easyGo

Roadside and on board equipment

Annex 2.2 to

Joint Venture Agreement
Toll Service Provider Agreement

Document:	202
Version:	3.0
Date:	4 May 2017

Table of contents

Document revision history

Version	Date	Author	Main changes
1.0	2012.03.14	TCL / ASK / SR	Approved by steering committee with minor comments
2.0	2013.05.02		Approved by SC
2.1	2016.08.17	ASK	General update including restructuring of appendices Clarification of EFC applications and security New OBEs in EasyGo basic Clarification of new features of EasyGo services
2.11	1.9.2016	HHA	Review HHA
2.12	20.09.2016	HHA	Review results ASK added
2.2	16.11.2016	HHA	Private attributes for “EN15509 (EasyGo basic)” removed; Release version
3.0	2017.05.04		Approved by Steering Committee

1 Introduction

This document defines the basic requirements for interoperability between the DSRC[1]-based electronic toll collection systems in EasyGo with regards to Road Side Equipment (RSE) and On Board Equipment (OBE). The scope of these specifications is primarily for use within EasyGo, but also to enable interoperability with external TSPs and TCs as well as other EFC[2] systems in Europe including the European Electronic Toll Service - EETS.

It should be emphasized that this document only specifies the overall principles and requirements for technical interoperability between RSE and OBE. To enable implementation of the individual EFC-application (see chapter 2.3) the detailed specifications of these applications must be included.

The document also describes personalisation of the OBEs, what takes place when a vehicle equipped with an OBE passes through an EFC toll lane and the requirements to equipment and functionality in an interoperable environment.

As illustrated below the vehicle is equipped with an OBE while the RSE consists of a beacon for communication and a roadside controller. An EFC lane will normally also be equipped with sensors and other equipment but for the explanation of the OBE – RSE functionality only the components shown below are relevant.

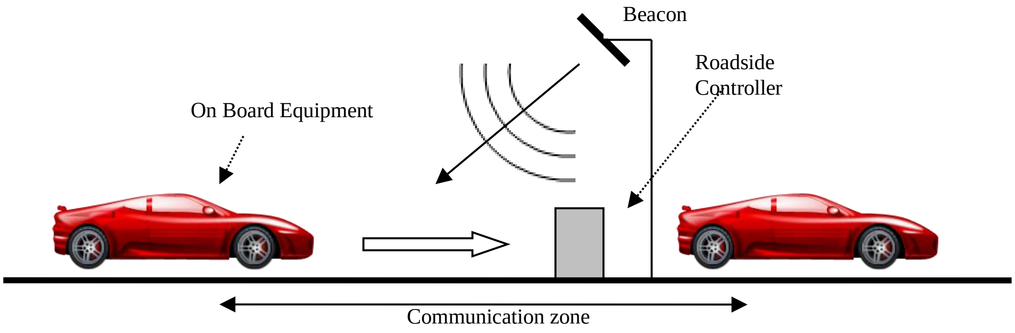

Figure 1: DSRC lane basic layout

The beacon in the EFC lane continuously emits a DSRC microwave signal (5.8 GHz). When an OBE enters the communication zone of the beacon the OBE is awakened (normally it sleeps to increase the battery lifetime) and responds by transmitting its credentials (who am I, who has issued me etc.).

When receiving data from the OBE, many types of beacons are capable of measuring the physical position of the OBE. The position of the OBE combined with sensor data positioning the vehicle allows the roadside controller to match vehicle and OBE. Such

[1] Digital Short Range Communication

[2] Electronic Fee Collection

functionality is a vital requirement in multi-lane free flow systems but detailed requirements concerning this functionality are not included in this document.

The communication between OBE and RSE must be completed within a limited time while the vehicle is inside the communication zone of the beacon.

The following topics and types of requirements are described in this document:

- Chapter 2 gives a general introduction to which types of data are stored in the OBE and in the RSE and the communication between these units. It also describes relevant standards employed and the features and differences between the different EFC-applications accepted by EasyGo.
- Chapter 3 describes the data sets, communication protocols and logical structure of the roadside controller and the beacon
- Chapter 4 describes requirements to OBE including personalisation before use, data sets and communication capabilities
- Chapter 5 describes the communication between OBE and RSE
- Chapter 6 gives an overview of alternative validation criteria used within EasyGo

- A number of appendices (chapter 7) gives additional information about the following topics:
    - Appendix A gives an overview of relevant directives, standards and regulations that are relevant to the EasyGo services and to EETS on the RSE – OBE level and referenced EasyGo documents within this document
    - Appendix B explains PAN notations
    - Appendix C gives an overview of EFC context marks and PAN content
    - Appendix D describes some security aspects of EasyGo. Additional information about security aspects in EasyGo can be found in EasyGo document 103 “EasyGo security policy” and is also referred to in the document

Additional details on the EasyGo+ OBEs and RSE can be found in EasyGo documents202-A – 202-E.

Certification of OBEs and RSE is described in EasyGo document 206 “EasyGo Test strategy”.

2 General description of the OBE – RSE functionality

2.1 Goals

The primary goal of this specification is to describe the general roadside principles of an interoperable EFC service involving different DSRC standards and operating policies and practises. The EasyGo services combine several EFC-applications and have defined a common architecture, but with flexibility for national/local variations. However, the local variations must not specify any requirements that contradicts or causes non-conformance to the base solution described in this document.

There are two EasyGo services:

- EasyGo basic allows Scandinavian Service Users (SU) to use their OBEs at all EasyGo TCs in Norway, Sweden and Denmark
- EasyGo+ is an additional service for vehicles above 3.5 tons going between Austria and the Scandinavian countries

All EasyGo+ OBEs as well as all new OBEs for EasyGo basic shall be based on the EN 15509 standard. Because of this EN 15509 must be implemented on all RSE. EN 15509 is also mandatory in EETS.

The EasyGo+ service is based on EN 15509 security level 1. Also the newest generation of AutoPASS OBEs requires the same security level. Other EasyGo basic OBEs are based on security level 0. This means that all RSE throughout EasyGo must be able to handle both security levels 0 and 1.

2.2 Overview of roadside functionality

The RSE should be able to perform transactions with all the OBE types that are approved for EasyGo basic and EasyGo+ with the following exceptions:

- Austria only accepts EasyGo+ OBE
- Many limited parties only accept passenger cars and do not need to read EasyGo+ OBE therefore.

Transactions must be processed according to the characteristics of each type of OBE. The RSE should be able to recognise the types of OBEs being used by the EFC -applications listed in chapter 2.3 and perform the type of transaction which conforms to this OBE and the corresponding EFC-application.

Depending on the data received from the OBE, the RSE validates the OBE according to rules associated with the transaction and the user agreement. The output of the decision flow is a logical transaction result which can have one of the following values:

- Valid
- Valid, but warning (if supported)
- Not valid

Transaction data, including the validation result, should be transferred to the Central System (CS) of the Toll Charger (TC). This interface is described in EasyGo document 203.

