



Sistema de Identificação
Electrónica de Veículos

OBU Technical Specification

Document Name	OBU Technical Specification
File Name	OBU_Technical_Specification_v1_0.doc
Version	1.0
Date	07 October 2010
Distribution	Public

Developed by:

Organization Name	Abbreviation	Country
SIEV - Sistema de Identificação Electrónica de Veículos, S. A.	SIEV, SA	Portugal
Instituto Superior de Engenharia de Lisboa	ISEL	Portugal

With contributions from:

Organization Name	Abbreviation	Country
Via Verde Portugal	VVP	Portugal
Q-Free	Q-Free	Norway
Kapsch	Kapsch	Austria

Index

INDEX	I
FIGURE LIST	IV
TABLE LIST	V
ACRONYMS LIST	VI
1. INTRODUCTION	1
2. SYSTEM ARCHITECTURE	3
2.1 MAPPING TO OBU REFERENCE ARCHITECTURE	3
2.2 MANUFACTURERS.....	4
2.3 PROVIDERS AND ISSUERS.....	4
2.4 INFORMATION STRUCTURE	5
2.5 APPLICATIONS AND ELEMENTS	6
2.6 DE AND PROVIDERS RELATION.....	8
2.7 SECURITY STRATEGY	9
2.7.1 <i>Security level 0 (based on EN-15509)</i>	10
2.7.2 <i>Security level 1 (based on EN-15509)</i>	10
2.8 DSRC-MDR TRANSACTION PHASES.....	12
2.9 PAYMENT METHODS.....	14
2.10 PERSONALISATION	15
2.11 GENERAL MODEL FOR DE LIFECYCLE MANAGEMENT.....	15
2.11.1 <i>DE Unique Identifier</i>	15
2.11.2 <i>DE Acquisition</i>	16
2.11.3 <i>DE distribution</i>	16
2.11.4 <i>DE Lifecycle</i>	16
2.11.5 <i>Maintenance</i>	17
2.12 FOREIGN VEHICLES	17
2.13 PROVIDER EXCHANGE	17
3. OBU DSRC-MDR SPECIFICATION	18
3.1 OBU FUNCTIONAL REQUIREMENTS	18

3.1.1	<i>Installation requirements</i>	18
3.1.2	<i>Lifetime and Compatibility</i>	18
3.1.3	<i>Human Machine Interface</i>	18
3.1.4	<i>Application Data support</i>	19
3.1.5	<i>DSRC interface requirements</i>	19
3.1.6	<i>Mechanical Requirements</i>	19
3.1.6.1	Dimensions.....	19
3.1.6.2	Security.....	19
3.1.6.3	Safety	19
3.1.6.4	Marking	20
3.1.6.5	Environmental Requirements	20
3.2	APPLICATIONS AND ELEMENTS DATA	20
3.2.1	<i>Management of security keys</i>	21
3.2.2	<i>System Element (EID = 0)</i>	21
3.2.3	<i>Electronic Fee Collection application (AID = 1)</i>	22
3.2.3.1	Electronic Fee Collection element (EID = 1, AID = 1, security level 0)	24
3.2.3.2	Electronic Fee Collection element (EID = 2, AID = 1, security level 1)	26
3.2.4	<i>Automatic Vehicle Identification (AID=11)</i>	29
3.2.4.1	Electronic Registration Identification element (EID = 3, AID = 11, security level 1).....	29
3.2.5	<i>An open specification for DE personalisation</i>	32
3.2.5.1	The Personalisation strategy.....	32
3.2.5.2	Personalisation requirements.....	33
3.2.5.3	Changing Attribute Values (RO/RW).....	34
3.2.5.4	Switching elements off.....	34
3.3	TRANSACTION MODELS	34
3.3.1	<i>Transaction Model for EFC (using EID = 1, AID = 1, security level 0)</i>	34
3.3.2	<i>Transaction Model for EFC (using EID = 2, AID = 1, security level 1)</i>	35
3.3.3	<i>Transaction Model for AVI (using EID = 3, AID = 11, security level 1)</i>	36
3.4	OBU MODULES	38

OBU Technical Specification

3.4.1	<i>Human-Machine Interface</i>	38
3.4.2	<i>Battery Measurement</i>	38
3.4.3	<i>Tamper Detection</i>	38
3.4.4	<i>Equipment Marking (including barcode)</i>	39
4.	CONCLUSION	40
	REFERENCES	41

Figure list

Figure 1 – OBUs manufacturers and providers.....	5
Figure 2 – DE information structure.	6
Figure 3 – DE information structure example.....	7
Figure 4 – Relation between DE and Providers.	8
Figure 5 – Relation between DE and Providers in an EFC transaction.....	9
Figure 6 – DSRC frames of initialization phase.....	13
Figure 7 – DSRC frames of presentation phase.	13
Figure 8 – DSRC frames of receipt phase including HMI (Human Machine Interface).....	13
Figure 9 – DSRC frames of closing phase.	13
Figure 10 – Example of DSRC complete transaction.....	14
Figure 11 – Open unified personalisation strategy for manufacturers that provides its DSRC personalisation protocol.....	33
Figure 12 – Open unified personalisation strategy for manufacturer that provides a software component.	33

Table list

Table 1 – Typical DSRC-MDR transaction phases (adapted from [EFC AID]).....	12
Table 2 – System Element Overview (EID = 0).....	21
Table 3 – System Element Factory Default Values (EID = 0).	21
Table 4 – EN15509 Security Level 0 Element Overview (EID = 1).....	24
Table 5 – EN15509 Security Level 0 Element Default Values (EID = 1).	25
Table 6 – EN15509 Security Level 0 Element VST Parameter (EID = 1).....	26
Table 7 – EN15509 Security Level 1 Element Overview (EID = 2).....	27
Table 8 – EN15509 Security Level 1 Element Default Values (EID = 2).	27
Table 9 – EN15509 Security Level 1 Element VST Parameter (EID = 2).....	28
Table 10 – ERI Element Overview based on [ERI No] (EID = 3).	29
Table 11 – ERI Element Default Values (EID = 3).....	30
Table 12 – ERI Element VST Parameter (EID = 3).	31
Table 13 – Transaction Model for EFC (using EID = 1, AID = 1, Security Level 0).....	35
Table 14 – Transaction Model for EFC (using EID = 2, AID = 1, Security Level 1).....	35
Table 15 – Transaction Model for AVI (using EID = 3, AID = 11, Security Level 1).	36
Table 16 – Buzzer sounds.....	38

Acronyms list

AID	Application Identifier
AVI	Automatic Vehicle Identification
CTK	Configuration Transport Key
DE	Dispositivo Electrónico (OBU, as referred to in Portuguese laws and regulations) Dispositivo Electrónico de uma Entidade de Cobrança de Portagens
DECP	(OBU with personalised contract with an ECP, as referred to in Portuguese laws and regulations) Dispositivo Electrónico de Matrícula
DEM	(OBU and Vehicle Electronic License Device, as referred to in Portuguese laws and regulations) Dispositivo Temporário
DT	(OBU with temporary validity, and anonymous, as referred to in Portuguese laws and regulations) Dispositivo de Detecção e Identificação Electrónica
DDIE	(Road Side Equipment, as referred to in Portuguese laws and regulations)
DSRC	Dedicated Short Range Communication
EAK	Element Access Key Entidade de Cobrança de Portagens
ECP	(Toll Collection Issuer or Provider, as referred to in Portuguese laws and regulations)
EETS	European Electronic Toll Service
EFC	Electronic Fee Collection
EID	Element Identifier
ERI	Electronic Registration Identification
HMI	Human Machine Interface
ICT	Information and Communication Technology
IMTT	Instituto da Mobilidade e dos Transportes Terrestres, I. P.

	(Public Institute for Mobility and Land Transport)
ISEL	Instituto Superior de Engenharia de Lisboa (High Institute of Engineering of Lisbon)
LDR	Low Data Rate
MDR	Medium Data Rate
MLFF	Multi Lane Free Flow
MMI	Man Machine Interface
MTTF	Mean Time To Failure
OBE	On Board Equipment
OBU	On Board Unit
PISTA	Pilot on Interoperable Systems for Tolling Applications
RSE	Road Side Equipment
RSU	Road Side Unit
SAM	Secure Access Module
SIEV	Sistema de Identificação Electrónica de Veículos (Portuguese Vehicle Electronic Registration System)
SIEV, SA	SIEV - Sistema de Identificação Electrónica de Veículos, SA (Public company responsible for managing SIEV)
VST	Vehicle Service Table

1. Introduction

According to the Portuguese laws establishing SIEV (*Sistema de Identificação Electrónica de Veículos*) and the overall DE (*Dispositivo Electrónico*) framework¹, a DE is the equipment to be installed on board of a vehicle for toll payment purposes (and eventually other private services), commonly known as OBU (On Board Unit) or OBE (On Board Equipment) and based on 5.8GHz DSRC (Dedicated Short Range Communication) technology.

This document refers only to the OBU DSRC-MDR (Medium Data Rate) specification and does not include the specification of the current Via Verde OBU DSRC-LDR (Low Data Rate). Nevertheless, according to Portuguese laws and regulations, the OBU DSRC-LDR can be used as a DE device as well. Thus, from this point forward, “OBU” refers only to OBU DSRC-MDR, and when “DE” is referred the current Via Verde OBU DSRC-LDR is also considered.

This document aims to present the technical description and specification of the DE considering the following main issues:

- System Architecture of the DE framework;
- OBU functional requirements;
- OBU’s information structure (applications/elements);
- Transaction Models;
- Security strategy;
- Life cycle management;
- Others issues.

The document presents an overview of the DE framework architecture and the required information for DE manufacturers and distributors, including issues related to the final customer. It is a reference regulation document for the stakeholders involved in DE framework, such as: Manufacturers, Providers, Toll Chargers and SIEV, SA (*SIEV - Sistema de Identificação Electrónica de Veículos, SA*).

¹ Decree-Laws nº111/2009, nº112/2009 and nº113/2009, all dated 18th May 2009, as altered by Law nº46/2010, dated 7th September.

The DE and the RSE (Road Side Equipment) also identified as RSU (Road Side Unit) are both addressed, though the RSE will be described in detail in another technical document.

