PD CEN/TR 16152:2011

BSI Standards Publication

Electronic fee collection — Personalisation and mounting of first mount OBE

National foreword

This Published Document is the UK implementation of CEN/TR 16152:2011.

The UK participation in its preparation was entrusted to Technical Committee EPL/278, Road transport informatics.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 67647 5

ICS 35.240.60

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 May 2011.

Amendments issued since publication

Date	Text affected

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 16152

March 2011

ICS

English Version

Electronic fee collection - Personalisation and mounting of first mount OBE

Perception de télépéage - Personnalisation et installation des équipements embarqués en première monte

Elektronische Gebührenerhebung - Personalisierung und Einbau von Fahrzeuggeräten der Erstausstattung

This Technical Report was approved by CEN on 17 January 2011. It has been drawn up by the Technical Committee CEN/TC 278.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

Foreword 3

Introduction 4

1 Scope 5
1.1 Background and expected benefits of first-mount OBE 5
1.2 Personalisation concept 5

2 Normative references 6

3 Terms and definitions 6

4 Symbols and abbreviations 6

5 Context Description 7
5.1 General 7
5.2 Actors and Roles 8
5.3 Overview of Assets 10
5.4 Use cases 12
5.4.1 Initialisation: Mounting of OBE 12
5.4.2 Initialisation: Assignment of individual data 12
5.4.3 Initialisation: Assignment of vehicle data 13
5.4.4 Contracting of the OBE with the Service Provider 14
5.4.5 Enabling long range mobile communication 15
5.4.6 Change of the vehicle for the same contract 16
5.4.7 Cancellation of an existing contract 17
5.4.8 Change of the contract for the same vehicle 17
5.4.9 Normal EFC use cases: charging and enforcement 18
5.4.10 Repair and upgrade of the OBE 19
5.4.11 Change of vehicle properties 20
5.4.12 Decommissioning and replacement of the OBE 21

6 Personalisation concept 22
6.1 Overall requirements 22
6.1.1 Functional requirements 22
6.1.2 Security Requirements 26
6.2 Vehicle interface requirements and constraints 34
6.2.1 Introduction 34
6.2.2 Installation principles 35

7 Personalisation data 35
7.1 EFC Attibutes 35
7.2 OBE related data 37
7.3 Access protection information 37
7.4 Vehicle registration data 37

8 Recommendations 38

Bibliography 40

Foreword

This document (CEN/TR 16152:2011) has been prepared by Technical Committee CEN/TC 278 “Road transport and traffic telematics”, the secretariat of which is held by NEN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

Introduction

With the increased use of OBE for EFC, the need for effective distribution is growing. The OBE could potentially be integrated into the vehicle by the vehicle manufacturer as part of manufacturing process. The EETS provider (according to EC's European Electronic Toll Service business model) would in such a scenario be faced with the issue on how to personalize the data in the OBE, including the data related to the contract between him and the user. This issue is relevant for both DSRC and satellite based OBEs.

The issues addressed by the document include:

1) vehicle interfacing requirements and constraints

   a) vehicle data buses

   b) requirements and constraints from the automotive industry (e.g. in terms of electronic, mechanics…)

   c) safety

   d) security

2) personalization requirements and constraints

   a) Access to the protected data inside the OBE e.g. ContractNumber

   b) Where are the EETS and contract data located? (inside the OBE or in a smart card).

   c) Activation and deactivation of the OBE

This Technical Report is not a substitute for regulations and standards and these should always be respected and used by manufacturers.

1 Scope

1.1 Background and expected benefits of first-mount OBE

It could be foreseen that in future the DSRC OBE will be delivered by car manufacturer as a feature of the vehicle as they do today with car radio which are parts of the most sold vehicles. For the vehicle owner, the OBE supplier is the car manufacturer acting as an OEM (Original Equipment Manufacturer).

The integration of first mount OBE by car manufacturer is the only way to create a future mass market for EFC application based upon DSRC as well as GNSS/CN, as at present the integration of this type of OBEs cannot be achieved except for heavy goods vehicles. Regarding DSRC, this is also an opportunity to extend the capability of today's EFC technologies by providing increased quality of service, and possibly a greater range of services using in-vehicle electronics and resources.

1.2 Personalisation concept

The personalisation procedure is the procedure where the EFC Service Provider initialize, customise, and finally activate the EFC interoperable service to OBE, for a customer with or without existing account. Two different kinds of personalisation methods can be defined:

a) the personalisation procedure can be done "over the air". In such case, personalisation data can be encoded in the OBE by the Service Provider over a secure air-link, or

b) personalisation data can be loaded directly by the driver into the OBE or Service Provider via a personal storage media.

Theses are two fundamentally different approaches. The second method is perfectly fitted for critical initialisation data, such as encryption keys, to enable the driver to use the same EFC contract in different vehicles, and also to send personalisation data via post to a large number of customers.

In any case, the personalisation procedure shall be implemented in a practical way. It was reminded that the very large majority of Service Provider distribution networks (and related point of sales) are not suited to allow point-to-point communication with vehicles. They are suited mainly for front-desk operations such as initialisation of an account, data collection of user information, and so on.

For both methods, all access protection information, OBE contract information, shall be stored in a secure storage area within the OBE. During the personalisation procedure, any OBE and Service Provider service point will only communicate, but only further to a successful check of access rights.

The use of an air-link for personalisation purposes includes some risks with respect to the security of the EFC system. The present document addresses appropriate measures to counteract these risks. Security services such as integrity protection and authentication protocols shall be defined to prevent unauthorised access to the content of the OBE memory area retaining personalisation data. This statement of principles summarises essential aspects to be taken into account for the personalisation of OBE. These principles are valid:

a) whether the EFC system is based upon DSRC, GNSS-CN, or a combination of both technologies;

b) for permanently installed OBE;

c) for both original equipment manufacturers (first mount) and after sales permanently attached to the vehicle by OBE manufacturers.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN ISO 14906, *Road transport and traffic telematics — Electronic fee collection — Application interfaces definition for dedicated short-range communication (ISO 14906:2004)*

CEN ISO/TS 17575–1, *Electronic fee collection — Application interface definition for autonomous systems — Part 1: Charging (ISO/TS 17575-1:2010)*

ISO 11568-2, *Banking — Key management (retail) Part 2: Symmetric ciphers, their key management and life cycle*

prEN ISO 17573, *Electronic fee collection — System architecture for vehicle related tolling (ISO 17573:2010)*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
on-Board Equipment (OBE)
equipment fitted within or on the outside of a vehicle and used for toll purposes

3.2
electronic fee collection (EFC)
toll charging by electronic means via a wireless interface

3.3
roadside equipment
equipment located along the road transport network, for the purpose of communication and data exchanges with on-board equipments

3.4
Toll Charger
legal entity charging toll for vehicles in a toll domain

3.5
Toll Service Provider
legal entity providing to his customers toll services on one or more toll domains for one or more classes of vehicles

NOTE The Toll Service Provider may provide the OBE or may provide only a magnetic card or a smart card to be used with OBE provided by a third party (like a mobile telephone and a SIM card can be obtained from different parties). The Toll Service Provider is responsible for the operation (functioning) of the OBE.

4 Symbols and abbreviations

CC	Common Criteria
AID	Application Interface Definition
BST	Beacon Service Table
CESARE	Common EFC System for ASECAP Road tolling European system

DSRC	Dedicated Short-Range Communication
DTCO	Digital TaCOgraph
EAcK	Element Access Key
EAuK	Element Authentication Key
EC	European Commission
ECU	Electronic Control Unit
EID	Element Identifier
EFC	Electronic Fee Collection
HGV	Heavy Goods Vehicle
KVC	Key Verification Code
L1	Layer 1 of DSRC (Physical Layer)
L2	Layer 2 of DSRC (Data Link Layer)
L7	Layer 7 of DSRC (Application Layer)
LLC	Logical Link Control
MAC	Message Authentication Code
MEAcK	Master Element Access Key
MEAuK	Master Element Authentication Key
MMI	Man-Machine Interface
OBE	On-Board Equipment
OBU	On-Board Unit
PAN	Personal Account Number
RSE	Road-Side Equipment
T-APDU	Transfer-Application Protocol Data Unit
VST	Vehicle Service Table

5 Context Description

5.1 General

In many existing systems OBEs are delivered by the Service Provider. The process to add vehicle and service user data is normally a part of the contract between the Service Provider and the OBE manufacturer. In this situation there is one Security Domain within which full trust must exist. As it is foreseen that the OBE will be integrated with the vehicle the personalization process of the OBE must support that the OBE is mounted to the Vehicle when the personalisation takes place.

Furthermore, it is possible that different contracts issued by different Service Providers will be in place and related sets of personalisation assets implemented in the same OBE throughout its lifetime.

5.2 Actors and Roles

The following actors have been identified as actors who are related to assets related to the OBE.

a) Toll Charger. He is responsible for the collection of road usage charges on a specific part of the road infrastructure. He is interested in personalisation data as far as he needs them for the determination or checking of the charges. His special interest is in the correctness of the vehicle data and of the Service Provider identification (assuming that the Service Provider guarantees him for the payment of the fees if he can proof the usage of the road infrastructure).

b) Service Provider. He offers the EFC service to users of the road infrastructure. A user subscribing to the service will pay the fees to the Service Provider who will forward them to the appropriate toll charger according to the usage. To contribute to the determination of the road usage and the charges due, the Service Provider will operate the OBE mounted to the vehicle of the service user, after having added his personalization data to it. Anyway, the personalization data responsibility is kept by the Service Provider towards the User and the Toll Charger. His interest is that only road usages of customers having subscribed his service are charged to him and that he can assign the charges to the appropriate service user.

c) OBE Manufacturer. He produces the OBE and delivers it to the vehicle manufacturer to be mounted to a vehicle.

d) Vehicle Manufacturer. He is responsible for the integration of the OBE into the vehicle.

e) Vehicle registration authority. The involvement of this actor in the personalization of first mount OBE is to be defined. In any case it may serve as a trusted source of at least part of the vehicle data.

f) EFC service user. He subscribes to the EFC service of a Service Provider for a specific vehicle with an OBE. His interest is that he is charged only for his road usage.

g) Mobile communication provider (in case of GNSS system). He offers a wide range communication service that may be used not only during EFC, but also for personalization of the OBE. The OBE has to be initialized for the specific service before it can use the communication channel.

These actors are present in the EFC environment independent from the issue of personalisation of first mount OBE. Not all of them must have an active role in personalisation - some of them may just have a specific interest (like for instance the toll charger).

For retrofitted OBE it is usually assumed that the overall responsibility for this OBE is at the Service Provider. This also covers the responsibility for the personalisation. The Service Provider may get the OBE from the OBE Manufacturer at a stage where part of the personalisation took place already. But as soon as the Service Provider takes over the OBE, the OBE Manufacturer is not involved any more and in case there is some information needed on the personalisation or something is found to be wrong with it, the Service Provider is the actor to be addressed.

For first mount OBE the responsibilities are not that obvious. For instance the OBE may be mounted to the vehicle at a stage where there is no Service Provider. There may be several Service Providers over the OBE lifetime. The way to deal with this situation, as proposed for this technical report, is to introduce roles related to the personalisation of first mount OBE. Each role has to be assigned to an actor, but for some of the roles there are several candidates. Assigning the roles to specific actors leads to an implementation of the personalisation on the organisational level.

The following roles with no clear assignment to an actor are introduced:

h) OBE issuer. He has the overall control on the OBE lifecycle. For retrofitted OBE it is clear that the Service Provider takes this role. For first mount OBE there is no need for a Service Provider to be assigned to the OBE during the whole OBE lifetime. Therefore it has to be determined which actor takes the role of the OBE issuer. As soon as there is a valid contract for the OBE, the Service Provider is responsible towards the Toll Charger for the correct functioning of the OBE. In case he does not take himself the role of the OBE issuer from the beginning of the OBE lifetime, he has to rely on the OBE issuer to fulfil his obligations towards the Toll Charger. Therefore it is assumed that there is some contractual relation between OBE issuer and Service Provider.

i) Vehicle data issuer. He collects the relevant vehicle data of the vehicle, to which the OBE is mounted, and transfers them to the OBE. As soon as there is a valid contract for the OBE, the Service Provider is responsible towards the Toll Charger for the correctness of the vehicle data. In case he does not take himself the role of the vehicle data issuer, he has to rely on the vehicle data issuer to fulfil his obligations towards the Toll Charger. Therefore it is assumed that there is some contractual relation between vehicle data issuer and Service Provider.

j) OBE owner. This is expected to be the same as the vehicle owner, as the OBE is mounted to the vehicle at the time it is sold.

k) OBE repairer. He is contacted to repair or replace the OBE in case it does not work correctly. As soon as there is a valid contract for the OBE, the Service Provider is responsible towards the Toll Charger for the correct functioning of the OBE. In case he does not assume himself the role of the OBE repairer, he has to rely on the OBE repairer to fulfil his obligations towards the Toll Charger. Therefore it is assumed that there is some contractual relation between OBE repairer and Service Provider.

l) Mobile communication customer. He is the holder of the mobile telecommunication agreement with the Mobile Communication Provider.

Possible assignments of actors to roles shows possible assignments of roles to actors. Note that some roles can be assigned to different actors during the OBE lifetime. At any time it should be assigned only to one actor.