The transaction data provide all information required to charge the SU.

2.3 EFC-applications

There are several types of DSRC systems (OBEs and RSE) with different EFC-applications. By “EFC-application” is meant “a definition of the data exchange over the DSRC interface for central account based charging”.

AutoPASS, BroBizz and PISTA were the three EFC-applications originally used in the EasyGo (basic) service and had to be implemented by all EasyGo basic TCs. Later the EN 15509 standard has been introduced and all new OBEs shall now be based upon the EN 15509 standard while the three original EFC-applications still need to be supported as long as there are OBEs using these applications.

To differentiate between AutoPASS and BroBizz OBEs introduced before and after the introduction of the EN 15509 standard, the OBEs which do not comply to the EN 15509 standard are called “Old AutoPASS” and “Old BroBizz” respectively.

The following EFC-applications are supported in the EasyGo services and in EETS:

		EFC Applications				
		EN 15509 based (EasyGo basic)	EN 15509 (CEN)	PISTA	Old AutoPASS	Old BroBizz
Services	EasyGo Basic	OK		OK	OK	OK
	EasyGo +	-	OK	-	-	-
	EETS	-	OK	-	-	-

Table 1: EFC applications

The reason for differentiation between “EN15509 (EasyGo basic)” and “EN15509 (CEN)” is that for EN15509 (EasyGo basic) only an attribute subset of CEN EN15509 is used. Further security level 0 or 1 is in use in NO for “EN15509 (EasyGo basic)”.

2.4 Levels of specifications and standards

There are a number of conditions for interoperability between different EFC equipment at the OBE/RSE level. These are:

Communication link compatibility

The first condition for interoperability is that equipment from various manufacturers must be able to communicate with each other. This is obtained through a set of EN standards for DSRC specifications worked out by Technical Committee CEN/TC 278 "Road transport and traffic telematics". All the EFC-applications described in chapter 2.3 conform to the base standards as shown below:

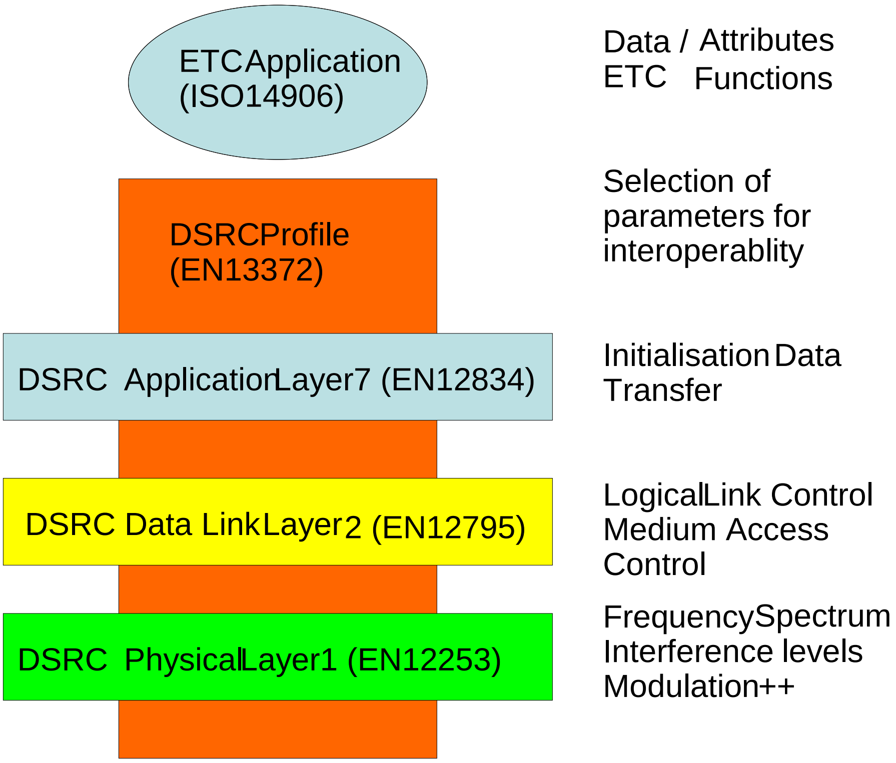
ETCApplication (ISO14906)
DSRCProfile (EN13372)
DSRC ApplicationLayer7 (EN12834)
DSRC Data LinkLayer2 (EN12795)
DSRC PhysicalLayer1 (EN12253)
Data / Attributes
ETC Functions
Selection of parameters for interoperablity
InitialisationData Transfer
LogicalLink Control
Medium Access Control
FrequencySpectrum
Interference levels
Modulation++

Figure 2: Communication link

It should be noted that DSRC Layer 1 (physical), 2 (data link) and 7 (application) in the figure above reflects the OSI model (Open Systems Interconnection Reference Model**)**. The OSI model (http://en.wikipedia.org/wiki/OSI_model) divides network architecture into seven layers which, from top to bottom, are the Application (7), Presentation (6), Session (5), Transport (4), Network (3), Data-Link (2), and Physical Layers (1). A layer is a collection of conceptually similar functions that provide services to the layer above it and receives service from the layer below it. The layers 3 to 6 in the OSI model are not applicable for DSRC communication between OBE and RSE.

Transaction Data

The data transmitted over the link carry application information such as identification number of OBE and other vital data. The application information is organised in data structures and accessed through the use of functions. This is obtained through Transponder Data Specifications (TDS) which describe the data content of the OBE for the supported EFC-applications.

Transaction Model

The sequence of data access represents a transaction. Each application supported defines a transaction model and specifies in detail an EFC transaction.

Security Architecture

Toll transactions lead to money transfers and may be subject to various attacks. Each EFC-application defines a transaction data security scheme, e.g. based on the use of an encryption algorithm, which enables a very highly protected transaction scheme.

The different EFC-applications have separate specifications with regard to Transaction Data, Transaction Model and Security Architecture. These specifications are listed in the table below:

EFC-application	Transaction Data	Transaction Model	Security Architecture
Old AutoPASS	TDS* AutoPASS	AutoPASS	AutoPASS
Old BroBizz	TDS* TFL	DCAS UK DCAS-V2-1	(Annex A in BroBizz doc.)
PISTA	TDS* ASETA	PISTA 3.4	PISTA 3.7
EN 15509 based (EasyGo basic)	EN 15509	EN 15509	EN 15509 security level 0 or 1 in NO
CEN EN15509	EN15509	EN15509	EN15509 Security level 1

*Transponder Data Specification

Table 2: Transaction Data, Transaction Model and Security Architecture

2.5 Related standardisation work and external conditions

The EN 15509 standard defines an Application Profile based on a set of base standards. The elaboration of EN15509 is based on the experiences from a large number of implementations and projects throughout Europe. The standard makes use of the results from European projects such as CARDME, PISTA and CESARE, as they represent the fruit of European EFC harmonisation and have been used as the basis for several national implementations. The development of EETS also calls for the definition of an interoperable EFC service.

