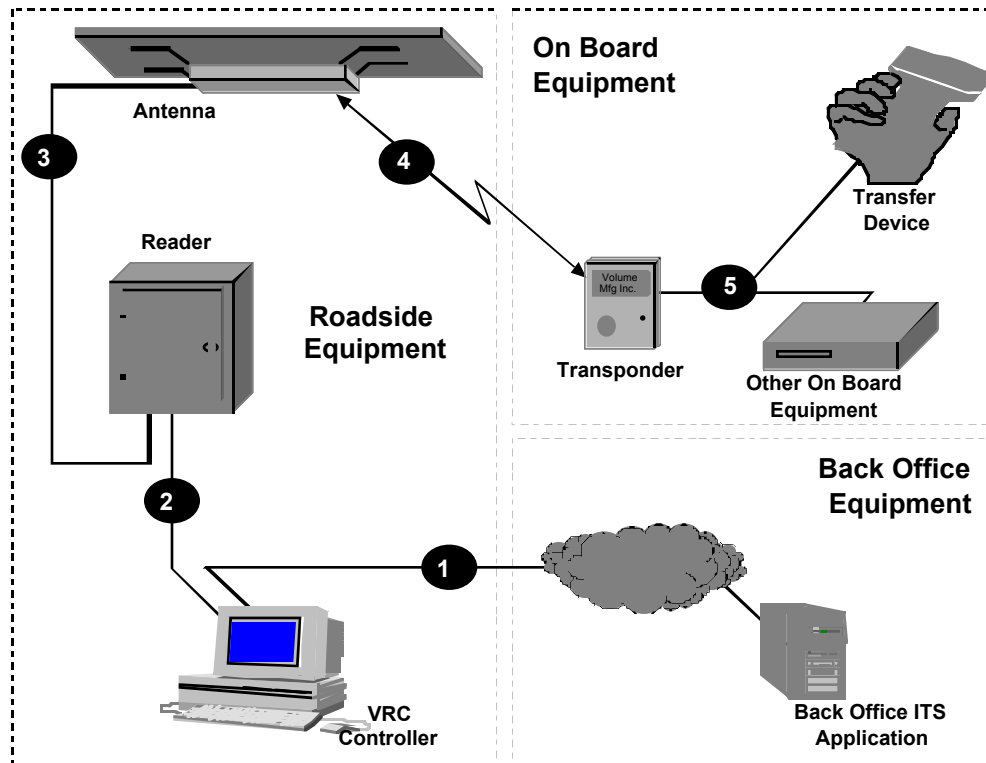


Figure 1 – DSRC system interfaces

- This standard specifies the Layer 7 protocols that shall be used to complete the communications stack between the data link layer and higher level processing. This information will be used by transponder and beacon manufacturers when developing compliant equipment.
- This standard specifies the manner in which roadside DSRC equipment shall manage transponder resources. This information will be used by manufacturers of such RSE when developing software that utilizes transponder resources.
- This standard specifies the messages that shall be used to communicate information between ITS applications using DSRC. This information will be used by ITS application developers when they design and implement systems that use DSRC.
- This standard specifies the manner in which new systems achieve backward compatibility or noninterference with existing systems.

This standard specifies an overall structure for DSRC. System components may be selected within the compliant range allowed within this standard. For example, the user agencies may select specific messages from Clause 8. To achieve interoperability between agencies, it is essential that the user agencies enter into institutional agreements that coordinate their designs.

1.3 Standards maintenance

This standard provides three categories of data elements that have values with specific meanings within the context of the standard.

- *Available for uncontrolled use.* Values assigned to data elements in this category are not controlled by this standard and may be defined by the vendor or user.

- *Available for registration.* Values assigned to data elements in this category have been preallocated within this standard for future assignment to a specific agency or vendor.

Currently, ranges of available values are listed in this standard for specific uses. An agency or vendor must submit a request to the IEEE to have a specific value, from a listed range of available values, designated as uniquely registered to that agency or vendor.

- *Reserved.* Values assigned to data elements in this category have been predefined within this standard to have specific meanings. These predefined values shall not be assigned to those data elements as having any other meaning.

A maintenance process associated with this standard will be required to control data element registration and coordinate clarifications, corrections, or modifications to this standard. This maintenance process will be defined by the IEEE.

1.4 Interoperability and noninterference

Four possible relationships between equipment and this standard exist:

- *Compliant equipment.* Transponders and RSE that meet all requirements of this standard are defined as compliant. Such equipment may omit some or all of the optional features defined in this standard.
- *Interoperable transponder.* Transponders that meet all requirements of this standard and provide the set of optional features identified in 5.3 and commands identified in 6.6 are defined as interoperable. This class of equipment is intended to specify transponders that may be used by multiple BOAs.
- *Interoperable RSE.* RSE that meets all requirements of this standard and includes a resource manager that services multiple BOAs is defined as interoperable.
- *Noninterfering equipment.* Transponders and RSE that substantially meet all requirements of this standard, but omit required capabilities in a manner that is transparent to compliant equipment, are defined to be noninterfering. For example, a noninterfering transponder may utilize a page of memory in a manner that does not comply with the Clause 8 message definitions as long as that memory page is protected against access by other compliant RSE. This class of equipment is intended to facilitate backward compatibility during system migration towards this standard.

1.5 Precedence of data representation

This standard contains cases where a specified data element includes both an Abstract Syntax Notation One (ASN.1) representation and a binary representation of that data element. If any conflict arises between the ASN.1 and binary representation of a given data element, the binary representation shall be considered normative and shall take precedence over the ASN.1 definition.

2. References

The following documents shall be used, when applicable, in the process of developing equipment and systems that will be compliant with the DSRC standard. When the following documents are superseded by an approved revision, then that revision shall apply.

ANSI X3.38-1988 (R1994), Codes—Identification of States, the District of Columbia, and the Outlying and Associated Areas of the United States for Information Interchange.¹

¹ANSI publications are available from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA (<http://www.ansi.org/>).

ASTM Draft Standard, Dedicated Short-Range Communication (DSRC) Data Link Layer, E xxx-99, Version 5.0.²

CEN Draft Document: prENV278/9/#65 Dedicated Short Range Communication (DSRC)—Application Layer (Layer 7).³

IEEE Std 1489-1999, IEEE Standard for Data Dictionaries for Intelligent Transportation Systems—Part 1: Functional Area Data Dictionaries.⁴

GSS Global Specification For Short Range Communication. The platform for Interoperable Electronic Toll Collection and Access Control.⁵

ISO 3166-1:1997, Codes for the representation of names of countries and their subdivisions—Part 1: Country codes.⁶

ISO 3779:1983, Road vehicles—Vehicle identification numbering (VIN)—Content and structure.

ISO/IEC 7498-1:1994 Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model

ISO 7498-2:1989 Information processing systems—Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture

ISO/IEC 7498-3:1997 Information technology—Open Systems Interconnection—Basic Reference Model: Naming and addressing

ISO/IEC 7498-4:1989 Information processing systems—Open Systems Interconnection—Basic Reference Model—Part 4: Management framework

ISO 3780:1983, Road vehicles—World manufacturer identifier (WMI) code.

ISO/IEC 8824-1:1995, Information technology—Abstract Syntax Notation One (ASN.1): Specification of basic notation.

ISO/IEC 8825-2:1996, Information technology—ASN.1 encoding rules: Specification of Packed Encoding Rules (PER).

ISO TC204 WG15 Committee Of Japan TICS/DSRC—DSRC Application Layer High Data Rate.

3. Definitions, abbreviations, and acronyms

For the purposes of this standard, the following terms, definitions, abbreviations, and acronyms apply. For terms not defined in this clause, English words are used in accordance with their definitions in the latest

²ASTM publications are available from the American Society for Testing and Materials, 100 Barr Harbor Drive, West Conshohocken, PA 19428-2959, USA (<http://www.astm.org/>).

³CEN publications are available from Nederlands Normalisatie-Instituut (NNI), Attn: Mr. J. A. Dijkstra, Kalfjeslaan 2, P.O. Box 5059, 2600 GB Delft, The Netherlands; telephone +31 15 2 690127; telefax. +31 15 2 690 242; jelte.dijkstra@nni.nl.

⁴IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA (<http://www.standards.ieee.org/>).

⁵GSS publications are available from Global Specification for Short-Range Communication.

⁶ISO publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembe, CH-1211, Genève 20, Switzerland/Suisse (<http://www.iso.ch/>). ISO publications are also available in the United States from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA (<http://www.ansi.org/>).

editions of *Webster's New Collegiate Dictionary*. Electrical and electronic terms not defined in this clause or in *Webster's New Collegiate Dictionary* are used in accordance with their definitions in IEEE Std 100-1996.

3.1 Definitions

3.1.1 access credentials: Data that are transferred to establish the claimed identity of a roadside equipment (RSE) application.

3.1.2 antenna: A device used to send or receive radio waves.

3.1.3 application identifier (AID): An identifier that defines the category of dedicated short-range communications (DSRC) applications to which a specific application belongs. The only category currently defined by this standard is Mailbox.