Table 1 — Possible assignments of actors to roles

	Toll Charger	Service Provider	OBE manufacturer	Vehicle manufacturer	Vehicle registration authority	EFC service user	Mob. comm. provider
OBE issuer		X	X	X			
Vehicle data issuer		X		X	X	X	
OBE owner		X	X	X		X	
OBE repairer		X	X	X			
Mob. comm. customer		X	X	X		X	

Currently there are too many open issues to go for a specific role assignment. Developing a concept for first mount OBE based on the roles without assigning actors to them, leaves the flexibility not to be in conflict with future decisions and local specialities.

5.3 Overview of Assets

Figure 1 below identifies different set of assets in the OBE. An asset is something that has a value to the system and needs protection measures to be taken. Examples of protection measures which might apply are authorisation before access, detection of manipulation, verification of authenticity and provision of confidentiality. In Figure 1 the different assets that are used in an EFC system are identified.

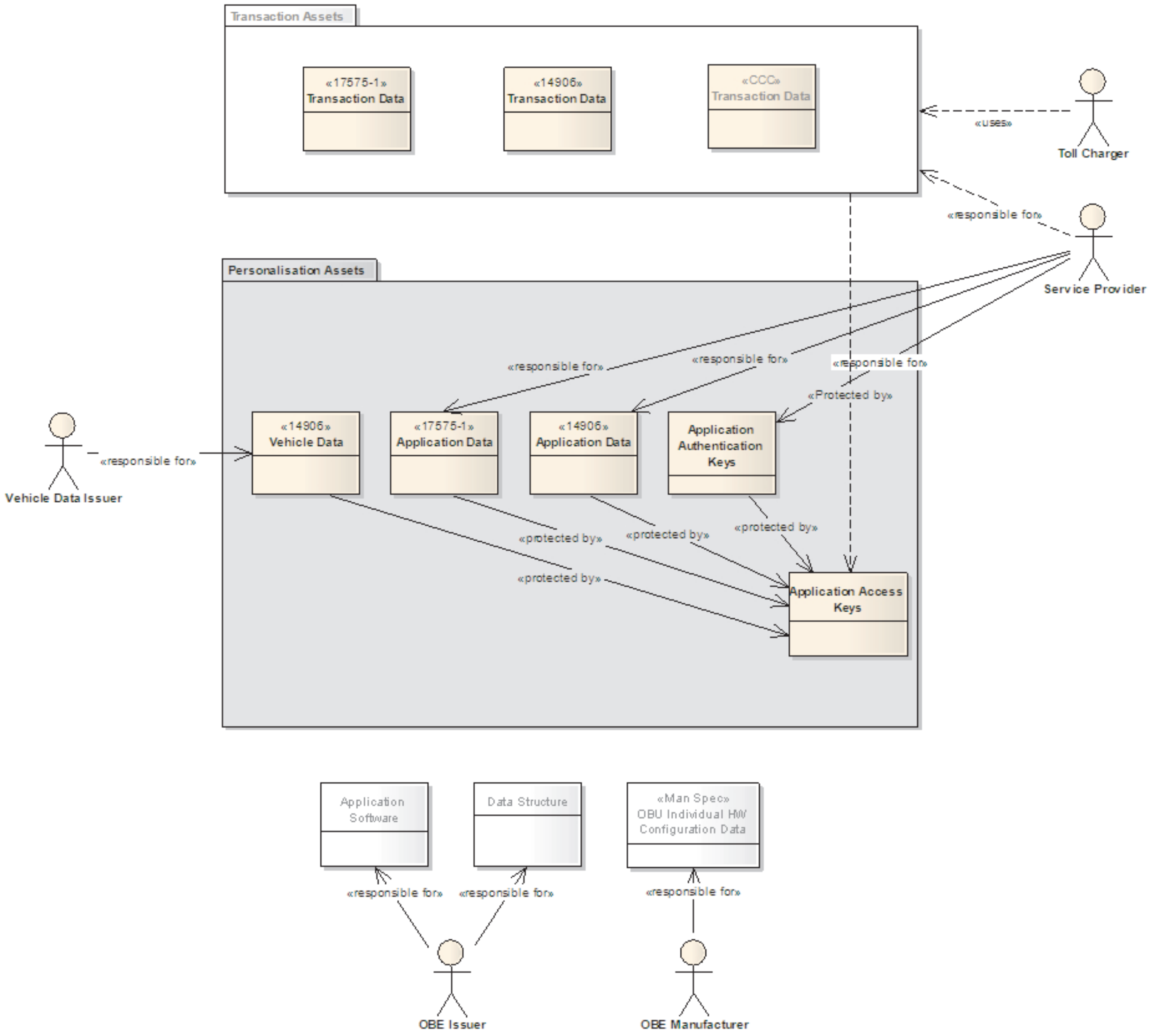

Figure 1 — Overview of Assets

The following assets exist:

a) Transaction Data Assets

b) Personalisation assets

c) OBE Manufacturer Specific Assets

The Transaction Data Assets consists of assets that are updated during a transaction e.g. when the OBE passes a DSRC station or GPS positions are received from satellites. These assets have to be taken care of during decommissioning and replacement of the OBE.

The Personalisation Assets consists of assets that are used by the Service Provider and are under his responsbility. The issue is how to enter, remove and update them in the OBE in a controlled way when the OBE has already been integrated to the vehicle. Each Service Provider might have its own set of personalisation assets that he is responsible for. The most common case up to now is that only one set of personalisation assets exists.

The Personalisation Assets consists of Application keys, Application Data and Vehicle data.

The Application keys consists of Access keys are used in service to grant access to application data Authentication keys which are used to secure the authenticity of the OBE and the data integrity of the application data assets. At personalisation of an application defined by the DSRC standard a number generation of Authentication keys may be loaded.

The Application Data consist of data that is used by the Service Provider to support a service. Example of Application data is Contract Data in CEN ISO/TS 17575-1, Payment Means and EFC Context Mark in EN ISO 14906.

Vehicle data is also part of the personalisation assets but it is reasonable that this asset is common to all applications.

The OBE Manufacturer Specific Assets are assets that are put into the OBE before integration to the vehicle. The way of adding these assets will be manufacturer specific and is outside the scope of this document. Typical examples of these assets are Data structure, Application software, physical individual calibration values and Individual IDs.

A number of roles have been identified and their responsibilities are indicated. Responsibility in this context means ensuring the correctness of the assets it is responsible for. It is foreseen that more than one Service Provider may exist.

The role of the Service Provider is defined in prEN ISO 17573. According to prEN ISO 17573 he is responsible for the operation (functioning) of the OBE. This implies that he is responsible for the correctness of the personalisation assets towards the Service user and the Toll Charger. As has been pointed out already, for first mount OBE there might exist no Service Provider at the time of personalisation. In this case entities different from the Service Provider take over the OBE personalization role. The responsibility of these entities towards the Service Provider and their contractual relation with the Service Provider is an issue to be dealt with.

It is the Service Provider who sets the access conditions and decides who shall have the possibility to read or write the assets.

The OBE issuer should have a contract with the OBE Manufacturer which allows him to put in the initial elements in the OBE which are necessary in order to personalise the OBE.

The OBE Manufacturer is responsible for adding hardware specific data to make the OBE work.

5.4 Use cases

5.4.1 Initialisation: Mounting of OBE

It is the basic assumption in this technical report that the mounting of the OBE is part of the manufacturing process of the vehicle, which means that it is done before the vehicle is delivered to the customer. The OBE may be a standard component of the vehicles of a given make, or may be an option for the customer. In any case it must be possible to mount whole series of OBE with the same hardware and software to series of vehicles.

On a technical level the mounting of the OBE includes the fixing of the OBE housings to the vehicle, if required the connection to the power supply of the vehicle, possibly the establishment of a communication link between the OBE and the vehicle electronics, the installation of a human machine interface (HMI) and the fitting of antennas for the mobile communication of the OBE (at least DSRC and long range communication). It is possible that some components of the OBE are shared with other applications, like for instance the mobile communication devices, road map data and the HMI.

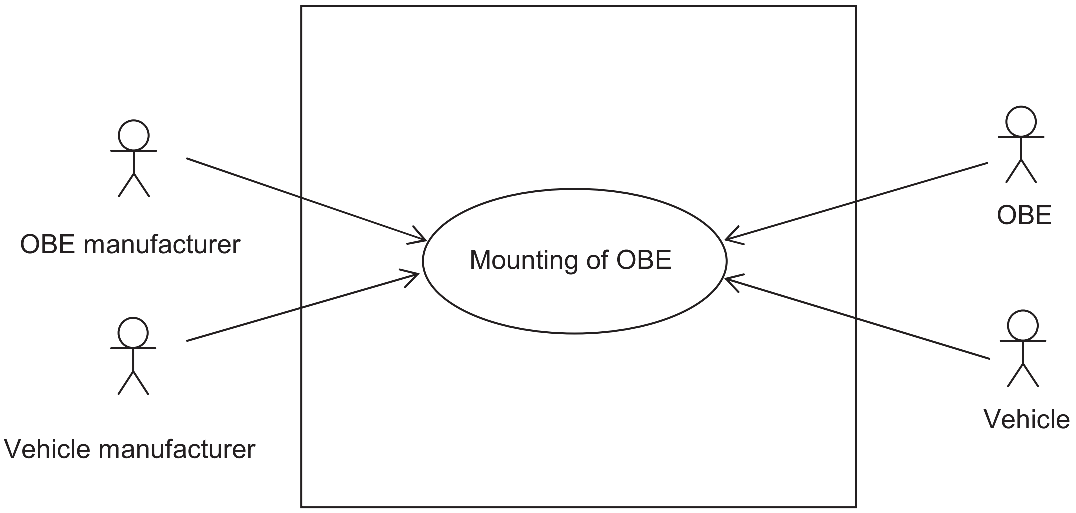

Figure 2 — Use case “Mounting of OBE” involving the OBE, the OBE manufacturer, the vehicle and the vehicle manufacturer

5.4.2 Initialisation: Assignment of individual data

Initially all OBE of a given OBE make look the same. At the final stage of the OBE mounting it must be possible to address individual OBE, which means that each OBE must have some property allowing to distinguish it from all others. Thus some individual properties have to be assigned to each OBE, like a serial number (which for instance could include the VIN of the vehicle, to which the OBE is mounted). At least some of these properties must be available when exchanging data with the OBE and therefore corresponding data have to be stored in the OBE. But in general there is also a need to centrally store data corresponding to the individual properties of each OBE, such that they can be used to record further data related to specific OBE. As a consequence, the process of assigning individual properties to an OBE includes both data storage in the OBE and at some place outside the OBE. The assignment of the individual properties is the starting point of the OBE lifetime.

The assignment of individual properties can take place before the OBE is mounted to the vehicle or afterwards. The two processes are independent from each other.

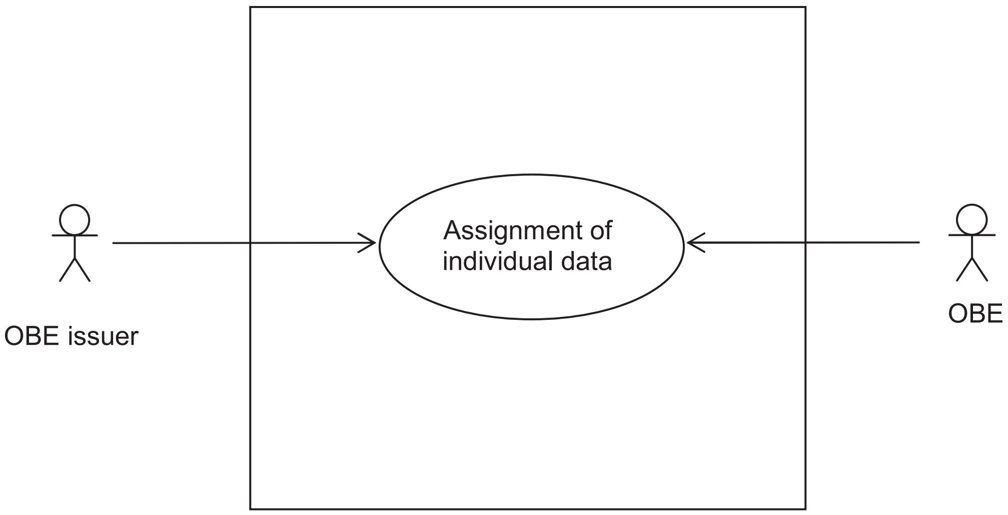

Figure 3 — Use case “Assignment of individual data” involving the OBE and the OBE issuer

5.4.3 Initialisation: Assignment of vehicle data

Each OBE is mounted to one specific vehicle. As the charging may depend on vehicle properties and identification of the vehicle may be part of the compliance checking with interrogation of the OBE (see 5.4.9), data related to the vehicle have to be available in the OBE, which means that they have to be stored there before starting the EFC process.

There is an important difference between first mount OBE and retrofitted OBE. Retrofitted OBE is assigned to one specific provider of the EFC service in the personalisation phase. It is the responsibility of this Service Provider to record the vehicle data and to make them available at the OBE in the way he uses them for the EFC service. In case of a first mount OBE, it is reasonable to consider the assignment of vehicle data as a process not necessarily involving the Service Provider. With this, the vehicle data can be assigned at an early stage when no Service Provider has been selected for the OBE.