Appendix A lists a.o. the relevant directives, standards and regulations referred to in this document.

3 Requirements to RSE

3.1 General

As shown in figure 1, the roadside equipment normally consists of the following main modules:

- Beacon: Device that localises and communicates with passing OBEs.
  Please note, that some functionalities assigned afterwards to beacons could be implemented on an external common beacon controller too (depending on the RSE suppliers system architecture, e.g. for time critical MLFF systems)
- Roadside controller: Computer responsible for collecting information from beacon and other subsystems, and generating a corresponding transaction for each vehicle passage, which is transferred to the CS
- Other submodules and peripherals: These include e.g. vehicle detection system which is responsible for detecting, positioning and – if applicable – classifying a vehicle. It may also include a video registration system, traffic lights and barriers. The equipment/modules in this category vary between different TCs. It is outside the scope of this specification to describe such equipment and modules

3.2 Requirements to data sets in beacon

The RSE shall support the EFC-applications and thereby the transaction models defined for PISTA, old BroBizz, old AutoPASS and EN 15509 to provide the EasyGo basic and EasyGo+ services. In case of only EasyGo+ service is to be offered, in minimum EN 15509 shall be supported. As a valid OBE type is identified through the content of EFC-ContextMark contained in the OBE (ref. chapter 4.1), the beacon must hold a list of all EFC-ContextMarks with the data sub elements ContractProvider, TypeOfContract and ContextVersion to be accepted by the RSE. This list is called here as “Contract Issuer List” (CIL) to differentiate to the TSP List used by the roadside controller which has a different purpose described in chapter 3.4. Further the beacons must store the DSRC keys in a secure manner.

3.3 Requirements to functionality in beacon

A TC has to update its CIL and DSRC keys as soon he has entered into a contractual agreement with a new TSP. CIL data contents will be composed from AIT information and OBU dependant properties. CIL updates must be possible during operation when initiated through the RSE-CS interface.

If the content of the EFC-ContextMark matches one of the entries in the CIL, the beacon shall automatically select the associated EFC-application (EN 15509 based for EasyGo basic, CEN EN15509, PISTA, old BroBizz or old AutoPASS) and assigned keys to perform the correct transaction.

The beacon must be able to handle erroneous transactions in the event that the processing of an OBE is not in accordance with the specific DSRC specification.

The communication between OBE and RSE must be fully compliant with the EFC applications for DSRC listed in chapter 2.4.

The beacon must be compliant with the EU Directive 1999/05 on Radio and Telecommunication Terminal Equipment and must be type approved in accordance with EN 300 674-2-1.

3.4 Requirements to data sets in roadside controller

The roadside controller must read and process all information necessary to create an EasyGo transaction according to the interface specification. The roadside controller produces the following information which is communicated to the CS:

- Transaction information list: A list of all EFC transactions with all relevant information, including result of validation
- Failure transaction list: A list of incomplete or erroneous EFC transactions (if information is not included in the Transaction information list; implementation is up to the TC)

In order to perform the appropriate OBE validation checks, the roadside controller must contain validation lists to be downloaded from the CS. For the EasyGo services, the following lists are needed at the roadside controller:

- Status lists: Contains identification of all valid OBEs assigned to national/local user agreements
- TSP list: Contains a “mask” of legal OBE ID ranges for each specific TSP having a contract with an EasyGo service. This TSP list is used to filter unused OBE ID ranges in order to reduce the size of the Black list
- Black list: Contains identification of all invalid OBEs assigned to foreign user agreements
- HGV list (if applicable): This is a list of all Heavy Goods Vehicles assigned to foreign user agreements. This table may reside in the roadside controller, but the task of identifying foreign HGVs may also be handled without transferring HGV list to RSE (ref. description in chapter 6.3.3)

The format of the lists above must follow the interface specifications for the relevant EFC application (See annex 2.3).

3.5 Requirements to functionality in roadside controller

The main task of the roadside controller, related to EFC transactions, is to validate the OBEs of passing vehicles. The validation logic is described in chapter 5. The roadside controller must be able to give the correct signal to the SU to inform if the passage is OK or not OK (or open the barrier if the lane is equipped with such). If the system supports additional signals to the user, e.g. if a user account has low balance, the controller must be able to give such a signal.

3.6 Transfer of data to RSE – CS

The RSE shall communicate the transaction data to the CS of the TC according to predefined procedures and intervals. There must be mechanisms that prevent repeated transfers of the same transaction lists, and there must be mechanisms detecting and reporting unsuccessful or missing transfers of transaction data. It must be possible to manually repeat transfers of missing transaction data. Transaction data must under no circumstances be lost.

All lists and tables needed at RSE must be frequently updated in the RSE in order to ensure correct transaction result at the roadside. Updates of tables must be sent from the CS at least once a day. There must be secure transfer mechanisms that detect and report unsuccessful or missing transfers of validation tables to the roadside.

3.7 Requirements to data storage in roadside equipment

In case of communication error with the CS, it must be possible to buffer transaction data for at least 5 days (if no longer buffer period is requested by the TC). The storage capacity must be dimensioned after transaction volume in addition to other storage requirements.

4 Requirements to OBE

4.1 Requirements to data sets in OBE

General

All the data elements used in the communication between RSE and OBE are compliant with the EN ISO 14906 standard. These data, also called attributes, should be defined and initialised during the personalisation process of the OBE.

Personalisation of OBEs can partly be carried out by the supplier of the OBEs and partly by the TSP. There is no standard describing who shall do what and this may therefore vary for different populations of OBEs. In EasyGo basic the suppliers carry out a limited personalisation of the OBEs while the TSP does not add any data. In EasyGo+ the TSPs personalise each OBE with customer specific data.

Attributes are addressed by the Attribute identifier (AttrID). The attributes differ between the various EFC-applications as shown in table 3 below.. The EasyGo+ service is based on EN 15509 security level 1. Also the newest generation of AutoPASS OBEs (EN15509 (EasyGo basic)) requires security level 1. Other EasyGo basic OBEs are based on EN 15509 security level 0. For details to DSRC security see chapter 7.4.