The DE framework defined in Portuguese laws and regulations, managed by SIEV, SA, involves a non-mandatory (although promoted) use of the DE for toll payment purposes and eventually other private services. Note that, at the choice of the owner, the DE can be converted (logically) into a DEM (Dispositivo Electrónico de Matrícula), which in fact is a DE that is also an electronic license registration. Nevertheless, the use of the DEM is limited by law to the payment of tolls and other services, since presently a national electronic vehicle registration obligation does not exist.

The DE technical specification, leaded and sponsored by SIEV, SA, has been enhanced with contributions from different stakeholders and the technical support from ISEL (*Instituto Superior de Engenharia de Lisboa*). The current version follows already closed applicable standards for EFC (Electronic Fee Collection) and, in the case of AVI/ERI (Automatic Vehicle Identification/ Electronic Registration Identification), an adapted version of [ERI No] was considered, even though for future use only, so that presently adopted OBUs are able to comply with eventual future requirements, namely if decided at European level.

Furthermore, when applicable, the EETS (European Electronic Toll Service) discussions were considered and given the lack of closed standards at European interoperability level, an evolving approach was adopted to cope with upcoming developments on Pan-European tolling and road-pricing and service payment policies.

2. System Architecture

This chapter aims to provide an overview of the system architecture of the overall DE framework, both for people that are not fully familiar with DSRC technology and for experts. It will consider issues related to:

- Manufacturer (like: Kapsch, Q-Free, ...);
- Provider/Issuer (like: Via Verde, ...);
- Toll Charger/Operator/Concessionaire (like: Brisa, Ascendi, ...);
- User (vehicle-owner, driver,...);
- DE lifecycle management;
- DE specific features supporting different services;
- Security and privacy issues;

The privacy is one of the main concerns and will deserve a special attention considering its importance for citizen confidence. One important strategy to follow is to adopt what is named Privacy by Design that advocates an integrated approach to privacy considering i) the ICT (Information and Communication Technology) systems; ii) business practices / organizational processes of the involved stakeholders; and iii) physical technology infrastructure.

2.1 Mapping to OBU reference architecture

Generally speaking, the introduction of OBU may have implications in many aspects from vehicle to the information systems of the participating organizations (public and private). The automotive industry might be involved for the European objective to adopt a unified approach to AVI (Automatic Vehicle Identification). In a foreseen future, the vehicles might embed a transponder configured for a specific customer during vehicle acquisition process and accessible for automatic identification in a diversity of contexts like:

- Identification in tolled roads;
- Police authorities (automatic radio frequency identification);
- Vehicle inspection;
- Other services: parking lots, gas stations, etc.

These contexts establish different applications with specific requirements and as a base for a Pan-European interoperability, considering both interactions with the OBU on-board system and a mechanism offering a similar facility as nowadays exists associated to the telecom roaming. This last aspect requires an open framework able to allow a diversity of stakeholders (private and public) in each country to participate in services on behalf of or in collaboration with the original service provider (customer contractor).

Furthermore, other important aspect is the role of the regulation authorities in their responsibility to guarantee quality of service, identification integrity and privacy, besides the moderation of cost policies.

2.2 Manufacturers

The OBU can be supplied by different manufacturers, as long as their products are approved by SIEV, SA. In order to be approved they must comply with the requirements and specifications defined by SIEV, SA (the OBU Technical Specification presented in this document). The OBU models can be submitted for approval by manufacturers and providers.

2.3 Providers and Issuers

A Provider is identified in Portuguese regulations as a toll collection Issuer or Provider or *Distribuidor Grossista*. The Provider is responsible for supplying the OBUs to the market (directly or through distribution agents authorized by SIEV, SA), assuring that they comply with the present Technical Specification. Via Verde Portugal will be a Provider under the DE framework, continuing its previous activities as a provider of the private Via Verde OBU DSRC-LDR scheme. Nevertheless, the DE framework and this Technical Specification consider the possibility of other new Providers being authorized.

Portuguese laws and regulations also define the Contract Provider or Contract Issuer or ECP (*Entidade de Cobrança de Portagens*), who is responsible for establishing the collection relation between the Toll Chargers (concessionaires/operators) and the DE owners. Any Provider should also be an ECP. At least one of the ECPs will act as a special payment entity, with financial responsibilities related to the post-payment method to be offered in MLFF (Multi Lane Free Flow, without any manual or self-service payment lanes).

Therefore, competing OBU manufacturers can supply different Providers with SIEV, SA approved OBUs in Portugal (see Figure 1).

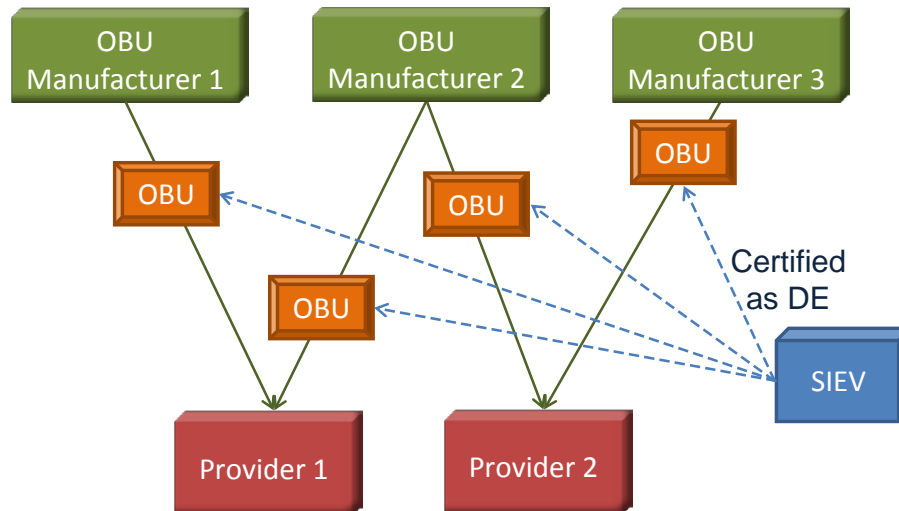


Figure 1 – OBUs manufacturers and providers.

Besides toll collection, an ECPSIEV, SA can offer other optional services that might be associated to the use of the DE. The regulation² of Providers and ECPs is out of the scope of this specification.

2.4 Information structure

According the ISO-14906 DSRC standard OBU's information structure is organized in applications with an associated unique identification (AID). Each application must have at least one element with an associated unique identifier (EID). Each element is organized in a number of attributes each one answering to specific application requirements.

The OBU structure includes also a system application with a single system element with specific attributes that are of manufacturer's responsibility (see Figure 2).

For the personalisation process, each element is secured through an EAK (Element Access Key) or a similar security method.

² Portaria nº314-B/2010, 14 June 2010, and Portaria nº1033-C/2010, 6 October 2010.

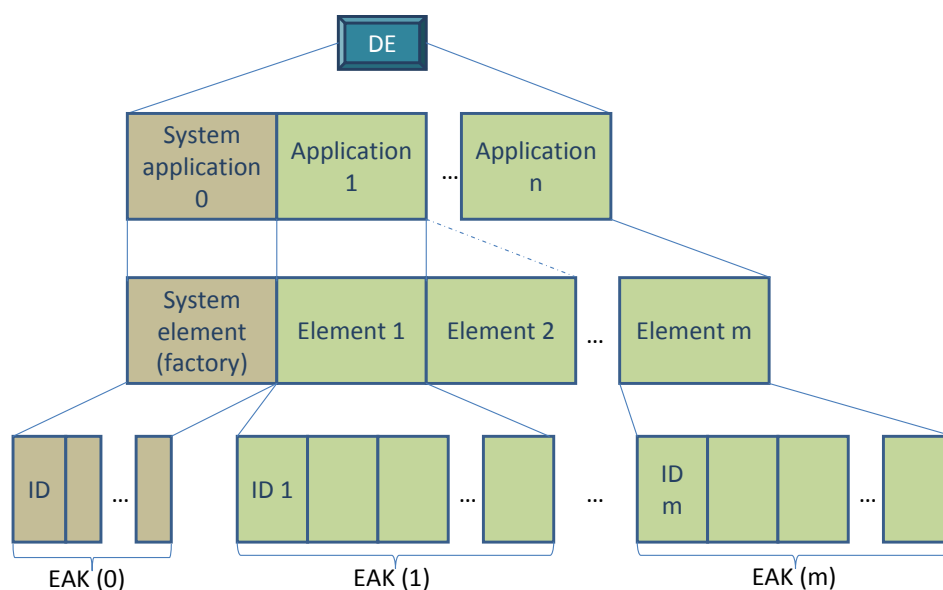


Figure 2 – DE information structure.

In Chapter 3, further detail on the information stored in the OBU is presented.

2.5 Applications and elements

The two applications adopted by SIEV, SA (Figure 3) for the implementation of DE system are:

- Automatic Vehicle Identification (AVI);
- Electronic Fee Collection (EFC).

The DE AVI application, based on [ERI No], for Portugal is based on three attributes: **ManufacturerID**, **CSI IssuerSerialNumber** and **Private1 (VehicleClass)** (vehicle toll class), from the unique associated element. The DE AVI application consists on a subset of the already defined attributes and a set of private ones. This application will be exclusively accessed by authorities (police and other authorized entities) under security level 1, as it guarantees authentication of both OBU and RSE (DDIE *(Dispositivo de Detecção e Identificação Electrónica)* according to the Portuguese law terminology). This application is for future use only, so that presently adopted OBUs are able to comply with eventual future requirements, namely if decided at European level.

The EFC application will be used for tolling, parking and gas stations payment, and for other electronic collection services, in line with the current uses of Via Verde OBU DSRC-LDR already offered services.

The EFC application, based on EN 15509, is defined as having two elements, one for security level 0 and other for security level 1. Although a change in the EFC application is not expected, it is a mandatory feature the inclusion of the possibility to disable/switch off element 1 (security level 0) from the EFC application. This is necessary when security level 1 is adopted locally, according to SIEV, SA's and Stakeholders' common decision and/or for Pan-European interoperability (the security framework is described further in the sub-chapter 3.2.5.4).