For this reason a specific role is introduced to take the responsibility for the assignment of the vehicle data to the OBE and for the correctness of the vehicle data stored in the OBE: the vehicle data issuer. Depending on the set-up of the whole EFC organisational model this may be the vehicle manufacturer, an authority responsible for vehicle registration, the user or the first Service Provider operating the OBE.

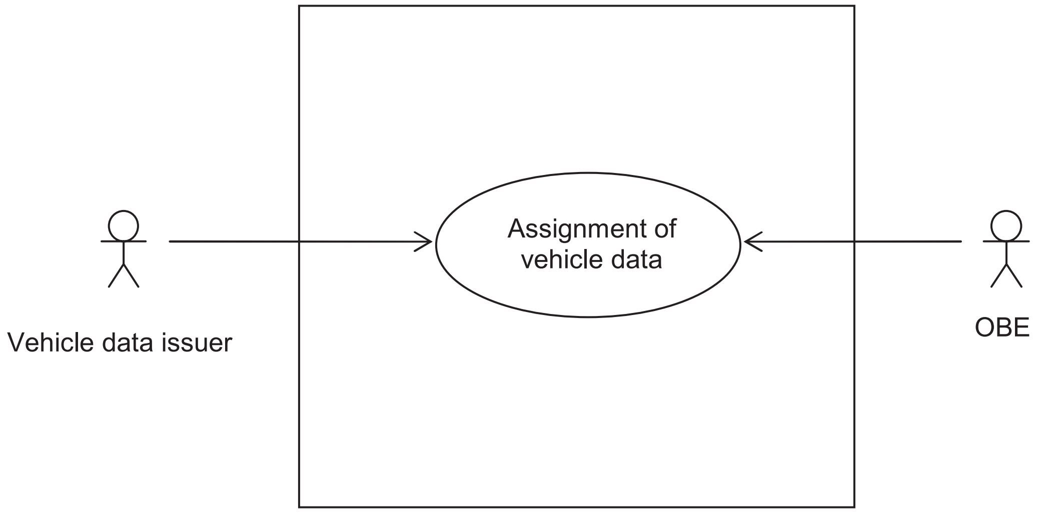

Figure 4 — The use case "assignment of vehicle data" involving the OBE and the vehicle data issuer

5.4.4 Contracting of the OBE with the Service Provider

For EFC there must be a contract between the user of the EFC service and the Service Provider (see for instance prEN ISO 17573). The contract is assigned to a specific vehicle or group of vehicles with specific OBE. Charges for a vehicle are recorded with a reference to this contract, such that the Service Provider is able to claim the payment from the appropriate user under appropriate terms. Therefore data related to the contract must be available at the OBE during the charging process as application data (see 5.3). They have to be transmitted to the OBE to enable the use of the OBE for charging.

The use case deals neither with the way the contract is established nor with the content of the contract as such. It just establishes the transfer of the contract related data to the OBE, and the transfer of the OBE or vehicle related data to the Service Provider at the contracting stage, if such a transfer is required.

As soon as the contract is valid, the OBE can start its normal EFC operation and determine fees based on the contract. From this time on the Service Provider has to guarantee the correct functioning of the OBE towards the Toll Charger. This means that within the contracting process the Service Provider has make sure that the OBE is properly manufactured and installed, that it has the right personalisation data and that it has not been changed in an inappropriate manner since its installation. For this he has to verify information that the OBE manufacturer, the OBE issuer, the vehicle data issuer and the OBE repairer have generated.

In some cases the Service Provider intends to use his own software or configuration data in the OBE. Then the download of this software or data is part of the contracting use case.

The user as a contracting party has to agree not only on the contract as such, but also on the intention to link the contract to the OBE of his vehicle. Therefore, the user is an actor in this use case, even though in some scenarios his contribution may only be modest.

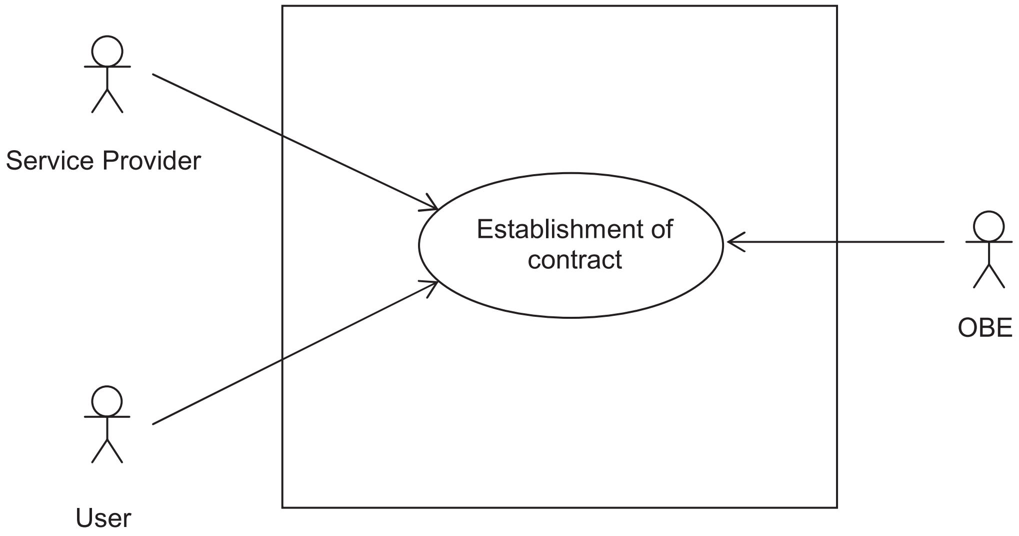

Figure 5 — The use case “Establishment of contract” involving the OBE, the Service Provider and the user

5.4.5 Enabling long range mobile communication

OBE supporting GNSS/CN based charging requires a long range mobile communication link. It is assumed that this link is enabled based on a commercial arrangement with a mobile communication provider. Data related to this agreement have to be present at the OBE, such that the payment for the use of the communication link can be managed.

It is reasonable not to invent new procedures for this use case and to introduce new technical means for it, but to use what is common in the mobile telecommunication domain (like for instance a SIM card for the agreement related data). Nevertheless the use case is relevant in the context of first mount OBE, because it interacts with the other use cases.

There are different options on who is the customer towards the mobile communication provider: it may be for instance the service user, the OBE issuer or the Service Provider. Not to prejudge a specific choice, the corresponding actor is just called mobile communication customer.

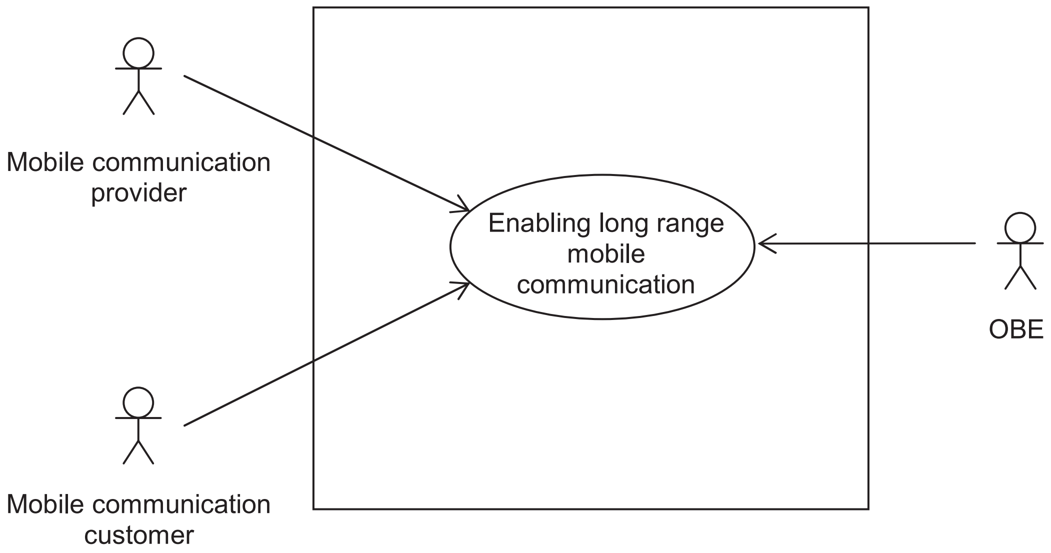
Mobile communication provider
Enabling long range mobile communication
OBE
Mobile communication customer

Figure 6 — The use case “Enabling long range mobile communication” involving the OBE, the mobile communication provider and the mobile communication customer

5.4.6 Change of the vehicle for the same contract

It is assumed that a first mount OBE stays in the same vehicle during the whole lifetime of this vehicle. If a user changes his vehicle, then there is the option that he gets a new OBE. In case he had a contract with a Service Provider assigned to the old vehicle and OBE, he might want to continue the contractual relation with this Service Provider. Of course it will be possible in any case to cancel the contract assigned to the old vehicle and OBE, and to sign a new contract for the new vehicle and OBE. But it would be practical if the Service Provider could, in some cases, offer the possibility that the old contract is kept and assigned to the new vehicle and OBE.

A seamless handover from the old OBE and vehicle to the new OBE and vehicle is crucial for this use case. As soon as the contract is assigned to the new OBE and vehicle, it must be guaranteed that it is not used any more for the old OBE and vehicle.

The use case may involve a first mount OBE for the old vehicle, for the new vehicle or for both of them.

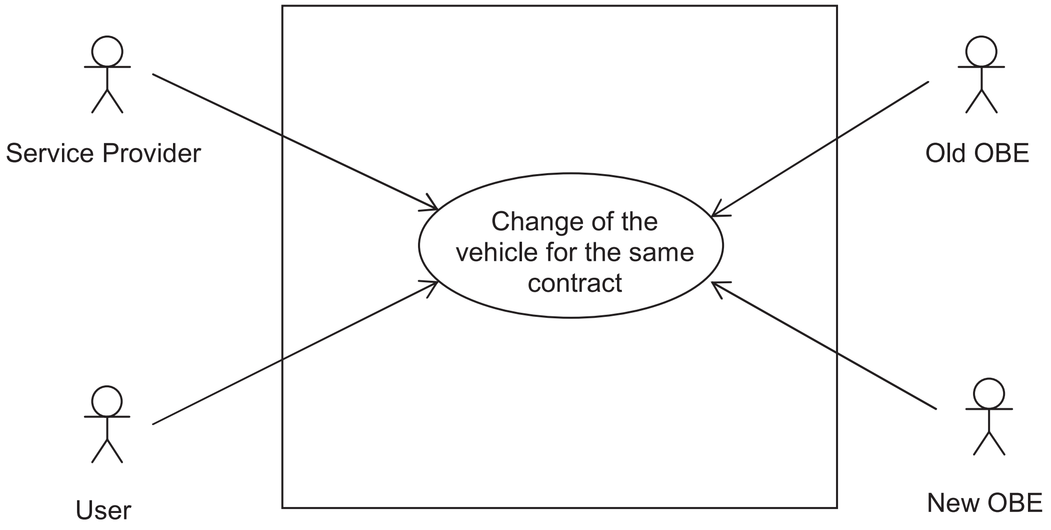

Figure 7 — The use case "Change of the vehicle for the same contract" involving the Service Provider, the user, the old and the new OBE

5.4.7 Cancellation of an existing contract

Both the Service Provider and the user may want to cancel an existing contract for a specific vehicle and OBE. It is not sufficient for them to inform the other side about the cancellation. It must be guaranteed that from the time of the cancellation on the OBE is not used any more. For this the OBE has to be involved in the use case to adapt its contract information. As long as no new contract is established, the OBE has to remain inactive. Note that the immediate replacement of the contract with a new one is covered in the next use case.

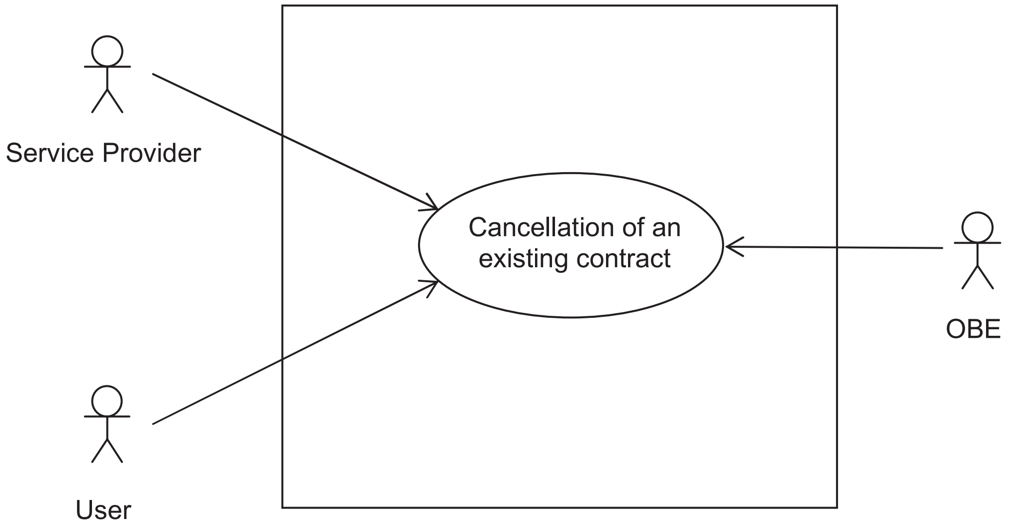

Figure 8 —The use case "Cancellation of an existing contract" involving the Service Provider, the user and the OBE

5.4.8 Change of the contract for the same vehicle

There are various reasons to change the contract with the Service Provider for the same vehicle and OBE:

a) The contract may have expired, without an option to extend its validity period;

b) The user may wish to contract with a different Service Provider;

c) The Service Provider or the user may want to switch to a contract with different contract terms;

d) The Service Provider may want to terminate the contractual relation with the user and the user has to find a new Service Provider;

e) The vehicle may have been sold to a different owner.