Attribute ID		**EFC Application**				
Attribute name	**Id**	**EN 15509 based (EasyGo Basic)**	**CEN EN15509**	**PISTA**	**Old BroBizz**	**Old AutoPASS**
Security level (EN15509)		**0 (0 or 1 in NO)**	**1**			
Contract *(Information associated with the service rights of the TSP of the EFC service)*						
EFC Context Mark	0	Yes	Yes	Yes	Yes	Yes
Contract Authenticator	4	-	-	Yes		
Vehicle *(Identification and characteristics of the vehicle.)*						
Vehicle Licence Plate No	16		Yes			
Vehicle Class	17		Yes			
Vehicle Dimensions	18					
Vehicle Axles	19		Yes			
Vehicle Weight Limits	20					
Vehicle Specific Characteristics	22		Yes			
Vehicle Authenticator	23	-	-			

Attribute ID		**EFC Application**				
Attribute name	**Id**	**EN 15509 based (EasyGo Basic)**	**CEN EN15509**	**PISTA**	**Old BroBizz**	**Old AutoPASS**
Security level (EN15509)		**0 (0 or 1 in NO)**	**1**			
Equipment *(Identification of the OBE and general status information*						
Equipment OBE ID	24	Yes	Yes	Yes		
Equipment Status	26		Yes	Yes		
Payment *(Data identifying the Payment means and its validity)*						
Payment Means (PAN)	32	Yes	Yes	Yes		
NTD Data 1 (NO OBE ID)	99					Yes
PAN/OBE ID (BroBizz no.)	101				Yes	
Receipt *(Financial and operational information associated with a specific session.)*						
Receipt Data 1	33		*)	Yes		
Receipt Data 2	34	Yes	*)	Yes		
Other data (private attributes)						
Private Licence plate number	91			Yes		
Private shadow class	92			Yes		
Private reserve	93			Yes		
Private Blacklist	94			Yes		
NTD Data 2	100					Yes
NTD Data 3	127					Yes

*) …optional, set and use up to the TC

Table 3: Attributes

This document does not contain a detailed description of the data elements involved in the communication including length and format. However, some of the most vital data elements are shortly described in the following:

Vehicle Service Table

The Vehicle Service Table (VST) is a data structure that is sent by the OBE in the initialisation phase of a DSRC communication to RSE.

EFC-ContextMark

According to CEN standard EN 14906 a contract is identified by the EFC-ContextMark that is contained in the VST. The EFC-ContextMark is used to select the EFC Application – and thereby the protocol - to be used in the communication. The EFC-ContextMark contains the following elements:

- ContractProvider
- TypeOfContract
- ContextVersion

The element ContractProvider identifies the OBE issuer (TSP). Each TSP has been assigned a unique identifier that consists of a country code and a number that is assigned nationally. The ContractProvider identification system is defined according to ISO 14816. In other words, the EN ISO 14906 base standard has indirect references to the EN ISO 14816 on numbering and data structures.

TypeOfContract and ContextVersion are elements that identify certain contractual or technical choices that are available with each TSP's ContractProvider data. Both elements must be in accordance with content of OBE stated by the OBE issuer.

An overview of context marks and PAN numbers for individual contract providers is shown in appendix C

Identification of OBE account

Another essential data element is the identification of the individual OBE. The identifier used for the purpose of identifying the OBE account is "PersonalAccountNumber" (PAN) or the "OBE ID", depending on EFC application resp. the TC or TSP.. The PAN/OBE ID is contained in different OBE Attribute IDs for the different EFC applications.

- PISTA and EN 15509 use Attribute ID no. 32 for PAN in PaymentMeans, EN15509 contains the EquipmentOBUId in attribute 24, which forms the OBU ID together with the data for ContractProvider and OBE manufacturer ID for OBE identification in Austria for EasyGo+ OBE.
- Old BroBizz uses Attribute ID no. 101 (OBE ID)
- Old AutoPASS uses Attribute ID no. 99 (part of NTD Data 1).

The RSE must be able to select the correct attribute depending on the protocol to be selected.

The PAN has a standard syntax defined in ISO 7812. However, the Old AutoPASS and Old BroBizz applications do not comply with this ISO standard. Annex A in this document describes the different OBE identification syntaxes used in the supported EFC-applications.

4.2 Requirements to response times

The OBE must be able to communicate correctly and reliable with the beacon, independent of vehicle speeds, even under multilane free flow conditions. A precondition for this requirement is that the roadside equipment does not limit the communication sequence.

4.3 Requirements to personalisation

All OBEs must be initialized by the supplier prior to use by setting values for agreed EFC attributes.

Other EFC attributes must be individually personalised by the TSP. Only EasyGo+ OBEs are, as of today, personalised by the TSP.

For further details on personalisation of EasyGo+ OBEs see EasyGo document 202-B.

5 Requirements to interface OBE-RSE

5.1 General principles

The RSE is the master of the communication and is therefore generally free to request any available data attribute stored in the OBE. It can decide which transaction to perform with the present OBE. The OBE only responds to "requests" from the RSE. Therefore, the RSE shall decide which data to retrieve and hence which transaction to perform.

The interface consists of the following main steps:

1. Initialisation
2. Identification of OBE type
3. Transaction

Note that this figure does not depict the actual flow of the transaction, but only the logical flow to determine the result of the transaction. The actual flow always respects the relevant specification. Access to data in the OBE may be regulated by specific security mechanisms. If the OBE answers with an access denial, the transaction is aborted.