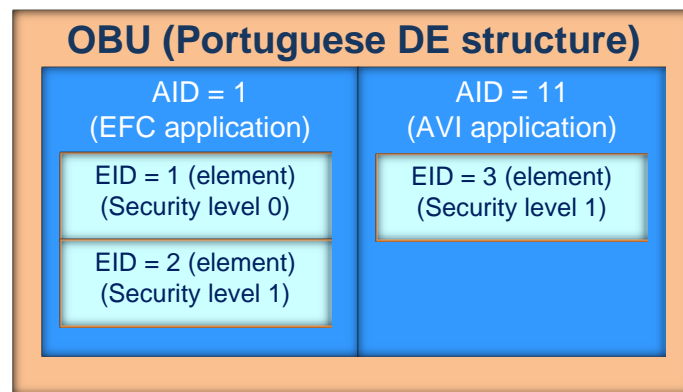


Figure 3 – DE information structure example.

Summarizing, the adopted strategy considers:

- The adoption of security level 0 for EFC, allows compatibility with current (legated) tolling services provided by Via Verde OBU DSRC-LDR scheme and interoperability with Spain as soon as an agreement is achieved. Until a complete migration from LDR OBU is finished, an open security strategy is defined for the RSE network and interactions among involved entities;
- The possibility to fully migrate to security level 1 for EFC, through a personalisation process, and disabling/switching off the EFC element 1 (security level 0). This would occur when the migration is decided, according to SIEV, SA's and Stakeholders' (Providers, TollChargers,...) common decision and/or for Pan-European interoperability (the security framework is described further in the sub-chapter 3.2.5.4);
- The immediate adoption of the AVI element (based on [ERI No]), considering security level 1.

2.6 DE and Providers Relation

In Figure 4, the relation between DEs, Toll Chargers and Providers is shown. In a road DSRC transaction, the Toll Charger identifies the DE Provider and the registered transaction is processed accordingly.

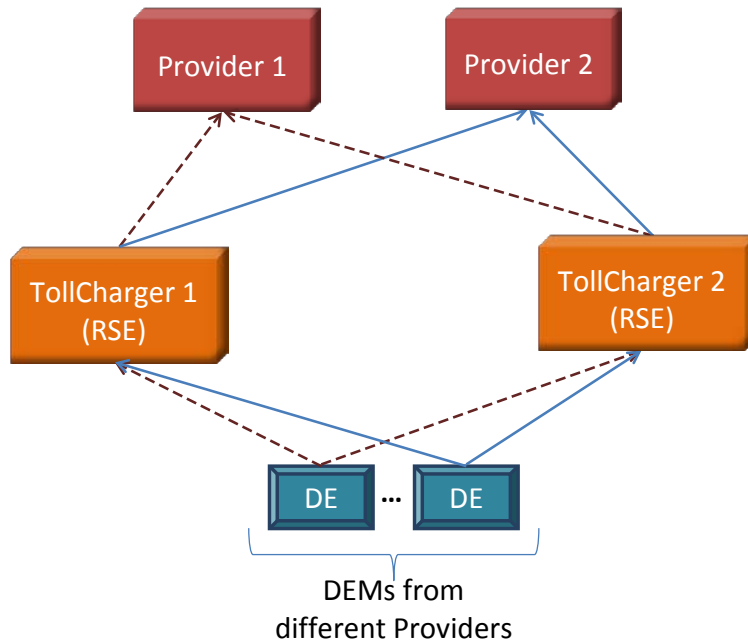


Figure 4 – Relation between DE and Providers.

The toll collection process is shown in more detail in Figure 5 where data flow for EFC transaction involving the different equipments and entities, such as DE, RSE (DDIE), Toll Charger and Provider is presented.

For each DSRC transaction, the Toll Charger identifies the DE Provider, by checking the *EFC-ContextMark* attribute of the EFC application, and processes the transaction accordingly.

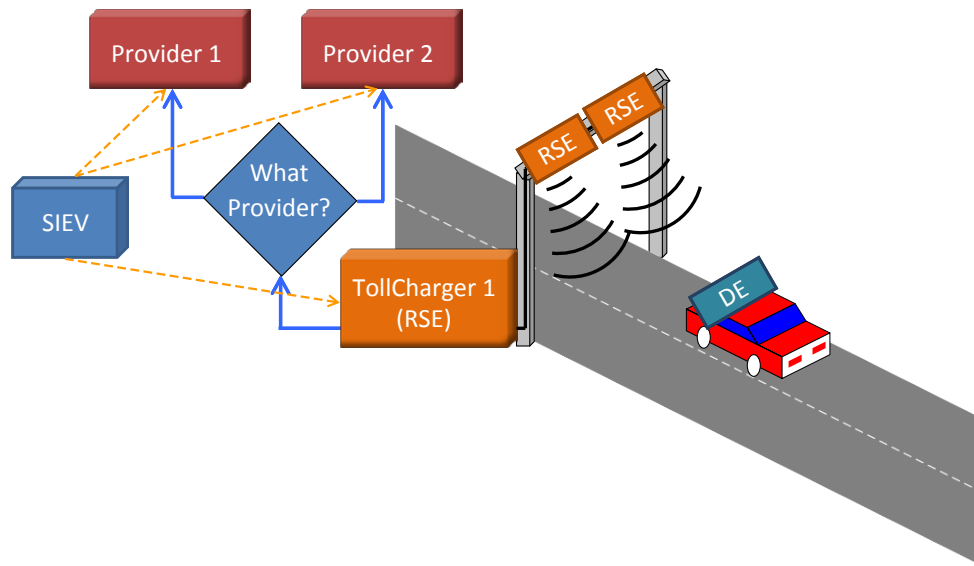


Figure 5 – Relation between DE and Providers in an EFC transaction.

Every DE has an associated Provider. It is the responsibility of Toll_Chargers (concessionaires/operators) to register the transactions based on the DE and deliver them to the respective Provider. Based on ECP’s status information, the Toll Chargers will separate transactions as having a valid DE or not, and will manage them accordingly.

2.7 Security strategy

According to EN-15509 standard for EFC and EETS Expert Group 12 (Security aspects of EETS) document, each OBU element of an application can be implemented under two security levels:

- Security level 0 – mandatory;
- Security level 1 – optional.

The security level 0, assumed as mandatory by the standard, considers the authentication of the OBU based on 8 (eight) authentication keys stored in the element implementing this security level (based on a symmetric cryptographic algorithm defined in EN-15509).

The security level 1, assumed as optional by the standard, considers, besides the OBU authentication (security level 0), the authentication of the RSE (Road Side Equipment) based on an additional access credential key. The 8 authentication keys of both element 1 and element 2 of EFC application and the access credential key of

element 2 (security level 1) are derived from master keys stored in a (SAM) Secure Access Module and generated and managed under rigorous security measures.

Each OBU security key (derived key) is generated from a unique master key. Therefore, a SAM should store the number of master keys that map to the derived ones stored in the OBUs.

The security keys stored in the OBUs are derived from master keys uniquely identified by the value of the *EFC-ContextMark* attribute. Furthermore, the derived security keys are different for each OBU, since they are generated considering unique attribute values. In sub-chapters 3.2.3 and 3.2.4.1, a specification of the key derivation process allowing a full interoperability among the involved stakeholders is presented.

2.7.1 Security level 0 (based on EN-15509)

As already explained, the security level 0 should allow the RSE (or an authentication process in a central system) to verify if the OBU is authentic. Any of the 8 authentication keys from an OBU element can be used by the RSE to authenticate the OBU. This authentication can be done using any one of the 8 key pairs (OBU derived authentication key, and the respective master key) making possible for different stakeholders to use different master keys (from the original set) to validate the OBUs.

This level is only used in the *GET-STAMPED.request* and *GET-STAMPED.response* DSRC messages. In the request, the RSE sends a key reference and, in the response using that key, OBU answers an authenticator with 4 bytes for the RSE to verify the OBU authenticity. This verification can be executed online (in real time - DSRC transaction time) or off-line. Considering that a security level 0 framework is not standardized for the RSE and its relation to central systems, a specialized specification addressing security issues will be adopted by SIEV, SA, namely following the TC278/WG1 standardisation group in order to maintain, as much as possible, the openness of the developed integrated solutions.

2.7.2 Security level 1 (based on EN-15509)

The security level 1 should allow the OBU to authenticate the RSE. In addition to the 8 authentication keys as discussed for the security level 0, this security level requires an access credential key to be associated to each element implementing security level 1.

Under this security level, the OBU will only send relevant data if the verified RSE is authentic. This is done by the OBU between the *GET-STAMPED.request*, and/or *GET.request* or *SET.request* and the OBU response (only if an authenticated RSE).





An important difference between security level 0 and 1 is that security level 1 is only executed online (in real time - DSRC transaction time). Thus, in the DSRC initialization, the RSE collects data from the OBU to know which access credential key must be used in the transaction, which is derived from the access credential master key presented in the SAM associated to the RSE. In a following transaction with another OBU, it is necessary to access again the SAM to achieve the derived key for this new OBU.

The OBU authentication (by the RSE) in security level 1 requires the utilization of the ***GET-STAMPED message*** used in security level 0 as a way to verify if the OBU is authentic.

2.8 DSRC-MDR Transaction phases

A typical DSRC-MDR transaction involves four phases, as presented in Table 1.

Table 1 – Typical DSRC-MDR transaction phases (adapted from [EFC AID]).

Phase	Icon	Short description
Initialisation		<p>“Hello, welcome, where do you come from, how do you want to pay”.</p> <p>Negotiation of the EFC contract to use.</p>
Presentation		<p>“Please give me your payment details and your entry ticket”.</p> <p>The RSE reads OBU data (details on contract, account, vehicle classification, last transaction, etc.).</p>
Receipt		<p>“Here is your receipt”</p> <p>The RSE writes an electronic receipt (which may also serve as an entry ticket).</p>
Closing		<p>“Thank you and good bye”.</p> <p>The RSE tracks the vehicle through the communication zone and eventually closes the transaction.</p>

From Figure 6 to Figure 9 different transaction phases mapped to the typical DSRC frames are shown. It is important to highlight that this is only an example of a DSRC transaction.

