

Australian Standard™

**Electronic toll collection—Transaction
specification for Australian
interoperability on the DSRC link**



This Australian Standard was prepared by Committee IT-023, Transport Information and Control Systems. It was approved on behalf of the Council of Standards Australia on 2 August 2005.
This Standard was published on 16 September 2005.

The following are represented on Committee IT-023:

AUSTROADS

Australian Automobile Association
Commonwealth Department of Transport and Regional Services
Federal Chamber of Automotive Industries
ITS Australia
Monash University
Roads and Traffic Authority of NSW
Society of Automotive Engineers, Australia

Additional Interests:

Boulderstone Hornibrook
Connect East
CrossCity Motorway
Interlink Roads
Kapsch TrafficCom Australia
Parsons Brinckerhoff Australia
Q-Free Australia
Queensland Motorways
Roads and Traffic Authority of NSW
Statewide Roads
TollAust (M2)
Transcore Australia
Transtoll

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about Standards can be found by visiting the Standards Web Shop at www.standards.com.au and looking up the relevant Standard in the on-line catalogue.

Alternatively, the printed Catalogue provides information current at 1 January each year, and the monthly magazine, *The Global Standard*, has a full listing of revisions and amendments published each month.

Australian Standards™ and other products and services developed by Standards Australia are published and distributed under contract by SAI Global, which operates the Standards Web Shop.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to the Chief Executive, Standards Australia, GPO Box 476, Sydney, NSW 2001.

This Standard was issued in draft form for comment as DR 05240.

Australian Standard™

Electronic toll collection—Transaction specification for Australian interoperability on the DSRC link

Originated as AS 4962(Int)—2001.
Second edition 2005.

COPYRIGHT

© Standards Australia

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Published by Standards Australia, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 0 7337 6863 6

PREFACE

This Standard was prepared by the Standards Australia Committee IT-023, Transport Information and Control Systems, and Subcommittee IT-023-05, Electronic Tolling and Traffic Management. It supersedes AS 4962(Int)—2001.

The objective of this Standard is to provide an agreed scheme of interoperability for toll operators, EFC system integrators and equipment suppliers. The interoperability only relates to the sequences between vehicle and roadside.

Electronic fee collection (EFC) is a telematics service offered by road operators or concessionaires as a service to their customers. In order to provide for a seamless service across the concession areas, an agreed scheme of interoperability is required. A seamlessly interoperable service requires harmonization of technical interfaces (e.g. the short range radio link between in-vehicle equipment and roadside stations), common definitions of operational data (e.g. tariff class definitions), and contractual arrangements (e.g. covering clearing among operators).

Australian operators have decided to offer EFC services based on the 5.8 GHz microwave dedicated short-range communication (DSRC) link according to CEN Standards. It was quickly recognized that the Standards provide for a toolbox of functions required to define individual EFC applications according to local needs. The Standards provide for a well defined common technical interface but do not by themselves provide for interoperability on higher levels, i.e. describe the data to exchange on the link or the sequence of communication steps to perform.

From the first installations it became evident that without agreed Standards relating to communication on higher levels, every new EFC installation would probably use a new, or at least slightly modified, EFC transaction variant. Such modifications could result from the local needs of operators or from preferred solutions of the equipment supplier. Users would not be able to enjoy interoperable service.

The terms ‘normative’ and ‘informative’ have been used in this Standard to define the application of the appendix to which they apply. A ‘normative’ appendix is an integral part of a Standard, whereas an ‘informative’ appendix is only for information and guidance.

CONTENTS

	<i>Page</i>
1 SCOPE	4
2 REFERENCE DOCUMENTS.....	5
3 DEFINITIONS.....	5
4 ABBREVIATIONS.....	6
5 INTEROPERABILITY FRAMEWORK.....	7
6 CODING.....	14

APPENDICES

A RECOGNIZED EFC TRANSACTION TYPE A	23
B RECOGNIZED EFC TRANSACTION TYPE B	33
C OVERVIEW: DATA USED IN RECOGNIZED TRANSACTIONS.....	48
D DATA SECURITY CODING EXAMPLES	50
E AUSTRALIAN REPOSITORY OF DSRC DATA TYPES	55
F SPECIFIC DATA FORMATS.....	58

STANDARDS AUSTRALIA

Australian Standard

**Electronic toll collection—Transaction specification
for Australian interoperability on the DSRC link****1 SCOPE**

This Standard specifies a framework for interoperable electronic fee collection (EFC) based on dedicated short-range communication (DSRC). Specification of the technical details of the radio communication is simply done by reference to the applicable CEN Standards. In addition, data to be used in interoperable Australian EFC transactions are specified. Depending on the on-board equipment type, these data may be transferred by different EFC transaction sequences. Two transaction sequences are defined in this document, both supporting central account payment. More transaction sequences might be recognized in the future should the need arise (e.g. in order to support payment based on values carried inside the on-board equipment).