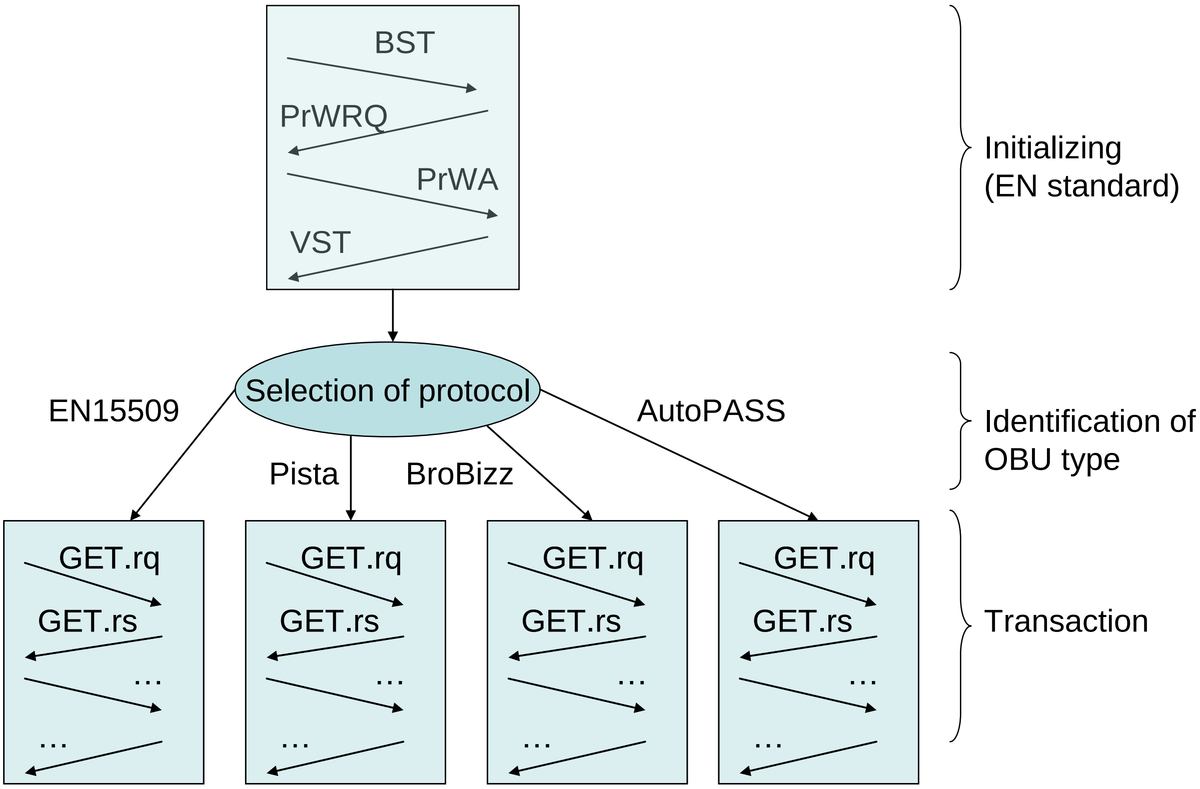

Figure 3: RSE – OBE communication

Initialisation phase

The beacons periodically broadcast a Beacon Service Table (BST) with ApplicationID = 1 (EFC). At the passage of a vehicle with a system compliant OBE under the RSE, the OBE receives the BST. It answers with a PrWRQ (Private window request) and the RSE returns a PrWA (Private window allocation). If the OBE contains an EFC-Context Mark with ApplicationId = 1, it answers with a Vehicle Service Table (VST). Each time the RSE receives a VST from an OBE, it analyses the attribute EFC-ContextMark and the data elements EquipmentClass/ManufacturerID in order to decide how to handle the OBE (i.e. which application to use).

Identification of OBE type

The OBE's type is detected through the content of EFC-ContextMark. If the elements in EFC-ContextMark (ContractProvider, TypeOfContract, ContextVersion) match one of the entries in the CIL (a table contained in the beacon with all valid EFC-ContextMark data), the RSE will use the associated application (EN15509 for EasyGo basic, CEN EN 15509, PISTA, BroBizz or AutoPASS) to perform a transaction. If the VST contains a list of (more than one) EFC-ContextMark, the first entry will be used that can be matched with the CIL.

Transaction

If the EFC-ContextMark/EquipmentClass/ManufacturerID matches a valid entry, the transaction starts with the Presentation phase; otherwise the transaction is directly released with the Closing phase. A communication that does not reach the Presentation phase is not considered as a "transaction": it will not be further registered by the RSE and no transaction record will be created.

The different applications have different transaction models that represent the protocols and thus control the data exchange in this communication.

The RSE requests the OBE to present some parts or all of its data. This is done by requesting the content of specific data attributes in the OBE (GET.Request). Additionally, the RSE can request the OBE to send an authenticator for some data (GET_STAMPED.Request).

Use of AccessCredentials, authentication, is also controlled by the application-dependant protocol.

5.2 Transit Information Record

At completion of the DSRC transaction, a data record is created at the RSE for each transaction. This record is stored in the database at the RSE in order to be transferred to the CS. The transit information record contains a.o.:

- Date and time of the transaction
- Location of the transaction, according to the RSE location numbering scheme
- Application data retrieved from/written into the OBE
- If applicable: The account balance of an OBE with on-board account before debiting the fee

- The fee due and actual debited fee
- The completeness of the transaction
- The transaction result

Transactions which are interrupted after the Presentation phase are marked as incomplete or exceptions.

5.3 Coding of data elements

The detailed content and the format of the transaction list are application dependent (For details see EasyGo documents 201, 202 A-E and 203.

6 OBE validation

6.1 Main principles

When an OBE passes through a charging point, the RSE must determine if the OBE is valid or not and confirm the validity of the OBE to the SU by showing an audible and optionally a light signal in the OBE and / or by opening the barrier. This verification process will also determine the transaction data that needs to be registered and forwarded to the TSP.

The main principles of the process are described below:

The validation of OBEs by the RSE includes two levels:

1. Validation of the EFCContextMark (drawn in yellow in figure 4)
2. Validation of PAN number resp.OBE ID against tables in RSE (Status lists, Black list etc., drawn in blue in figure 4).

An OBE may be rejected in both levels.

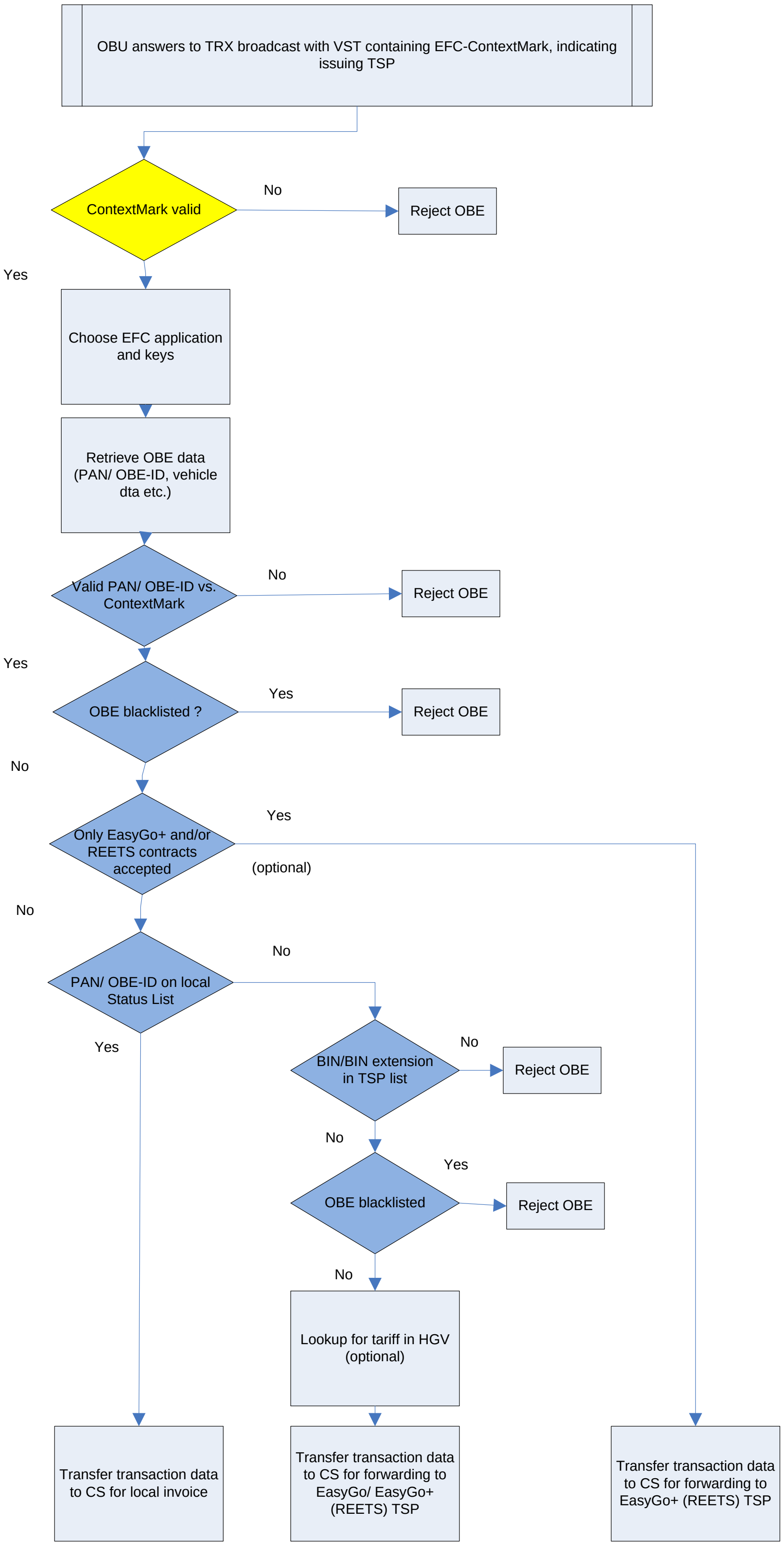
OBU answers to TRX broadcast with VST containing EFC-ContextMark, indicating issuing TSP
ContextMark valid
No
Reject OBE
Yes
Choose EFC application and keys
Retrieve OBE data (PAN/ OBE-ID, vehicle dta etc.)
Valid PAN/ OBE-ID vs. ContextMark
No
Reject OBE
Yes
OBE blacklisted ?
Yes
Reject OBE
No
Only EasyGo+ and/or REETS contracts accepted
Yes
(optional)
No
PAN/ OBE-ID on local Status List
No
Yes
BIN/BIN extension in TSP list
No
Reject OBE
No
OBE blacklisted
Yes
Reject OBE
No
Lookup for tariff in HGV (optional)
Transfer transaction data to CS for local invoice
Transfer transaction data to CS for forwarding to EasyGo/ EasyGo+ (REETS) TSP
Transfer transaction data to CS for forwarding to EasyGo+ (REETS) TSP