3.1.4 back office application (BOA): Intelligent transportation system (ITS) or other application that resides and executes on the back office equipment (BOE). BOAs exchange messages with the onboard equipment (OBE) via the resource manager.

3.1.5 back office equipment (BOE): Computer equipment that hosts the applications and data required for some intelligent transportation system (ITS) function. Data is exchanged with the OBE via the vehicle-to-roadside communications (VRC) controller.

3.1.6 beacon: A roadside system at which dedicated short-range communications (DSRC) can be accomplished. A beacon typically consists of a reader and an antenna.

3.1.7 beacon service table (BST): A data structure created and transmitted by a beacon. It contains data such as the application identifier (AID) relevant for initiating communication with an onboard equipment (OBE) transponder. The reception of the BST by an OBE transponder results in a vehicle service table (VST) being sent back to the beacon.

3.1.8 broadcast mode: Beacon-initiated transmissions that are intended for all onboard equipment (OBE) in the communications zone.

3.1.9 command: A package of information transmitted from the roadside to the vehicle that requests that the transponder on the vehicle perform a specific action.

3.1.10 communications zone: The area of space within which a beacon can communicate with transponders in or on passing vehicles.

3.1.11 credentials: Information supplied to authenticate a communication.

3.1.12 digital signature: Information supplied with a transmission that allows the receiver to verify that the transmission has not been modified after initial generation.

3.1.13 element identifier (EID): A numeric identifier generated by the application on the onboard equipment (OBE) transponder. An EID is unambiguous within the context of a complete exchange of messages with an application on the roadside equipment (RSE). Multiple EIDs can be maintained between the RSE and OBE over a single data link session (LID).

3.1.14 invoker identifier (IID): The specific element identifier (EID) of a responding transponder.

3.1.15 kernel element (KE): An abstraction of data processing and data communication resources. An application KE represents a logical component of application layer functionality.

3.1.16 link identifier (LID): A string identifier generated by the lower layer service on the onboard equipment (OBE) transponder each time the transponder initiates a new session with a lower layer service on the roadside equipment (RSE).

3.1.17 lower layer service: A generic service required by this standard that provides the minimum subset of the functionality defined by Layers 4 through 1 of the open systems interconnection (OSI) model.

3.1.18 mailbox: The mechanism for storing and retrieving intelligent transportation systems (ITS) messages between the back office equipment (BOE) and onboard equipment (OBE). The specific processing mechanisms are defined by the resource manager.

3.1.19 memory image: A series of bits that can be stored within a contiguous portion of transponder memory and that may be passed as a parameter within commands initiated by the roadside equipment (RSE).

3.1.20 memory page: A segment of transponder memory that is assigned a unique location by which it may be referenced.

3.1.21 message: A package of information meeting a standard format that is sent to or from a transponder's memory.

3.1.22 nonce: A random or pseudo-random value used within an authentication system.

3.1.23 onboard equipment (OBE): Equipment located within a vehicle that supports the information exchange with roadside equipment (RSE).

3.1.24 private page: A memory page that has been reserved for the exclusive use of a particular agency or function. Access credentials may be required to reference the page.

3.1.25 profile: A unique numeric identifier that indicates a set of communications parameter values to be used in establishing a physical session.

3.1.26 public page: A memory page that may be used by any agency or application. No access credentials are associated with such a page.

3.1.27 reader: A component of a roadside beacon that provides the capabilities for radio wave communications with a transponder.

3.1.28 roadside equipment (RSE): Equipment located at a fixed position along the road transport network, providing communication and data exchange with the onboard equipment (OBE).

3.1.29 service data unit (SDU): The data associated with a service primitive.

3.1.30 service primitive: A function in the external interface of a kernel element (KE) that may be invoked to access services provided by the KE.

3.1.31 session: A series of transactions exchanged between the roadside and the vehicle while the vehicle is within a beacon's communications zone.

3.1.32 transaction: A functionally continuous and complete exchange of information between the roadside equipment (RSE) and the vehicle transponder.

3.1.33 transponder: The onboard component of a dedicated short-range communications (DSRC) system. Transponder elements are defined in Clause 5.

3.1.34 vehicle service table (VST): The answer of the onboard equipment (OBE) application layer in response to a received beacon service table (BST). The VST contains the identifier of applications supported by the OBE and profiles used for further point-to-point communication.

3.2 Abbreviations and acronyms

AID	application identifier
ASDU	application service data unit
ASN.1	Abstract Syntax Notation One
ASTM Draft 7	ASTM Draft Standard Dedicated Short Range Communications (DSRC) Data Link Layer: Medium Access and Logical Link Control Exxx-97.
B-KE	broadcast kernel element
BCD	binary coded decimal
BLOB	binary large object
BOA	back office application
BOE	back office equipment
BSDU	broadcast service data unit
BST	beacon service table
CEN	Comité Européen de Normalisation
CMV	commercial motor vehicle
CV	commercial vehicle
CVO	commercial vehicle operations
DSRC	dedicated short-range communications
DUNS	Dun & Bradstreet number
EID	element identifier
ETC	electronic toll collection
ETTM	electronic toll and traffic management
FIFO	first in first out
GSS	Global Specification for Short Range Communication
Hex	hexadecimal
ICC	Interstate Commerce Commission
IID	invoker identifier
I-KE	initialization kernel element
ISDU	initialization service data unit
ITS	intelligent transportation systems
KE	kernel element
LED	light emitting diode
LID	link identifier
LLC	logical link control
OBE	onboard equipment
OSI	open systems interconnection
PDA	personal digital assistant
PDU	protocol data unit
PER	Packed Encoding Rules

RF	radio frequency
RSE	roadside equipment
SDU	service data unit
T-KE	transfer kernel element
TSDU	transfer service data unit
UI	user interface
VRC	vehicle-to-roadside communications
VST	vehicle service table

4. Architecture and communications flow summary

Figure 2 illustrates this standard's DSRC architecture and the relationship between this standard and related standards. Within this architecture this standard governs

- The configuration of transponder resources (primarily specified in Clause 5).
- The commands to which the transponder responds (primarily specified in Clause 6).
- The Layer 7 protocols used to connect the transponder resources (on the vehicle) and the resource manager (on the roadside) with the lower layer protocols that physically accomplish the information transfer (primarily specified in Clause 9).
- The resource manager that manages and controls transponder resources in response to information received from BOAs (primarily specified in Clause 7).
- The messages used by BOAs to exchange information using DSRC (primarily specified in Clause 8).

4.1 DSRC context and processing flow

In the context of the architecture shown in Figure 2, and using the typical DSRC equipment configuration shown in Figure 1, the DSRC processing flow is typically as follows [use of the beacon service table (BST) and vehicle service table (VST) are fully defined in Clause 9]:

- a) Compliant RSE and OBE, including beacons and transponders, are installed as appropriate. As illustrated in Figure 2, the complementary Layer 1, Layer 2, and Layer 7 processing in the RSE and OBE provides the basic structure for higher level information transfers.
- b) At the time of installation, information such as the identifier registered to that service agency, may be written into the transponder's memory. It is anticipated that this transfer will typically be done by a dedicated beacon at a central facility, using the transponder commands defined in Clause 6.
- c) Handheld data transfer devices or onboard computers may also store messages in areas of the transponder's memory. The interface for accomplishing this transfer is not controlled by this standard.
- d) In transponders that support the optional memory-partitioning feature, memory may be partitioned by the vendor or the user agency. Subsequent memory page reservations may reference a defined partition.
- e) In transponders that support access control, a memory page may be reserved by an agency. Such pages are referred to as "private pages," and all other pages are referred to as "public pages." This reservation may require that the requesting agency provide access controls and will result in a region of memory being permanently allocated for use exclusively by the agency. Access controls may be used to enforce this exclusivity. It is anticipated that this reservation will typically be done by a dedicated beacon at a central facility, using the transponder commands defined in Clause 6.