The framework specified herein relies on the following philosophy:

- (a) All equipment used will support the same radio link functionality, without variants.
- (b) Roadside equipment has to support all recognized transaction sequences specified in Appendix A and B (in order to be able to perform transactions with every type of on-board equipment).
- (c) On-board equipment has to support only one of the recognized transaction sequences.

The above rules apply to the domain of interoperability only. For local usage, operators or other DSRC system users are free to make use of other data and transaction sequences, as long as they comply with the DSRC Standards. The DSRC Standards already provide for the selection/switching mechanism required to negotiate the applications between roadside and on-board equipment.

The framework thus allows both for full interoperability through tightly specified recognized EFC transactions and for flexibility for future expansions and local needs through the negotiation mechanism inherent in the DSRC Standards. Additional Transactions may be added in the future by introducing a Recognized Type C transaction.

This Standard defines the protocol stack for communication between roadside equipment and on-board equipment using DSRC to perform EFC.

It specifies:

- (i) The complete DSRC communication stack (OSI Layers 1, 2, and 7).
- (ii) The supported EFC transaction types.
- (iii) The EFC transaction data including security elements.

Tests and requirements regarding compliance of equipment with this specification, such as type approval procedures, lie outside the scope of this document.

2 REFERENCED DOCUMENTS

The following documents are referenced in this Standard.

ISO

- 3166 Codes for the representation of names of countries and their subdivisions
- 3166-1 Part 1: Country codes
- 14906 Road transport and traffic telematics—Electronic fee collection—Application interface definition for dedicated short-range communication

ISO/IEC

- 9797 Information technology—Security techniques—Message Authentication Codes (MACs)
- 9797-1 Part 1: Mechanisms using a block cipher

ISO/TS

- 14816 Road transport and traffic telematics—Automatic vehicle and equipment identification—Numbering and data structures

CEN

- EN 12253 Road transport and traffic telematics (RTTT). Dedicated short range communications (DSRC). Physical layer using microwave at 5.8 GHz
- EN 12795 Road transport and traffic telematics (RTTT). Dedicated short range communication (DSRC). DSRC data link layer. Medium access and logical link control
- EN 12834 Road transport and traffic telematics (RTTT). Dedicated short-range communications (DSRC). Application layer
- EN 13372 Road transport and traffic telematics (RTTT). Dedicated short-range communication (DSRC). Profiles for RTTT applications

ANSI

- INCITS-92 Data Encryption Algorithm

NIST

- SP 800-67 Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher

ETSI

- EN 300 674 ERM; RTTT; Technical characteristics and test methods for DSRC transmission equipment operating in the 5.8 GHz ISM band

3 DEFINITIONS

For the purpose of this document, the following definitions apply.

3.1 Access Credentials

Data that is transferred to On-Board Equipment, in order to establish the claimed identity of Roadside Equipment application process entity.

3.2 Application Phase

The central part of an EFC Transaction where the Roadside Equipment and the On-Board Equipment exchange data related to the EFC service.

3.3 Beacon Service Table (BST)

Data transmitted by the Roadside Equipment during the Initialization Phase in order to indicate available services (transaction types).

3.4 Dedicated Short-Range Communication (DSRC)

Radio communication link according to the CEN set of Standards, EN 12253, EN 12795, EN 12834, EN 13372.

3.5 Electronic Fee Collection (EFC)

The collection of fees for use of road infrastructure by means of electronic equipment mounted on the roadside and in vehicles.

3.6 Initialization Phase

First part of an EFC transaction, comprising all information exchange between transmission of the Beacon Service Table and reception of a Vehicle Service Table by the Roadside Equipment.

3.7 On-Board Equipment (OBE)

Equipment residing in a vehicle and supporting DSRC information exchange with Roadside Equipment.

3.8 Operator

The provider of an Electronic Fee Collection service, i.e. the organizational entity that issues and accepts payment means for the right to use a certain infrastructure.

3.9 Profile

A set of parameter values that determine the behaviour of the DSRC. Profile is negotiated in the Initialization Phase of a DSRC Transaction and is defined in a DSRC Standard document EN 13372.

3.10 Recognized EFC Transaction

Part of an EFC Transaction as specified in Appendix A and B of this document, comprising a sequence of EFC functions and EFC data as defined in the EFC Application Interface Standard ISO 14906:2003 and which are approved. Refer to 'Transaction'.

3.11 Roadside Equipment (RSE)

DSRC equipment for the purpose of collecting payment from vehicles passing some road infrastructure.

3.12 Tag

Refer to 'OBE'.

3.13 Tracking/Closing Phase

Final part of a Transaction where no EFC transaction data are transferred. The Tracking/Closing Phase serves operational purposes, namely to localize the On-Board Equipment and/or to release the On-Board Equipment from the transaction.

3.14 Transaction

The entire information exchange between the Roadside Equipment and the On-Board Equipment required to complete an Electronic Fee Collection operation over the DSRC. A transaction comprises the three phases: Initialization Phase, Application Phase and Tracking/Closing Phase. Refer to 'Recognized EFC Transaction'.