Figure 4: OBE validation

6.2 Validation process for a passing OBE to be accepted at RSE

The first validation is done by the DSRC beacon by checking the EFCContextMark of the OBE. An OBE which does not contain EFC-ContextMark data matching an entry in the CIL will be rejected.

If the EFC-ContextMark of the OBE is approved, the following sequence is initiated:

i. The EFC-ContextMark includes information that decides to continue the communication with the OBE
ii. When the (contract-) type of OBE is determined, the type of EFC application and thereby the structure of the OBE content is known
iii. From the data content of the OBE the validation of the OBE can be further performed by checking the PAN and/or OBE ID and after that …
iv. The necessary data is retrieved from the OBE in order to save the information in the Transit Information record

6.3 Further Treatment of OBE

After OBE validation acc. to ch. 6.2 following checks will be carried out:

6.3.1 OBE assigned to a local/national agreement

Some countries use Status lists to validate local/national agreements. The check against the local Status list is the first control in order to find out if there is a local agreement assigned to the OBE.

Local Status lists can contain any type of OBE authorized for use in EasyGo. This is according to the overall requirement that all EasyGo OBEs can be used for local agreement. If the OBE is valid on the local Status list it will be accepted and treated according to the local agreement.

The format of the local Status list is decided locally and is not a part of the EasyGo specifications.

If the OBE is not on the local Status list it must be treated as an OBE with a possible EasyGo agreement. Therefore, the next check will be:

6.3.2 OBE valid in a foreign EasyGo agreement

Validation of EasyGo OBEs is based on an TSP list and a Black list. In order to reduce the size of the Black list, the validation logic first checks the OBE against the TSP list.

The TSP list is produced based on information from all EasyGo TSPs concerning own OBEs numbering system and ranges of OBEs issued. The first 6 digits in the PAN /OBE ID are called BIN (Binary Identification Number), and the next 6 digits are called BIN extension. An TSP list contains information about legal PAN /OBE ID ranges, represented in a “BIN/BIN-extension mask”, for all TSPs. If the OBE is outside the valid range of BIN/BIN-extension it will be rejected. TCs are responsible to perform this control. TCs which also has the role of a TSP may choose to exclude own OBEs from this control in order to avoid double control.

The tablets list with intervals of approved BIN no. for each TSP must be updated each time a new TSP is introduced in the system, or each time a new PAN /OBE ID series outside the current defined range is introduced.

In order to check the validity of the OBE further a check against the Black list must be executed. The Black list includes full OBE (PAN) number for all invalid OBE.

If the OBE is on the Black list, the OBE will be handled according to the specified parameter “Action to take” in the Black list. In EasyGo only rejection of the OBE is used as a valid action to take.

Reason of rejection is stated in order to inform SU when rejected. The TC must include this information according to agreement in EasyGo.

6.3.3 EasyGo agreements for vehicles registered on the HGV list

EasyGo basic OBEs do not carry information about the vehicle classification (weight, dimensions, axles, emission etc.). As some countries do not employ automatic classification at the charging points, the vehicle category of foreign vehicles therefore cannot be determined.. Due to this, a HGV (Heavy Goods Vehicle) register has been established which contains a list of all heavy vehicles (> 3500 kg). TSPs provide input to these HGV lists. The EasyGo HUB compiles this input and a global HGV list is forwarded to all EasyGo TCs.

Also many passenger cars have gradually been included on the HGV list to allow a match between vehicle and license plate number in those cases where the TSP does not employ a one-to-one relation between OBE and license plate. If such a link is not present, the TC cannot identify the SU if the OBE is not correctly read.

Austria has introduced differentiated toll fees based on the emission class of the HGVs and it is mandatory for heavy vehicles to be equipped with an approved OBE from which the relevant vehicle characteristics can be read.

Norway is preparing the introduction of toll fees based on environmental characteristics for passenger cars as well as for HGVs. The emission classes, fuel types etc. of vehicles with EasyGo basic OBEs need to be determined from the HGV list. A solution is being prepared, where it will become mandatory for foreign vehicles (passenger cars and HGVs) to be registered on the HGV list with the relevant vehicle characteristics, to be able to determine the correct price.

The content of the HGV list is described in EasyGo document 203 in detail.

The HGV list includes full OBE (PAN) number for all OBEs issued for valid agreements for HGVs. If the OBE ID read at the beacon is on the HGV list, the information can be used by the TC to price the transaction. Information regarding declared licence plate - if this is provided - will be sent to the TSP in order to fulfil the SU’s need for information on the invoice.