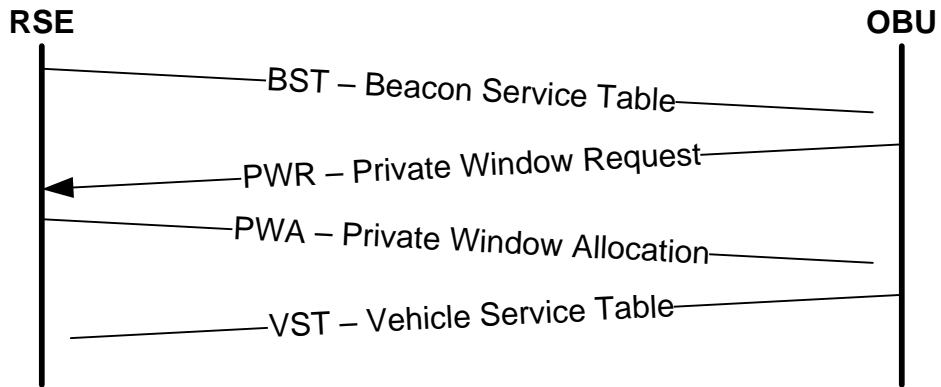


Figure 6 – DSRC frames of initialization phase.

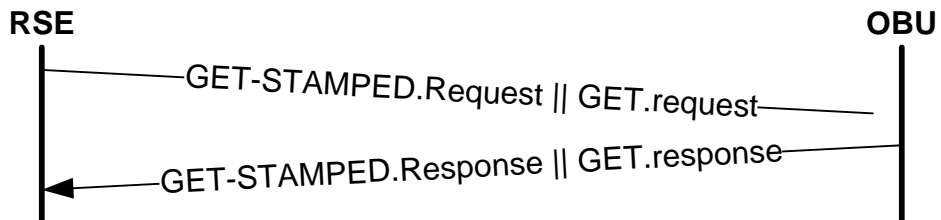


Figure 7 – DSRC frames of presentation phase.

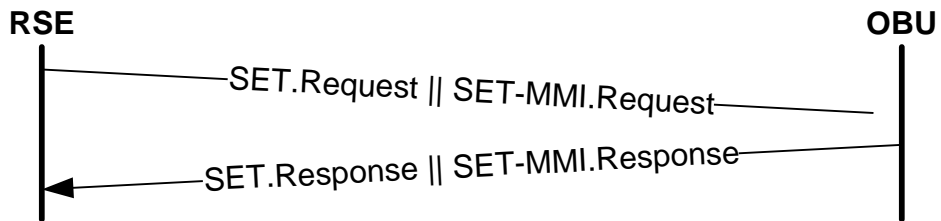


Figure 8 – DSRC frames of receipt phase including HMI (Human Machine Interface).



Figure 9 – DSRC frames of closing phase.

Different colours are used in Figure 10 to show the different phases of a DSRC transaction. The names of the frames exchanged between RSE and OBU are the same for both security levels. However, the content of the *VST* (Vehicle Service Table), *GET-STAMPED.Request*, *GET.Request* and *SET.Request* frames need additional fields in security level 1, as shown in bold and underlined in Figure 10 example.

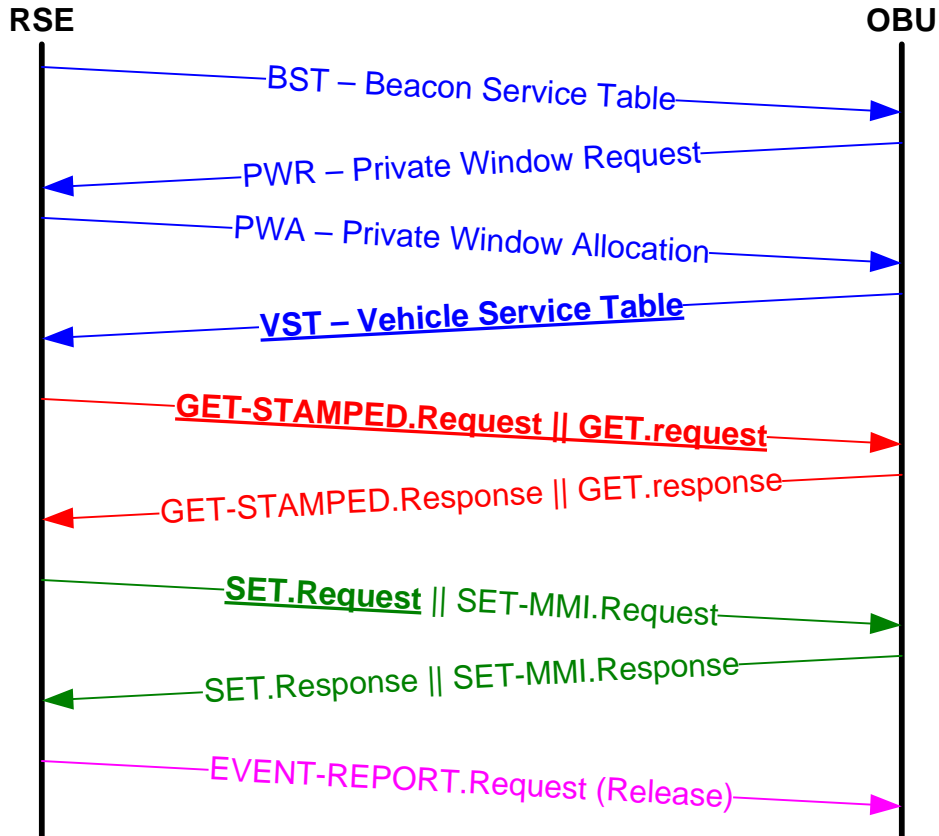


Figure 10 – Example of DSRC complete transaction.

2.9 Payment methods

The DE framework regulations define three associated payment methods for tolling:

- Bank/payment account (or credit card) debit contract;
- Pre-payment contract;
- Anonymous pre-payment.

At least one Contract Provider or ECP will support any of the above mentioned payment methods. Using the same OBU *EFC-ContextMark* attribute, a Contract Provider should be able to manage different contractual relations, based on backoffice information processing and not on the OBU's attributes.

The processes to implement these methods are out of the scope of this document.

2.10 Personalisation

The personalisation process aims to change OBUs user data after the production process. For this purpose, an open architecture and specification for the personalisation processes is adopted. This personalisation process supports the following features:

- Changing Attribute Values (RO/RW);
- Switching elements off.

This topic is described in sub-chapter 3.2.5.

2.11 General model for DE lifecycle management

2.11.1 DE Unique Identifier

The **DE unique identifier** (6 octets) is obtained by concatenating:

- *ManufacturerID* (sent in VST) 2 octets;
- Manufacturer Serial Number 4 octets.
 - (4 least significant octets from *EquipmentOBUID* which are equal to 4 least significant octets from *CSI IssuerSerialNumber*)

The value of the DE unique identifier cannot be changed/rewritten in any OBU device that has entered the DE framework, by being registered as a new DE (pre-register at IMTT (*Instituto da Mobilidade e dos Transportes Terrestres, I.P.*)).

The DE unique identifier definition for OBU DSRC-MDR must consider the existing identifiers in the Via Verde OBU DSRC-LDR domain. Therefore, a DE unique identifier must be guaranteed for both LDR and MDR transponders.

2.11.2 DE Acquisition

The OBUs purchased from the Manufacturers by the Providers must be pre-registered at IMTT by indicating, for each lot delivered, the purchased unique identifiers range. Only these pre-registered OBUs can be sold as DEs to the vehicle owners.

2.11.3 DE distribution

The distribution of the DE, through ECPs and other authorized distributors, implies that the vehicle owner will be able to freely choose between three different DEs, although all supported on the same OBU Technical Specification:

- **DECP** (*Dispositivo de uma Entidade de Cobrança de Portagens*) – a DE with a personalised contract with an ECP; can be used with bank account debit contract or prepayment contract;
- **DEM** (*Dispositivo Electrónico de Matrícula*) – a DE with a personalised contract with an ECP and associated to the vehicle's licence plate number; can be used with bank account debit contract or prepayment contract;
- **DT** (*Dispositivo Temporário*) – a DE with temporary validity, although renewable, anonymous, over-the-counter, to be used with anonymous prepayment only.

If a DEM is adopted, there will be an association of the following data:

- DE unique identifier;
- Vehicle Licence Plate Number.

A DEM database will be set up in IMTT, registering not only the DEs available for installation, but also all associations (and cancellations) of DEMs to vehicle licence plate numbers.

Any time after installing a DEM or after converting (logically) a DE into a DEM, the vehicle owner is free to convert back the DEM into a simple DE, maintaining the same OBU.

2.11.4 DE Lifecycle

The DE is property of the vehicle owner or user, and during its lifecycle can be converted (logically) into a DEM and converted back into a DE as many times as the owner wants.

The DE can be used in different vehicles during its lifecycle, but can only be used, at any given moment, in the vehicle for which it has a valid contract with an ECP.

2.11.5 Maintenance

Providers are responsible for warranty and maintenance of the DEs they supply.

2.12 Foreign vehicles

Until EETS is in place, foreign vehicles visiting Portugal must use a DE, either buying a DECP for longer stays or renting a DT for shorter stays. The logistics and distribution process of DT's for foreign vehicles – the lease of which will be managed by the Contract Providers or ECP's³ – is out of the scope of this specification.

2.13 Provider exchange

The DE framework establishes that more than one Provider can be authorized into the Portuguese market. The coexistence of two or more Providers implies the use of different EFC security keys, since they are not shared between Providers. Therefore, if the user wants to exchange Providers, he may have to purchase a new OBU device due to the lack of security key interoperability agreement between Providers and eventual device warranty loss, when the new Provider does not have any business relation with the Manufacturer of one particular device.

The Provider change process is out of the scope of this specification.

³ *Portaria* n°314-B/2010, 14 June 2010, and *Portaria* n°1033-C/2010, 6 October 2010.

3. OBU DSRC-MDR specification

This chapter details the technical aspects supported by OBU device and its relation to the different services/applications and to RSEs.

3.1 OBU Functional Requirements

This sub-chapter describes a set of minimum rules and requirements that every OBU must comply with, in order to be prepared to operate in the Portuguese market and comply with the DE framework.

3.1.1 Installation requirements

- [R1] The OBU shall be delivered with an installation manual.
- [R2] The OBU shall be delivered with a base that can be firmly attached to the windscreen.
- [R3] The OBU shall support a removal detection mechanism where removal from the base is detected and indicated to the RSE.

