

**Draft explanatory notes for the  
EN 15509 top-up specification**

Department for Transport  
Road Pricing Framework Division  
Zone 3/01  
Great Minster House  
76 Marsham Street  
London  
SW1P 4DR  
Contact Mr Mark Bosly

## Change Control

Version	Status	Date	Responsible	Nature of change
1.0	Draft	08.11.2007	Department for Transport	1 <sup>st</sup> released draft

## Contents

1 Scope .....	4
2 Normative references .....	5
3 Terms and definitions .....	5
4 Abbreviations.....	5
5 Conformance.....	5
5.1 OBU.....	5
5.1.3 DSRC L7 and EFC functions.....	5
5.1.4 Data requirements .....	5
5.2 RSE .....	6
5.2.3 DSRC L7 and EFC functions.....	6
5.2.4 Data requirements .....	6
5.2.5 Security requirements .....	6
Annex A – Data specification .....	7
Annex B – Security calculations .....	9
Annex C – ICS proforma .....	9
Annex D - IAP taxonomy and numbering.....	9
Annex E – Security computation examples.....	9
Annex F – Security considerations.....	9
Annex G – Inter layer management .....	9
Annex H – Vehicle classification data .....	9
Annex I – Using this standard .....	9
Annex J – Mounting guidelines for OBU.....	9

## **Introduction**

These explanatory notes are intended to supplement the draft EN 15509 top-up specification published by the DfT.

### **1 Scope**

The draft EN 15509 top-up specification and the various underlying standards are limited in scope to technical requirements. These explanatory notes set those technical requirements in context by outlining air interface requirements for DSRC EFC applications. Like the EN 15509 top-up specification, these explanatory notes mirror the structure of EN 15509. They are proposed as a means of delivering interoperable DSRC EFC applications, subject to further refinement and ratification by stakeholders through the Interoperability Forum.

## 2 Normative references

No additional notes to EN 15509 or the draft EN 15509 top-up specification

## 3 Terms and definitions

No additional notes to EN 15509 or the draft EN 15509 top-up specification

## 4 Abbreviations

No additional notes to EN 15509 or the draft EN 15509 top-up specification

## 5 Conformance

### 5.1 OBU

#### 5.1.3 DSRC L7 and EFC functions

EN 15509 specifies that all SetMMIRq values defined in Annex A of EN ISO 14906:2004 shall be supported. As an example “signal ‘OK’ via buzzer” is given. To ensure that the user experience is consistent, the DfT expects them as a minimum to be equipped with a buzzer to provide feedback about transaction results.

The signalling with OBU buzzers shall be used consistently:

SetMMIRq	OBU buzzer signal	Meaning
0	1 “beep”	Charging transaction ok
1	4 “beeps”	Charging transaction not ok
2	2 “beeps”	Charging transaction ok, contact OBU issuer
255	No signal	-

The main difference between SetMMIRq (1) and (2) is that the user is still seen as compliant within the respective scheme owners rules if SetMMIRq (2) is sent (however the OBU issuer wants the user to contact him), whereas SetMMIRq (1) indicates that no charging transaction has been completed and that the user still needs to pay using a different payment channel.

Since OBUs featuring optical signals through LEDs or text displays are currently not widely distributed, the DfT does not see a need to specify details about how to implement signalling using those MMIs yet. However if operators wish to distribute such OBUs on a larger scale the subject is expected to be discussed with the DfT first.

It shall be noted that the DfT has made reference to design guidelines for safety of in-vehicle information systems [TRL project report PA3721/01]. Further a European Statement of Principles on the Design of Human Machine Interaction for in-vehicle information and communication systems (2005) exists, alongside with the results of the AIDE project. All these should be considered by OBU manufacturers and OBU issuers before introducing equipment to the market.

#### 5.1.4 Data requirements

Table 2 “Overview of the OBU EFC application” data has been adapted to reflect security level 1 and takes into account that the attributes listed all are defined and explained in depth in Annex A of the draft EN 15509 top-up specification. It shall be noted that also security related data requirements exist, which are defined in Annex A of the draft EN 15509 top-up specification, with rules related to their calculation being defined in Annex B of EN 15509.