The use case consists of two parts: the old contract is cancelled and the new contract is established. For the OBE this means that the data related to the old contract have to be deleted or made ineffective, whereas the data related to the new contract have to be stored and prepared for use.

The actors in this use case are essentially the same as in the contracting use case (see 5.4.4), with the difference that there may be a different Service Providers and a different user for the old and new contract.

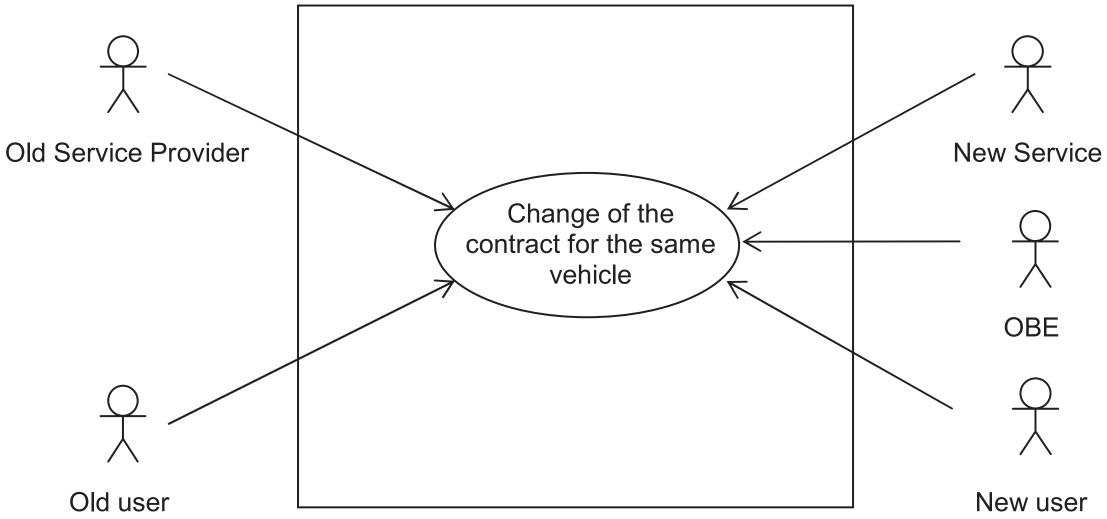

Figure 9 — Use case “Change of the contract for the same vehicle” involving the OBE, the old and new Service Provider (possibly being identical) and the old and new user (possibly being identical)

5.4.9 Normal EFC use cases: charging and enforcement

The use cases of the normal OBE operation – charging and compliance checking – are not part of the personalisation, but are listed here because they have implications for the personalisation process. Charging involves the OBE as a supplier of charging data and in some cases for the recording and processing of such data. The OBE may be interrogated to check if it complies with the intended charging process and to identify the responsible party in case of non-compliance.

The use case as such is not part of the personalisation and will not further be described. But it is relevant as it is based on the personalisation, and listed here to give a complete picture of all personalisation aspects.

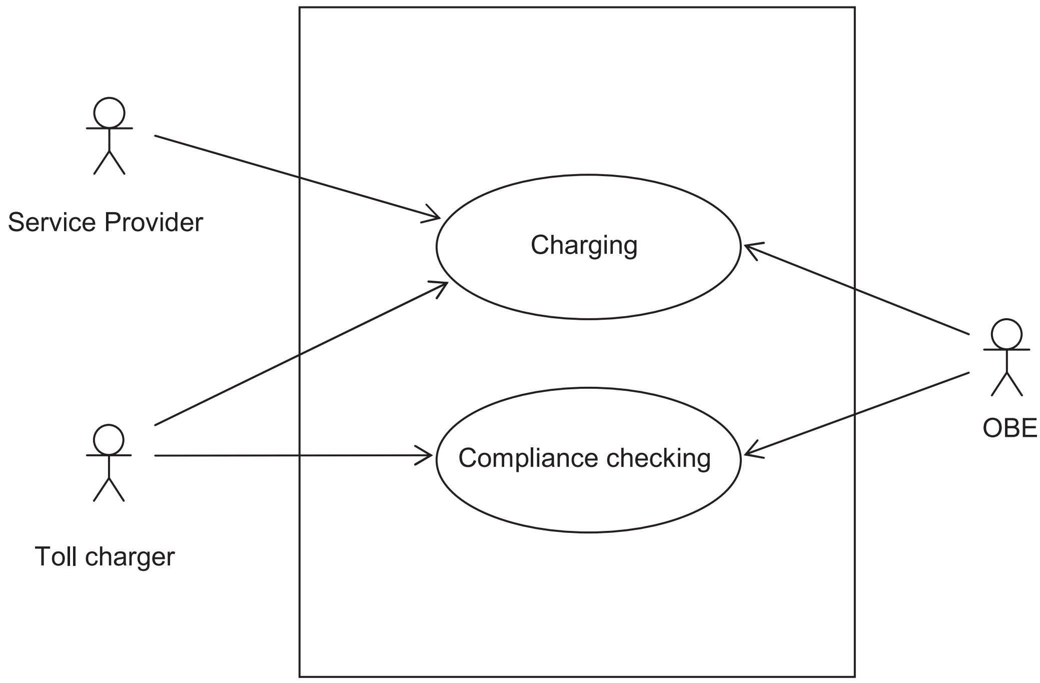

Figure 10 — The use cases "Charging" and "Compliance checking" involving the OBE, the Service Provider and the toll charger.

5.4.10 Repair and upgrade of the OBE

This use case applies to changes of the OBE intended to re-establish or to improve its normal operation. A defect or the need for an upgrade is reported to a repairer, who then performs the required changes. The change may consist of a repair or replacement of hardware components, the addition of new hardware components or the update of the software. The use case involves the user of the OBE, who has to bring the OBE to the repairer in case a remote repair (via the long range mobile communication link) is not possible.

Even though the OBE is only operational when a contract has been established, repair or upgrades may also be required at times when there is no contract, just to avoid a situation where a contract is established but the OBE is not immediately ready for operation.

In any case the Service Provider having established a contract for the OBE (see 5.4.4) has to verify and accept the repair or upgrade. If there is a contract at the time of the repair or upgrade, then the acceptance process may be part of the use case, which means that the Service Provider is directly involved. If the contract is established later on, then the acceptance process is part of the use case establishing the contract (see 5.4.4).

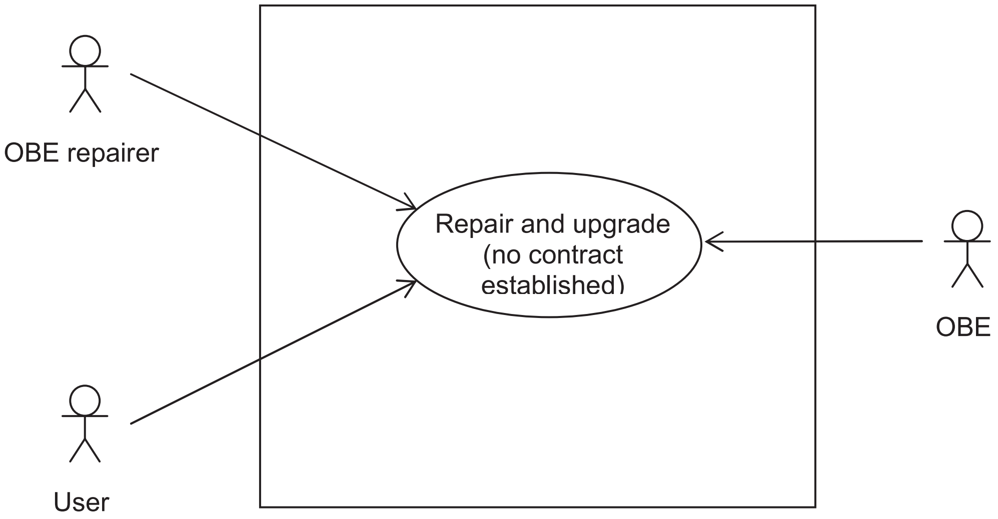

Figure 11 — The use case "Repair and upgrade" involving the OBE, the OBE repairer and the user

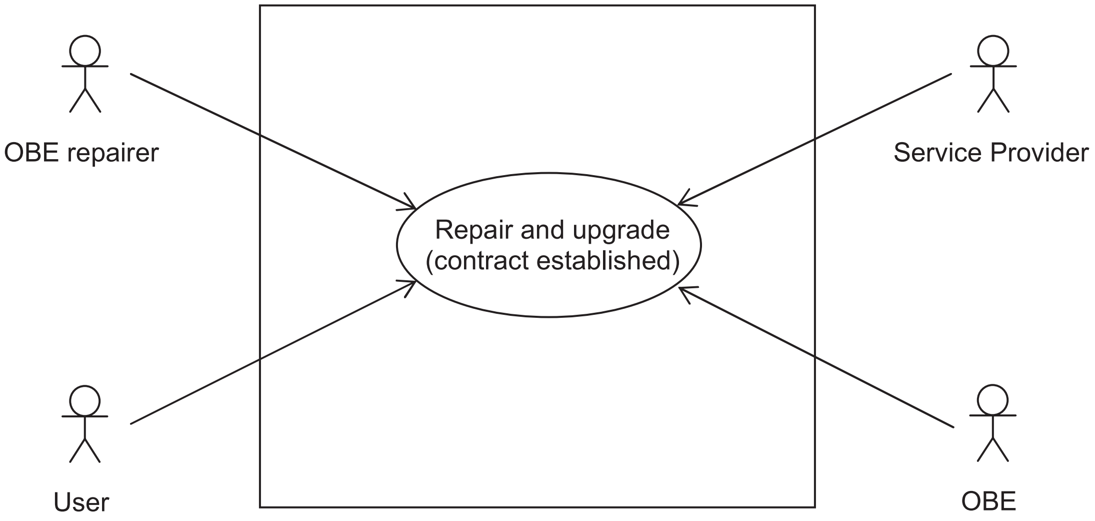

Figure 12 — The use case "Repair and upgrade" in case a contract with a Service Provider is established. The use case involves the OBE, the OBE repairer, the Service Provider and the user

5.4.11 Change of vehicle properties

The vehicle data relate, among others, to vehicle properties relevant for charging. This includes the problem of presence of the trailer, and related personalisation. These properties may be static or variable. Some changes of vehicle properties, like for instance those related to attaching and detaching trailers, may happen frequently and there may be specific features of the OBE to cope with them, like for instance their detection via a communication link to the vehicle electronics or the possibility for the user to declare them via HMI. Such changes are excluded from this use case, as they are covered in the normal charging use case (see 5.4.9). The use case only deals with property changes that are handled essentially in the same way as the initial assignment of vehicle data, which means that those properties not applying any more are deleted within the vehicle data and the new properties are added to them. Reasons for such a change of vehicle properties may be as follows:

a) an error in the vehicle data has been detected;

b) non-revocable changes to the vehicle have been executed, like a change of the vehicle colour or the change of the emission properties leading to the assignment of a different emission class;

c) some administrative procedure leads to different vehicle properties, like for instance the change of the maximum allowed weight in the vehicle registration document.

The use case involves the same actors as the assignment of vehicle data. Clarification is needed on how the vehicle data issuer gets the information that the vehicle properties have changed. If the user profits from the change (in terms of lower fees), then it can be expected that he initiates the procedure of the use case. Else the use case has to be linked to some administrative procedures.

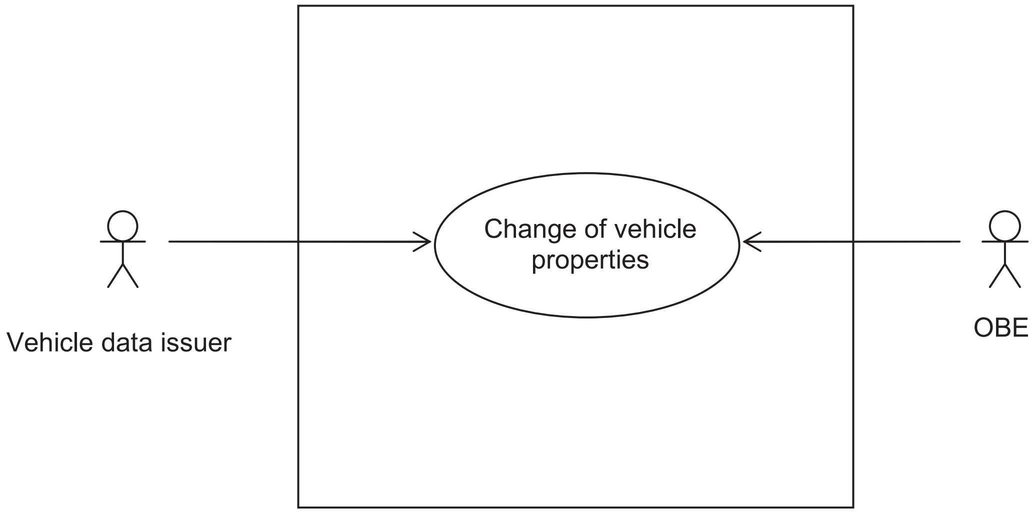

Figure 13 — The use case “Change of vehicle properties” involving the OBE and the vehicle data issuer

5.4.12 Decommissioning and replacement of the OBE

This use case includes also the deactivation of the OBE.