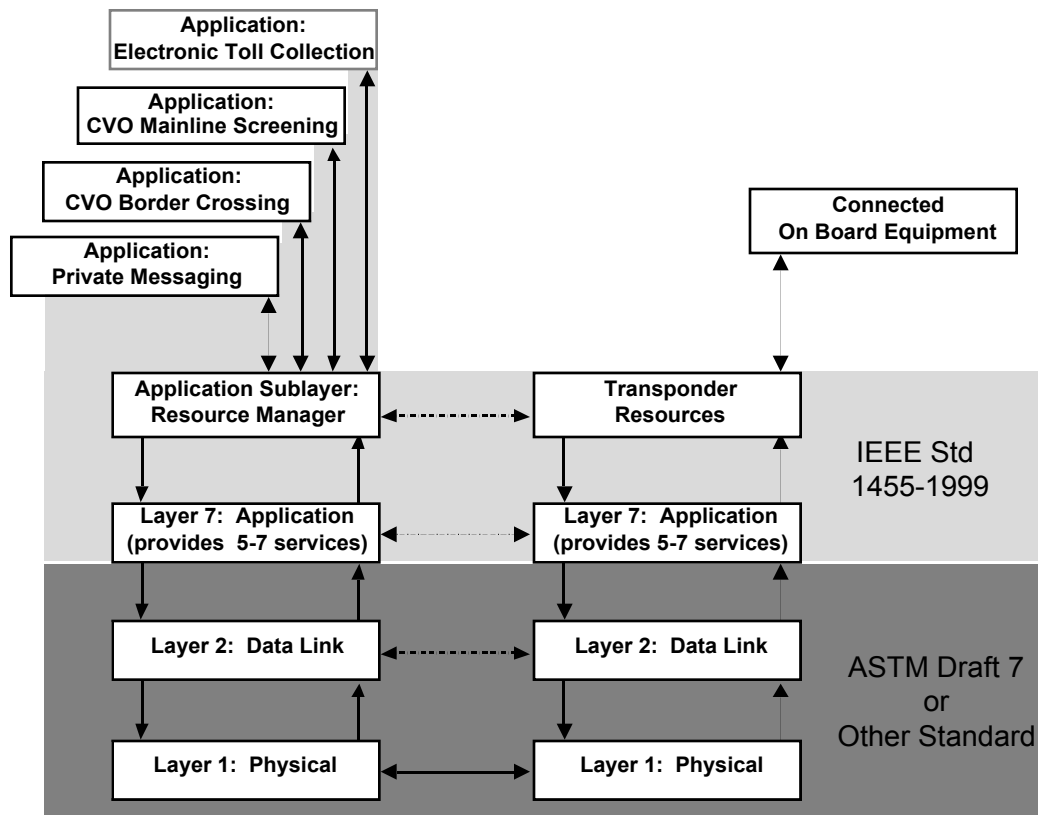


Figure 2—DSRC architecture and related standards

- f) It is expected that the VRC controller will host the resource manager process. The BOAs that are connected with the VRC controller will register their data requirements with the resource manager. This registration may specify virtual page identifiers that shall be used to filter undesired transponders. The registration may also specify the information, including specific messages, that is desired from each relevant transponder that passes through the beacon's capture zone. However, this interface is not controlled by this standard.
- g) As the transponder passes within the communication zone of the beacon, the beacon will transmit a BST. In response, the transponder will transmit a VST. Within this standard, the transponder's read-only, short read/write, and long read/write memory regions have been formatted to meet the VST definition as established by the Comité Européen de Normalisation (CEN).
- h) The resource manager will process the received VST and transmit the information within it to the BOAs that have registered for that information.
- i) Based upon previously received registrations, the resource manager may also use the transponder commands listed in Clause 6 to fetch images of additional memory pages. Those pages will also be processed and the information within them transmitted to the BOAs that have registered for that information.
- j) Based upon the received information, the connected BOAs may request that the resource manager delete some existing messages or add new messages to a memory page. The resource manager shall respond to these requests and shall then transfer the updated memory image(s) to the transponder.

4.2 Access control flow summary

This standard provides for communications control fields and access control commands that may be used to restrict the set of commands to which the transponder will respond. These access control features are in all cases optional and may be omitted or only partially implemented within compliant equipment. It is anticipated that regulatory agencies, user agencies, or associations of user agencies may require that transponders used within their DSRC systems incorporate specific access control features as defined within this standard. However, such requirements do not preclude the manufacture and use of transponders that do not meet those agency's requirements, though such transponders could not be used to obtain services within such a user agency's system.

Access controls are typically used to provide data protection, data privacy, or data authentication. However, data privacy and authentication may also be accomplished by compliant equipment by using methods other than those defined by this standard. For example, Clause 8 states that message bodies may be encrypted using user-specific algorithms.

It is anticipated that, when implemented by the manufacturer and incorporated into a user agency's processing, these access control capabilities will typically be utilized as follows:

- a) The transponder manufacturer will implement one or more security-related algorithms within the transponder's basic firmware. These algorithms will be suitable for confirming access control credentials that may be later received in conjunction with commands from the roadside.
- b) Either as part of the initial fabrication or as a subsequent configuration process, the transponder's manufacturer may modify the firmware so that specific transponder commands or memory page references are governed by a set of access credentials. The selection of controlled commands and the access credentials used to control them may be requested by an end user agency. The method used by the manufacturer to perform this initial transponder configuration is not controlled by this standard. However, the manufacturer is encouraged to use the Reserve Memory Page and Release Memory Page commands defined in Clause 6.
- c) In some cases the manufacturer may also configure the transponder with master credentials that allow the release of any previously reserved memory pages without presenting the access credentials specified at the time of the page reservation. This option is not governed by this standard.
- d) In many cases a user agency will wish to utilize a reserved page with access controls to store essential or sensitive information, such as a financial account balance. In this case, assuming that the user agency has obtained a transponder that supports its selected security algorithms, the user agency may then reserve additional pages of memory using the Reserve Memory Page command and may specify the access credentials that will be used to control access to those pages as part of the Reserve Page command. This may typically be done at a central site using a controlled beacon installation.
- e) Once configured by the user agency, the transponder may be installed in a consumer vehicle. When the vehicle passes through a beacon's communication zone, the beacon may issue a command to the transponder. Based upon the previous configurations imposed by the manufacturer or the user agency, the transponder may require that access controls be provided prior to executing the received command. Each of the commands specified in Clause 6 provides for the transmission of such access credentials with the command.
- f) Many different security algorithms are currently available, and this standard does not govern the selection of such algorithms for DSRC. In general, the processing flow associated with such security algorithms requires a series of transactions between the roadside and the transponder, such as those illustrated in Figure 3. The transponder commands and responses specified in Clause 6 provide for the information transmission required by this figure.

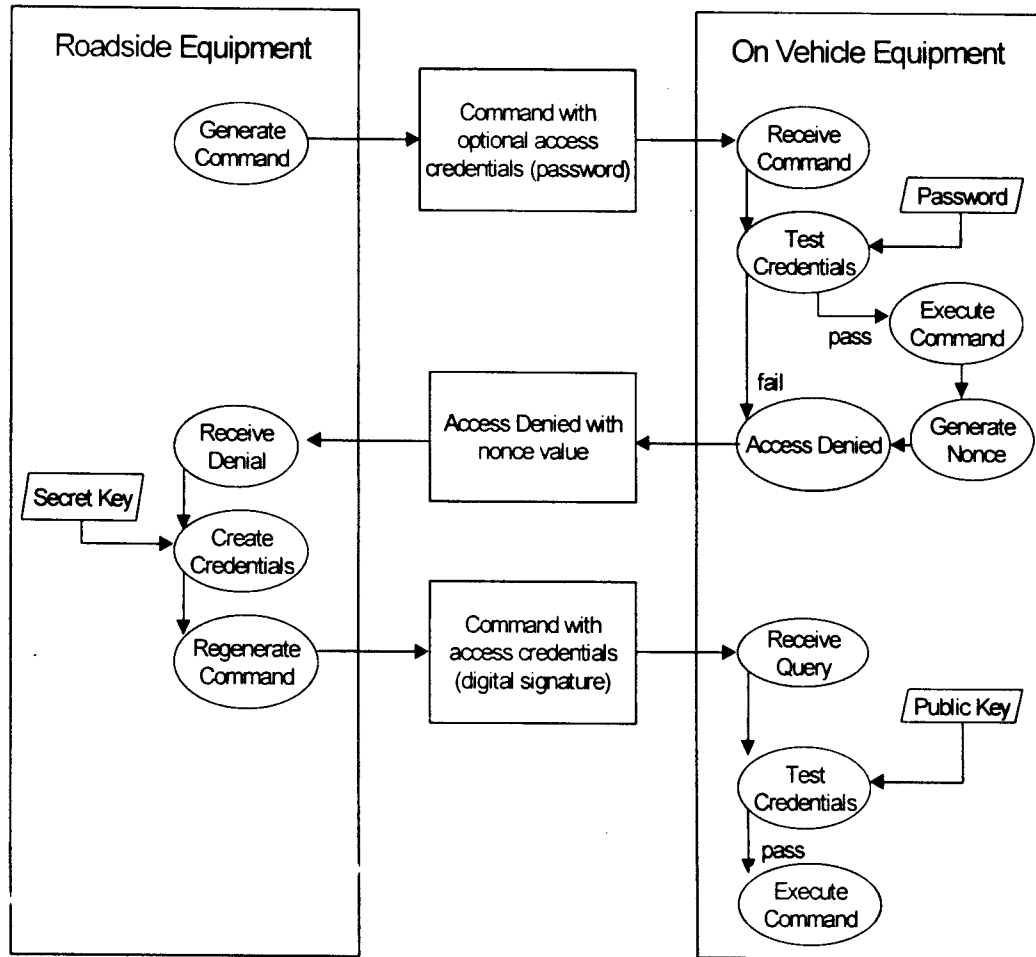


Figure 3—Access control processing flow

5. Transponder resources

Transponders that are compliant with this standard shall provide internal resources in accordance with the specifications described in this clause. While a range of transponders having various capabilities may be defined in a manner compliant with those specifications, the basic structure and the capabilities definitions shall be adhered to in all cases. Not all resources defined in this clause are mandatory in compliant transponders.