3.15 Vehicle Service Table (VST)

Data transmitted by the On-Board Equipment in order to indicate details of supported services.

4 ABBREVIATIONS

AVI	Automatic vehicle and equipment identification
AID	Application Identifier
BST	Beacon Service Table

CBC	Cypher Block Chaining
CEN	Comité Européen de Normalisation, European Committee for Standardisation
DES	Data encryption service; 1DES: Single DES; 3DES: Triple DES
DLL	Data Link Layer
DSRC	Dedicated Short Range Communication
EID	Element Identifier number
EFC	Electronic Fee Collection
ERM	Electromagnetic capability and Radio Spectrum Matters
FCS	Frame Check Sequence
IID	Invoker ID
ISM	Industrial, Scientific and Medical
LID	Link Identifier = Address of OBE
LLC	Logical Link Control. Upper sub-layer of the DLL
LPDU	LLC Protocol Data Unit
MAC	This abbreviation has two different meanings: Medium Access Control: Lower sub-layer of the DLL Message Authentication Code: Data security authenticator
MMI	Man Machine Interface
NNI	Netherlands Standardisation Institute
PrWA	Private Window Allocation
PrWRq	Private Window request
OBE	On-Board Equipment
PDU	Protocol Data Unit
RSE	Roadside Equipment
RTTT	Road Transport and Traffic Telematics
TSMC	Toll Station Management Computer
VST	Vehicle Service Table

5 INTEROPERABILITY FRAMEWORK

5.1 General

All On-Board Equipment and Roadside Equipment used for Electronic Fee Collection and employing DSRC technology shall comply with this specification.

The operator of DSRC equipment is responsible for ensuring that both the RSE and the OBE which are brought into circulation, are compliant with the DSRC Standards and conformance testing of DSRC-L1 shall be performed according to EN 300 674.

This Standard specifies two recognized transactions within the Application phase. These variants are specified in Appendices A and B.

OBE that complies with this Australian Standard, shall support at least one of the Recognized EFC Transactions and both Profile 0 and Profile 1 as defined in EN 12253.

RSE that complies with this Australian Standard support all Recognized EFC Transactions and both Profile 0 and Profile 1 as defined in EN 12253.

RSE shall be designed in a way that enables updating with new recognized EFC Transactions.

NOTE: Additional recognized EFC transaction types may be added in the future to support, for example, new payment means, e.g. a special E-cash Chipcard. All operators then need to update their RSE software to recognize this new transaction type and to enter clearing arrangements with the payment means provider (issuer or bank).

5.2 EFC Transaction Phases

5.2.1 General

EFC transactions consist of three distinct phases:

- (a) The Initialization Phase.
- (b) The Application Phase.
- (c) The Tracking/Closing Phase.

Transactions can be described completely by specifying the DSRC frames exchanged between RSE and OBE.

5.2.2 Initialization phase

5.2.2.1 General

The Initialization Phase specified in this document is mandatory for all DSRC EFC equipment.

In the Initialization Phase basic settings of the DSRC link are established and which transaction sequence is to be performed is negotiated. The Initialization Phase consists of the BST/VST exchange as illustrated in Figure 5.1. From the data given in the VST the RSE decides which Recognized Transaction to perform and which parameter settings to use (e.g. which security key generation). The BST/VST exchange is common to all Recognized EFC Transactions.

Figure 5.1 shows the basic frame exchange assuming no frames are lost on the air link. Procedures for handling lost frames are prescribed in the DSRC standards.

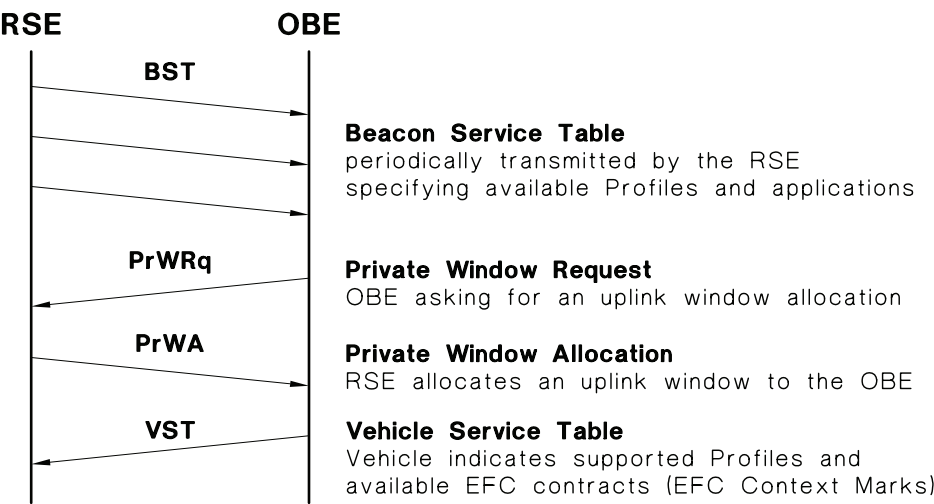


FIGURE 5.1 FRAME EXCHANGE IN THE INITIALIZATION PHASE

According to DSRC Standards, EN 12834, an OBE that does not support either any Profile or any application of the BST shall not try to initialize communication, i.e. the OBE shall not send a PrWRq.