What happens with OBE at the end of its lifetime? There are two reasons for a specific decommissioning process and not just to throw it away: it may still contain sensitive data and there may be misuse. It has to be brought into a stage where sensitive data cannot be retrieved from it and where it is impossible to further use it in an unintended way. The responsibility for this is assigned to the OBE issuer, as he is the actor having control on the OBE lifecycle and being able to act at every stage of this lifecycle. The user has to agree on the decommissioning.

In case there is a contract with a Service Provider fort he OBE, this use case includes the use case “cancellation of an existing contract” (see 5.4.7).

The OBE may be replaced and parts of it (like for instance antennas or the HMI) may be integrated into the new OBE.

The replacement OBE may be one assigned to a specific Service Provider (like the usual case of retrofitted OBE) or may be similar to a first mount OBE, which means that contracts with different Service Providers may apply.

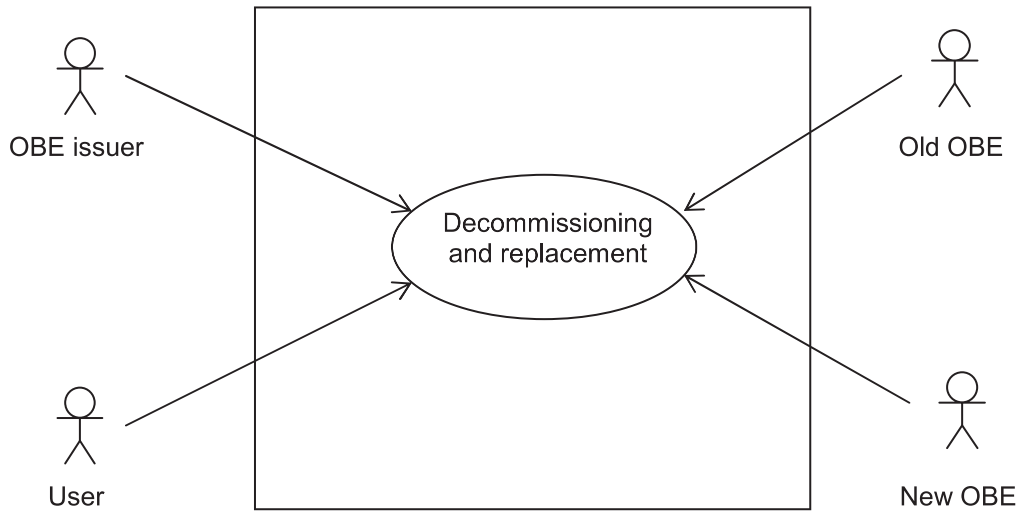

Figure 14 — The use case "Decommissioning and replacement", involving the OBE issuer, the user, the OBE and a new OBE in case of a replacement

6 Personalisation concept

6.1 Overall requirements

6.1.1 Functional requirements

The following list of functional requirements is derived from the use cases and from the list of assets. It considers what the assets are used for, what the interests of the various actors and roles in these assets are and how therefore the assets have to be protected on a functional level. The protection of the data as such against the various threats is dealt with in 6.1.2. Functional requirements marked with (g) are generic and not specific for first mount OBE.

RF1: Each single OBE must be distinguishable from all other OBE (g).

This first functional requirement just makes sure that if something happens with a specific OBE and needs to be recorded, the record can refer to this OBE and can be assigned to the right OBE later on. The OBE must have some property that allows distinguishing it from others, which means is unique among all OBE. The property may at this stage be physical (like for instance a number or bar code printed on it) or consist of data. If it consists of data, care has to be taken that these data cannot be removed from the memory of the OBE or changed (except when recording the change and keeping the record).

RF1.1: When exchanging data with other devices, the OBE must be able to present its specific properties, making it distinguishable from the others (g).

Personalization data may be added to the OBE or existing personalization data may be changed at any time. Assignment of the data to the right OBE must be guaranteed. Therefore the personalization data have to refer to the unique property of the OBE. To prevent personalization of the wrong OBE, the OBE must be able to prove that it is the one with the unique property according to RF1 in the data exchange for the personalization. Furthermore masquerade must be excluded, meaning that a different OBE can pretend it is the one to which the personalization data are assigned. In practice a solution to this authentication requirement would be that the OBE has some unique secret data like a cryptographic key and is able to show in a data exchange that it possesses these data. A reference has to be established between the data and the unique property of the OBE according to RF1.

RF1.2: Some of the properties, making the OBE distinguishable from others, have to be kept over the whole lifetime of the OBE (g).

There may be a need to replace cryptographic keys and other personalization data. Nevertheless it should be possible to keep track of the OBE throughout its lifetime. The easiest way to guarantee this is with some “identifier” of the OBE that never changes.

RF2: It must be possible to establish a contract with a Service Provider at the OBE, which means storing data related to this contract in the OBE and making these data available for the charging and compliance checking process (g).

The basic concept of the actors and their tasks in EFC assumes that the road user subscribes to an EFC service and is charged via the Service Provider of this service. As the OBE is a key contributor to the charging and compliance checking process, it must be able to refer to the Service Provider. The data linking the Service Provider and the service user are called contract data. They have to be present at the OBE and used in the charging and compliance checking process to make sure the road usage is assigned to the right Service Provider and service user. This does not mean that the service user has to be identified in the contract data. He may stay anonymous towards the Toll Charger and the contract data may include a contract identifier, which only the Service Provider is able to assign to the specific service user.

RF2.1: It must be possible to establish different contracts from different Service Providers at the OBE.

At the time the user buys the vehicle, he gets the OBE with it. At least in some situations getting a specific OBE should not mean that he has to subscribe to a specific Service Provider. In other words: it should be possible to separate the process of buying the vehicle and the process of subscribing to the EFC service of a specific Service Provider in the sense that for a vehicle and its OBE there is a choice between different Service Providers. But having subscribed to several EFC services at a time would make things unnecessarily complicated :

RF2.1.1: It must be guaranteed that at every time only one contract is established at the OBE. There may be phases where no contract is established.

It is always the user who decides if he wants to use an EFC service and which one it is. He might even sign several contracts “on paper”, intending to use a specific one of them at a given time. Therefore no automatism should be implemented in the sense that the Service Provider establishes the contract at the OBE (via an online communication) without involvement of the user:

RF2.2: The user must be able to suppress the establishment of a contract.

To decide on offering a contract and the appropriate contract terms, the Service Provider needs some OBE and vehicle specific data. It would be possible to have these data stored somewhere outside the OBE and to send them to the Service Provider on request. But it is much more practical if the OBE can deliver these data as the Service Provider has to contact the OBE anyway to establish the contract there. This saves a separate data exchange in the background system:

RF2.3: Before establishing a contract, the Service Provider must be able to retrieve data from the OBE, on which the establishment of the contract may depend, including the OBE make, hardware extensions, the software version, the vehicle data as well as data identifying the OBE issuer and the vehicle data issuer.

This requirement does not mean that in any case the Service Provider has to retrieve the data from the OBE. For instance in case of the establishment of the contract data with a chipcard, it is easier to get the data from an external source. But the idea is that the establishment of the contract via an air link has to be supported as well. The air link may be long range (like for instance UMTS) or short range (like for instance DSRC).

RF2.4: It must be possible to perform a change of the OBE configuration and, in case the OBE has software that can be updated, a software update in conjunction with establishing a contract.

According to the basic concept of actors and their tasks it is the responsibility of the Service Provider to guarantee the correct operation of the OBE. The service user has to support him in the sense that he uses the

OBE according to the instructions, does not use it if it indicates a defect etc. Furthermore the Service Provider relies on the OBE manufacturer having implemented all quality assurance measures when producing the OBE. But still in case of something not working in the way it should, the Toll Charger will held the Service Provider responsible for this. Therefore the Service Provider must be able to properly configure the OBE and install the appropriate software, if required. This possibly includes the installation of a different version of the OBE manufacturer software if the version installed is not suitable for his purpose (cf. RF4.2). Everything has to be in place before the charging and compliance checking process may start.

RF2.5: It should be possible to establish a contract in conjunction with the procedure to set up long range mobile communication at the OBE.

This requirement does not say that the long range mobile communication (cellular network or something similar) has to be set up at the time of contract establishment. In some cases such a communication might be required before the contract is established (and in other cases it might not be needed at all). But on the other hand there are cases when setting up the communication in conjunction with establishing the contract makes sense. For instance the Service Provider may have a general contract with a mobile communication provider for all his subscribers, which means that he has to set up the mobile communication with this provider at the time the user starts using his service, i.e. when establishing the contract at the OBE.

RF2.6: After the OBE has been informed on the cancellation of a contract, the corresponding contract data shall not be further used in normal operation and cannot be retrieved from the OBE.

This requirement is obvious: charges occurring after a contract has been cancelled could not be settled through the corresponding Service Provider. But the question is who informs the OBE about the cancellation – the Service Provider or the service user. The Service Provider might not be able to do it (because for a certain time he is not able to contact the OBE) and the service user might forget to do so. The highest reliability is achieved if both sides can do it.

RF2.6.1: It must be possible for both the Service Provider and the user to inform the OBE on the cancellation of the contract.

RF2.7: As soon as a contract assignment is moved from an old OBE to a new one, it must be guaranteed that the contract is no longer used with the old OBE.

It would certainly be possible to establish a new contract in case an OBE is replaced. Then RF8 applies for the old OBE and contract. But it is not yet clear if things will be handled that way. There is an advantage in keeping the contract at an OBE replacement: with a mechanism as imposed by RF2.7 it could be guaranteed at least in the case of OBE replacement that no OBE continues to work without contractual relation between the Service Provider and the service user. The mechanism could simply be that a contract, once activated, can only be reactivated, if there is a confirmation from the old OBE that it has been deactivated there.

RF2.8: It must be guaranteed that the contract data are not further used after the OBE has been detached from the vehicle (g).

Even for a first mount OBE it may be possible to detach it from the vehicle and use it in a different vehicle. It is obvious in this case that new contract data (especially new vehicle data) have to be established and the OBE does not continue to use the old data.

RF3: It must be possible to store data on vehicle properties and the vehicle registration in the OBE and to make them available for the charging and compliance checking process (g).

This basic requirement is obvious as vehicle data are needed for charging and compliance checking. But the vehicle data may change, for instance if the engine is modified and a new emission class applies, or if the registration became invalid and the vehicle received a new registration after it had been repaired.

RF3.1: It must be possible to establish and change the vehicle data in the OBE any time during the lifetime of the OBE (independent from the establishment of a contract) (g).

It is possible that the Service Provider acts as vehicle data issuer. Then no changes to these data are possible as long as there is no contract with a Service Provider. Each Service Provider will need to check the vehicle data and possibly change them before he establishes a contract. This is one option. But it is also possible that the vehicle data are handled independent from a Service Provider and that the vehicle data issuer does not want to wait until a contract is established.

RF3.2: Data allowing identifying the entity having provided the vehicle data (i.e. the vehicle data issuer) must be available at the OBE.

If something is wrong with the vehicle data, then it must be clear who is responsible.

RF4: If the OBE has software that can be updated, it must be possible to update it at any stage during the OBE lifetime (g).

The Service Provider updating the software of the OBE was dealt with in RF2.4. But there is also software in the responsibility of the OBE manufacturer or OBE issuer and it might need updates in case some bugs are found or the EFC system has been changed. This can happen at any time and it is practical to update all software more or less at the same time – even those without a contract with a Service Provider.

RF4.1: There must be a software version assigned to each specific software in use and the OBE must be able to indicate its software version (g).

A software version is not only required for the management of software updates. It is only relevant if in the charging or compliance checking process something does not work correctly.

RF4.2: The Service Provider must be able to prevent a software update.

It would be a nightmare for a Service Provider: The OBE manufacturer or OBE issuer updates the software of all his OBE because of a minor bug, and suddenly none of them works any more. As it is the responsibility of the Service Provider to guarantee the correct operation of the OBE (see comment on RF2.4), he must also have control on the software versions installed at the OBE.

RF5: Normal operation of the OBE shall only be possible if the vehicle data, a contract and if foreseen a long range mobile communication have been established.

The principle of this requirement is: normal operation only after personalization. With the establishment of a contract the Service Provider is expected to check that everything is prepared for a correct operation.

RF5.1: The OBE must be able to inform the user on its status related to normal operation and in case it is not ready for normal operation, on the reason for this (g).

For personalization only the corresponding reasons are relevant, like for instance no contract being established, the OBE having been detached from a vehicle and no new vehicle data being available, or an error being detected that needs to be repaired.

RF6: After a repair or upgrade of the hardware, the OBE shall only resume normal operation after confirmation from authorized personnel (g).