Many transponder identifiers provide for values that are available for registration. The registration process is controlled by the IEEE and is not defined within this document. See 1.3 for additional information on this topic.

5.1 Transponder resources definition

This clause functionally identifies and specifies the transponder resources requirements. These requirements shall in no way constrain the actual hardware implementation of transponders as long as the associated resources are partitioned in a manner compliant with this standard. A transponder compliant with this standard shall provide resources as defined in 5.1.1 through 5.1.12. These resources are illustrated in Figure 4.

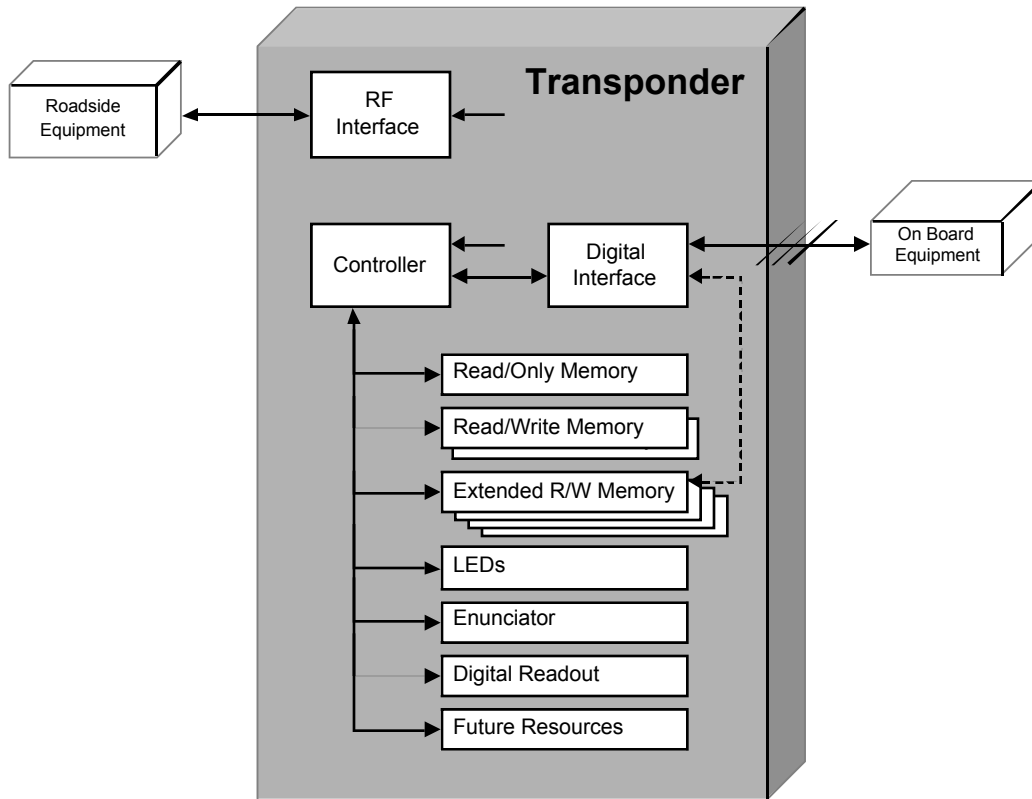


Figure 4—Transponder resources

5.1.1 Wireless interface

The transponder shall provide a wireless interface with the RSE. The characteristics of this interface are outside the scope of this standard. It is expected that this standard may be implemented in conjunction with a wide variety of radio frequency (RF) interfaces. However, the wireless interface must support the data transfers specified within this standard. This standard has been developed in coordination with ASTM Draft Standard for Dedicated Short-Range Communications (DSRC) Data Link Layer, Exxx-99⁷ and the ISO 7498 series of standards to ensure compatibility among these standards.

5.1.2 Controller

The controller shall interpret and implement commands (listed in Clause 6) when received across the wireless interface. Implementation of those commands will typically require access to or control of the other transponder resources listed in this clause. The controller may also implement the interface with other OBE.

5.1.3 External interface

Compliant transponders may provide an external interface. The availability and characteristics of this interface shall be indicated in the read-only memory (as defined in 5.2). If implemented, this interface shall provide other pieces of OBE with access to the transponder's resources and through those resources provide communications with the roadside. The characteristics of this interface and the command set used across the external interface are outside the scope of this standard. However, it is anticipated that the command set will be comparable to that implemented across the wireless interface with the roadside.

⁷Information on references can be found in Clause 2.

5.1.4 Memory management and page identification

Memory within the transponder is formatted into partitions and pages. A partition is an area of memory that may be controlled by access credentials within which pages may be allocated. A page is an area of memory within a partition, which may also be protected with access credentials and from which data may be read or written.

As defined in 5.1.5 through 5.1.7, transponders may provide read-only memory, read/write memory, and/or extended read/write memory. While read-only memory and read/write memory pages are predefined, commands defined in Clause 6 allow dynamic configuration of the extended read/write memory. This dynamic configuration may be accomplished by allocating partitions within the extended read/write memory or by reserving pages.

Pages may be reserved either within an existing partition or within the overall extended read/write memory area. A partition identifier is specified when a partition is allocated, and it is referenced when a page is reserved within the partition. A page identifier is specified when a page is reserved, and it is referenced when a page is accessed. A sample of partition identifiers is provided in Table 1. A complete listing of defined partition identifiers is provided in Table E.1.

Table 1—Sample partition identifiers

Partition number	Partition designation
hex(0000)	Reserved
hex(0001 – FFFF)	Available for registration

Compliant transponders shall comply with the following requirements:

- The minimum memory page size shall be 128 bits.
- The maximum memory page size shall be 64 Kbytes. This limitation is based upon the maximum length of a read/write memory page command.
- The first memory page shall always exist and shall be a read-only memory page as defined in 5.1.5.
- All memory pages shall have an associated 16-bit page identifier that can be used by the transponder commands described in Clause 6.
- The first three transponder memory pages shall always be assigned the Page Identifiers hex(1) through hex(3).
- Page Identifiers hex(4) through hex(7) refer to predefined combinations of the first three memory pages.
- The page identifiers associated with the transponder user interface (UI) shall be assigned from values above hex(FEFF). These default values may be overridden by aliasing other page identifiers to the default identifiers using the commands defined in Clause 6.
- Unreserved page identifiers may be assigned to agencies on an implementation-specific basis.

A sample of defined page identifiers is provided in Table 2. Page numbers shall be unique within a transponder, i.e., duplicate page numbers shall not be used in different partitions.

Table 2—Sample page identifiers

Page number	Page designation
hex(0)	Reserved
hex(0001 .. FFFF)	Specific values are defined in Table E.2

5.1.5 Read-only memory

Compliant transponders shall provide 16 bytes (128 bits) of read-only memory. The information within this region shall be formatted as specified in 5.2.

The read-only memory shall be transmitted to the RSE within the VST (as defined in 9.5). The VST is returned by the OBE in response to a BST received from the RSE. The read-only memory may also be accessed using other memory access commands listed in Clause 6.

This region of memory is “read only” from the roadside.

5.1.6 Read/write memory

Compliant transponders may provide zero, one, or two read/write memory regions. The availability of these memory regions shall be as indicated in the read-only memory as defined in 5.2.

When present, the read/write memory regions shall have the following characteristics:

- The short read/write memory region shall provide 16 bytes (128 bits) of storage.
- The long read/write memory region shall provide 32 bytes (256 bits) of storage.

The read/write memory images may be transmitted to the RSE within the VST command response, as defined in Clause 6. The read/write memory regions may also be accessed using other memory access commands listed in Clause 6.

5.1.7 Extended read/write memory

Compliant transponders may provide one or more extended read/write memory regions. The availability of these memory regions shall be as indicated in the read-only memory, as defined in 5.2. The extended memory may be configured into logical pages by the manufacturer and/or by issuance of the Reserve Memory Page command, as defined in 6.4.9. The size of a dynamically created page is specified as an operand of the Reservation command. Associated with each page is a 16-bit page number. Permanent page numbers shall be reserved for specific purposes or agencies by registering the number. Table E.2 provides a list of pre-assigned page numbers and their associated use. These pages may, optionally, have access credentials to protect the page for write or read/write access.

The list of reserved pages for a given transponder may be requested by issuing the Query Memory Configuration command, as defined in 6.4.11.

5.1.8 Lamps

Compliant transponders may provide a red, a green, and a yellow lamp; it is not necessary for all lamps to be present. The availability of these lamps shall be as indicated in the read-only memory, as defined in 5.2. Lamps are controlled using the Set User Interface command specified in 6.4.6.

5.1.9 Enunciators

Compliant transponders may provide one or more enunciators. The availability of these enunciators shall be as indicated in the read-only memory, as defined in 5.2. Enunciators are controlled using the Set User Interface command specified in 6.4.6.

5.1.10 Character readout

Compliant transponders may provide a digital readout. The availability of a digital readout shall be as indicated in the read-only memory, as defined in 5.2. The digital readout is controlled using the Set User Interface command specified in 6.4.6 and the Map User Interface command specified in 6.4.7.

