Roadside and on board equipment

Annex 2.2 to

Joint Venture Agreement
Toll Service Provider Agreement

This copy of the document was published on www.easygo.com and is for information purposes only. It may change without further notice.

Internet copy
www.easygo.com

Document: 202
Version: 2.0
Date: 2 May 2013

Table of contents

Internet copy www.easygo.com

Internet copy
www.easygo.com

Document revision history

Version	Date	Author	Main changes
0.1	2011.08.03	ASK / TCL	Draft
0.2	2011.08.10	HHA	Comments, changes for EasyGo+
0.21	2011.08.17	HHA	PAN for ASFINAG added
0.22	2011.11.18	HHA	Chapter 4.3 new EMC directive added, editorial changes
0.91	2012.01.25	TCL / ASK / SR	Minor changes / editorial changes
1.0	2012.03.14	TCL / ASK / SR	Approved by steering committee with minor comments
1.1	2013.04.23	HHA	Annex E (OBE Compatibility Tests) added
2.0	2013.05.02		Approved by SC

Internet copy
www.easygo.com

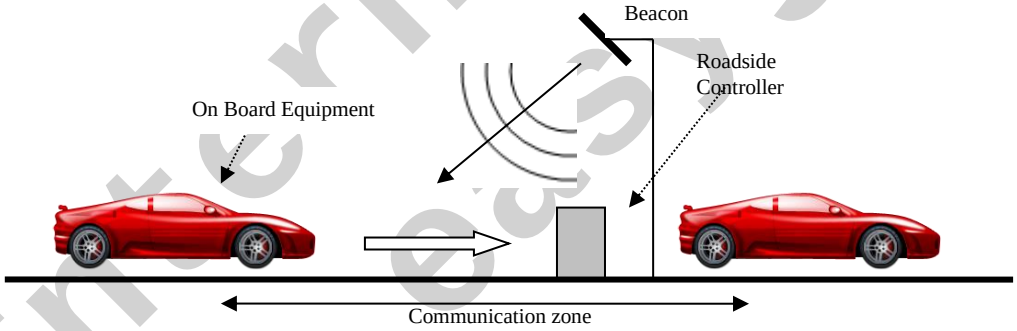
1 Introduction

This document defines the basic requirements for interoperability between the electronic toll collection systems with regards to roadside equipment and on board equipment. The scope of these specifications is primarily for use within EasyGo, but also to enable interoperability with other EFC systems in Europe including the planned European Electronic Toll Service - EETS.

It should be emphasized that this document only specifies the overall principles and requirements for technical interoperability between RoadSide Equipment (RSE) and On Board Equipment (OBE[1]). To enable implementation of the individual EFC-application (AutoPASS, BroBizz, PISTA and EN15509) the detailed specification of these applications must be included.

The document also describes personalisation of the OBE and 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 roadside equipment 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.



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 it 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] The terms «OBE» (On Board Equipment) and "OBU" (On Board Unit) are synonymous.

Internet copy
www.easygo.com

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. By different EFC-applications is meant existing systems such as AutoPASS, BroBizz and PISTA and the new standard EN 15509 which will be mandatory in the new European Electronic Toll Service – EETS.
- 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
- Chapter 7 describes the requirements related to certification of OBEs and RSE
- Chapter 8 explains the security mechanisms presently employed by EasyGo and the challenges and possible solutions in an EETS environment
- Chapter 9 gives an overview of relevant directives, standards and regulations that are relevant to the EasyGo service and a future EETS on the RSE – OBE level.
- Chapter 10 (Annexes) gives additional information or references to further documents:
    - Annex A explains PAN/ OBE ID notations
    - Annex B is listing additional EasyGo documentation available for details on related topics

Internet copy
www.easygo.com

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 service combines several EFC -applications and has 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.

It must be noted that the newest EFC application to be supported in the EasyGo service, which is EN 15509, shall be implemented at all EasyGo RSE. This is because the EasyGo+ service is based on this standard which is mandatory in implementing the EFC Directive.