In order to tolerate legacy OBE (according to the DSRC pre-Standards), the RSE shall be able to also handle OBE that answer with PrWRq and VST even in the case where the OBE supports no Profile or no application is listed in the VST. In this case the RSE shall not enter the Application Phase. The RSE may enter the Tracking/Release Phase.

Upon reception of the VST, the RSE inspects the EFC Context Mark(s) given in the VST. In the case where the RSE supports an EFC contract indicated by an EFC Context Mark, it enters the Application Phase, executing the Recognized Transaction that corresponds to the specific EFC Context Mark. In the case where the RSE supports more than one EFC contract indicated in the VST it selects one of them.

NOTE: The selection mechanism is beyond the scope of this document.

In the case where the RSE does not support an EFC contract indicated in the EFC Context Mark(s) given in the VST, it does not enter the Application Phase but enters the Tracking/Closing Phase and issues a Release to the OBE.

5.2.2.2 Coding of frames

The coding of the frames exchanged in the Initialization Phase is defined in the CEN Standards EN 12253, EN 12795, EN 12834 and EN 13372. In addition, the following restrictions apply:

- (a) Extension of value ranges is not supported.
- (b) Profile offered in the BST shall be either 0 or 1.
- (c) Applications listed in the Application List of the BST do not contain either an Application EID or an Application Parameter.

In order to avoid coding errors and ambiguity, coding is given in Clause 6.

5.2.2.3 Context Mark

The contents of the EFC-Context Mark indicate—

- (a) the operator issuing the OBE;
- (b) which Recognised EFC Transaction is supported by the OBE;
- (c) security key versions; and
- (d) further application specific matters.

NOTE: All current EFC-Context Marks are in Appendix F.

5.2.3 Application Phase

In the Application Phase the EFC data is transferred between RSE and OBE as specified in one of the Recognized EFC Transactions in Appendix A or B.

The Application Phase consists either of a frame exchange according to one of the Recognized EFC Transactions in Appendix A or B or of a frame exchange according to a local EFC transaction or to a different, non-EFC application.

All data exchange required to perform the EFC transaction is performed during the Application Phase.

5.2.4 Tracking/Closing Phase

5.2.4.1 General

In the Tracking/Closing Phase no transaction data are transferred, i.e. the EFC-specific data exchange is already finished. This phase serves operational purposes, namely to localize and/or to release OBE. This document specifies a common Tracking/Closing Phase for all Recognized EFC Transactions.

The Tracking/Closing Phase consists of two optional Sub-Phases: Tracking and Closing.

5.2.4.2 Tracking

Tracking serves to keep track of an OBE location in the communication zone under an RSE. Tracking is optionally performed; the RSE decides whether it wants to perform Tracking or not.

Tracking can be performed in two variants. Every recognized EFC Transaction is associated with one of the two Tracking variants. Every EFC OBE shall support at least one Tracking variant.

Both Tracking variants can be described by the frame exchange given in Figure 5.2.

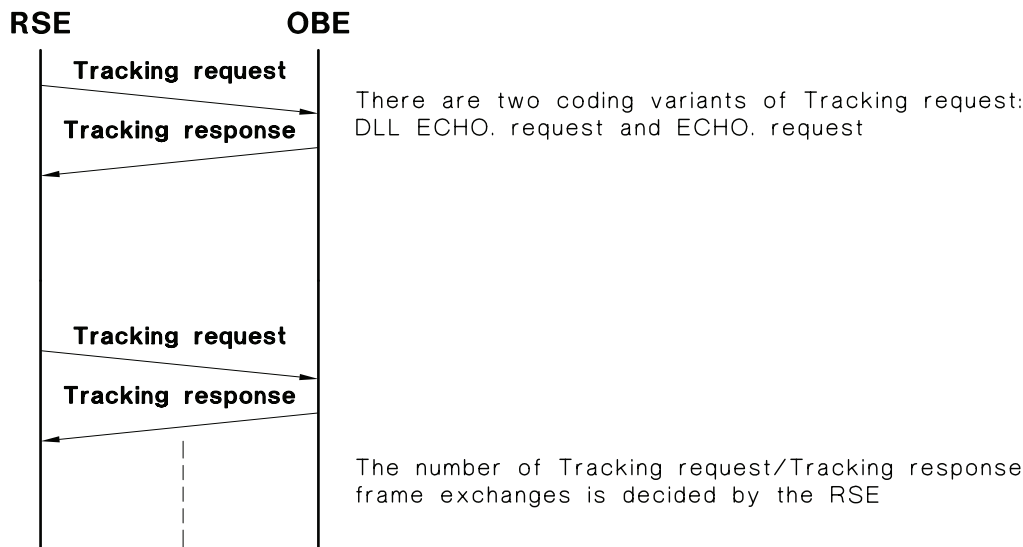


FIGURE 5.2 FRAME EXCHANGE IN THE TRACKING PHASE

5.2.4.3 Closing

Closing is an explicit release of an OBE from a DSRC communication. All RSE support Closing in order to release OBE that do not support the Profiles/applications offered by the RSE.