The use of HGV list on the CS level or RSE level is optional for the national EFC-applications. The national tolling systems may choose different solutions to incorporate HGV information at the RSE. Alternative solutions that are implemented are e.g.:

- Using the HGV list directly at the roadside. In this case an OBE ID/PAN is checked against the HGV list after the accepted Black list validation
- By inserting the OBEs from HGV list on the local Status list. In this case the OBE will be validated in a similar way as an OBE assigned to a local agreement even if it is a foreign EasyGo transaction

Note that the latter solution requires that OBEs on the HGV list only should contain valid agreements. When an OBE is no longer valid it will be removed from HGV list and consequently from local Status list.

Generally, if the HGV list is not present at roadside equipment it is the TC responsibility to ensure that the information from the HGV list is included before the EasyGo transaction is sent to the foreign TSP.

6.3.4 Possible alternative check procedure for systems without basic EasyGo agreements

If there is no need for an RSE to support basic EasyGo OBE, but only EasyGo+ and CEN EN15509 OBE (like REETS OBE) a simpler OBE check procedure involving only a Black list could take place after OBE validation (See ch. 6.1/ Fig 4).

7 Appendices

7.1 Appendix A - Directives, standards and regulations and referenced EasyGo documents

7.1.1 Tolling related EC Decisions, Directives and regulations

- EFC Directive 2004/52/EC on the interoperability of electronic road toll systems in the community
- Commission Decision 2009/750/EC on the definition of the European Electronic Toll Service and its technical elements

7.1.2 Tolling related Standards

Standard	**What**	**Year *)**	**Document name**
EN 12253	Layer 1 OSI-model for DSRC		Road Transport and Traffic Telematics (RTTT) – Dedicated Short-Range Communication (DSRC) Physical layer using microwave at 5.8 GHz
EN 12795	Layer 2 OSI-model for DSRC		Road Transport and Traffic Telematics (RTTT) – Dedicated Short-Range Communication (DSRC) – DSRC data link layer: Medium access and logical link control
EN 12834/ ISO15628	Layer 3 OSI-model for DSRC		Road Transport and Traffic Telematics (RTTT) – Dedicated Short-Range Communication (DSRC) – Application Layer
EN 13372	DSRC Profiles		Road Transport and Traffic Telematics (RTTT) – Dedicated Short-Range Communication (DSRC) – Profiles for RTTT applications
EN ISO 14816	Numbering system	2005	Road Traffic and Transport Telematics (RTTT) – Automatic Vehicle and Equipment Identification – Numbering and Data Structures
ISO/FDIS 14906:2011 with Amd1:2015EN	EFC Application Interface	2011/ Amd1 :2015 2011	Road Traffic and Transport Telematics (RTTT) – Electronic Fee Collection – Application interface definition for dedicated short range communication
EN 15509	Application	2014	Road Traffic and Transport Telematics (RTTT) – Electronic

Standard	What	Year *)	Document name
	profile for a DSRC standard		Fee Collection – Interoperability application profile for DSRC
EN 14907	EFC Application Interface test		Part 1: To prescribe procedures and conditions for tests of EFC-related equipment Part 2: To prescribe conformance tests for On –Board equipment, conforming to ISO 14906
ISO 7812	Numbering system of PAN/OBE ID	2006	ISO/IEC 7812-1:2006 Identification cards -- Identification of issuers -- Part 1: Numbering system ISO/IEC 7812-2:2007 Identification cards -- Identification of issuers -- Part 2: Application and registration procedures

Table 4: Standards

*) For dated references, subsequent amendments to or revisions of any of these publications apply only when incorporated in it by amendment or revision. For undated references, the latest edition of the referenced publication applies.

7.1.3 Referenced EasyGo documents

EasyGo Document	EasyGo JVA or TSPA Contract Annex	Date / Version	Document title
103	1.3		EasyGo security policy
202	2.2		EasyGo: Roadside and on board equipment (This document)
202-A			EasyGo+: OBE Functional requirements (Enclosure A to EasyGo document 202)
202-B			EasyGo+ OBE Personalization, Configuration and Operating Parameters (Enclosure B to EasyGo document 202)
202-C			EasyGo+: DSRC Transaction for Tolling and Enforcement (Enclosure C to EasyGo document 202)
202-D			EASYGO+: RSE Functional Requirements (Enclosure D to EasyGo document 202)

EasyGo Document	EasyGo JVA or TSPA Contract Annex	Date / Version	Document title
202-E			EASYGO+: OBE Compatibility Tests (Enclosure E to EasyGo document 202)
206	2.6		EasyGo test trategy

Table 5: EasyGo documents

7.2 Appendix B – PAN- (OBE ID-) notations in EasyGo

PAN’s in EasyGo should generally follow the ISO 7812 identification numbering system. This standard is also used for card numbers. The different digits are divided as follows:

```
    1          2-6              7-v         last
+-----+--------------------+------------+-------------+
| MII | TSP identifier     |            |             |
+-----+--------------------+ account #  | check digit |
| TSP identification #     |            |             |
+--------------------------+------------+-------------+
|          ISO 7812 identification number             |
+-----------------------------------------------------+
```

MII = Major Industry Identifier as follows:

0 - for ISO/TC 68 and other industry assignments

1 - airlines

2 - airlines and other industry assignments

3 - travel and entertainment

4/5 - banking/financial

6 - merchandizing and banking

7 - petroleum

8 - telecommunications and other industry assignments

9 - for national assignment

If the number starts with 9, the next three digits are the numeric country code as defined in ISO 3166 and the remainder of the numbers is as defined by that national standards body for that country.

Account numbers are variable length up to a maximum of 12 digits.

The check digit is calculated modulo 10 by the Luhn formula over all the preceding digits as specified in ISO 7812.

PISTA (implementation of PISTA for Storebælt)

This implementation has chosen ”9” as a MII. Other implementations of PISTA have chosen 3, 4 or 6 as a MII. “9” as a MII means that position 2-4 should be used as a country code in accordance with ISO3166-1. In Denmark this country code is 208. Since there are only 2 digits left to define Issuer it is recommended from ISO to use 2 characters from Individual account for this purpose. For Storebælt the TSP identifier is 6062. This recommendation has been a standard. The total length may be 16-19 digits. The PISTA implementation for Storebælt uses 16 digits. A full overview of the syntax is then:

MII:	1 character
Country code:	3 characters
TSP code:	4 characters
Individual account:	7 characters
Luhn-kode:	1 character

PISTA (implementation of PISTA for Øresund)

This implementation has chosen”6” as a MII means that position 2-6 should be used as the TSP identifier. The PISTA implementation for Øresund has the identifier 04882 and uses 16 digits.

EN 15509

EN 15509 uses the same ISO 7812 coding as described for PISTA

Old BroBizz

BroBizz has a proprietary format of PAN which does not conform to ISO 7812. The format is:

Contract Provider*:	6 characters
Individual account:	9 characters
Luhn-code:	1 character

*) For the BroBizz implementation it was chosen to use Contract Provider as the first 6 characters. Contract Provider is a code read from EFC-ContextMark. For Storebælt this is 978003 and for Øresund 460010 (originally the ContractProvider is A40001 for Øresund, but since it was not possible to use alphanumeric for this purpose, it was converted to 460010). Contract Provider consists of Country Code (10 bits) and Issuer code (14bits).