The digital readout shall display Text String messages (defined in 8.7.1) that are stored in the memory page to which the digital readout is mapped. Controls may be provided that enable the user to scroll from one message to another within the mapped memory page.

5.1.11 Keypad

Compliant transponders may provide a keypad. The availability of a keypad shall be as indicated in the read-only memory, as defined in 5.2.

The data that are entered using the keypad shall be stored as a Text String message in the memory page to which the keypad is mapped. The memory-related commands specified in Clause 6 shall be used to retrieve data entered at the keypad and to clear previously entered data.

5.1.12 Future resources

Future revisions of this standard may provide for additional UI resources. The availability of these resources is defined in 5.2; they shall be controlled using the Set User Interface command specified in 6.4.6 and the Map User Interface command specified in 6.4.7.

5.2 Read-only memory definition

Information within the read-only memory region shall be formatted as defined in Table 3 and described in 5.2.1 through 5.2.18. The read-only memory region corresponds exactly to the fixed length portion of the VST (the VST “header”) defined in 9.5.2.

Table 3—Read-only memory fields

Field name	Location (bits)	Length (bits)	Specification and description
T-APDU Tag	0-3	4	ASN.1 tag for an INITIALISATION.response (i.e., a VST) = hex(9)
Fill	4-7	4	Nonfunctional bits used to maintain byte boundaries
Profile	8-15	8	Profile field of VST
Number of Applications	16-23	8	Number of applications in the applications list = hex(1)
Application Identifier (AID)	24-31	8	Mailbox AID = hex(D)

Table 3—Read-only memory fields (continued)

Field name	Location (bits)	Length (bits)	Specification and description
EID/Revision Level	32-39	8	EID; shall be used for the IEEE Std 1455-1999 revision level
Container Tag	40-47	8	Octet string tag = hex(4); used to encapsulate the VST parameter
Octet String Length	48-55	8	The actual length (in octets) of the subsequent data in the octet string
Octet String Data		Includes following fields	An octet string used for ASN.1 compliance, which comprises the subsequent fields defined in this table
Returned Pages Flag	56-57	2	Bits that correspond to the two memory images returned, as specified in the BST
Reserved 1	58-60	3	Reserved by IEEE for future use
Memory Configuration	61-63	3	Defines the availability of various memory regions
Transponder Configuration	64-71	8	Defines the availability of various transponder peripherals, such as lamps and enunciators
Service Agency	72-87	16	Identifies the unique agency that is primarily responsible for issuing statements corresponding to services received by the transponder's user
Serial Number Type	88-91	4	Indicates how the serial number and manufacturer identifier should be interpreted
Manufacturer Identifier	92-107	16	Identifies the manufacturer of the transponder
Serial Number	108-127	20	Uniquely identifies the transponders produced under a single Manufacturer Identifier value

5.2.1 T-APDU Tag

The T-APDU Tag field is required to provide ASN.1 compliance (see the ASN.1 definition of T-APDUs in Annex A). This field shall be set to hex(9) to indicate an INITIALISATION.response.

5.2.2 Fill

The Fill field is required to maintain byte boundaries. This field shall be set to hex(0).

5.2.3 Profile

The Profile field contains communications profiles as defined by the specific lower layer service. The values for this field are defined in Table E.3, and a sample is shown in Table 4.

5.2.4 Number of Applications

This field contains the number of applications in the subsequent application list. The value for this field shall always be set to hex(1).

Table 4—Sample profile field values

Value	Definition
hex(0)	Reserved
hex(1)	Unspecified profile
hex(0 .. FF)	Available for registration

5.2.5 AID

The AID field is required to provide compatibility with the CEN VST definition. This field shall be set to hex(D), which is the AID for the Mailbox application.

5.2.6 EID/Revision Level

The EID field is required to provide compatibility with the CEN VST definition. Within this standard, the EID/Revision Level field indicates the revision level of this standard with which the transponder complies. Values shall be interpreted as defined in Table 5.

Table 5—EID/Revision Level field values

Value	Interpretation
hex(0)	Reserved
hex(1)	Prerelease (field testing; current value)
hex(2)	Initial release
hex(3 .. FF)	Reserved

5.2.7 Container Tag

The Container Tag field is required to provide ASN.1 compliance. This field shall be set to hex(4), which indicates an octet string.

5.2.8 Octet String Length

The Octet String Length field, which is required to provide ASN.1 compliance, indicates the length of the subsequent octet string data. The low order bit of octet string length must always be set to zero for ASN.1 compliance (meaning that this octet is used for actual length designation). The remaining 7 bits of the Octet String Length field contain the actual length (in octets) of the subsequent data in the octet string. Therefore, the maximum length for the data is 127 bytes.

The Octet String Length field shall be overwritten dynamically by the OBE transponder application during VST transmission. It is overwritten with a value that represents the sum of the size of the memory images being returned in the VST, which includes the read-only memory.

5.2.9 Octet String Data

The Octet String Data field is descriptive only and has no actual bit representation in and of itself. The purpose of this descriptive field is to indicate that the octet string data that follow the Octet String Length field include the subsequent fields defined for read-only memory and represent the balance of the VST structure.

5.2.10 Returned Pages Flag

The Returned Pages Flag field indicates which memory pages requested in the BST are present in the transponder and, therefore, which memory pages are being returned as part of the VST. This field shall be interpreted as defined in Table 6.

Table 6—Returned Pages field interpretation

Location (bits)	Interpretation
0	First page flag; a value of 1 indicates that the first page is returned within the VST
1	Second page flag; a value of 1 indicates that the second page is returned within the VST

5.2.11 Reserved 1

The Reserved 1 field is required to maintain byte boundaries. This field shall be set to hex(0).

5.2.12 Memory Configuration

The Memory Configuration field indicates which read/write memory regions are present. Values shall be interpreted as defined in Table 7.

Table 7—Read/write Memory Configuration field values

Value	Interpretation
hex(0)	No read/write memory present
hex(1)	Short read/write memory present
hex(2)	Long read/write memory present
hex(3)	Short read/write and long read/write memory present
hex(4)	Extended memory present
hex(5)	Short read/write and extended memory present
hex(6)	Long read/write and extended memory present
hex(7)	Short read/write, long read/write, and extended memory present

5.2.13 Transponder Configuration

The Transponder Configuration field indicates the configuration of installed transponder peripherals. The method of interpreting the field values is dependent upon the status of Bit 7. If Bit 7 is 1, then the remaining seven bits shall be individually interpreted to determine the peripherals configuration as defined in Table 8. If

Bit 7 is 0, then the remaining seven bits shall be interpreted as an enumerated value using Table E.4 (sample shown in Table 9).

Table 8—Transponder Configuration field interpretation, Bit 7 Set to 1

Location (bits)	Interpretation
7 (msb)	Always 1 when field is interpreted as binary flags rather than an enumerated value; if 0, then Table 9 applies
6	Red, yellow, and green lamps all present
5	Enunciator present
4	External network interface present
3	Character readout present
2	Keypad present
1	Reserved
0 (lsb)	Reserved

Table 9—Transponder Configuration enumerated field values, Bit 7 Set to 0

Value	Interpretation
hex(0)	Reserved
hex(1 .. 7)	Available for registration. Specific values are defined in Table E.4.

5.2.14 Service Agency

The Service Agency field indicates the service agency that is responsible for collecting fees incurred by the person using this transponder. Values shall be interpreted as defined in Table E.5. Sample table is shown below in Table 10.

Table 10—Sample Service Agency field values

Value	Interpretation
hex(0)	Reserved
hex(0001 .. FFFF)	Available for registration

5.2.15 Serial Number Type

The Serial Number Type field indicates the nature of the Manufacturer Identifier and the Serial Number fields when they are transmitted to the RSE. Those fields may be protected by encryption or masking, as indicated by the Serial Number Type field. The Serial Number Type field shall not be encrypted or masked. Values shall be interpreted as defined in Table 11.

Table 11—Serial Number Type field values

Value	Interpretation
hex(0)	Reserved
hex(1)	Clear; Manufacturer Identifier and Serial Number fields are not altered
hex(2)	Encrypted; Manufacturer Identifier and Serial Number fields are encrypted
hex(3)	Masked; Manufacturer Identifier and Serial Number fields are masked
hex(4 .. F)	Reserved

5.2.16 Manufacturer Identifier

The Manufacturer Identifier field indicates the manufacturer that produced the transponder. Values shall be interpreted as defined in Table E.6. Sample table is shown below in Table 12. The Manufacturer Identifier field may be masked or encrypted when transmitted to the RSE.

Table 12—Manufacturer Identifier field values

Value	Interpretation
hex(0)	Reserved
hex(0001 .. FFFF)	Available for registration

5.2.17 Serial Number

The Serial Number field shall uniquely identify a transponder within a set of devices having the same Manufacturer Identifier field value. The method of assigning values to this field shall be entirely controlled by the manufacturer. However, uniqueness shall be preserved. The Serial Number field may be masked or encrypted when transmitted to the RSE.