Closing is an optional part of an EFC Transaction. Closure is actioned after the Application Phase unless the Tracking Phase is present. The RSE logic determines whether it executes Closing after the Application Phase or after Tracking dependent upon whether the Type A or B equipment (refer to Appendix A or B) is present and the Tag is still in the Detection Zone.

As shown in Figure 5.3 the Event_Report request requires no answer from the OBE.

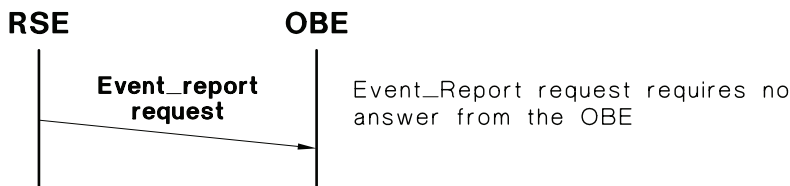


FIGURE 5.3 FRAME EXCHANGE IN THE CLOSING PHASE

5.3 EFC Data

5.3.1 General

In the OBE data are stored for either read and/or write access. Both types of access may be controlled by certain security means. Addressing of data is done via the Element Identifier EID and attributeID as defined in ISO 14906:2003 and EN 12834. An EID is unique within a certain OBE. An attributeID is unique within a certain EID.

5.3.2 EFC Context Mark Data

Equipment compliant with this document shall maintain the following data arrangements for the EFC Context Mark data issued in the VST.

Country Code:	Always Australia (796) ₁₀
IssuerID:	Issued by the Registration Authority
Type of Contract:	For each IssuerID, TypeOfContract shall increment in value as the Operator introduces a new Transaction version into the ETC system.
Context Version:	Used to Track Key Generations for Security, incrementing each time a new Key Ref or Generation is installed.

The EFC Context Mark supplies to the RSE sufficient information for the RSE to select Type A or B transactions defined in Appendix A or Appendix B.

NOTE: Appendix F lists the range of numbers for each State, and allocated IssuerID Numbers.

5.3.3 Common EFC Data

Equipment compliant with this document has the following EFC (Table 5.1 and 5.2) data available for transfer over the DSRC link. Recognized EFC Transactions transfer at least these data. Additional data may be transferred for local usage.

Note that in Table 5.1 only value ranges are specified. The coding of data may differ among recognized EFC Transactions.

There is no impact on AttributeID for VehicleClass for the Type A Transaction.

TABLE 5.1
PERSONALIZATION DATA — READ ONLY

Data element	Applicative meaning	Value range
Contract Serial Number	Number designating a centrally held account in the domain of the Issuer identified in the EFC-Context Mark. This number shall be unique for each Issuer ID.	Zero to $2^{32} - 1$
Vehicle Class	Class of Vehicle	Range 0 – 255 (refer to Appendix E)
DateOfIssue	Date when OBE was issued	Type A Transactions — represented in standard Unix Time format in 4 octets. Type B Transactions — represented in 2 octets as a binary integer (0...65535) being the number of days since 01/01/1970. For example, 0010 1011 0001 1110 = 11 038 days or 21/3/2000.

NOTE: The public VehicleClass data Attribute Number in the Type B transaction is enumerated with the value 16. This is not in conformance with the EFC Transaction Specifications as per ISO 14906:2003, and is a legacy of the MCL EFC Transaction specification where VehicleClass Attribute ID was chosen to be 16 rather than the standardized value of 17.

Hence, for the Australian context, all current and future implementations of the Dual Protocol EFC systems should use the VehicleClass Attribute Number equal to decimal 16.

It should also be noted that VehicleClass is a Read/Write Attribute in Melbourne City Link Tags, but is Read Only data in all other suppliers' Tags.

TABLE 5.2
DYNAMIC DATA — READ/WRITE

Data element	Applicative meaning	Size/Comment
Short Transaction Report	Read/Write memory area to transfer passage information from one tolling location to another. Refer to Appendix F for full data description.	6 Bytes Refer to Appendix F for Specific data formats. ShortTransactionReport is a Private Attribute for both Type A and B transactions.
ReceiptServicePart	Read/Write memory area to transfer passage information from one tolling location to another, using public Attributes.	12 Bytes. Used only in Type A Transactions Use values from Appendix F.
FlagBits	8 Flag bits available in 1 octet; Bit 2 used for Green Flag validation.	1 Byte NOTE: Green Flag when set on is used to decommission Type B tags
Reserved	Reserved for future use	1 Byte

5.3.4 MMI Codes for Tag Beeper

Codes transmitted to OBEs by the RSE to signal a transaction result shall follow the codes set down in the definition of the function SET_MMI.rq in ISO 14906:2003, as shown in Table 5.3.