This requirement is mainly to avoid that the user changes the OBE, which would open the door for tampering with it. Authorized personnel means personnel having the role of an OBE repairer (cf. 5.2). The provision to be able to held the authorized personnel responsible for the changes on the OBE is dealt with in the next requirement:

RF7: The OBE shall record important events related to its lifecycle, at least including the following:

a) date and time of the recording or change of the vehicle data together with data allowing to identify the vehicle data issuer;

b) date and time when the OBE is detached from the vehicle;

c) date and time of the establishment and cancellation of a contract together with data allowing to identify the Service Provider;

d) initial software version as well as date and time of software updates with the new version installed;

e) date and time of repairs together with data allowing to identify the authorized personnel having confirmed the repair.

With this requirement it is not only possible to find out at each time about the status of the OBE, but also to find out who is responsible in case something is not as it should be.

RF7.1: The OBE shall disclose the recordings on lifecycle related events only to authorized personnel.

This requirement is for privacy protection.

RF8: An OBE not intended to be further used has to be brought into a stage where contract related data cannot be retrieved from it and no new contract can be established (g).

This last requirement applies for instance to an OBE that has been tampered with and where a correct operation cannot be guaranteed any more. For the first part cf. RF2.6.

6.1.2 Security Requirements

6.1.2.1 Threat analysis of Assets

The objective of this threat analysis is to identify threats within Personalisation Security context shown in Figure 1 and perform a threat analysis. The output will then be used to specify security requirements and security counter measures. The analysis below is currently focusing on technical threats and will be extended to also include more “soft” threats like agreements.

The severity of the consequence that is a result of that the threat is materialized is given a value between 1 and 5.

Where

1:	the consequences are not severe
5:	the consequences are very severe

The adversaries are defined in Table2.

Table 2 — Definition of adversaries

Service User:	The intended user of the service
Hacker:	Someone manipulating the system for fun or for getting a challenge
Agent:	Someone acting on behalf of a service user e.g. an employee who has access to personalisation equipment.

The analysis does not cover threats that occur during normal operation of the service.

6.1.2.1.1 Application Data Threat analysis

Table 3 — Application data threat analysis

No	Threat Description	Adversary
1.	A: Adversary **manipulates** application data during the personalisation of the OBE.	Hacker Service User Agent
	Consequence	**Severity**
	A.1 Unauthorised usage of service or wrong service fee is charged	
	A.1.1 Loss of revenue for the Service Provider	3
	A.1.1.1 Lowering of system acceptance	4
	A.2 Wrong service user is charged	
	A.2.1 Inconvenience for service user who is subject to the threat	5
	A.2.1.1 Lowering of system acceptance	4
No	**Threat Description**	**Adversary**
2.	B: Adversary **eavesdrops** the personalisation interface.	Hacker Competing Service Provider
	Consequence	**Severity**
	B: Privacy infringements	
	B.1 Private data such as trips made or payment means will be revealed	3

No	Description of Countermeasures	Remarks
3.	Add individual access protection to personalisation assets in OBE	Applies to threat A
4.	Encrypt personalisation assets during storage and transmission to OBE.	Applies to threat B

No	Description of Detection measures	Remarks
1.	Add signatures or MACs to provide data integrity protection.	Applies to threat A

6.1.2.1.2 Application Key Threat analysis

Table 4 — Application key threat analysis

No	Threat Description	Adversary
2.	A: Adversary **eavesdrops** the personalisation interface during loading of application keys.	Hacker Competing Service Provider
	Consequence	**Severity**
	A: Unauthorised access to OBE	
	A.1 Possibility to debit/credit on-board accounts	
	A.1.1 Inconvenience for service user who is subject to the threat	5
	A.1.1.1 Lowering of system acceptance	4
	A.1.2 Loss of revenue for the Service Provider (in case of credit)	3
	A.2 Possibility to add fake information	
	A.2.1 Cause problems for Service User => bad reputation	5
	A.2.2 Loss of revenue for the Service Provider (e.g. changed vehicle data)	3
	A.3 Unauthorised use of OBE	
	A.3.1 Service Provider that have no contract service user may make use of the OBE, e.g. for identification purposes	3

No	Description of Countermeasures	Remarks
3.	Encrypt personalisation data during storage and transmission to OBE	
4.	Personalisation keys must never be handled in plain text	

6.1.2.2 Security Concept for countermeasures

It was identified in the threat analysis that the access to assets in the OBE has to be controlled during personalisation. As have been described earlier, different actors are involved in the personalisation of different assets. The EFC standards supports that more than one Service Provider uses the OBE for different services. The concept must therefore support that all actors can add there assets which they are responsible for in a secure way.

To be able to achieve this, the Assets in the OBE will be split into different Security Domains. Each Security Domain is protected by a set of maintenance keys which have to be set up in a secure way. The procedure for entering different maintenance keys is described in 6.1.2.2.4.

The OBE manufacturer will add initial security, provide data structure and software. This is done prior to the personalisation at first mount. Possibly additional software is added or updated to the OBE at personalisation. The use cases for adding different assets are described in 5.3. The most common case in EFC up to know is that one Service Provider is responsible for the personalisation of an OBE. In this case the Service Provider and the OBE issuer are the same actor.

RS1.1: The OBE Manufacturer shall be responsible for initial security in the OBE.

RS1.2: The OBE manufacturer shall have policies which ensure that initial security is not revealed to unauthorised parties.

RS1.3: The OBE shall be prepared with initial security before the OBE shall be personalised.

RS1.4: The OBE shall be prepared with data structure before the OBE shall be personalised.

RS1.5: The OBE should be prepared with software before the OBE shall be personalised.

RS1.6: The OBE shall have a function with which it is possible to load maintenance keys.

RS1.7: The OBE shall have a function with which it is possible to activate/deactivate the OBE.

NOTE The expected behaviour of the OBE when deactivated need to be defined. As an example it could mean that the OBE only responds to personalisation activation commands.

6.1.2.2.1 Access protection to personalisation assets in OBE

In order to update assets a dynamic access credentials shall be calculated using the applicable maintenance access key. This is done by the sending party requests a challenge from the OBE and calculates a cryptographic checksum.

RS2.1: The OBE shall support access protection of application data and application keys.

RS2.2: The sender of the personalisation assets shall have to present a valid dynamic access credentials calculated using the maintenance access key.

6.1.2.2.2 Protection against manipulation of data during personalisation

The data integrity must be secured during the transmission of the personalisation assets. The way of achieving this depends on the asset. For assets which are not keys the way to do it is to retrieve an authenticator over the asset that was written to the OBE together with some random data provided by the sender in order to prevent replay attacks. The sender is then able to verify the asset authenticity. Keys can not be verified in that way after have being personalised into the OBE. For symmetric keys the authenticity can be verified be requesting a key verification code, KVC, value from the OBE. The KVC calculation is done by performing an encryption of a 0-vector with the applicable key and keeping the leftmost 3 bytes as described in ISO 11568-2. For asymmetric keys the authenticity can be verified by requesting a digital signature to be calculated by the OBE over some data and verify it using the corresponding certificate.

RS3.1: The OBE shall support retrieval of application data from the OBE with an appended authenticator.

RS3.2: The authenticator shall be calculated over the application data and a challenge provided by the sender.

RS3.3: The OBE shall support calculation of a 3 byte KVC over application symmetric keys according to ISO 11568-2 if applicable.

6.1.2.2.3 Protection against eavesdropping

Since assets consisting of application keys and other sensitive application data are transmitted during the personalisation the transmission must be protected against eavesdropping. This is done by encrypting the data with the maintenance encryption key.

RS4.1: The OBE shall support encryption of all personalisation messages using the maintenance encryption key.

6.1.2.2.4 Management of maintenance keys

The use of maintenance key to protect personalisation of assets within different Security Domains has been described in previous chapter. The maintenance keys that are used needs to be entered by the respective Security Domain responsible. The full scope of the security infrastructure is out of scope of this document. A top down approach would have been preferable but since the security infrastructure is not in place when writing this document this chapter should be revisited when it does.

First of all an initial security is needed to be able to anything at all in a secure way with the OBE. The initial security is assumed to be set up in a secure facility under control of the OBE manufacturer. In this environment the OBE Manufacturer puts in OBE Manufacturer Specific Assets e.g. individual HW related configuration data, application SW (if applicable), data structures, initial security and a manufacturer identifier. Example of HW configuration data is physical calibration parameters necessary from the production process.

The entering of initial security will take place before first mount and is outside the scope of this analysis. However the result is that the OBE is split in Security Domains which are individually protected by a set of maintenance keys. Initially the OBE Manufacturer puts in maintenance keys for all Security Domains. The actor in possession of a set of maintenance keys can modify the contents in the related Security Domain. Figure 15 shows the structure of the OBE after initial security is added. This is an example with four different Security Domains.

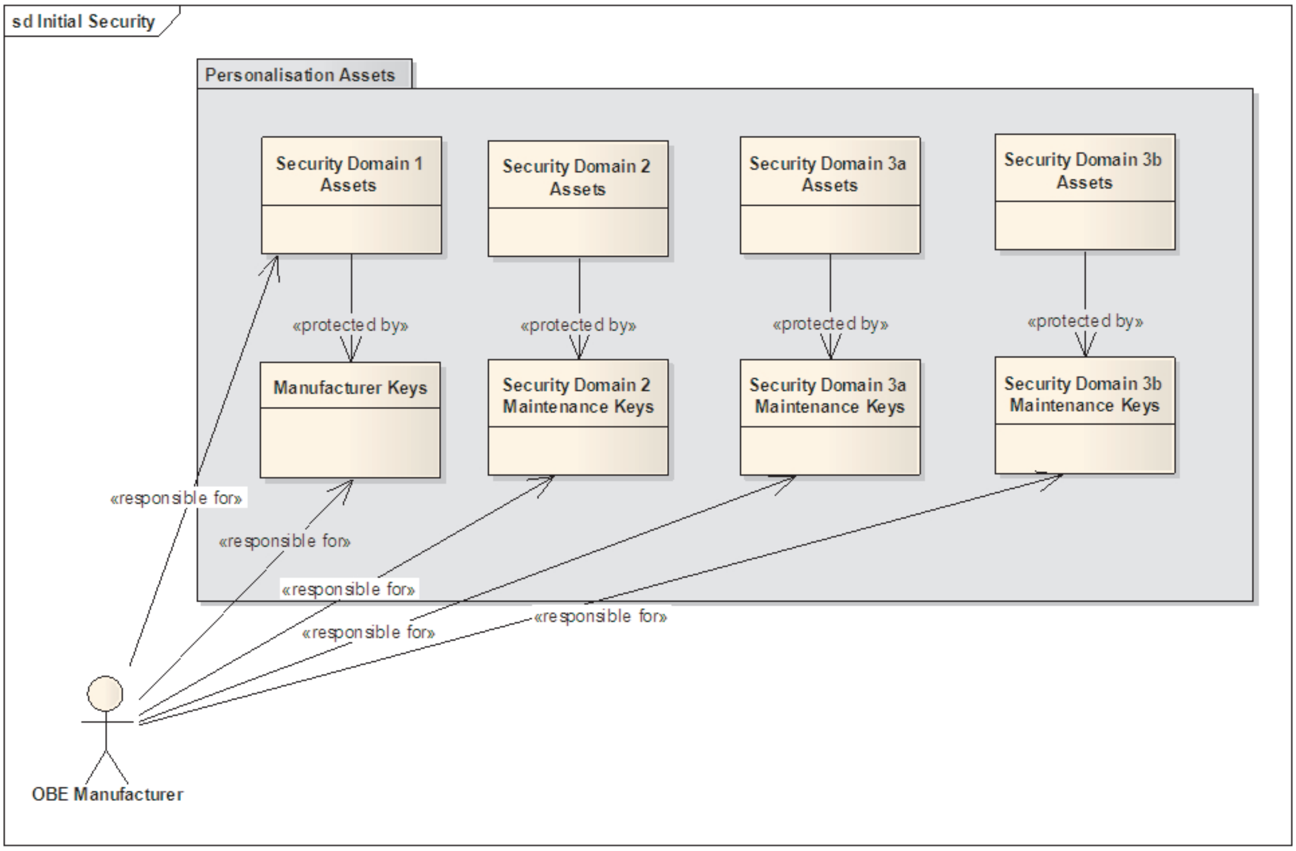

Figure 15 — Initial security

The question is how to distribute the pre generated maintenance keys from the OBE Manufacturer to the other actors that are responsible for a Security Domain. One possibility would be that the OBE manufacturer is responsible for updating the Security Domain 2 assets. Similarly the actor responsible for Security Domain 2 is responsible for maintaining Security Domain 3. This way of handling the key distribution requires that a trust relation must exist throughout the OBE life cycle, i.e. Security Domain <x> responsible must have trust in Security Domain <x-1> responsible.

An alternative way which removes this trust relation in the OBE is to require that the OBE allows the maintenance key set for a Security Domain to be updated by the current maintenance key set only. This concept results in that different actors are responsible for different Security Domains in the OBE independently. The Security Domain <x> responsible initially generates maintenance keys for Security Domain <x+1>. The generated maintenance keys will be handed over to the responsible of Security Domain <x+1>. After receiving them he will immediately change them and after that he is the only one who knows these keys and will thus be in charge of that Security Domain and possible Security Domains above. Hence the maintenance keys needed for personalisation of an Security Domain can be exchanged outside the personalisation environment. Figure 16 shows the responsibilities after the personalisation, i.e. all Security Domain responsible have received their respective keys.