5.2.18 Unique identifier

The 40-bit sequence of data consisting of the Serial Number Type, Manufacturer Identifier, and Serial Number fields may be referred to as the transponder's unique identifier. The characteristics of the constituent fields shall be preserved as defined in 5.2.15 through 5.2.17.

5.3 Interoperability requirements

As defined in 1.4, compliant transponders meet all the requirements specified in this standard. Interoperable transponders additionally provide optional features. The following features defined in this subclause shall be provided in interoperable transponders:

- Read-only memory (128 bits), which shall not be protected by access credentials.
- Short read/write memory (128 bits), which shall not be protected by access credentials.

- Long read/write memory (256 bits), which shall not be protected by access credentials.
- Extended read/write memory (at least 512 bits).
- Red, yellow, and green lamps.
- An enunciator.

Interoperable transponders may also provide additional optional features such as using access credential protection.

Additional interoperability requirements are specified in 6.6.

6. Transponder commands and memory access

6.1 Basic concepts

Transponders that are compliant with this standard shall provide the capability to process the commands specified in this clause. These commands reference the memory, processing, and UI resources that may be present on the transponder. The commands are independent of the BOA that may be utilizing those resources. The availability of the resources that may be referenced by commands is indicated by bits allocated in read-only memory that are defined in 5.2 and by the results of the Query Memory Configuration command.

The RSE shall not intentionally generate commands to the transponder that reference resources known to be absent from the addressed transponder. However, each of the commands defined in this clause specifies the behavior that shall be exhibited when such absent resources are referenced.

The OBE is not in all cases required to provide the full set of behaviors specified for each of the commands specified in this clause. For each command, abnormal behaviors are specified that include the method (if any) by which the OBE shall notify the RSE if a received command is optional and has not been fully implemented in the receiving OBE.

Some of the commands defined in this clause, such as Read Memory Page and Write Memory Page, require transmission of an entire memory page image. The End Of Data message (defined in 8.7.4) may be used to terminate the region of a memory page that contains valid messages. When an End Of Data message is present, the RSE and OBE may transmit only that initial portion of a memory page that contains valid messages. If this optional feature is not implemented, then the area of a memory image that does not contain valid messages shall be transmitted and shall be set to zeroes.

6.2 Command set template

Each command shall consist of the fields shown in Table 13 and described in 6.2.1 through 6.2.6.

Table 13—Command set fields

Command Identifier	Command Transaction Identifier	Command Length	Access Control Length	Access Control	Command Parameters
1 byte	1 byte	2 bytes	1 byte	1 to 32 bytes	Variable

6.2.1 Command Identifier

6.2.1.1 Length

The length of the Command Identifier field shall be 1 byte.

6.2.1.2 Usage

The Command Identifier field shall identify the command to be performed and shall take on the values shown in Table 14. The high order bit (bit 7) of this field indicates the presence or absence of access credentials in the command. If bit 7 is 1, then the Access Control Length and Access Control fields shall be present after the Command Length field. If bit 7 is 0, then the Access Control Length and Access Control fields shall be omitted and the Command Length field shall be followed by the Command Parameter field.

Table 14—Command Identifiers

Codes	Codes with credentials	Meaning	OBE command support
hex(0 .. F)	hex(80 .. 8F)	Reserved	
hex(10)	hex(90)	Read Memory Page	Required to access memory other than through memory images returned in the VST
hex(11)	hex(91)	Write Memory Page	Optional* (required if read/write memory is present)
hex(12)	hex(92)	Append Message	Optional* (required if read/write memory is present)
hex(13)	hex(93)	Initialize Circular Queue	Optional (required for circular queues)
hex(14)	hex(94)	Write Circular Queue	Optional* (required for circular queues)
hex(15) .. (1F)	hex(95) .. (9F)	Reserved	
hex(20)	hex(A0)	Set User Interface	Optional* (required if OBE has UI)
hex(21)	hex(A1)	Map User Interface	Optional
hex(22 .. 2F)	hex(A2 .. AF)	Reserved	
hex(30)	hex(B0)	Sleep Transponder	Optional
hex(31.. 3F)	hex(B1.. BF)	Reserved	
hex(40)	hex(C0)	Reserve Memory Page	Optional (required if extended memory is present)
hex(41)	hex(C1)	Release Memory Page	Optional (required if Reserve Memory Page command is implemented)
hex(42)	hex(C2)	Query Memory Configuration	Optional (required if Reserve Memory Page command is implemented)

Table 14—Command Identifiers (continued)

Codes	Codes with credentials	Meaning	OBE command support
hex(43)	hex(C3)	Reserve Memory Partition	Optional
hex(44)	hex(C4)	Release Memory Partition	Optional (required if Reserve Memory Partition command is implemented)
hex(45 .. 6F)	hex(C5 .. EF)	Reserved	
hex(70 .. 7F)	hex(F0 .. FF)	Available for manufacturer-specific testing	Optional—shall not be used in production units deployed in the field

*These commands are supported in broadcast mode.

6.2.2 Command Transaction Identifier

6.2.2.1 Length

The length of the Command Transaction Identifier field shall be 1 byte.

6.2.2.2 Usage

The Command Transaction Identifier field shall be an identifier that is uniquely calculated for each instance of a command. This identifier is returned in the command response and allows the resource manager to match a received response to a specific sent command.

6.2.3 Command Length

6.2.3.1 Length

The length of the Command Length field shall be 2 bytes.

6.2.3.2 Usage

The Command Length field shall specify the total length in bytes of the command instance, including all fields except the Command Identifier field, the Command Transaction Identifier field, and this Command Length field. The maximum value of this field effectively constrains the maximum size of a transferred memory image.

6.2.4 Access Control Length

6.2.4.1 Length

The length of the Access Control Length field shall be 1 byte.

6.2.4.2 Usage

The Access Control Length field shall specify the length of the Access Control field in bytes. This field, if present, will never be zero.

6.2.5 Access Control

6.2.5.1 Length

The length of the Access Control field shall vary up to 32 bytes, as specified by the Access Control Length field.

6.2.5.2 Usage

The Access Control field shall be used to provide access controls for command instances. The actual value of the Access Control field is implementation-specific and would typically follow some type of encryption and/or authentication scheme.

6.2.6 Command Parameters

6.2.6.1 Length

The length of the Command Parameters field shall be fixed for each command except for the Write Memory, Append Message, Write Circular Queue, and Set User Interface commands, which have variable parameter lengths.

6.2.6.2 Usage

The Command Parameters field shall be specific to each command set.

6.3 Command information flow

This standard provides for two communication modes. In the “connected” mode, all communications are prefaced by a BST/VST exchange that connects the RSE to a specific transponder. In the “broadcast” mode, transponder commands are broadcast from the RSE to all passing transponders without first establishing an RSE-to-OBE connection using a BST/VST. Transponders shall remain ready to receive a communication at all times, subject to vendor-specific power consumption optimization.

The connected mode is recommended because it allows the RSE to verify the transponder configuration before additional commands are transmitted to the transponder. However, the broadcast mode may be appropriate in certain applications where the communication opportunity is constrained.

Clause 9 discusses all application layer services in detail. Annex C provides illustrations for the flow of commands from the resource manager to the OBE transponder application via the application layer.

6.3.1 Connected mode information flow

In the connected mode, the following RSE-to-OBE information flow shall be observed:

- a) The resource manager shall register itself as part of its startup sequence by using the RegisterApplicationBeacon service in the application layer. This registration causes the RSE application layer to construct a BST and initiate communication with potential OBE transponders.
- b) The connection is established when the OBE application layer returns a VST to the resource manager.
- c) The resource manager shall determine appropriate commands, based upon registration requests from the connected BOAs.
- d) The resource manager shall formulate the command instance using supplied information.

- e) The resource manager shall use the ACTION.request service in the application layer to transmit the command to the OBE. The OBE shall provide a response if required by the Mode field in the Action.request.
- f) The OBE shall process the command received from the resource manager as an ACTION.indication service and shall respond, if required, using the ACTION.response service of the OBE application layer.
- g) The resource manager shall process the received ACTION.confirm, potentially resending the command with appropriate access controls.

6.3.2 Broadcast mode information flow

The broadcast mode is used to transmit a command or a fixed set of commands to every transponder that passes through the RSE communication zone. In the broadcast mode, the following RSE-to-OBE information flow shall be observed:

- a) The resource manager may use the BroadcastData.request service of the RSE application layer to broadcast to the OBE.
- b) In that case, the OBE transponder application shall use the GetBroadcastData.request service of the OBE application layer to access a command or command set that was broadcast from the resource manager.
- c) The resource manager may also use the ACTION.request service of the RSE application layer to broadcast a command or command set in a broadcast mode. This may be accomplished by setting the LID field of the ACTION.request to a global LID; in this case a response from the OBE may also be requested by setting the Mode field of the ACTION.request.
- d) This ACTION.request will fail if the lower layer service associated with the application layer does not support the optional DATASEND_RESPOND_REPEAT or DATASEND_NORESPOND_REPEAT messages defined in 9.3.2. In this case, the RSE application layer may choose to repeat the command.