EasyGo+ is based on EN15509 security level 1 while EN15509 security level 0 will be used for the basic EasyGo service.

2.2 Overview of roadside functionality

The RSE should be able to perform transactions with all the OBE types that are approved for the services. These 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 not described in this document.

The transaction data provide all information required to charge the customer's account for the due fee.

2.3 EFC-applications to be supported

The following EFC-applications are supported in the EasyGo service:

Internet copy
www.easygo.com

EFC-application	Description	Service
Auto-PASS	Norwegian DSRC-based toll collection system administrated by the Norwegian Public Roads Administration. AutoPASS is an national interoperable service	EasyGo
BroBizz	Danish/Swedish DSRC-based toll collection system developed for Storebælt and Øresund.	EasyGo
PISTA	"*Pilot on Interoperable Systems for Tolling Applications*". Its origin was 5th RTD Framework Programme. The mission of this project was to demonstrate on the feasibility of implementing interoperable EFC systems along different toll highway facilities in several countries belonging to EU.	EasyGo
CEN EN 15509	The European Committee for Standardisation - CEN - has developed a European Standard for DSRC interoperability. EN15509 is being referenced as the CEN standard that provides a basis for industry to manufacture interoperable EFC-applications for DSRC-enabled road charging systems. EasyGo+ is based on EN15509 security level 1 while EN15509 security level 0 will be used for the basic EasyGo service. It is not yet decided if EETS will use security level 0 or 1.	EasyGo EasyGo+ EETS

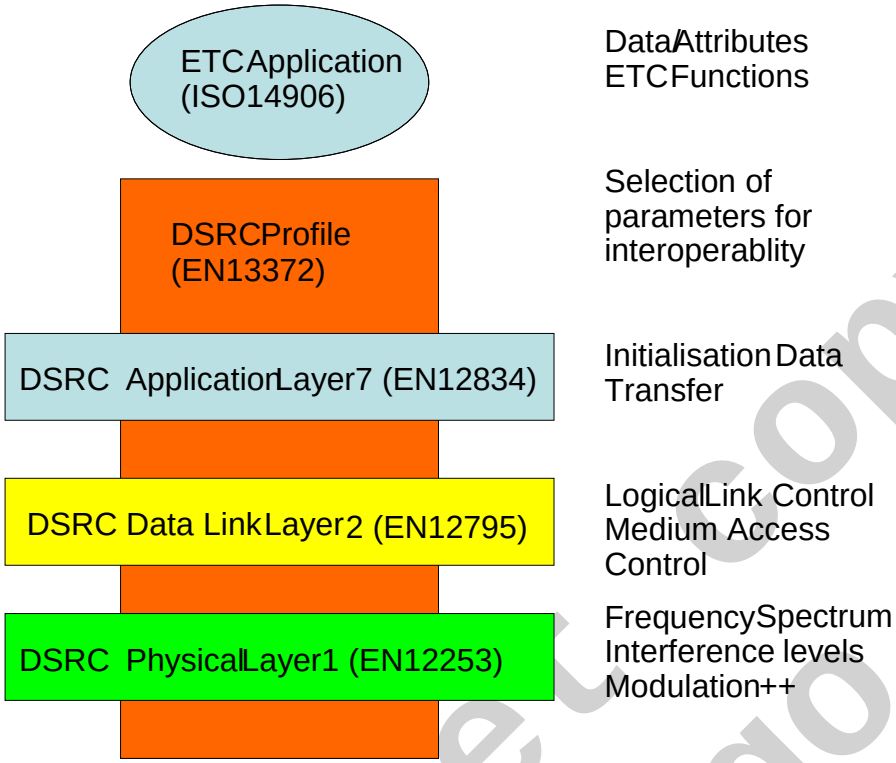
2.4 Levels of specifications and standards

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:

Internet copy www.easygo.com



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.