3.1.2 Lifetime and Compatibility

- [R4] The OBU must have a designed battery lifetime of at least 7 years before battery is depleted causing unit malfunction.
- [R5] The OBU must have a battery low voltage detection mechanism setting a status bit in the OBESstatus attribute of EID0 (system element).
- [R6] The minimum MTTF of the OBU shall be 14 years (it does not include the battery).
- [R7] The OBU must conform to ISO 14815 class A2/B3/H3.

3.1.3 Human Machine Interface

- [R8] The OBU must have a buzzer.

3.1.4 Application Data support

- [R9] The OBU must include the 3 elements specified in this document.
- [R10] The OBU must support the change (programming) of attributes' values (RO/RW) after production, through DSRC interface. This personalisation process is described in sub-chapter 3.2.5.3.
- [R11] The change (programming) of attributes' values must be independent for each application. This personalisation process is described in sub-chapter 3.2.5.3.
- [R12] The OBU must support switching off elements after production, through DSRC interface. This process is described in sub-chapter 3.2.5.4.

3.1.5 DSRC interface requirements

- [R13] The OBU shall conform to EN 12253 (DSRC L1).
- [R14] The OBU shall conform to EN 12795 (DSRC L2).
- [R15] The OBU shall conform to EN 12834 (DSRC L7).
- [R16] The OBU shall conform to EN ISO 14906 (EFC application standard).
- [R17] The OBU shall conform to EN 13372 (RTTT Profiles).
- [R18] The OBU shall conform to ISO 17264 (AVI interfaces).

3.1.6 Mechanical Requirements

3.1.6.1 Dimensions

- [R19] The physical size of the OBU shall not cause obstruction to the driver view field.

3.1.6.2 Security

- [R20] The plastic housing shall have a warranty detection mechanism giving a visible and irreversible indication if the OBU case was tampered.

3.1.6.3 Safety

- [R21] The OBU shall comply with LVD (Low Voltage Directive).

3.1.6.4 Marking

- [R22] The OBU marking shall allow for a manufacturer's product identification.
- [R23] The OBU marking shall include the WEEE (EN 50419) Trash Bin symbol.
- [R24] The OBU shall comply with the CE marking directive 93/68/EEC.
- [R25] The OBU shall allow a joint SIEV, SA/Provider's label, to be applied on the top side.

3.1.6.5 Environmental Requirements

- [R26] The OBU shall operate according to IEC 60721-3-5 Class 5K2/5B1/5C1/5S1/5F1/5M2. Considering the air temperature parameter alone, OBU must have at least an operation temperature range from -25°C to +85°C, due to the Portuguese climate.
- [R27] The OBU encapsulation shall comply with IP 40 as specified in IEC529.
- [R28] The OBU shall comply with Directive 99/5/EC R&TTE.
- [R29] The OBU shall comply with the EMC Directive 2004/108/EC.
- [R30] The OBU shall comply with EN300 674-2-2 (ERM, RTTT, DSRC).
- [R31] The OBU must comply with the WEEE directive 2002/96/EC.
- [R32] The OBU must comply with the RoHS directive 2002/95/EC.
- [R33] The OBU must comply with the Low Voltage Directive LVD 73/23/EC EN 60950-1.

3.2 Applications and elements data

This sub-chapter presents the OBU user memory factory default values. The OBU user memory is according to [IAP] organised in elements, as one System Element, two EFC elements and one ERI element.

The system element belongs to each manufacturer, however, it is defined the minimum set of required attributes used in DSRC transactions and formats.

Each element contains different attributes containing specific application data. The OBU has a set of factory default attribute values, configured according to this specification.

3.2.1 Management of security keys

The life cycle management of the security keys necessary for the EFC Application follows SIEV’s specifications and are managed by authorized ECPs. Each ECP manages their own master keysets in a key distribution centre (KDC), on the assumption that, if and when necessary, SIEV, SA can access them.

Considering the need for an integrated management for the AVI master keys, SIEV, SA will delegate its management and distribution to a SIEV, SA’s authorized and certified security entity. It is this entity’s responsibility to distribute the necessary AVI master keys for OBU production according the ECPs needs. The master keys are exchanged in a secure way according to SIEV, SA’s specific file transfer format.

The derived OBU keys for production of both EFC and AVI applications are generated by manufacturers according to this specification.

The distribution of master keys according infra-structure needs (EFC and AVI) will be detailed in specific normalization documents.

3.2.2 System Element (EID = 0)

The System Element is intrinsic to the OBU and is identified as EID = 0. The mandatory attributes for this element are presented in Table 2, once they are used in DSRC transactions. These attributes are presented in VST frame without requiring Access Credentials, even for elements with security level 1, the use of access credentials to access other attributes (if exists) of this element are optional.

Table 2 – System Element Overview (EID = 0).

Name of Attribute	Attr.ID	Type	Length (Octets)	Access rights RSE
ManufacturerID	1	Octet String	2	Read Only (RO)
EquipmentClass	3	Octet String	2	RO
OBEStatus	10	Octet String	2	RO or RW
OBEGroupID	17	Octet String	2	RO

Table 3 – System Element Factory Default Values (EID = 0).

Name of Attribute	Factory Default Data Contents ¹
ManufacturerID	00 xx
EquipmentClass	xx xx
OBEStatus	xx xx ²

Name of Attribute	Factory Default Data Contents ¹
OBEGroupID	xx xx (00 00 – 00 FF: Random generated number)

¹ All values in hexadecimal;

² It must be implemented according to [GSS], namely to Low battery and tampering flags.

3.2.3 Electronic Fee Collection application (AID = 1)

In order to allow interoperability with Europe (EETS) and in particular with Spain, 2 elements for the EFC application are defined:

- One element implementing security level 0, and
- A second element implementing security level 1.

This way, the OBU announces both elements (security level 0 and 1). This enables the interoperability, from day one, with systems that only support security level 0, as it is the case of all current services provided by Via Verde (including tolls, parking, gas stations), and the interoperability with Spain in near future. This strategy, of adopting both security level 0 and 1, allows a smooth transition of the infrastructure from the already implemented level 0 to the enhanced security level 1, which is the one expected to be adopted in pan-European interoperability (for EETS).

The attributes *ContractAuthenticator* and *VehicleAuthenticator* were added to security level 0 EFC element, to ensure data compatibility with PISTA. These attributes can be null in the OBU element, because Portuguese Providers will probably discard these data, even when a transaction is made in Spain. However, if the Provider wishes to make use of such attributes, it should define the algorithm to be used by the manufacturers in order to calculate them.

Key derivation:

- **AuthenticationKeys** → according EN15509, annex B.4.2;
- **AccessCredentialKey** → according EN15509, annex B.4.3;
- **ContractAuthenticatorKey** → Since *ContractAuthenticator* attribute can be null, SIEV will not specify the algorithm however, the Provider must notify SIEV in case it is required;

- **VehicleAuthenticatorKey** → Since *VehicleAuthenticator* attribute can be null, SIEV will not specify the algorithm however, the Provider must notify SIEV for the case it is required.
- **ElementAccessKey** → Key used for personalisation. Since each manufacturer implements its process, SIEV, SA does not define the specific key derivation process, however, it will analyse each solution at security level.

These 2 EFC elements have independent attributes values. Therefore, the same attribute can have different values associated to each element. Examples of such a situation occur with the Read/Write attributes:

- ReceiptData1;
- ReceiptData2;
- EquipmentStatus.

The following Read Only attributes must be different for both elements:

- EFC-ContextMark;
- EFC-Authentication Key1;
- EFC-Authentication Key2;
- EFC-Authentication Key3;
- EFC-Authentication Key4;
- EFC-Authentication Key5;
- EFC-Authentication Key6;
- EFC-Authentication Key7;
- EFC-Authentication Key8.

The following attributes must have the same value in both elements, even after personalisation. Therefore, the OBU manufacturer and Provider shall guarantee a process to maintain the data consistency (see also sub-chapter 3.2.5):

- VehicleLicencePlateNumber;
- VehicleClass;
- VehicleDimensions;
- VehicleAxles;

- VehicleWeightLimits;
- VehicleSpecificCharacteristics;
- EquipmentOBUID.

The following attributes can or cannot have different values for both elements, depending on the Provider requirements:

- PaymentMeans;
- EFC-Element Access Key.

The following attributes are mandatory according to EN15509 but are set with zeros according to the current specification:

- VehicleLicencePlateNumber;
- VehicleDimensions;
- VehicleAxles;
- VehicleWeightLimits;
- VehicleSpecificCharacteristics.

3.2.3.1 Electronic Fee Collection element (EID = 1, AID = 1, security level 0)

This Electronic Fee Collection (EFC) Element with EID=1 and AID=1 belongs to the EFC Provider.

The EN15509 security level 0 element has identification number EID=1. To ensure data compatibility with PISTA, the *ContractAuthenticator* and *VehicleAuthenticator* attributes were added.

Table 4 – EN15509 Security Level 0 Element Overview (EID = 1).

Name of Attribute	Attr.ID	Length (Octets)	Access Rights RSE
EFC-ContextMark	0	6	RO
ContractAuthenticator	4	5 (1+4)	RO
VehicleLicencePlateNumber	16	17	RO
VehicleClass	17	1	RO
VehicleDimensions	18	3	RO
VehicleAxles	19	2	RO
VehicleWeightLimits	20	6	RO
VehicleSpecificCharacteristics	22	4	RO
VehicleAuthenticator	23	5 (1+4)	RO

OBU Technical Specification

Name of Attribute	Attr.ID	Length (Octets)	Access Rights RSE
EquipmentOBUID	24	5 (1+4)	RO
EquipmentStatus	26	2	RW
PaymentMeans	32	14	RO
ReceiptData1	33	28	RW
ReceiptData2	34	28	RW
EFC-Authentication Key1	111	8	No Access
EFC-Authentication Key2	112	8	No Access
EFC-Authentication Key3	113	8	No Access
EFC-Authentication Key4	114	8	No Access
EFC-Authentication Key5	115	8	No Access
EFC-Authentication Key6	116	8	No Access
EFC-Authentication Key7	117	8	No Access
EFC-Authentication Key8	118	8	No Access
EFC-ElementAccessKey	XXX	XX	No Access

Table 5 – EN15509 Security Level 0 Element Default Values (EID = 1).