EN 15509 does not give any indications of personalisation requirements (they are explicitly stated as outside the scope of the standard). For OBUs the minimum requirements are:

- The EFContextMark shall be defined by the OBU issuer, using an Issuer-ID assigned by the registrar (currently the DfT)
- Of the PaymentMeans, as a minimum the PersonalAccountNumber shall be encoded on the OBU
- The EquipmentOBUID shall be personalised by the OBU manufacturer; implicitly the standards also require the ManufacturerID to be set by the OBU manufacturer
- The EquipmentStatus shall be filled with '0's upon first issuing of the OBU
- Any vehicle specific attributes can be personalised at the discretion of the issuer but if personalised, they shall conform with EN 15509 and the draft EN 15509 top-up specification
- All unused fields shall be zeroed out (0'B).

Note that none of the personalisation requirements above imply that the OBU issuer has to perform the personalisation process itself for every single OBU issued. Instead it is expected that bulk orders to OBU manufacturers can be placed, stating a range of PANs to be pre-programmed in the equipment during the mass manufacturing process. However, the option to personalise OBUs is open to OBU issuers. This option has to be considered particularly when assessing the security regime. A decision has to be made by each OBU issuer if OBU manufacturers will be trusted to be given the MasterKeys for the creation of the derived AccessKey and AuthenticationKeys (derived using the PersonalAccountNumber).

## **5.2 RSE**

### **5.2.3 DSRC L7 and EFC functions**

The RSE shall use the SetMMIRq parameters according to the OBU signal interpretations, set out in section 5.1.3 of this document.

### **5.2.4 Data requirements**

Due to the requirement to support OBUs of both security levels 0 and 1, the RSE shall support OBUs transmitting ApplicationContextMark of the length of either 6 or 16 octets.

For interoperability reasons no tag issuer or scheme operator should rely on any other than the attributes listed in section 5.1.4 to be available to read out from OBUs complying with EN 15509. The use of private data attributes for charging purposes therefore shall be avoided.

### **5.2.5 Security requirements**

#### **5.2.5.1 General**

To be able to read EN 15509 security level 0 compliant OBUs from foreign issuers, the RSE needs to be able to read out OBUs supporting either of the two security levels.

Further the RSE shall be prepared to securely store (preferably within a SAM) copies of the MasterAccessKeys and MasterAuthenticationKeys made available to the RSE operator by interoperable OBU issuers.

Therefore the RSE also will need to support look-up tables for key references.

It will be subject to discussions in the Interoperability Forum whether there will be centrally issued AuthenticationKeys for operators or if it will be left to the discretion of OBU issuers. The Interoperability Forum will also ensure that the necessary regime, processes and specifications for either solution will be available.

## Annex A – Data specification

To reduce the onus of the reader comparing the updates made in the draft EN 15509 top-up specification to the underlying standard, it has been decided to replace the whole of Annex A, including table A.4 where no changes or additions have been made to EN 15509.

Before starting to operate an EFC system, tag issuers and scheme operators need to register with the Department for Transport to acquire an Issuer Identifier to use in the EFCContextMark of their OBUs.

NOTE (DSRC beacon) EFC operators who do not issue tags still need to register with the Department for Transport for obtaining an identifier (which is used by the RSE when writing the ReceiptData SessionServiceProvider data field onto the OBU).

As they are needed to calculate the AuthenticatorKeys, tag issuers need to assign PersonalAccountNumbers to their OBUs. Therefore operators need to register for an Issuer Identifier Number (IIN). ISO / IEC 7812-2 “Identification cards – Identification of issuers – Part 2: Application and registration procedures” defines the procedures to follow. Currently the Registration Authority can be contacted at:

c/o Technical Services Division c/o ISO/IEC 7812 Registration Authority  
American Bankers Association  
1120 Connecticut Avenue N. W., Suite 600  
US-Washington, DC 20036  
USA  
Tel: +1 202 663 53 12  
Fax: +1 202 828 50 57  
Email: [dsmit@aba.com](mailto:dsmit@aba.com)

Alternatively the PersonalAccountNumber may start with a “9”, followed by “826” (=the country code for UK according to ISO 3166). In that case the remainder of the number is defined by the national standards body for a country (the BSI for the UK). The procedure to register is defined in BS 7227:1990 “Procedures for the application of ISO 7812 to allocate UK Issuer Identification Numbers (UK IINs) for use on identification cards”. However as OBUs may in the future be used as payment means abroad, registering for an IIN with the ABA is seen as the preferable option.