Internet copy
www.easygo.com

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
AutoPASS	TDS* AutoPASS	AutoPASS	AutoPASS
BroBizz	TDS* TFL	DCAS UK DCAS-V2-1	(Annex A in BroBizz doc.)
PISTA	TDS* ASETA	PISTA 3.4	PISTA 3.7
CEN EN 15509	EN 15509	EN 15509	EN 15509

*Transponder Data Specification

2.5 Related standardisation work and external conditions

The DRSC specification standardisation work done by Technical Committee CEN/TC 278 "Road transport and traffic telematics", WG9, has a history back to 1993. Pre-standards were approved in the period 1997-1999, and full standards were established in 2000-2001.

The European Standard EN 15509:2007 defines an Application Profile based on a set of base standards. The elaboration of EN 15509 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 a common European Electronic Toll Service (EETS) for the implementation of the European EFC Directive (2004/52/EC) also calls for the definition of an interoperable EFC service.

Chapter 9 lists the relevant directives, standards and regulations referred to in this document.

Internet copy www.easygo.com

3 Requirements to RSE

3.1 General

The roadside equipment normally consists of the following main modules:

- Beacon: Device that localises and communicates with passing OBEs
- 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 barrier. The equipment/modules in this category vary for 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, BroBizz, AutoPASS and EN15509 to provide the EasyGo and EasyGo+ services. In case of only EasyGo+ service is to be offered, in minimum EN15509 shall be supported. As the OBE type is detected through the content of EFC-ContextMark contained in the OBE (ref. chapter 4), the beacon must contain a list of all authorized elements in EFC-ContextMark (ContractProvider, TypeOfContract, ContextVersion). This list is called TSP List (sometimes also called the Contract Issuer List, but this list must not be confused with the Issuer List contained in the roadside controller which has a different purpose described in chapter 3.4).

3.3 Requirements to functionality in beacon

The RSE beacon has to update its TSP list as soon they have entered into a contractual agreement with a new TSP. The updating mechanisms of the TSP list must be done through the RSE-CS interface during operation.

If the content of the EFC-ContextMark matches one of the entries in the TSP list, the beacon must automatically select the associated EFC-application (EN15509, PISTA, BroBizz or AutoPASS) to perform the correct transaction. Functionality for each of these applications must reside in the beacon.

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.

Internet copy www.easygo.com

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 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 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 service, the following lists are needed at the roadside controller:

- Status lists: Contains identification of all valid OBEs assigned to national/local user agreements
- Issuer list / TSP list: Contains a "mask" of legal OBE ID ranges for each specific TSP having a contract with the EasyGo service. This Issuer 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 roadside controller, but the task of identifying foreign HGVs may also be handled without transferring HGV list to RSE (ref. description in chapter 6.5)

The format of the lists above must follow the interface specifications for the relevant EFC application.

3.5 Requirements to functionality in roadside controller

The main task of the roadside controller related to EFC transactions is to validate the OBE of passing vehicles. The validation logic is described in chapter 5. The roadside controller must be able to give the correct signal to the customer 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 transfer of missing transaction data. Transaction data must under no circumstances be lost.

Internet copy www.easygo.com

The validation tables “Status list”, “Black list” and (if applicable) “HGV list” 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 in at least 5 days. The storage capacity must be dimensioned after transaction volume in addition to other storage requirements.

Internet copy
www.easygo.com

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.

Attributes are addressed by the Attribute ID identifier (AttrID). The attributes used differ from the various EFC-applications as shown in the table below. EN15509 security level 0 is used for the basic EasyGo service. Security level 1 is used for EasyGo+.