EID	Attr.ID	Attribute	OBU data contents ¹
1	0	EFC-ContextMark	68 4X XX XX XX XX ²
1	4	ContractAuthenticator	04 (length) + 00 00 00 00 or 04 (length) + xx xx xx xx ³
1	16	VehicleLicencePlateNumber	68 40 (Country Code + LatinAlphabetNo1) 0E (length) + 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (Licence Plate) ⁴
1	17	VehicleClass	6X ⁵
1	18	VehicleDimensions	00 00 00
1	19	VehicleAxles	00 00
1	20	VehicleWeightLimits	00 00 00 00 00 00
1	22	VehicleSpecificCharacteristics	00 00 00 00
1	23	VehicleAuthenticator	04 (length) + 30 30 30 30 or 04 (length) + XX XX XX XX ⁶
1	24	EquipmentOBUID	04 (length) + XX XX XX XX (Manufacturer Serial Number)
1	26	EquipmentStatus	00 00
1	32	PaymentMeans	II II II XX XX XX XX XX XX XX ⁷ (PersonalAccountNumber) XX XX (PaymentMeansExpiryDate) 00 00 (PaymentMeansUsageControl)
1	33	ReceiptData1	00 00
1	34	ReceiptData2	00 00
1	111	EFC-Authentication Key1	XX XX XX XX XX XX XX XX
1	112	EFC-Authentication Key2	XX XX XX XX XX XX XX XX
1	113	EFC-Authentication Key3	XX XX XX XX XX XX XX XX
1	114	EFC-Authentication Key4	XX XX XX XX XX XX XX XX

EID	Attr.ID	Attribute	OBU data contents ¹
1	115	EFC-Authentication Key5	XX XX XX XX XX XX XX XX
1	116	EFC-Authentication Key6	XX XX XX XX XX XX XX XX
1	117	EFC-Authentication Key7	XX XX XX XX XX XX XX XX
1	118	EFC-Authentication Key8	XX XX XX XX XX XX XX XX
1	XXX ⁸	EFC-ElementAccessKey	XX XX XX XX XX XX XX XX ⁸

- ¹ All values in hexadecimal;
- ² EFC-ContextMark is specified by the Provider. It must be different from the EFC-ContextMark of the other element;
- ³ If the Provider wants to define an algorithm to achieve the value for this attribute;
- ⁴ VehicleLicencePlateNumber can be personalised in the future. Considering that is not a standard format it should be used the sequence of characters (without separator character) before coding ex: 01AB23 for the Portuguese licence plate 01-AB-23. Afterwards, it is codified in LatinAlphabetNo1;
- ⁵ According to EN15509. Local vehicle class, from 1 to 5. This attribute must allow personalisation for European vehicle class according to EN15509. Therefore, this attribute must be able to have both classes and the RSE should be capable to read them;
- ⁶ If Provider desires to define an algorithm to achieve the value for this attribute;
- ⁷ According to EN ISO/IEC 7812-1, where:
- II II II: Issuer identifier number;
- XX XX XX XX XX XX XX: Account number (range specified by each Issuer) + Luhn checksum over complete PersonalAccountNumber + Fill bits;
- ⁸ The AttributeId field and octets length of EFC-ElementAccessKey depend of the manufacturer implementation.

Table 6 – EN15509 Security Level 0 Element VST Parameter (EID = 1).

Parameter	Size	Value	
EFC-ContextMark	6	68 4X XX XX XX XX	Contents of EID1 attribute 0

3.2.3.2 Electronic Fee Collection element (EID = 2, AID = 1, security level 1)

This Electronic Fee Collection (EFC) Element with EID=2 and AID=1 belongs to the EFC Provider.

OBU Technical Specification

The EN15509 security level 1 element has identification number EID=2. Access Credentials are required to access the attributes of this element, according to security level 1 of EN15509.

Table 7 – EN15509 Security Level 1 Element Overview (EID = 2).

Name of Attribute	Attr.ID	Length (Octets)	Access Rights RSE
EFC-ContextMark	0	6	RO or RO/AC
VehicleLicencePlateNumber	16	17	RO/AC
VehicleClass	17	1	RO/AC
VehicleDimensions	18	3	RO/AC
VehicleAxles	19	2	RO/AC
VehicleWeightLimits	20	6	RO/AC
VehicleSpecificCharacteristics	22	4	RO/AC
EquipmentOBUId	24	5 (1+4)	RO/AC
EquipmentStatus	26	2	RW/AC
PaymentMeans	32	14	RO/AC
ReceiptData1	33	28	RW/AC
ReceiptData2	34	28	RW/AC
EFC-Authentication Key1	111	8	No Access
EFC-Authentication Key2	112	8	No Access
EFC-Authentication Key3	113	8	No Access
EFC-Authentication Key4	114	8	No Access
EFC-Authentication Key5	115	8	No Access
EFC-Authentication Key6	116	8	No Access
EFC-Authentication Key7	117	8	No Access
EFC-Authentication Key8	118	8	No Access
EFC-Access Credential Key	120	8	No Access
EFC-Element Access Key	XXX	XX	No Access

Table 8 – EN15509 Security Level 1 Element Default Values (EID = 2).

EID	Attr.ID	Attribute	OBU data contents ¹
2	0	EFC-ContextMark	68 4X XX XX XX XX ²
2	16	VehicleLicencePlateNumber	68 40 (Country Code + LatinAlphabetNo1) 0E (length) + 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (Licence Plate) ³
2	17	VehicleClass	6X ⁴
2	18	VehicleDimensions	00 00 00
2	19	VehicleAxles	00 00
2	20	VehicleWeightLimits	00 00 00 00 00 00
2	22	VehicleSpecificCharacteristics	00 00 00 00
2	24	EquipmentOBUId	04 (length) + XX XX XX XX (Manufacturer Serial Number)
2	26	EquipmentStatus	00 00
2	32	PaymentMeans	II II II XX XX XX XX XX XX XX ⁵ (PersonalAccountNumber) XX XX (PaymentMeansExpiryDate) 00 00 (PaymentMeansUsageControl)

OBU Technical Specification

EID	Attr.ID	Attribute	OBU data contents ¹
2	33	ReceiptData1	00 00
2	34	ReceiptData2	00 00
2	111	EFC-Authentication Key1	XX XX XX XX XX XX XX XX
2	112	EFC-Authentication Key2	XX XX XX XX XX XX XX XX
2	113	EFC-Authentication Key3	XX XX XX XX XX XX XX XX
2	114	EFC-Authentication Key4	XX XX XX XX XX XX XX XX
2	115	EFC-Authentication Key5	XX XX XX XX XX XX XX XX
2	116	EFC-Authentication Key6	XX XX XX XX XX XX XX XX
2	117	EFC-Authentication Key7	XX XX XX XX XX XX XX XX
2	118	EFC-Authentication Key8	XX XX XX XX XX XX XX XX
2	120	EFC-Access Credential Key	XX XX XX XX XX XX XX XX
2	XXX	EFC-Element Access Key	XX XX XX XX XX XX XX XX ⁶

- ¹ All values in hexadecimal;
- ² EFC-ContextMark is specified by the Provider. It must be different from EFC-ContextMark of the other element;
- ³ VehicleLicencePlateNumber can be personalised in the future. Considering that is not a standard format it should be used the sequence of characters (without separator character) before coding ex: 01AB23 for the Portuguese licence plate 01-AB-23. Afterwards, it is codified in LatinAlphabetNo1;
- ⁴ According to EN15509. Local vehicle class, from 1 to 5. This attribute must allow personalisation for European vehicle class according to EN15509. Therefore, this attribute must be able to have both classes and the RSE should be capable to read them;
- ⁵ According to EN ISO/IEC 7812-1, where:
 - II II II: Issuer identifier number;
 - XX XX XX XX XX XX XX: Account number (range specified by each Issuer) + Luhn checksum over complete PersonalAccountNumber + Fill bits;
- ⁶ The AttributeId field and octets length of EFC-ElementAccessKey depend of the manufacturer implementation.

Table 9 – EN15509 Security Level 1 Element VST Parameter (EID = 2).

Parameter	Size	Value	
EFC-ContextMark	6	68 4X XX XX XX XX	Contents of EID2 attribute 0
n/a	2	02 02	Encoding, octet string length 2
AC_CR_Keyreference	2	xx xx	Contents of EID0 attribute OBEGroupID
n/a	2	02 04	Encoding, octet string length 4
RndOBU	4	xx xx xx xx	Random number

3.2.4 Automatic Vehicle Identification (AID=11)

The AVI application must implement the following (unique) element:

- Electronic Registration Identification element (EID = 3, AID = 11, security level 1) based on [ERI No].

3.2.4.1 Electronic Registration Identification element (EID = 3, AID = 11, security level 1)

This Electronic Registration Identification (ERI) element with EID=3 and AID=11 is a responsibility of the ERI issuer (SIEV, SA).

The ERI element has identification number EID=3. The *AccessCredentials* are used for EID=3. The security mechanisms include: *AccessCredential* and *Authenticationkeys* generation and associated keys diversifications.

Information about the status of the tamper detection is coded in the data element OBESatus which shall be present in the VST.

Table 10 – ERI Element Overview based on [ERI No] (EID = 3).

Name of Attribute	Attr.ID	Length (Octets)	Access Rights <i>RSE</i>
AVI-ContextMark	0	3	<i>RO or RO/AC</i>
CS1 IssuerSerialNumber	1	7	RO/AC
CS4 VehicleLicencePlateNumber	4	17	RO/AC
CS5 Vehicle Identification Number	5	17	RO/AC
Private1 (VehicleClass)	88	2 (1+1)	RO/AC
Private2	89	7 (1+6)	RO/AC
Private3	90	7 (1+6)	RO/AC
Private4	91	7 (1+6)	RO/AC
Private5	92	7 (1+6)	RO/AC
Private6	93	7 (1+6)	RW/AC
Private7	94	7 (1+6)	RW/AC
Private8	95	7 (1+6)	RW/AC
Private9	96	7 (1+6)	RW/AC
ERI-Authentication Key1	111	8	No Access
ERI-Authentication Key2	112	8	No Access
ERI-Authentication Key3	113	8	No Access
ERI-Authentication Key4	114	8	No Access
ERI-Authentication Key5	115	8	No Access
ERI-Authentication Key6	116	8	No Access
ERI-Authentication Key7	117	8	No Access
ERI-Authentication Key8	118	8	No Access
ERI-AccessCredentialKey	120	8	No Access
ERI-ElementAccessKey	XXX	XX	No Access

OBU Technical Specification

Table 11 – ERI Element Default Values (EID = 3).