Tags should emit consistent audible responses to the user when presented with the above valid Codes.

TABLE 5.3
MMI CODES

MMI value	Meaning as per ISO 14906:2003	Examples
0	OK	Transaction successful and complete
1	Not OK	Transaction could not be completed Tag blacklisted Enforcement actioned
2	Contact Operator	Operator requires tag to be returned Low Balance account User to Contact Operator

5.4 Security

Security is achieved by means of authentication. Data are transferred via the DSRC link in plain text, i.e. without encryption. The authentication code is calculated based on the DES algorithm, according to NIST SP 800-67, either single DES or triple DES. The Message Authentication Code computations based on ISO 9797-1 use a final truncation of the 8 octets result into 4 octets.

The payment transaction is secured by a two way authentication process which varies as shown in Table 5.4, depending on whether a recognized EFC Transaction A or Transaction B is invoked.

TABLE 5.4
DATA FLOW FOR TRANSACTION

Data flow	Transaction A	Transaction B
RSE reading data from OBE	No access credentials required to read data	RSE presents valid access credentials before reading data
RSE writing data in OBE	RSE presents valid MAC	RSE presents valid access credentials

The following security requirements shall be satisfied before a transaction is completed:

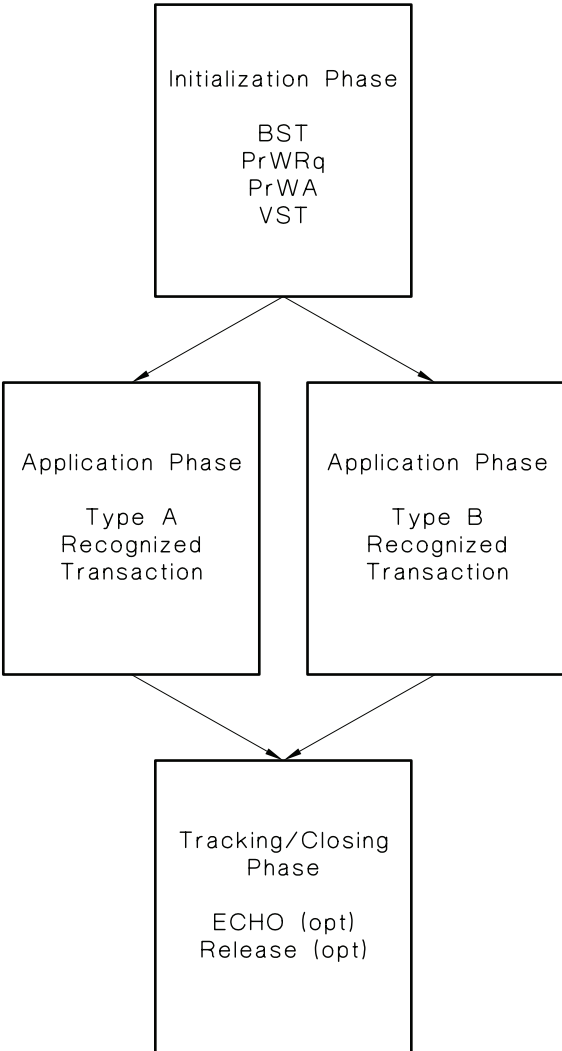
- In order to read data from a Type B OBE, the RSE shall present valid Access Credentials to the OBE.
- In order to set any data into the OBE, the RSE shall present a valid MAC (Type A) or Access Credentials (Type B) to the OBE.
- Before the RSE accepts data from the OBE, the OBE shall present a valid MAC to the RSE.

The data security scheme for both Type A and Type B EFC Transactions is described in detail in Appendices A and B respectively.

6 CODING

6.1 General

Figure 6.1 describes the structure of the Australian EFC Transaction Specification.



NOTE: Appendix A and Appendix B give details of Type A and Type B recognized transactions.

FIGURE 6.1 FLOW DIAGRAM

Tables 6.1 to 6.9 show the coding of Layer 2 frames, excluding flags and FCS. (The physical bit stream comprises the data given in the tables, plus leading Preamble and Start Flag, plus trailing FCS and End Flag.)

The number of octets are counted in the first column. The second column indicates the attribute in an ASN.1-like syntax. The third column gives the sequence of coded bits. The last column provides additional description.

6.2 Initialization Phase

6.2.1 Coding of the BST

A BST offering only one Profile and two mandatory applications, namely EFC (AID=1) and a private application (AID=29), is coded as shown in Table 6.1.