Take current element structure of a CEN DSRC OBE as an example. When mounting the OBE in the vehicle the OBE manufacturer gives the maintenance keys for Security Domain 2 to the OBE Issuer who adds some assets, e.g. individual data, vehicle data etc. He then hands over the maintenance keys for Security Domain 3a to Service Provider A. Service Provider A changes the Security Domain 3a maintenance keys which makes him independent of the OBE issuer. Service Provider A can add application data, application authentication keys and access credential keys to Security Domain 3a. The Service Provider A may share the application keys with Service Providers he trusts.

The OBE issuer handles Service Provider B in the same way.

In the end The OBE Issuer, Service Provider A and B can choose to grant access to there respective Security Domain.

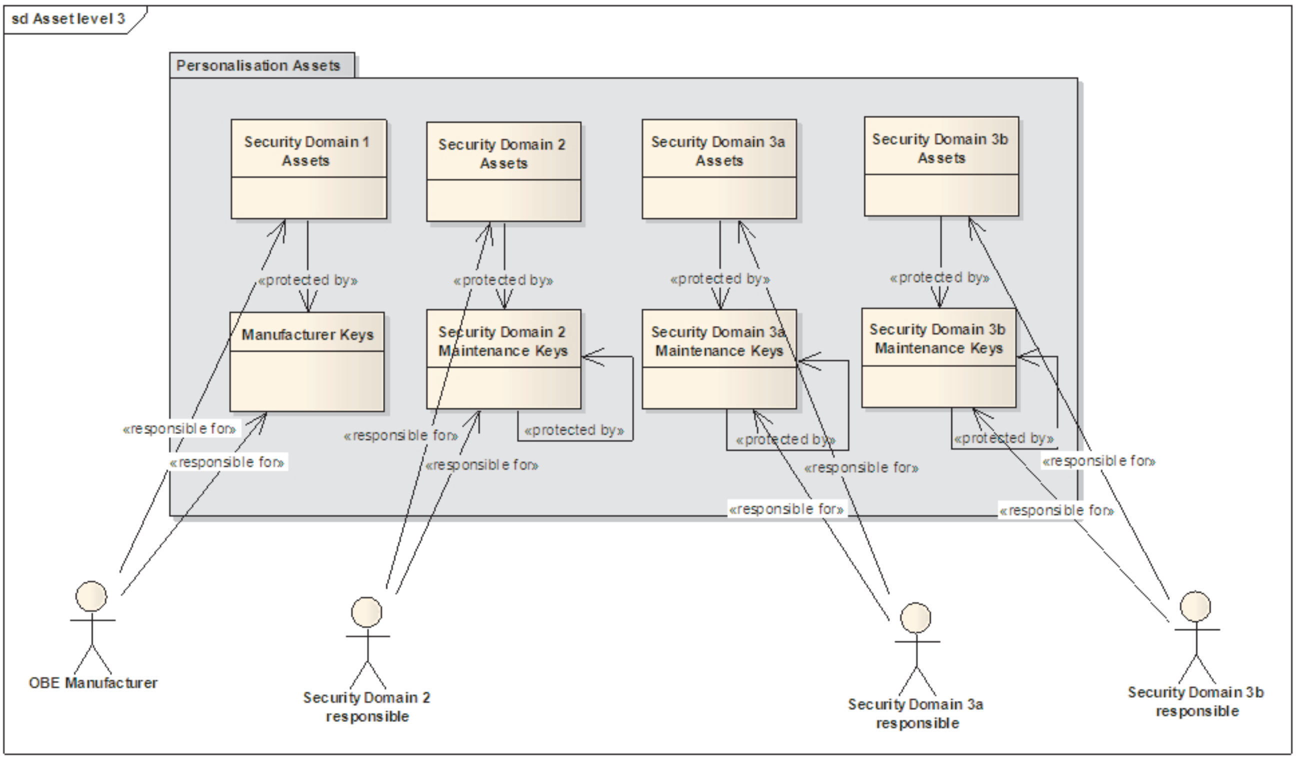

Figure 16 — Security Domains with distributed responsibility

In a system as described above with one OBE Issuer and more than one Service Provider, each of them have to remove the data they have entered. There is no single actor responsible for all assets entered at personalisation.

In such a system an alternative would be to assign the Security Domain 2 responsible the role of OBE Security Domain responsible. The difference would be that the maintenance keys in Security Domain 3a and

3b can only be changed by Security Domain 2 responsible. Applying that on the previous would result in that the OBE Issuer is responsible for the personalisation and for the Security Domain 3a and 3b. The Security Domain 3a and 3b responsible have to trust him to change their maintenance keys. The OBE Issuer is the trusted third party which all Security Domain responsible have to trust. The resulting trust relations are described in Figure 17.

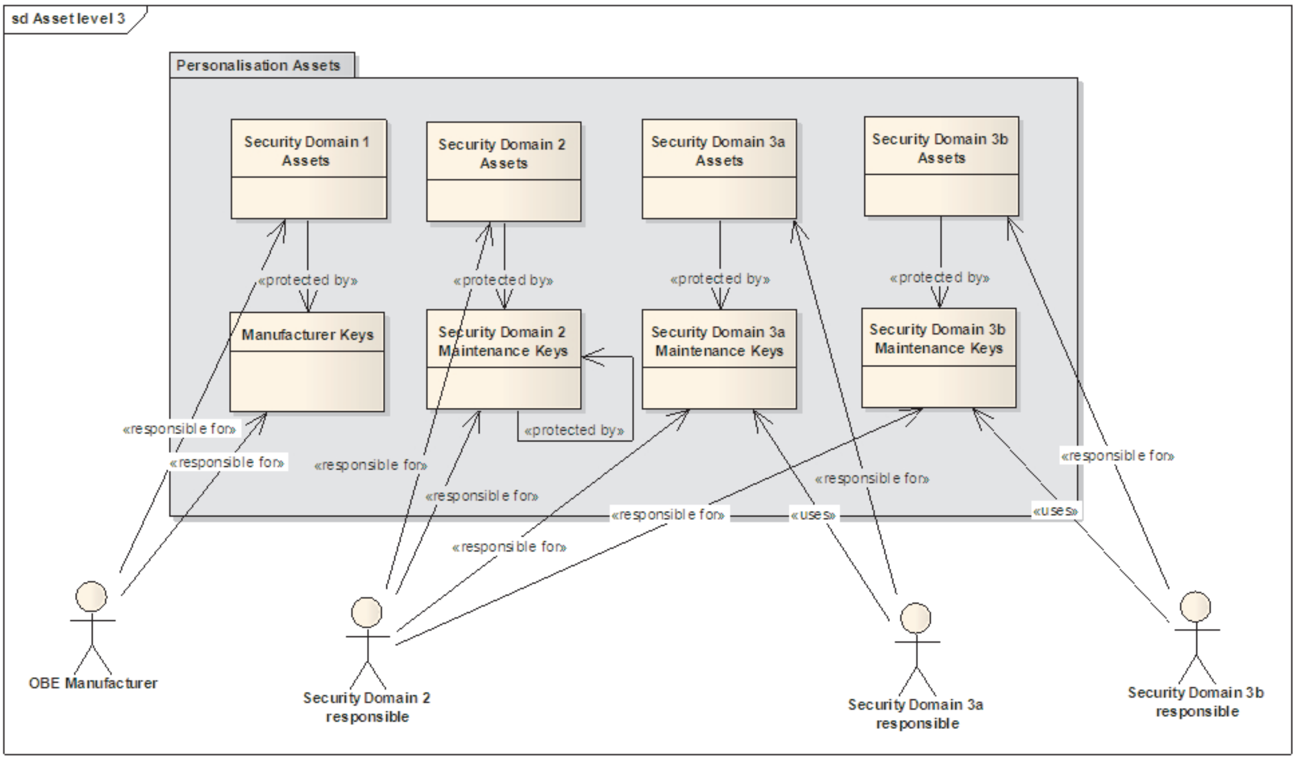

Figure 17 — Security Domains with trusted third party

What does the Security Domain <x> Maintenance Keys consist of? In response to the threat analysis the set shall consist of a maintenance encryption key, a maintenance access key and a maintenance authentication key.

What does the Security Domain <x> Maintenance Keys consist of? That depends on whether symmetric or asymmetric cryptographic algorithms are used. However keys must exist which support encryption, OBE access protection and mutual authentication. Next section will describe different approaches.

6.1.2.3 Cryptographic algorithms for the maintenance keys

The concept described in previous chapter can be implemented using either symmetric keys or asymmetric keys. There are pros and cons with both.

6.1.2.3.1 One secret symmetric key vs asymmetric key pairs

One conceptual difference is that in the symmetric solution sender and receiver must be in procession of the same secret key. The asymmetric solution has the advantage over the symmetric solution that you do not have to handle secret keys since you only transmit the certificates which contains the public key. Each communicating part generates its own key pair. The private key has to be kept in a secure storage. The public key can be sent in plain in a certificate to the communicating part. However even if the public key does not have to be kept secret you need a secure environment for identification of the communicating parts so you will not suffer from man-in-the-middle-attacks.

6.1.2.3.2 Number of keys needed

From an OBE issuer/Service Provider(s) point of view they would in theory be required to handle keys individually for each OBE. This would create a huge administrative task which is not feasible. Therefore they store master keys instead which they use to derive the individual key for the actual OBE based on some derivation data provided by the OBE. These master keys must be kept in a secure storage both in the OBE and in the personalisation environment at the Security Domain <x> responsible premises.

In a symmetric solution when assets are to be loaded to the OBE, three different keys must exist: One for encryption, one for mutual authentication and one for authorisation of the OBE issuer/Service Provider depending on which security domain that are to be accessed.

From the OBE point of view he has to store one set of keys for each security domain as described in Figure 17.

In the asymmetric solution the OBE will have one key pair for authenticating himself towards the OBE issuer/Service Provider(s). The OBE public key used for authentication is signed by the OBE Certificate Authority (CA) and stored as a certificate in the OBE. The OBE also need to store one certificate for the CA of each security domains for authorisation purposes. When the OBE issuer/Service Provider(s) wants to access a security domain in the OBE they will present a certificate which contains specific access rights. The OBE will then use the applicable security domain CA certificate to verify these rights.

When it comes to transmitting data which have to be kept secret, asymmetric cryptography key negotiation protocol exist which are used to negotiate symmetric encryption session keys. The advantage is that it does not have to handle secret encryption keys. The down side is that the solution is more complex. This solution works well for large assets. If information is very small one could think of encryption using asymmetric keys. Example could be DSRC symmetric keys which need to be transmitted to the Service Providers Security Domain <x> Assets as indicated in Figure 17.

6.1.2.3.3 Data volume

When it comes to data volumes the asymmetric solution need to transmit certificates containing the public key. These certificates is occupies much more data than the corresponding symmetric solution. Whether this is feasible or not depends on the physical interface. A certificate which is larger than 128 byte is currently not supported by EN 15509 standard. On the other hand other physical interface might be used for personalisation purposes which can cope with this larger data.

6.1.2.3.4 Performance

Yet another difference is performance where symmetric cryptography operations are faster than asymmetric cryptography operations. Whether this is an issue or not depends on the computational power of the OBE and personalisation equipment. An important issue is generation of key pairs which consumes a lot of time if it shall be done in the OBE secure storage. Probably the setting up of initial security at the OBE manufacturer will be the most time critical part of the concept. An alternative would be generating the OBE outside the OBE which in fact, from a security point of view, will be the same as loading a symmetric key.

So in conclusion the decision whether to choose a symmetric or an asymmetric solution is not isolated to the personalisation process. It depends on a number of factors e.g.:

- which physical interfaces to the OBE exist for personalisation purposes;
- what does the system security infrastructure look like;
- how many security domains shall exist in the OBE etc.

6.1.2.4 Security level of different algorithms and key lengths

One important issue when selecting cryptographic algorithms is how long it will take an attacker to break the security. Different algorithms in combination with different keys sizes offer security levels which can be expressed in required security bits. This figure is independent of which algorithm that is used. Different analysis has been done by different security experts with slightly different results as outcome. In IST-2002-507932 these results have been summarised and a recommendation has been provided.

According to IST-2002-507932 the required security level in order to achieve approximately 10 years protection is 96 security bits and 112 bits to achieve approximately 20 years. The tricky thing is to estimate for how long time the security has to last. If we assume 10 year lifetime of the OBE it seems reasonable to go for 96 bits security level.

RS5.1: The OBE shall perform all cryptographic calculations using algorithms and key lengths which offers a security level corresponding to secure protection over 10 years of OBE operation.

So the question is which security algorithm to go for based on security level. Today's DSRC standard is based on DES or 2-key triple DES (112bit 3DES). According to IST-2002-507932 112-bit 3DES is re-affirmed by NIST only through the year 2010. Using AES algorithm with 128 bit keys, which is the smallest key size of for the AES standard, results in a security level of 128 security bits. That is estimated to offer protection for approximately 30 years.

The strength of asymmetric cryptographic algorithms with a given key length can be expressed in security bits as well. According to IST-2002-507932 a RSA key should be 2048 bit long in order to achieve a security level of 96 security bits. An asymmetric alternative to RSA is Elliptic Curves which offers much shorter keys and also shorter calculation times compared to RSA. The ECC key should be twice the number of security bits to achieve a certain security level i.e. the ECC key should be 256 bits long to achieve a security level of 128 security bits.

6.2 Vehicle interface requirements and constraints

As a general comment on this clause, most of detailed technical issues are out of the scope of CEN/TC278 and should be addressed directly by ISO/TC22.