Also, subject to the capabilities of the lower layer media, the RSE must provide for the case that multiple transponders are within the communications zone at the time of transmission. The OBE transponder application shall use the ACTION.response service of the OBE application layer to send command responses back to the resource manager in response to a command received as a result of the resource manager sending that command using a broadcast ACTION.request.

6.4 Command definitions

The commands shall be created by the RSE and processed by the OBE as specified in 6.4.1 through 6.4.13. The command identifier values are shown with the Access Credential flag set to 0. The Command Parameter field locations are shown as if the Access Control Length and Access Control fields were not present. Details regarding command responses are provided in 6.5.

6.4.1 Read Memory Page (mandatory)

The Read Memory Page command shall initiate transmission of the specified OBE memory pages to the RSE.

6.4.1.1 Command set definition

The Read Memory Page command shall consist of the fields shown in Table 15.

Table 15—Read Memory Page command fields

Field name	Location (bytes)	Length	Specification and description
Command Identifier	0	1	hex(10) / hex(90)
Command Transaction Identifier	1	1	Identifies an instance of a command
Command Length	2 .. 3	2	Defines the total length (bytes) of all fields in this command excluding the length of the Command Identifier field, Command Transaction Identifier field, and this Command Length field
Access Control Length	4	0/1	(Optional.) Number of access credential bytes. A nonzero value indicates that the Page Identifier field will be offset by the indicated number of bytes (max. 32)
Access Control	5 .. n	0/1 .. 32	(Optional.) Access credentials
Command Parameter: Page Identifier	End of Access Control field + 1 End of Access Control field + 2	2	Identifies referenced memory page (as per specification in Table E.2)

6.4.1.2 OBE normal behaviors

The OBE shall access the memory page specified by the Read Memory Page command.

If the OBE successfully executes the Read Memory Page command, the OBE shall send a response with the Response Identifier field set to Command Success, the Response Data Length field set to the length of the read memory image, and the memory image itself in the Response Data field.

6.4.1.3 OBE abnormal responses

The following Response Identifier field values defined in Table 29 may be returned for abnormal conditions. See Table 29 for definitions.

- Command Not Recognized
- Access Control Error
- Page Not Defined
- Memory Access Error
- Command Failed

6.4.2 Write Memory Page (optional)

The Write Memory Page command is suffixed by a memory image that shall be stored in the specified OBE memory page.

6.4.2.1 Command set definition

The Write Memory Page command shall consist of the fields shown in Table 16.

Table 16—Write Memory Page command fields

Field name	Location (bytes)	Length	Specification and description
Command Identifier	0	1	hex(11) / hex(91)
Command Transaction Identifier	1	1	Uniquely identifies an instance of a command
Command Length	2 .. 3	2	Defines the total length (bytes) of all fields in this command excluding the length of the Command Identifier field, Command Transaction Identifier field, and this Command Length field
Access Control Length	4	0/1	(Optional.) Number of access credential bytes
Access Control	5 .. n	0/1 .. 32	(Optional.) Access credentials
Command Parameter: Page Identifier	End of Access Control field + 1 End of Access Control field + 2	2	Identifies referenced memory page (as per specification in Table E.2)
Memory Image	End of Access Control field + 3 .. n		The information that shall consist of sequenced messages followed by zero-fill bytes or an End Of Data message identifier. The length of this image is only constrained by the maximum command length defined in 6.2.3.

6.4.2.2 OBE normal behaviors

The OBE shall store the memory image within the received command by completely overwriting the referenced agency memory page.

If the OBE successfully executes the Write Memory Page command, the OBE shall send a response with the Response Identifier field set to Command Success. The response shall contain no data in the Response Data field.

6.4.2.3 OBE abnormal responses

The following Response Identifier field values defined in Table 29 may be returned for abnormal conditions:

- Command Not Recognized
- Access Control Error
- Page Not Defined
- Page Length Mismatch
- Memory Access Error
- Command Failed

6.4.3 Append Message (optional)

The Append Message command is suffixed by a message image that shall be appended to the end of the previously used memory within the specified OBE memory page.

6.4.3.1 Command set definition

The Append Message command shall consist of the fields shown in Table 17.

Table 17—Append Message command fields

Field name	Location (bytes)	Length	Specification and description
Command Identifier	0	1	hex(12) / hex(92)
Command Transaction Identifier	1	1	Uniquely identifies an instance of a command
Command Length	2 .. 3	2	Defines the total length (bytes) of all fields in this command excluding the length of the Command Identifier field, Command Transaction Identifier field, and this Command Length field
Access Control Length	4	0/1	(Optional). Number of access credential bytes
Access Control	5 .. n	0/1 .. 32	(Optional). Access credentials
Command Parameter: Page Identifier	End of Access Control field + 1 End of Access Control field + 2	2	Identifies referenced memory page (as per specification in Table E.2)
Message Image	End of Access Control field + 3 .. n		The information that shall be appended to the specified memory page

6.4.3.2 OBE normal behaviors

The OBE shall append the message image within the command to the end of existing messages in the specified page. Positioning within the page shall be determined by chaining through the stored messages until the first occurrence of either an End Of Data message or hex(00) following a message, where the next message header would begin. The message image shall be inserted at this point, overwriting the End Of Data message, if present. The new data shall be suffixed by either an End Of Data message or by zero filling the remainder of page.

If the OBE successfully executes the Append Message command, the OBE shall send a response with the Response Identifier field set to Command Success. The response shall contain no data in the Response Data field.

6.4.3.3 OBE abnormal responses

The following Response Identifier field values defined in Table 29 may be returned for abnormal conditions:

- Command Not Recognized
- Access Control Error

- Page Not Defined
- Insufficient Memory
- Memory Access Error
- Command Failed

6.4.4 Initialize Circular Queue (optional)

The Initialize Circular Queue command shall cause all of the memory within the specified OBE extended memory page to be cleared to zeros and shall set any control data to indicate that the queue is empty.

6.4.4.1 Command set definition

The Initialize Circular Queue command shall consist of the fields shown in Table 18.

Table 18—Initialize Circular Queue command fields

Field name	Location (bytes)	Length (bytes)	Specification and description
Command Identifier	0	1	hex(13) / hex(93)
Command Transaction Identifier	1	1	Uniquely identifies an instance of a command
Command Length	2 .. 3	2	Defines the total length (bytes) of all fields in this command excluding the length of the Command Identifier field, Command Transaction Identifier field, and this Command Length field
Access Control Length	4	0/1	(Optional.) Number of access credential bytes
Access Control	5 .. n	0/1 .. 32	(Optional.) Access credentials
Command Parameter: Page Identifier	End of Access Control field + 1 End of Access Control field + 2	2	Identifies referenced memory page (as per specification in Table E.2)

6.4.4.2 OBE normal behaviors

The OBE shall clear the specified page to zeros and shall set any control data to indicate that the queue is empty.

If the OBE successfully executes the Initialize Circular Queue command, the OBE shall send a response with the Response Identifier field set to Command Success. The response shall contain no data in the Response Data field.

6.4.4.3 OBE abnormal responses

The following Response Identifier field values defined in Table 29 may be returned for abnormal conditions:

- Command Not Recognized
- Page Not Defined

- Access Control Error
- Memory Access Error
- Command Failed

6.4.5 Write Circular Queue (optional)

The Write Circular Queue command is suffixed by a message image that shall be written to the end of the circular queue within the specified OBE memory page.

6.4.5.1 Command set definition

The Write Circular Queue command shall consist of the fields shown in Table 19.

Table 19—Write Circular Queue command fields

Field name	Location (bytes)	Length	Specification and description
Command Identifier	0	1	hex(14) / hex(94)
Command Transaction Identifier	1	1	Uniquely identifies an instance of a command
Command Length	2 .. 3	2	Defines the total length (bytes) of all fields in this command excluding the length of the Command Identifier field, Command Transaction Identifier field, and this Command Length field
Access Control Length	4	0/1	(Optional.) Number of access credential bytes
Access Control	5 .. n	0/1 .. 32	(Optional.) Access credentials
Command Parameter: Page Identifier	End of Access Control field + 1 End of Access Control field + 2	2	Identifies referenced memory page (as per specification in Table E.2)
Message Image	End of Access Control field 3 .. n		The information that shall be written to the end of the circular queue in the specified memory page

6.4.5.2 OBE normal behaviors

The OBE shall write the message image within the received command by locating the end of the current circular queue contained in the referenced memory page, placing the message image at the end of the queue, and updating any queue control information. Existing messages shall be deleted on a first-in-first-out (FIFO) basis if required to create sufficient available memory for the insertion of the message image. All memory in the page that is not used for message storage shall be set to zero.

If the OBE successfully executes the Write Circular Queue command, the OBE shall send a response with the Response Identifier field set to Command Success. The response shall contain no data in the Response Data field.