TABLE 6.1
BEACON SERVICE TABLE

Octet #	Attribute/Field	Bits in Octet b ₇ b ₀	Description
0	Broadcast LID	1111 1111	Link address for broadcast
1	MAC control field. L	1	The frame contains an LPDU
	MAC control field. D	0	Direction is down link
	MAC control field. A	1	Private Up Link Window is allocated
	MAC control field. C/R	0	Command LPDU
	MAC control field. S	S	Value irrelevant. Set to 0
	MAC control field. Reserved bits	000	Reserved
2	LLC control field. M	000	UI command
	LLC control field. P/F	0	
	LLC control field. M	00	
	LLC control field. Reserved bits	11	Not used. Always set to 11
3	Fragmentation header	1fff f001	No fragmentation. ffff ≠ 0000 and ≠ 0001
4	BST SEQUENCE	1000	INITIALIZATION.request
	{		
	OPTION indicator	0	Non mandatory applications not present
	BeaconId.ManufacturerId INTEGER (0..65535),	mmmm	(MSB) See list of manufacturers as formalized in ISO 14816
5		Mmmmm mmmmm	
6		mmmm m	
	BeaconId.IndividualId INTEGER(0..2 ²⁷ -1),	iii	(MSB) 27 bit ID available for Manufacturer
7		iiii iiii	
8		iiii iiii	
9		iiii iiii	
10	Time TimeReal	tttt tttt	(MSB) 32 bit UNIX real time
11		tttt tttt	
12		tttt tttt	
13		tttt tttt	
14	Profile INTEGER(0..127,...)	0ppp pppp	No extension, Profile p (= 0 or 1)
15	MandApplications SEQUENCE(0..127,...) OF	0000 0001	No extension, Number of MandApplications=1
	{		
16	OPTION indicator	0	EID not present
	OPTION indicator	0	Parameter not present
	AID DSRCApplicationEntityID	00 0001	No extension, AID = 1 (EFC)
	}		
	{		
17	OPTION indicator	0	EID not present
	OPTION indicator	0	Parameter not present
	AID DSRCApplicationEntityID	01 1101	No extension, AID = 29 (private)
	}		
18	Profile List SEQUENCE(0..127,...) OF	0000 0000	No extension, number of profiles in list = 0
	}		

6.2.2 Coding of the MAC Frames *PrWRq* and *PrWA*

Table 6.2 and Table 6.3 show the coding for *PrWRq* and *PrNA* respectively.

TABLE 6.2
PRIVATE WINDOW REQUEST (UP LINK)

Octet #	Attribute/Field	Bits in Octet b ₇ b ₀	Description
0	Private LID	xxxx xxx0	Link address of a specific OBE
1		xxxx xxx0	
2		xxxx xxx0	
3		xxxx xxx1	
4	MAC control field. L	0	The frame contains no LPDU
	MAC control field. D	1	Direction is up link
	MAC control field. R	1	Private Up Link Window is requested
	MAC control field. C/R	0	Command LPDU
	MAC control field. Reserved bits	0000	Reserved

TABLE 6.3
PRIVATE WINDOW ALLOCATION (DOWN LINK)

Octet #	Attribute/Field	Bits in Octet b ₇ b ₀	Description
0	Private LID	xxxx xxx0	Link address of a specific OBE
1		xxxx xxx0	
2		xxxx xxx0	
3		xxxx xxx1	
4	MAC control field. L	0	The frame contains no LPDU
	MAC control field. D	0	Direction is down link
	MAC control field. A	1	Private Up Link Window is allocated
	MAC control field. C/R	0	Command LPDU
	MAC control field. S	S	Sequence bit. Set to 0 for absolute first allocation to this LID
	MAC control field. Reserved bits	000	Reserved

6.2.3 Coding of a VST

A VST containing two applications, one with an Application-Context Mark for EFC (AID=1, containing an EFC-Context Mark plus a Contract Serial Number) and one for a private application (with AID=29₁₀, containing a 6-Byte private Application Context Mark), is coded as shown in Table 6.4.

TABLE 6.4
VEHICLE SERVICE TABLE

Octet #	Attribute/Field	Bits in Octet b ₇ b ₀	Description
0	Private LID	xxxx xxx0	Link address of a specific OBE
1		xxxx xxx0	
2		xxxx xxx0	
3		xxxx xxx1	
4	MAC control field. L	1	The frame contains a LPDU
	MAC control field. D	1	Direction is up link
	MAC control field. R	0	Private Up Link Window is not requested
	MAC control field. C/R	0	Command LPDU
	MAC control field. Reserved bits	0000	Reserved
5	LLC control field. M	000	UI command
	LLC control field. P/F	0	
	LLC control field. M	00	
	LLC control field. Reserved bits	11	Not used. Always set to 11.
	Fragmentation header	1fff f001	No fragmentation, ffff.PDU number set to 0010 ₂ . (0000 ₂ . or 0001 ₂ . are invalid).
7	VST SEQUENCE	1001	INITIALISATION.response
	{		
	Fill BIT STRING (SIZE(4))	0000	Set to 0
8	Profile INTEGER(0..127,...)	0ppp pppp	No extension, profile p (0 or 1), shall match the profile used in BST
9	Applications SEQUENCE(0..127,...) OF	0000 0010	No extension, two applications
10	{		Start of first application list entry
	OPTION indicator	1	EID present
	OPTION indicator	1	Parameter present
	AIDSRCAApplicationEntityID	00 0001	No extension, AID = 1 (EFC)
11	EID	0000 0001	EID=1
12	Parameter Container	0000 0010	OCTET STRING = 2
13		0000 1010	No extension, octet string length = 10 ₁₀
14	EFC-ContextMark SEQUENCE		
	{		
	ContractProvider SEQUENCE		
	{		
	CountryCode BIT STRING(SIZE(10))	1100 0111	(MSB) 10 bit country code according to
15		00	ISO 3166-1 11 0001 1100 ₂ = 796 ₁₀ for Australia
	IssuerIdentifier INTEGER(0..16383)	ii ii ii	(MSB) 14 bits issuer identifier (operator)
16		ii ii ii ii	
17	}		
	TypeOfContract OCTET STRING (SIZE(2))	tttt tttt	(MSB) Type of contract.
18		tttt tttt	
19	ContextVersion INTEGER(0..127,...)	0vvv vv vv	No extension. Context Version
	}		
	}		