EID	Attr.ID	Attribute	OBU data contents ¹
3	0	AVI-ContextMark	00 00 TT ²
3	1	CS1 IssuerSerialNumber	68 4B B9 KK KK KK KK ³ (Manufacturer Serial Number)
3	4	CS4 VehicleLicencePlateNumber	68 40 (Country Code + LatinAlphabetNo1) 0E (length) + 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (Licence Plate) ⁴
3	5	CS5 Vehicle Identification Number	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3	88	Private1 (VehicleClass)	01 6X ⁵
3	89	Private2	06 00 00 00 00 00 00 00 ⁶
3	90	Private3	06 00 00 00 00 00 00 00 ⁶
3	91	Private4	06 00 00 00 00 00 00 00 ⁶
3	92	Private5	06 00 00 00 00 00 00 00 ⁶
3	93	Private6	06 00 00 00 00 00 00 00 ⁶
3	94	Private7	06 00 00 00 00 00 00 00 ⁶
3	95	Private8	06 00 00 00 00 00 00 00 ⁶
3	96	Private9	06 00 00 00 00 00 00 00 ⁶
3	111	ERI-Authentication Key1	XX XX XX XX XX XX XX XX
3	112	ERI-Authentication Key2	XX XX XX XX XX XX XX XX
3	113	ERI-Authentication Key3	XX XX XX XX XX XX XX XX
3	114	ERI-Authentication Key4	XX XX XX XX XX XX XX XX
3	115	ERI-Authentication Key5	XX XX XX XX XX XX XX XX
3	116	ERI-Authentication Key6	XX XX XX XX XX XX XX XX
3	117	ERI-Authentication Key7	XX XX XX XX XX XX XX XX
3	118	ERI-Authentication Key8	XX XX XX XX XX XX XX XX
3	120	ERI-AccessCredentialKey	XX XX XX XX XX XX XX XX
3	XXX	ERI-ElementAccessKey	XX XX XX XX XX XX XX XX ⁷

¹ All values in hexadecimal;

² TT: Profile Version (FF for test purposes, 01 for final OBUs);

³ KK KK KK KK: Manufacturer Serial Number (least significant 4 octets of EquipmentOBUID attribute used in EFC elements);

⁴ It can be personalised in the future. Considering that is not a standard format it should be used the sequence of characters (without separator character) before coding ex: 01AB23 for the Portuguese licence plate 01-AB-23. Afterwards, it is codified in LatinAlphabetNo1;

⁵ According to EN15509. Local vehicle class, from 1 to 5. In factory, this attribute must be equal to the value present in the EFC VehicleClass attribute. This attribute must allow personalisation for European vehicle class according to EN15509. Therefore, this attribute must be able to have both classes and the RSE should be capable to read them;

⁶ Octet string type format;

⁷ The AttributeId field and octets length of ERI-ElementAccessKey depend of the manufacturer implementation.

The key derivation process is described below, and it must allow a full interoperability between different stakeholders. It includes manufacturers, namely, considering the same master keys values, the derived keys for an OBU must be the same for all RSEs independently of its manufacturer.

Key derivation:

- **ERI-Authentication Key** → Calculation of derived Authentication Key for ERI:

The ERI Authentication Key of a Key Generation k shall have a length of 8-octets and shall be derived from the 16 octets ERI Master Authentication Key as described below:

- Let the ERI Master Authentication Key for a given generation k be: ERI-MAuK(k);
- Let the derived Authentication Key for a given generation k be: ERI-AuK(k);
- Compute the 8 octets value VAL concatenating the ManufacturerID (1 byte – use of least significant byte) and CS1 (7 bytes):

$$VAL = \text{'ManufacturerID} \parallel \text{CS1'}$$

- Compute the ERI-AuK(k) for a given generation k as follows:
ERI-AuK(k) = ede [ERI-MAuK(k)] (VAL)

- **ERI-AccessKey:** → according EN15509, annex B.4.3;
- **ERI-ElementAccessKey** → Key used for personalisation. Since each manufacturer implements its process, SIEV, SA does not define the specific key derivation process, however, it will analyse each solution at security level

Table 12 – ERI Element VST Parameter (EID = 3).

Parameter	Size	Value	
AVI-ContextMark	3	00 00 TT	Data in ERI transaction phase only, ProfileVersion 01: final OBUs Profile Version FF: Test purposes
n/a	2	02 02	Encoding, octet string length 2
AC_CR_Keyreference	2	xx xx	Contents of EID0 attribute

			OBEGroupID
n/a	2	02 04	Encoding, octet string length 4
RndOBU	4	xx xx xx xx	Random number

3.2.5 An open specification for DE personalisation

An open architecture and guidelines for a manufacturer-independent personalisation, has been developed. However, considering the difficulties in generating a consensus with the two current DE suppliers, SIEV, SA considers that the content of this chapter is a convergence proposal and, until an open specification is developed and demonstrated by a reference implementation, DE suppliers are not obliged to be conforming to an open technical implementation strategy. Therefore, an open specification for DE/DSRC personalisation will be part of an independent specification to be published.

3.2.5.1 The Personalisation strategy

Considering personalisation requirements, manufacturers are invited to converge to one of the following strategies (preferably for the first one):

- Provide SIEV, SA with its proprietary DSRC personalisation specification (to be considered for the open specification development), as presented in Figure 11.
- Provide SIEV, SA with a software component (adapter) in a specific programming interface language to be integrated to support a unified personalisation application through a transparent RSE. This transparent RSE has a RS232 or other interface connection and adapts DSRC frames to the radio-frequency (DSRC 5.8GHz), as presented in Figure 12.

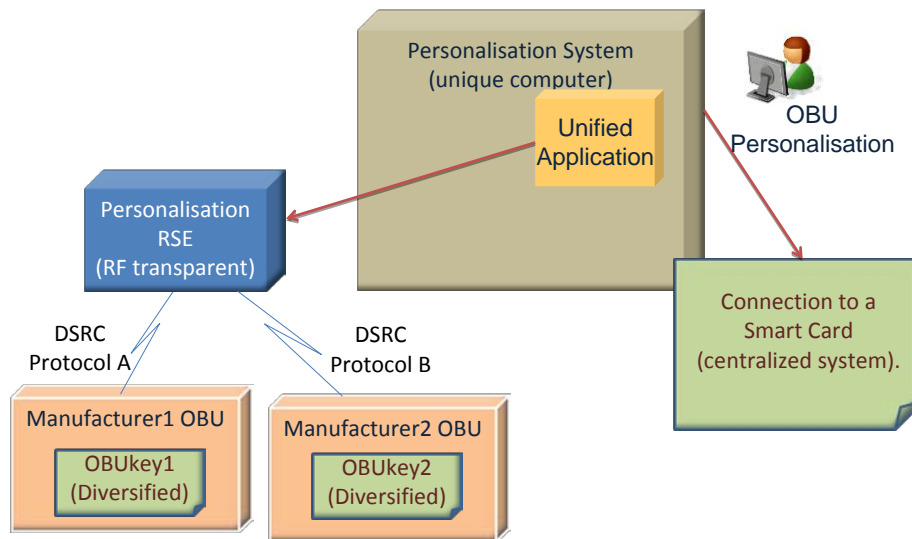


Figure 11 – Open unified personalisation strategy for manufacturers that provides its DSRC personalisation protocol.

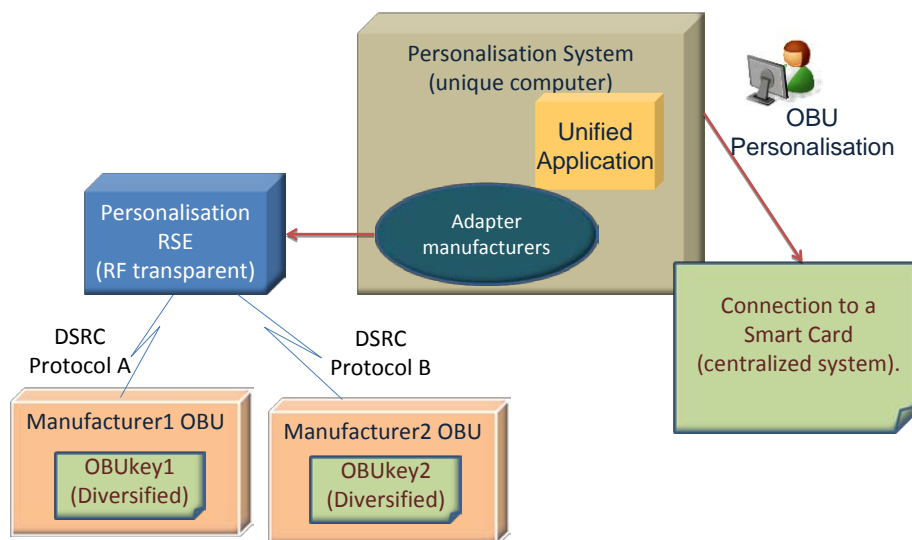


Figure 12 – Open unified personalisation strategy for manufacturer that provides a software component.

3.2.5.2 Personalisation requirements

The personalisation of data after production includes the following 2 features (described in sub-chapters 3.2.5.3 and 3.2.5.4):

- Changing Attribute Values (RO/RW);
- Switching elements off.

3.2.5.3 Changing Attribute Values (RO/RW)

The OBU must implement a personalisation process allowing programming/change of attribute values after production.

The EFC application personalisation should not change any attribute data of AVI application and vice versa.

The following attributes for both elements of EFC application must have the same values, even after personalisation:

- VehicleLicencePlateNumber;
- VehicleClass;
- VehicleDimensions;
- VehicleAxles;
- VehicleWeightLimits;
- VehicleSpecificCharacteristics;
- EquipmentOBUID.

3.2.5.4 Switching elements off

The OBU must support the switching off of elements, namely for EID1 element specified in this document. This functionality will be necessary for EFC when migrating to security level 1. The EID1 switching off process will be done in a migration process to be defined by SIEV, SA together and according with other stakeholders.