Attribute ID		EFC Application				
Attribute name	**Id**	**EN15509**		**PISTA**	**BroBizz**	**AutoPASS**
		Sec.lev 0	**Sec.lev 1**			
Contract *(Information associated with the service rights of the TSP of the EFC service)*						
EFC Context Mark	0		Yes	Yes	Yes	Yes
Contract Authenticator	4			Yes		
Vehcicle *(Identification and characteristics of the vehicle.)*						
Vehicle Licence Plate No	16		Yes			
Vehicle Class	17		Yes	Yes		
Vehicle Dimensions	18		Yes	Yes		
Vehicle Axles	19		Yes	Yes		
Vehicle Weight Limits	20		Yes			
Vehicle Specific Characteristics	22		Yes			
Vehicle Authenticator	23			Yes		
Equipment *(Identification of the OBE and general status information*						
Equipment OBE ID	24		Yes	Yes		
Equipment Status	26		Yes	Yes		
Payment *(Data identifying the Payment means and its validity)*						
Payment Means	32		Yes	Yes		
NTD Data 1	99					Yes
PAN/OBE ID	101				Yes	
Receipt *(Financial and operational information associated with a specific session.)*						
Receipt Data 1	33			Yes		
Receipt Data 2	34	Yes		Yes		

Internet copy
www.easygo.com

Attribute ID		EFC Application				
Attribute name	**Id**	**EN15509**		**PISTA**	**BroBizz**	**AutoPASS**
		Sec.lev 0	**Sec.lev 1**			
Other data						
Private Licence plate number	91			Yes		
Private shadow class	92	Yes		Yes		
Private reserve	93			Yes		
Private Blacklist	94	Yes		Yes		
Historic	95	Yes				
Service code/usage control	96	Yes				
PIN code	97	Yes				
NTD Data 2	100					Yes
NTD Data 3	127					Yes

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.

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.

Internet copy www.easygo.com

Identification of OBE account

Another essential data element is the identification of the individual OBE. The identifier commonly used for the purpose of identifying the OBE account is "PersonalAccountNumber" (PAN). AutoPASS does not use the notation "PAN", but an equivalent notation "OBE ID". The PAN/OBE ID is contained in different Attribute IDs for the different EFC applications.

- PISTA and EN15509 use Attribute ID no. 32 (PaymentMeans)
- BroBizz uses Attribute ID no. 101 (OBE ID)
- 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/OBE ID identification system has a standard syntax defined in ISO 7812. However, the AutoPASS and 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.

Internet copy
www.easygo.com

Overview of EFC-Context mark and PAN/OBE ID content in the EFC applications

EFC Application	EFC-ContextMark			PAN / OBE ID
	Contract Provider	Type of Contract	Context Version	
AutoPASS	30E0xx (xx = Issuer ID)	0001	01	578 000xx yyyyyyyyy (xx = Issuer ID)
BroBizz	Storebælt: 978003 Øresund: A40001	0000 0001 0001	01 01 01	978 003 xxxxxxxxxx 460 01x xxxxxxxxx
PISTA	Storebælt: 978003 Øresund: A40001	0001 0001	02 and 03 02	920860 6204 xxxx xxx 604882 xxxx xxxx xx
CEN EN 15509	Storebælt: 978003 Øresund: A40001 ASFINAG: C04001 (EasyGo+ only)	0001 0001 TBD	04 03 TBD	920860 6204 xxxx xxx 604882 xxxx xxxx xx 308417 xxxx xxxx xxxx x

4.2 Requirements to response times

The OBE must be able to communicate correctly and reliable with the beacon for vehicle speeds from 0 to 240 km/h, even under multilane free flow conditions. A precondition for this requirement is that the roadside equipment does not limit the communication sequence.

4.3 Environmental and physical requirements

The OBE must comply with EMC directive 2004/108/EC (formerly 89/336/EEC) (Electromagnetic Compatibility) with subsequent amendment and guidelines.

Internet copy www.easygo.com

The OBE should have a function for setting a flag for “battery low” when the battery is subject to discharge. This status flag may be reported to the RSE in the subsequent transactions.

With regards to size and weight, the OBE must be compliant with regulations EC 74/60 and ECE-R21 wherever relevant.

4.4 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.