The PaymentMeansExpiryDate should be used to limit the validity of the contract on the OBU to a reasonable timeframe. This for example could be the expected lifecycle of the battery. This is to tackle problems associated with growing numbers of “inactive” OBUs that can not be retrieved easily from their users. It also is a mechanism to limit any associated credit risk.

The PaymentMeansUsageControl is expected not to be needed by operators; however the DfT wishes to keep its eventual usage consistent across all implementations. Therefore the PaymentMeansUsageControl remains reserved for later DfT use, subject to discussions in the Interoperability Forum. The RSE may however need to support look-up tables for interpreting limitations imposed on the usage of OBUs / PaymentMeans of foreign issuers.

The VehicleLicensePlate attribute may be personalised (limiting the usage of the OBU to the vehicle carrying that VRM only) as OBU issuers may want to offer this as an extra security feature to their customers. EFC operators and their compliance processes shall not rely on the VRM to be available on OBUs.

To ensure consistent use of vehicle classification the DfT is currently reviewing the proposals of Expert Group 2 for the use of the VehicleClass attribute. This will also be subject of discussions within the Interoperability Forum. Until then the VehicleClass attribute remains reserved for later DfT use.

The intended contents of the VehicleDimensions attribute are seen to be too variable to form a suitable basis for vehicle classification. Scheme owners and compliance checks may still measure those characteristics to estimate actual vehicle class; a declaration made through the OBU however is not expected to be necessary for charge calculations. The attribute therefore shall not be used. However to comply with EN 15509, OBUs still need to make this data attribute available for later personalisation (potentially through or for foreign operators).

Similar to the VehicleDimensions, the VehicleFirstAxleHeight (part of VehicleAxles) attribute is not envisaged to be used.

The two bits for the TyreType within the VehicleAxles attribute are also not expected to be used. It is left to the OBU issuers to decide whether or not to personalise this information; if not the field shall be encoded with 00'B.

Of the VehicleWeightLimits attribute primarily the VehicleMaxLadenWeight octets are expected to be encoded on OBUs. For vehicles with a "plated" weight, the plated weight limit shall be used.

The copValue within the VehicleSpecificCharacteristics is currently not in use, it is mentioned for completeness only. EngineCharacteristics need to be defined in conjunction with the EURO value for HGVs and buses as the permitted EURO emission values may vary from engine type to engine type.

The EquipmentOBUID is only unique within a manufacturer's numbering scheme, therefore it can only be used in conjunction with the ManufacturerID from the VST to uniquely identify an OBU. It also is not within the (sole) control of the OBU issuer. OBUs may be used to store more than one EFC application, making it possible for two OBU issuers to share the same hardware platform. Accordingly, as well as for security reasons, the PersonalAccountNumber is seen as much better suited for charge allocation processing.

The first four bits of the EquipmentStatus are intended to be used for hotlisting of OBUs or similar applications for the flags. The usage will be defined by the DfT following discussions in the Interoperability Forum. The transaction counter shall be used according to EN 15509 and needs to be incremented by 1 for every charging transaction, with a rollover to '0' when its maximum value 4095 is reached and the counter needs to be increased again.

When using the ReceiptData fields for charging calculations (in closed EFC systems), scheme operators needs to consider the potential of the attributes being used by other scheme operators for different purposes as well.

Any fields not personalised shall be filled with '0's (binary) unless explicitly defined otherwise.

## **Annex B – Security calculations**

No additional notes to EN 15509 or the draft EN 15509 top-up specification

## **Annex C – ICS proforma**

Annex C has been modified to reflect the additional security requirements set out in the draft EN 15509 top-up specification

## **Annex D - IAP taxonomy and numbering**

No additional notes to EN 15509 or the draft EN 15509 top-up specification

## **Annex E – Security computation examples**

No additional notes to EN 15509 or the draft EN 15509 top-up specification

## **Annex F – Security considerations**

No additional notes to EN 15509 or the draft EN 15509 top-up specification

## **Annex G – Inter layer management**

No additional notes to EN 15509 or the draft EN 15509 top-up specification

## **Annex H – Vehicle classification data**

No additional notes to EN 15509 or the draft EN 15509 top-up specification

## **Annex I – Using this standard**

No additional notes to EN 15509 or the draft EN 15509 top-up specification

## **Annex J – Mounting guidelines for OBU**

No additional notes to EN 15509 or the draft EN 15509 top-up specification