As soon as an element is switched off, it will be not included/declared in a VST frame for EFC application under an OBU-RSE transaction.

3.3 Transaction Models

3.3.1 Transaction Model for EFC (using EID = 1, AID = 1, security level 0)

In Table 13 an example is shown considering a local tolling transaction using EID1. Each Provider/Toll Charger can define the attributes to be requested by the RSE since the attributes are defined in this element, as well as, an additional **GET-STAMPED.Request** and/or **GET.Request** frames.

Table 13 – Transaction Model for EFC (using EID = 1, AID = 1, Security Level 0).

RSE		OBU
Initialisation.Request (BST)	→	
	←	Initialisation.Response (VST) <ul style="list-style-type: none"> • EFC-ContextMark <ul style="list-style-type: none"> ○ ContractProvider ○ TypeofContract ○ ContextVersion • EquipmentClass • ManufacturerID • OBESStatus
GET-STAMPED.Request <ul style="list-style-type: none"> • PaymentMeans GET.Request <ul style="list-style-type: none"> • VehicleClass • EquipmentStatus • ReceiptData1 (last) 	→	
	←	GET-STAMPED.Response <ul style="list-style-type: none"> • PaymentMeans Get.Response <ul style="list-style-type: none"> • VehicleClass • EquipmentStatus • ReceiptData1 (last)
SET.Request <ul style="list-style-type: none"> • EquipmentStatus • ReceiptData1 (last) SET-MMI.Request	→	
	←	SET.Response SET-MMI.Response
EVENT-REPORT.Request (Release)	→	

3.3.2 Transaction Model for EFC (using EID = 2, AID = 1, security level 1)

An example of a local tolling transaction using EID2 is shown in Table 14. Each Provider/TollCharger can define the attributes to be requested by the RSE since the attributes are defined in this element, as well as, an additional **GET-STAMPED.Request** and/or **GET.Request** frames.

Table 14 – Transaction Model for EFC (using EID = 2, AID = 1, Security Level 1).

RSE		OBU
Initialisation.Request (BST)	→	
	←	Initialisation.Response (VST) <ul style="list-style-type: none"> • EFC-ContextMark <ul style="list-style-type: none"> ○ ContractProvider ○ TypeofContract ○ ContextVersion • OBUGroupId • RndOBU

		<ul style="list-style-type: none"> • EquipmentClass • ManufacturerID • OBESStatus
GET-STAMPED.Request <ul style="list-style-type: none"> • AC_CR(RndOBU, EFC-AccessKey) • PaymentMeans GET.Request <ul style="list-style-type: none"> • AC_CR(RndOBU, EFC-AccessKey) • VehicleClass • EquipmentStatus • ReceiptData1 (last) 	→	
	←	GET-STAMPED.Response <ul style="list-style-type: none"> • PaymentMeans Get.Response <ul style="list-style-type: none"> • VehicleClass • EquipmentStatus • ReceiptData1 (last)
SET.Request <ul style="list-style-type: none"> • AC_CR(RndOBU, EFC-AccessKey) • EquipmentStatus • ReceiptData1 (last) SET-MMI.Request	→	
	←	SET.Response SET-MMI.Response
EVENT-REPORT.Request (Release)	→	

3.3.3 Transaction Model for AVI (using EID = 3, AID = 11, security level 1)

In Table 15, an example of a transaction, according to [ERI No], done by authorities using EID3 is shown. The two presented attributes in the **GET-STAMPED.Request** and **GET.Request** are the minimum to be requested by the RSE, for an AVI transaction for the OBUs comply with this OBU specification. In the future, SIEV, SA can define other attributes to be requested by the RSE.

Table 15 – Transaction Model for AVI (using EID = 3, AID = 11, Security Level 1).

RSE		OBU
Initialisation.Request (BST)	→	
	←	Initialisation.Response (VST) <ul style="list-style-type: none"> • AVI-ContextMark • OBUGroupId • RndOBU • EquipmentClass • ManufacturerID • OBESStatus
GET-STAMPED.Request <ul style="list-style-type: none"> • AC_CR(RndOBU, AVI-AccessKey) • CS1 IssuerSerialNumber GET.Request	→	

<ul style="list-style-type: none"> • AC_CR(RndOBU, AVI-AccessKey) • Private1 (VehicleClass) 		
	←	GET-STAMPED.Response <ul style="list-style-type: none"> • CS1 IssuerSerialNumber Get.Response <ul style="list-style-type: none"> • Private1 (VehicleClass)
EVENT-REPORT.Request (Release)	→	

This RSE should be stand-alone for AVI and must provide as output the following data (including for current Via Verde OBU DSRC-LDR):

- DE unique identifier 6 octets;
 It is achieved with the concatenation of:
 - ManufacturerID (sent in VST) 2 octets;
 - Manufacturer Serial Number 4 octets;
 (4 least significant octets from CS1 IssuerSerialNumber)
- Private1 (VehicleClass) 1 octet.

3.4 OBU MODULES

The OBU must include the modules described in this sub-chapter.

3.4.1 Human-Machine Interface

The Human-Machine Interface is a buzzer controlled through the *ACTION.Set-MMI* RSE/DSRC message from an RSE to an OBU. The sound is generated by eight audible signals in timeslots of 100 milliseconds (B indicates beep, 0 indicates silence):

Table 16 – Buzzer sounds.

Action code	Action	Beep Sequence
0	OK:	B B 0 0 0 0 0 0
1	NOK:	B 0 B 0 B 0 B 0
2	Contact Operator:	B B B 0 0 B B B
255	No Signalling	0 0 0 0 0 0 0 0

For a single lane with a feedback light, the buzzer will not sound, therefore, RSEs in this lane type must set the noSignalling (255) in *SetMMIRq*.

For MLFF (Multi Lane Free Flow) RSEs must set OK (1) in *SetMMIRq* for transactions that occur without problems. If any fault occurs (low battery, for example) the RSEs should set the noSignalling (255) in *SetMMIRq*.

3.4.2 Battery Measurement

The Battery Measurement module in the OBU reports the battery status in the OBESStatus attribute from System Element, according to [GSS].

The RSE reads the battery status from the VST frame.

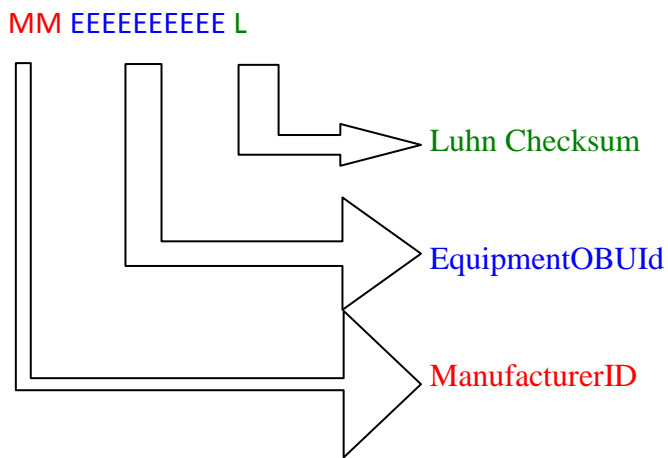
3.4.3 Tamper Detection

The information about the tamper detection mechanism status is coded in the OBESStatus attribute from System Element, according to [GSS].

The RSE reads the tamper status from the VST frame.

3.4.4 Equipment Marking (including barcode)

The OBU is identified during production with a printed line of text and a numeric (each digit from 0 to 9) bar code (MM EEEEEEEEEEE L) directly on the plastic case with the following information:



The local Vehicle Class should be identified on the plastic case of the OBU through a sticker.

4. Conclusion

This document presents the technical specification regarding OBU DSRC-MDR approved by SIEV, SA in the DE framework context.

It provides the information necessary for the OBU manufacturing process, topics on its lifecycle management, and relevant aspects from the DE architecture viewpoint.

The specification was developed by SIEV, SA with technical support from ISEL. It received valuable contributions from manufacturers, Q-Free and Kapsch, and from Via Verde Portugal.

This OBU specification establishes the requirements that OBUs must fulfil to be accepted as DE transponders, according to Portuguese laws and regulations.

Besides the special situation of the existing Via Verde DSRC-LDR OBU, this specification considers as complying any DSRC-MDR OBU that fulfils all requirements.

The information regarding the RSE (Road Side Equipment) will be described in detail in a separate technical specification.

References

- [AVI No] EN ISO 14816 Road Traffic and Transport Telematics (RTTT) – Automatic Vehicle and Equipment Identification – Numbering and Data Structures.
- [EFC AID] EN ISO 14906 Road Traffic and Transport Telematics (RTTT) – Electronic Fee Collection – Application interface definition for dedicated short range communication.
- [EN L1] EN 12253 Road Transport and Traffic Telematics (RTTT) – Dedicated Short-Range Communication (DSRC) – Physical layer using microwave at 5.8 GHz.
- [EN L2] EN 12795 Road Transport and Traffic Telematics (RTTT) – Dedicated Short-Range Communication (DSRC) – Medium access and logical link control.
- [EN L7] EN 12834 Road Transport and Traffic Telematics (RTTT) – Dedicated Short-Range Communication (DSRC) – Application Layer.
- [EN Profiles] EN 13372 Road Transport and Traffic Telematics (RTTT) – Dedicated Short-Range Communication (DSRC) – DSRC profiles for RTTT applications.
- [ERI No] ISO17264:2009 Road Transport and Traffic Telematics (RTTT) – Automatic Vehicle and Equipment Identification - Interfaces.
- [GSS] GSS – Global Specification for Short Range Communication - The platform for Interoperable Electronic Toll Collection and Access Control – version 3.2, August 2003.
- [IAP] EN15509 Road Traffic and Transport Telematics (RTTT) – Electronic Fee Collection – Interoperability application profile for DSRC.
- [PISTA] D3.4 Pilot on Interoperable Systems for Tolling Applications IST-2000-28597.
- [AVI/ERI] ISO/FDIS 17264 Draft Standards from TC 278 - Intelligent transport systems - Automatic vehicle and equipment identification – Interfaces; Secretariat: ANSI, voting begins on: 2009-08-27 and terminates on: 2009-10-27.