For details see additional documentation referenced in chapter 0

Internet copy
www.easygo.com

5 Requirements to interface OBE-RSE

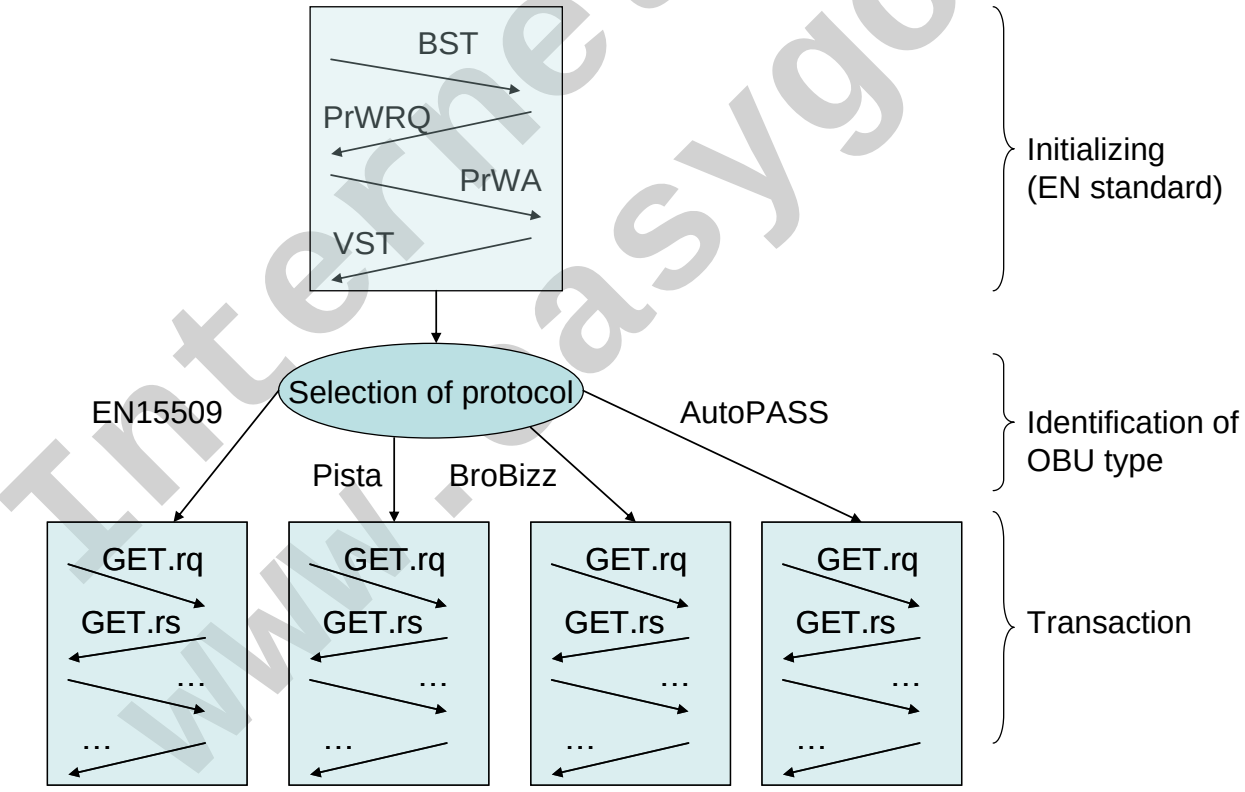
5.1 General principles

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” of 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. Initializing
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.



Internet copy
www.easygo.com

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 TSP List (a table contained in the beacon of all valid EFC-ContextMark data), the RSE will use the associated application (EN15509, 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 TSP List.

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 Transaction List Record

At completion of the DSRC transaction, a 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 transaction record is containing 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

Internet copy
www.easygo.com

- 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 additional documentation referenced in chapter 0).