(continued)

TABLE 6.4 (continued)

Octet #	Attribute/Field	Bits in Octet b ₇ b ₀	Description
20	OCTETS 20-23 ALTERNATIVE FOR TYPE A:	rrrr rrrr	(MSB) Contract Information (Type A)
21	ContractSerialNumber BIT STRING (SIZE(32))	rrrr rrrr	
22		rrrr rrrr	
23		rrrr rrrr	
20	OCTETS 20-23 ALTERNATIVE FOR TYPE B:	rrrr rrrr	Random Number (nonce) used together with EAcKey to calculate MAC1 (Type B)
21	RndOBE (OCTET STRING (SIZE(4)))	rrrr rrrr	
22		rrrr rrrr	
23		rrrr rrrr	
24	{		Start of second application list entry
	OPTION indicator	1	EID present
	OPTION indicator	1	Parameter present
	AID DSRCAApplicationEntityID	01 1101	No extension, AID = 29 (private application)
25	EID	0000 0010	EID=2
26	Parameter Container	0000 0010	OCTET STRING = 2
27		0000 0110	No extension, octet string length = 6 ₁₀
28	(Application Context Mark for private application)	xxxx xxxx	6 Byte of private data
29		xxxx xxxx	
30		xxxx xxxx	
31		xxxx xxxx	
32		xxxx xxxx	
33		xxxx xxxx	
	}		
34	OBConfiguration SEQUENCE		
	{		
	OPTION indicator	1	OBStatus present
	EquipmentClass INTEGER(0..32767)	ccc cccc	(MSB)
35		cccc cccc	
36	ManufacturerId INTEGER(0..65535)	nnnn nnnn	(MSB)
37		nnnn nnnn	
38	OBStatus INTEGER(0..65535)	ssss ssss	Status information according to manufacturer,
39		ssss ssss	See Appendix A and B for details
	} }		

6.3 Tracking/Closing Phase

6.3.1 Tracking Variant DLL-ECHO

In this Tracking variant Tracking.request and Tracking.response are performed using DLL-ECHO-services that are coded as shown in Table 6.5 and Table 6.6.

TABLE 6.5
DDL-ECHO.REQUEST

Octet #	Attribute/Field	Bits in Octet b ₇ b ₀	Description
0	Private LID	xxxx xxx0	Link address of a specific OBE
1		xxxx xxx0	
2		xxxx xxx0	
3		xxxx xxx1	
4	MAC control field. L	1	The frame contains a LPDU
	MAC control field. D	0	Direction is down link
	MAC control field. A	1	Private Up Link Window is allocated
	MAC control field. C/R	0	Command LPDU
	MAC control field. S	S	Sequence bit.
	MAC control field. Reserved bits	000	Reserved.
5	LLC control field. N	N	ACn command. Sequence bit
	LLC control field. M	11	
	LLC control field. P/F	0	No Polling
	LLC control field. M	01	
	LLC control field. Reserved bits	11	Not used. Always set to 1.

TABLE 6.6
DDL-ECHO.RESPONSE

Octet #	Attribute/Field	Bits in Octet b ₇ b ₀	Description
0	Private LID	xxxx xxx0	Link address of a specific OBE
1		xxxx xxx0	
2		xxxx xxx0	
3		xxxx xxx1	
4	MAC control field. L	1	The frame contains a LPDU
	MAC control field. D	1	Direction is up link
	MAC control field. R	0	Private Up Link Window is not requested
	MAC control field. C/R	1	Response LPDU
	MAC control field. Reserved bits	0000	Reserved
5	LLC control field. N	N	ACn command. Sequence bit
	LLC control field. M	11	
	LLC control field. P/F	0	Final bit set to zero
	LLC control field. M	01	
	LLC control field. Reserved bits	11	Not used. Always set to 1
6	LLC status field. RRRR	0100	NR_OK - Response LSDU not requested.
	LLC status field. CCCC	0000	Command accepted