6.4.5.3 OBE abnormal responses

The following Response Identifier field values defined in Table 29 may be returned for abnormal conditions:

- Command Not Recognized

- Page Not Defined
- Access Control Error
- Insufficient Memory
- Memory Access Error
- Command Failed

6.4.6 Set User Interface (optional)

The Set User Interface command is suffixed by data specifying UI behaviors that shall be implemented by the OBE. The RSE may determine the UI elements that are available for a transponder by interpreting the Transponder Configuration field that is stored in the OBE read-only memory and transmitted to the RSE within the VST. The Transponder Configuration field is defined in Table 3. The RSE shall not address UI elements that are absent for a given OBE.

6.4.6.1 Command set definition

The Set User Interface command shall consist of the fields shown in Table 20.

Table 20—Set User Interface command fields

Field name	Location (bytes)	Length	Specification and description
Command Identifier	0	1	hex(20) / hex(A0)
Command Transaction Identifier	1	1	Uniquely identifies an instance of a command
Command Length	2 .. 3	2	Defines the total length (bytes) of all fields in this command excluding the length of the Command Identifier field, Command Transaction Identifier field, and this Command Length field
Access Control Length	4	0/1	(Optional.) Number of access credential bytes
Access Control	5 .. n	0/1 .. 32	(Optional.) Access credentials
Command Parameter: User Interface Element	End of Access Control field + 1 End of Access Control field + 2	2	Each command will affect only the addressed elements defined as follows: Bit 0: Red lamp Bit 1: Yellow lamp Bit 2: Green lamp Bit 3: Enunciator Bit 4: Character display Bits 5-15: Additional UI elements
Type (ObeUICmdType)	End of Access Control field + 3	1	AbsoluteOff (0), AbsoluteOn (1), TimedCommand (2), Flashing Command (3), Reserved (4 .. 255)
Attributes: Absolute Command (0 bytes) Timed Command (2 bytes) Flashing Command (5 bytes)	End of Access Control field + 4 .. n	0 2 4 1	(Unused for Absolute Command) Time period in 125 ms increments Cycle state bitmap, 125 ms per bit Repetition count (1 .. 255)

6.4.6.2 OBE normal behaviors

The OBE shall alter the UI element specified within the command parameter in the following fashion, depending upon the value of the type parameter:

- *Absolute Off command.* Turns the addressed UI element off. State is maintained until changed by a subsequent command.
- *Absolute On command.* Turns the addressed UI element on. State is maintained until changed by a subsequent command.
- *Timed command.* Turns the addressed UI element on for a specified period of time. The time period is specified in 125 ms increments.
- *Flashing command.* Cycles the state of the addressed UI element based upon a 4-byte bit map. Each bit in the map represents an interval of 125 ms (the total bit map represents 4 s). A repetition byte indicates the number of times the bit map cycle pattern should be performed (1 to 255 times).

If the OBE successfully executes the Set User Interface command, the OBE shall send a response with the Response Identifier field set to Command Success. The response shall contain no data in the Response Data field.

The OBE may arbitrarily turn off any element after a preset period of time to preserve battery life.

The completion of a UI command shall not be affected by the reception of any other transmissions from the RSE except for an overriding UI command.

Table E.2 defines a memory page associated with an enunciator. This is intended to support systems that provide a synthetic speech interface or other sophisticated auditory cues. The Set User Interface command shall always be used to initiate changes to the UI, but the data in the enunciator memory page may be used to control the specific action.

Also, Table E.2 defines a memory page associated with the character readout. The Set User Interface command shall always be used to initiate changes to the character display, but the specific information shown may be retrieved from the character display memory page.

6.4.6.3 OBE abnormal responses

The following Response Identifier field values defined in Table 29 may be returned for abnormal conditions:

- Command Not Recognized
- Access Control Error
- Device Error
- Command Failed

6.4.7 Map User Interface (optional)

The Map User Interface command shall cause the OBE to map a page of memory to the specified UI component. This reservation shall include the establishment of access control procedures. Mapping a page of memory to a specified UI element affects the behavior of the transponder when a Set User Interface command is subsequently received by indicating the information that is enunciated or displayed.

6.4.7.1 Command set definition

The Map User Interface command shall consist of the fields shown in Table 21.

Table 21 — Map User Interface command fields

Field name	Location (bytes)	Length	Specification and description
Command Identifier	0	1	hex(21) / hex(A1)
Command Transaction Identifier	1	1	Uniquely identifies an instance of a command
Command Length	2 .. 3	2	Defines the total length (bytes) of all fields in this command excluding the length of the Command Identifier field, Command Transaction Identifier field, and this Command Length field
Access Control Length	4	0/1	(Optional.) Number of access credentials bytes
Access Control	5 .. n	0/1 .. 32	(Optional.) Access credentials
Command Parameter: User Interface Element	End of Access Control field + 1	1	Defines the UI element to be mapped 0: Keypad 1: Character Display 2: Enunciator voice 1 3-255: Reserved for additional UI elements
Page Identifier	End of Access Control field + 2	2	Identifies referenced memory page (as per specification in Table E.2)

6.4.7.2 OBE normal behaviors

The OBE shall first determine whether the specified page identifier has already been reserved. If the page identifier exists, then that page shall be used for all subsequent UI actions that reference the specified UI element. The predefined UI page identifiers listed in Table E.2 may always be used to reference the specific pages that have been currently selected using the Map User Interface command. See 5.1.8 through 5.1.11 for how the data within the UI memory pages shall be utilized.

If the OBE successfully executes the Map User Interface command, the OBE shall send a response with the Response Identifier field set to Command Success. The response shall contain no data in the Response Data field.

6.4.7.3 OBE abnormal responses

The following Response Identifier field values defined in Table 29 may be returned for abnormal conditions:

- Command Not Recognized
- Access Control Error
- Previously Reserved
- Device Error
- Command Failed

6.4.8 Sleep Transponder (optional)

The Sleep Transponder command shall cause the receiving transponder to sleep (disable RF reception and transmission) for a period of time specified in the command instance.

6.4.8.1 Command set definition

The Sleep Transponder command shall consist of the fields shown in Table 22.

Table 22—Sleep Transponder command fields

Field name	Location (bytes)	Length	Specification and description
Command Identifier	0	1	hex(30) / hex(B0)
Command Transaction Identifier	1	1	Uniquely identifies an instance of a command
Command Length	2 .. 3	2	Defines the total length (bytes) of all fields in this command excluding the length of the Command Identifier field, Command Transaction Identifier field, and this Command Length field
Access Control Length	4	0/1	(Optional.) Number of access credential bytes
Access Control	5 .. n	0/1 .. 32	(Optional.) Access credentials
Command Parameter: Sleep Duration	End of Access Control field + 1 End of Access Control field + 2	2	Sleep time duration in 125 ms increments

6.4.8.2 OBE normal behaviors

The OBE shall cause the transponder to cease responding to RF signaling for the specified period.

If the OBE successfully executes the Sleep Transponder command, the OBE shall send a response with the Response Identifier field set to Command Success. The response shall contain no data in the Response Data field. Upon completion, the link shall be considered terminated.

When an RSE wishes an OBE to reinitialize, a sleep duration of 0 will result in the OBE reinitializing with the next Frame Control Frame that it receives.

6.4.8.3 OBE abnormal responses

The following Response Identifier field values defined in Table 29 may be returned for abnormal conditions:

- Command Not Recognized
- Access Control Error
- Device Error
- Command Failed

6.4.9 Reserve Memory Page (optional)

The Reserve Memory Page command shall cause the OBE to reserve a page of memory for the specified agency. This reservation shall include the establishment of access control procedures.

6.4.9.1 Command set definition

The Reserve Memory Page command shall consist of the fields shown in Table 23.

Table 23—Reserve Memory Page command fields

Field name	Location (bytes)	Length	Specification and description
Command Identifier	0	1	hex(40) / hex(C0)
Command Transaction Identifier	1	1	Uniquely identifies an instance of a command
Command Length	2 .. 3	2	Defines the total length (bytes) of all fields in this command excluding the length of the Command Identifier field, Command Transaction Identifier field, and this Command Length field
Access Control Length	4	0/1	(Optional.) Number of access credential bytes
Access Control	5 .. n	0/1 .. 32	(Optional.) Access credentials
Partition Identifier	End of Access Control field + 1 End of Access Control field + 2	2	Specifies the partition identifier in which the memory shall be allocated (as per specification in Table E.1). A value of 0 implies that the page shall be allocated within unpartitioned memory.
Command Parameter: Page Size	End of Access Control field + 3 End of Access Control field + 4	2	Length (in bytes) of the memory page that is requested
Page Identifier	End of Access Control field + 5 End of Access Control field + 6	2	Specifies the page identifier that will be associated with the allocated memory (as per specification in Table E.2)
Page Access Credential Type and Length	(End of Page Identifier field + 1)	0/1	(Optional.) Bits 0 .. 1 indicate the access credential scope: Bit 0 = Access Credentials applied to Read access Bit 1 = Access Credentials applied to Write access Bits 2 .. 7 : Number of access credentials bytes that shall be applied to reserved page; max value = 32
Page Access Credentials	(End of Access Credential Type and Length + 1 .. n)	0/1 .. 32	(Optional.) Access credentials that shall be applied to reserved page