Internet copy
www.easygo.com

6 OBE validation

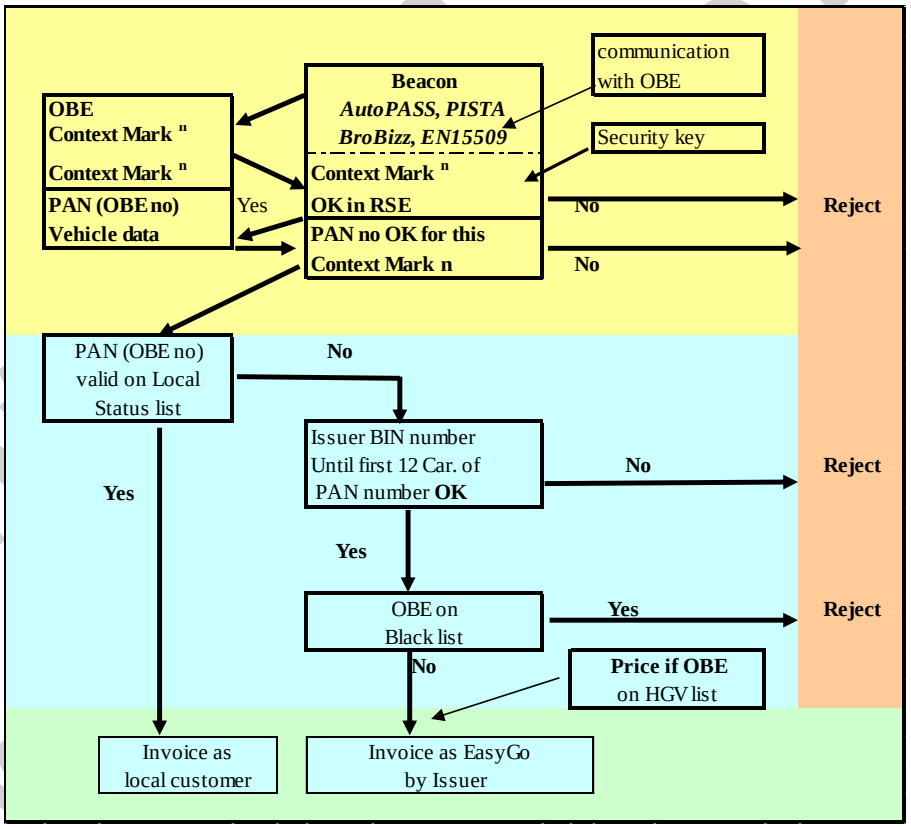
The roadside must determine if the OBE is valid or not. Chapters 6 - 6.5 describe the OBE validation process for EasyGo compatible RSE, while chapter 6.6 shows the OBE validation process for EN15509 OBE at RSE compatible only with EasyGo+.

6.1 Main principles

At the roadside the TC must determine if the OBE is valid in order to give the correct information to the customer whether the OBE is valid or not (light signal, open barrier, and/or acoustic signal from OBE). Control of EasyGo OBEs is based on the following levels:

1. Reading and control by DSRC beacon (drawn in yellow in figure)
2. Control of PAN (OBE ID) against tables in RSE to secure OBE validity (drawn in blue in figure).

An OBE may be rejected in both levels.



6.2 Reading and control by DSRC beacon

The first validation is done between the DSRC beacon and the OBE. An OBE which does not contain correct EFC-ContextMark data according to legal values in TSP List will be rejected.

If it is a known OBE, the EFC-ContextMark decides the further communication with this OBE ID (PAN number). When the type of OBE in the reading area is decided, the structure of the OBE content is known. Based on this information the validation of the OBE can be performed, and the necessary information from the OBE can be retrieved in order to save the information in the EasyGo transaction record.

The further control of the OBE is based on the PAN/OBE ID read at the beacon. The PAN/OBE ID must have correct length and syntax according to the EFC application.

The security controls will also be executed in the beacon depending on the EFC Application.

6.3 Checking the OBE for a valid local/national agreement

The first control of an EasyGo OBE after the beacon control is the following check:

Is the OBE assigned to a local/national agreement?

In both Norway and Denmark/Sweden, the national tolling system uses Status list to validate local/national agreements. The check against 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 Status list is decided locally outside EasyGo.