Old AutoPASS

AutoPASS has a proprietary format of OBE ID which does not conform to ISO 7812. The format is:

Country code:	3 characters
TSP code*:	5 characters
Individual account:	10 characters

The country code for Norway is 578 according to ISO3166-1.

*) Norwegian TSP codes are numbered from 1 and up. Today all TSP ID’s in Norway are < 100. The TSPs are registered in the standard ISO 14816.

7.3 Appendix C - Overview of EFC-Context marks and PAN content

The AIT list contains the same type of information as described in the table below. An updated version of the AIT list can be accessed from the EasyGo HUB.

EFC Application	EFC-ContextMark			PAN
	Contract Provider (hex)	Type of Contract (hex)	Context Version (hex)	(dec)
Old AutoPASS	30C0xx (xx = Issuer ID)	0001	01	578 000xx yyyyyyyyyy (xx = Issuer ID)
Old BroBizz	Storebælt: 978003	0000	01	978 003 xxxxxxxxxx
		0001	01	
	Øresund: A40001	0001	01	460 01x xxxxxxxxxx
PISTA	Storebælt: 978003	0001	02 and 03	920860 6204 xxxx xxx
	Øresund: A40001	0001	02	604882 xxxx xxxx xx
EN 15509	BroBizz: 978003	0001	04	920860 6204 xxxx xxx
	BroBizz (EasyGo+): 978003	0001	07	920860 6298 xxxx xxx
	Øresund: A40001	0001	03	604882 xxxx xxxx xx
	ASFINAG(EasyGo+): C04001	7100	05 … 08	308417 xxxx xxxx xxxx x
	AutoPASS 30C0xx (xx=issuer ID)	0001	02	957800xx yyyyyyyy

Table 5: Context marks

7.4 Appendix D - Security requirements and architecture

7.4.1 General security requirements

In order to obtain the desired level of security the different applications have security schemes. A security scheme is a set of cryptographic algorithms and security mechanisms related to the OBE and RSE operations defined in these specifications. The OBE and RSE shall implement the security mechanisms described in the security specifications

The OBEs and EFC Applications shall conform to ISO/TS 19299 (EFC security framework) and CEN ISO /TS 17574 (Guidelines for security protection profiles.).

A set of basic requirements that the security schemes must follow is listed below:

- Each OBE shall be uniquely identified and registered in a list of OBEs manufactured
- Each OBE shall be capable of authenticating itself to the RSE in a time variant manner to prevent replays by unauthorised devices trying to impersonate existing OBEs or trying to clone the functionality of the OBE
- Each OBE shall ensure the continued correct operation of its security functions and the integrity of stored critical data (such as cryptographic keys), in both normal and extreme environmental conditions.
- Unauthorized alteration by physical or logical tampering of critical data (such as cryptographic keys) or software stored in the OBE shall be prevented
- The OBE manufacturer shall keep an exact record of all the OBEs manufactured and initialized for a given TSP (TC)
- The OBE manufacturer shall take the appropriate measures to ensure the secure storage of the OBEs manufactured and initialized, and secure their delivery to the TSP (TC)
- The OBE manufacturer shall implement adequate procedures and protocols to ensure the security of the transfer and update of critical information (including but not restricted to: TSPs (TCs) own cryptographic keys, cryptographic keys belonging to other TSPs (TCs)
- The OBE manufacturer shall implement adequate procedures and protocols to ensure the security and the non-disclosure of the critical information (including but not restricted to the cryptographic master keys) used to initialize / personalize the OBEs
- The only keys which shall be stored in the OBE are diversified keys (diversified using the PAN / OBE ID)
- Each RSE shall be uniquely identified and registered
- Each RSE shall be capable of authenticating itself to selected other sub-systems (such as the CS)
- Unauthorized alteration of critical data (i.e. cryptographic keys) stored in the RSE shall be prevented
- The RSE shall support message integrity and authentication mechanisms for the data it transmits or receives
- The RSE shall provide protection to the critical data (i.e. cryptographic keys) stored in it against unauthorized disclosure by physical or logical tampering
- The transaction process shall include the authentication of the OBE by the RSE

- The integrity of ID information transmitted by the OBE shall be ensured
- The protocol used for communication between the OBE and the RSE shall provide adequate protection against replay
- Adequate protection shall be provided against threats to the availability of the interface OBE-RSE

7.4.2 Description of security architectures in EFC applications

The different EFC applications have different security architectures which are described in the following:

Old AutoPASS

The AutoPASS security scheme is based upon the following principle:

- two (2) types of keys are stored into the OBE, and for each type of keys, five (5) generations of cryptographic keys are stored in the OBE.
- two (2) Message Authentication Codes (MACs) are computed and returned by the OBE. Checking these MACs allows the TCs to take any appropriate actions in case the OBE is not authentic (i.e. a photo of the licence plate of the violating vehicle).

The first Message Authentication Code (MAC1) is used by a TC to check the authenticity of an OBE that the same TC/TSP has issued (it is usually a combined TC/TSP role in Norway). The second Message Authentication Code (MAC2) is used for interoperability purposes, to allow another TC/TSP than the one who issued the OBE to perform an early detection of a foreign vehicle equipped with an unauthorised/illegal/illicit OBE.

Old BroBizz

The same as PISTA (see below)

PISTA

The PISTA security architecture is based on two different and complementary levels of security, named respectively Data Certification and OBE Authentication. No access credentials mechanism is part of the common service, as the authentication of the RSE in front of the OBE has not been considered as necessary. Each OBE supports both levels of security, and the RSE is responsible for selecting the one to be applied by means of relevant function invocation. The OBE shall be fully initialised from the beginning and shall store all keys even if they shall not be used from the beginning. The common service shall be based upon the first level of security, Data Certification, and then eventually upgraded to higher levels of security, OBE Authentication, in case a significant level of fraud is detected. (See also the PISTA deliverable D3.7 Agreement on Security).

EN 15509

The European Standard EN 15509 defines security features and mechanisms based on the general security framework defined in EN ISO 14906. EN 15509 allows for implementation of two different security levels (0, 1). Security level 0 is mandatory while security level 1 is optional.

Security level 0 defines calculation of an authenticator to validate data integrity and origin of application data. A Message Authentication Code (MAC) is calculated using a DEA algorithm according to ANSI X3.92

Security level 1 supports in addition to calculation of authenticators the calculation of Access Credentials for protection against non-authorised access to sensitive user data and against use of OBE by non-authorised parties. In this calculation the OBE sends a VST that for each contract contains information about an Access Credential Reference and a random number. Access Credential Reference contains the diversifier and a reference to a secret master key that shall be used for the computation of a secret key.

Currently EasyGo+ OBEs and AutoPASS OBEs based on EN 15509 use security level 1. Other OBEs use security level 0.