6.2.1 Introduction

The current practice concerning installation of OBE is the after-sales installation of separate and removable OBE. Different levels of integration of OBEs for EFC within the vehicle can be considered. These vary from a standardised interface with an external transmission to the complete integration of the EFC application within the vehicle information system.

There are several reasons for integrating an OBE interface in the vehicle:

a) to supply energy to the OBE from the vehicle electrical system;

b) security and safety aspects (the system can, for instance, be integrated and type-approved by the vehicle manufacturer);

c) integration of the equipment into the car design, including improved man-machine interfaces;

d) reduced handling, installation and maintenance costs for toll chargers and services providers operators;

e) additional services can be provided via DSRC, or GNSS-CN, for example navigation services;

f) no duplication of devices (single multi-service equipment for EFC, for route guidance, fleet management, etc.).

6.2.2 Installation principles

The OBE should be located and fitted into the vehicle in accordance with relevant regulations, standards and manufacturers instructions for installing the system in vehicles.

a) No part of the OBE should obstruct the driver's view of the road scene, as defined by UN-ECE Regulation 43.

b) The OBE should not obstruct vehicle controls and displays required for the primary driving task.

c) Where available, visual displays should be positioned as close as practicable to the driver's normal line of sight.

d) In case of metallic windshield, the OBE transmission elements shall be installed according to the statement of principles defined in EETS-EG6 Report.

7 Personalisation data

7.1 EFC Attibutes

Personalisation data are a subset of data elements defined in Electronic Fee Collection standards such as EN ISO 14906 and CEN ISO/TS 17575-1. The essential data elements are indicated below.

It should be noted that a transaction can be made with a combination of Public and Private Attributes. Private Attributes, which are implementation dependent, can also be part of the personalisation dataset.

Which EFC attributes are present and which are not is implementation dependent. The implementation is identified by the context given in the EFC-ContextMark of the VST.

In the following table, EFC Attributes are grouped into data group tables and specified in terms:

a) the Attribute name;

b) the Attribute identifier;

c) the length in octets (PER coded).

Table 5 — EFC attributes

AttributeID	Attribute	Length in Octet	Data Group	Personalisation data
0	EFC-ContextMark	6	Contract	Yes
1	ContractSerialNumber	4		Yes
2	ContractValidity	6		Yes
35	ValidityOfContract	4		Yes
3	ContractVehicle	Variable		Yes
4	ContractAuthenticator	Variable		Yes
5	ReceiptServicePart	13	Receipt	No
6	SessionClass	2		No
7	ReceiptServiceSerialNumber	3		No
36	ReceiptFinancialPart	23		No
9	ReceiptContract	9		No
10	ReceiptOBUId	Variable		No
11	ReceiptICC-Id	Variable		No
12	ReceiptText	Variable		No
13	ReceiptAuthenticator	Variable		No
14	ReceiptDistance	3		No
33	ReceiptData1	28		No
34	ReceiptData2	28		No
15	VehicleIdentificationNumber	Variable	Vehicle	Yes
16	VehicleLicencePlateNumber	Variable		Yes
17	VehicleClass	1		Yes
18	VehicleDimensions	3		Yes
19	VehicleAxles	2		Yes
20	VehicleWeightLimits	6		Yes
21	VehicleWeightLaden	2		Yes
22	VehicleSpecificCharacteristics	4		Yes
23	VehicleAuthenticator	Variable		Yes
37	AxleWeightLimits	10		Yes
38	PassengerCapacity	2		Yes
39	Engine	4		Yes
40	SoundLevel	2		Yes
41	ExhaustEmissionValues	8		Yes
42	DieselEmissionValues	4		Yes
43	CO2EmissionValue	2		Yes
44	VehicleTotalDistance	4		Yes
45	TrailerLicencePlateNumber	Variable		Yes
46	TrailerCharacteristics	5		Yes
24	EquipmentOBUId	Variable	Equipment	Yes
25	EquipmentICC-Id	Variable		Yes
26	EquipmentStatus	2		Yes
27	DriverCharacteristics	2	Driver	Yes
47	ActualNumberOfPassengers	1		No
32	PaymentMeans	14	Payment	Yes
29	PaymentMeansBalance	3		Yes
30	PaymentMeansUnit	2		Yes
31	PaymentSecurityData	Variable		Yes

7.2 OBE related data

The following manufacturing related data shall be pre-encoded in the OBE, prior to its personalisation:

a) OBE manufacturer identifier;

b) OBE issuer identifier;

c) OBE serial number;

d) Software version.

7.3 Access protection information

The following security related data shall be part of the personalisation dataset:

a) AccessCredentialKeyRef (reference to the key used for access credentials calculations);

b) AccessCredentials;

c) Certificates (asymmetric solution only);

d) initialValue : initial value needed for encryption;

e) keyRefEncryption (reference to the key used for encryption);

f) challenge (challenge for MAC calculation);

g) keyRefMac (reference to the key used for access credentials calculations).

7.4 Vehicle registration data

The following table provides a mapping table between EFC Vehicledata attributes and European registration certificate. This table provides further details regarding the definition of personalisation attributes related to the vehicle characteristics such as VehicleIdentificationNumber and VehicleLicencePlateNumber. The vehicle registration certificate is defined by the COMMISSION DIRECTIVE 2003/127/EC of 23 December 2003 amending Council Directive 1999/37/EC on the registration documents for vehicles.

To ease the task of a Service Provider when he need to personalise an OBE on how he can obtain some vehicle data, the following table provide a correspondence between elements available inside the registration certificate and the data element that could use this information (coding according to EN ISO 14906).

Table 6 — Vehicle registration data

AttributeId	**EFC Attribute**	**Data Element**	**Registration certificate element**	
16	**LicensePlate**	VehicleLicence PlateNumber	(A)	registration number
20	**Vehicle Weight Limits**	VehicleMaxladenWeight	(F.2)	maximum permissible laden mass of the vehicle in service in the Member State of registration
20	**Vehicle Weight Limits**	VehicleTrainMaximumWeight	(F.3)	maximum permissible laden mass of the whole vehicle in service in the Member State of registration
20	**Vehicle Weight Limits**	VehicleWeightUnladen	(G)	mass of the vehicle in service with bodywork, and with coupling device in the case of a towing vehicle in service from any category other than M1
22	**VehicleSpecifics Characteristics**	EnvironmentalCharacteristics		
		copValue	(V.7)	CO2 (in g/km)
		euroValue	(V.9)	indication of the environmental category of EC type-approval; reference to the version applicable pursuant to Directive 70/220/EEC(2) or Directive 88/77/EEC(3)
22	**VehicleSpecifics Characteristics**	EngineCharacteristics	(P.3)	type of fuel or power source

8 Recommendations

The following section provides recommendations for future works in relation with physical integration of OBE.

As the first-mount OBE is part of the vehicle, interacts with its electrical connections, and forms part of the vehicle electrical system, it should at least be compliant with the relevant standardisation produced by ISO/TC22 in the ISO 16750 series related to:

a) Operating voltage;

b) Nominal voltage (e.g. 12 V, 24 V, DC);

c) Test voltage ;

d) Overvoltage ;

e) Operating temperature ;

f) Storage temperature.

Complementary, the design of the OBE and of the vehicle should take into account their interactions on the following items as they cannot standardised:

g) Interference with other vehicle systems (e.g. common interfaces, data buses etc.).

h) Standby facility: the OBE shall have a standby facility, which has a power requirement of below a reference value to be specified. The OBE power supply and standby facility must not require a current that will adversely affect the vehicle battery load and thus interfere with the starting and running of the vehicle.

i) Definition of the behaviour of the OBE when in a status without contract (behaviour on the DSRC contract, on the HMI, etc.). The OBE is without contract when the owner of the vehicle has not subscribed to an EFC service with a provider.

As already mentioned in 7.2 and 7.3, the personalisation data are already defined by the existing standards. The need on standardisation is related on the mechanisms to transfer these data inside the OBE (air-link and/or wire link).

Bibliography

List of relevant documents related to integration of OBE in the vehicles

NOTE 1 The following documents are related to integration of OBE in the vehicles and will provide valuable information on this subjec

[1] EETS-EG6 Report : INTEGRATION OF ON-BOARD UNITS INTO VEHICLES – FINAL REPORT - Prepared by: Expert Group 6: Integration of OBEs into vehicles Working to support the European Commission DG TREN

[2] RSI_WP3_D3.4 : RCI Project – Deliverable D3.4 - Road Charging Interoperability Security Architecture for interoperability

[3] IST-2002-507932, ECRYPT Yearly Report on Algorithms and Key Lengths (2007-2008)

List of relevant regulations related to integration of OBE in the vehicles

NOTE 2 The following regulations are affecting installation and integration of equipment, and some aspects of OBE mounting. A number of regulations that need to be observed by the design of the windscreen or the in-vehicle equipments affect the location of the OBE within the vehicle:

[4] COMMISSION DIRECTIVE 2004/104/EC of 14 October 2004 adapting to technical progress Council Directive 72/245/EEC relating to the radio interference (electromagnetic compatibility) of vehicles and amending Directive 70/156/EEC on the approximation of the laws of the Member States relating to the type-approval of motor vehicles and their trailers.

[5] COMMISSION DIRECTIVE 2006/28/EC of 6 March 2006 amending, for the purposes of their adaptation to technical progress, Council Directive 72/245/EEC of 20 June 1972 relating to the radio interference (electromagnetic compatibility) of vehicles and Council Directive 70/156/EEC on the approximation of the laws of the Member States relating to the type-approval of motor vehicles and their trailers.

[6] COMMISSION DIRECTIVE 95/54/EC of 31 October 1995 adapting to technical progress Council Directive 72/245/EEC on the approximation of the laws of the Member States relating to the suppression of radio interference produced by spark-ignition engines fitted to motor vehicles and amending Directive 70/156/EEC on the approximation of the laws of the Member States relating to the type-approval of motor vehicles and their trailers

[7] COMMISSION RECOMMENDATION of 21 December 1999 on safe and efficient in-vehicle information and communication systems: A European statement of principles on human machine interface (notified under document number C(1999) 4786) (Text with EEA relevance) (2000/53/EC)

[8] United Nations Economic Commission for Europe (UNECE) ECE-R43 (and all amendments): uniform regulations for the approval of safety glass and glazing materials. Important in this respect are the so-called A-zone and B-zone of the windscreen, two safety-critical sub-divisions of the windscreen in which transmission of light and optical distortion are subject to regulatory requirements.

NOTE 3 The above mentioned regulations rely on International Standards and may also refer to other equipment regulations such as European Directive 89/336/CEE or European Directive RTTE 1999/5/CE.

List of relevant standards from CEN/TC278

[9] EN 12795, *Road transport and traffic telematics — Dedicated Short Range Communication (DSRC) — DSRC data link layer: medium access and logical link control*

[10] EN 12834, *Road transport and traffic telematics — Dedicated Short Range Communication (DSRC) — DSRC application layer*

[11] EN 13372, *Road Transport and Traffic Telematics (RTTT) — Dedicated short-range communication — Profiles for RTTT applications*

[12] CEN ISO/TS 17575–2, *Electronic fee collection — Application interface definition for autonomous systems — Part 2: Communication and connection to the lower layers (ISO/TS 17575-2:2010)*

[13] FprCEN ISO/TS 17575–3, *Electronic fee collection — Application interface definition for autonomous systems — Part 3: Context data (ISO/DTS 17575-3:2010)*

[14] FprCEN ISO/TS 17575–4, *Electronic fee collection — Application interface definition for autonomous systems — Part 4: Roaming (ISO/DTS 17575-4:2010)*

[15] CEN/TR 15762:2008, *Road transport and traffic telematics — Electronic fee collection (EFC) — Ensuring the correct function of EFC equipment installed behind metallised windshield*

List of relevant standards from IEC and ISO

[16] IEC CISPR 12, *Vehicles, boats and internal combustion engines — Radio disturbance characteristics — Limits and methods of measurement for the protection of off-board receivers*

[17] IEC CISPR 25, *Radio disturbance characteristics for the protection of receivers used on board vehicles, boats, and on devices — Limits and methods of measurement*

[18] ISO 7637-1, *Road vehicles — Electrical disturbances from conduction and coupling — Part 1: Definitions and general considerations*

[19] ISO 7637-2, *Road vehicles — Electrical disturbances from conduction and coupling — Part 2: Electrical transient conduction along supply lines*

[20] ISO 7637-3, *Road vehicles — Electrical disturbances from conduction and coupling — Part 3: Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines*

[21] ISO 10605, *Road vehicles — Test methods for electrical disturbances from electrostatic discharge*

[22] IEC 1000-4-2, *Electromagnetic compatibility — Testing and measurement techniques - Electrostatic discharge immunity tests — basic EMC publication*

[23] ISO 16750-1, *Road vehicles — Environmental conditions and testing for electrical and electronic equipment — Part 1: General*

[24] ISO 16750-2, *Road vehicles — Environmental conditions and testing for electrical and electronic equipment —Part 2: Electrical loads*

[25] ISO 16750-3, *Road vehicles — Environmental conditions and testing for electrical and electronic equipment — Part 3: Mechanical loads*

[26] ISO 16750-4, *Road vehicles — Environmental conditions and testing for electrical and electronic equipment — Part 4: Climatic loads*

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.

...making excellence a habit.™