6.4 Checking the OBE for an EasyGo agreement

If the OBE is not on the local Status list it must be treated as a possible EasyGo transaction. Therefore the next control will be:

Is the OBE valid in a foreign EasyGo agreement?

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

The Issuer 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 Issuer list is containing 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 they will be rejected. TCs are responsible for performing this control. TCs which also has the role of TSP may choose to exclude own OBEs from this control in order to avoid double control.

Internet copy
www.easygo.com

Issuer table 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 new PAN /OBE ID series outside the current defined range, are taken in use.

In order to check the validity of the OBE a control 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 customer when rejected. The TC must include this information according to agreement in EasyGo.

6.5 Special treatment of EasyGo agreements for HGVs

The current BroBizz and AutoPASS OBEs do not carry information about the vehicle classification. Generally there is no automatic classification at the charging points in Norway. Foreign EasyGo transactions can therefore neither be classified by national Status lists nor by reading class from OBE. Due to this, a HGV (Heavy Goods Vehicle) register has been established which contains a list of all heavy vehicles (> 3500 kg). National Collection and Forwarding Centrals prepare a national HGV register based on information available from the national Status list. These tables - called HGV lists - are exchanged between the national systems.

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 customer's need for information on the invoice.

The use of HGV list on the CS level and 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:

- 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.

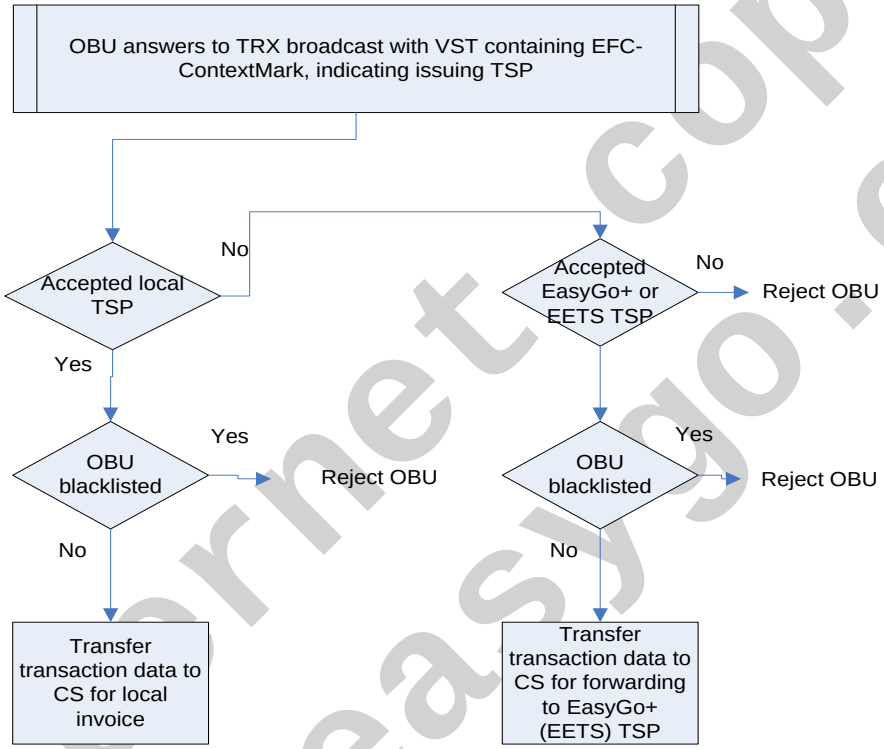
Generally, if the HGV list is not present at roadside equipment it is the TC responsibility to ensure that the information from the HGV list is included before the EasyGo transaction is send to the foreign TSP.

Internet copy
www.easygo.com

The HGV list may be regarded as a preliminary solution until all classification can be done by reading the vehicle class from the individual OBE.

6.6 Special treatment of a "clean" EasyGo+ solution

If there is no need for an RSE to support full EasyGo compatibility but only EasyGo+ / EN15509 OBE (i.e. not supporting PISTA, BroBizz and AutoPASS OBE), a simpler OBE validation logic involving only a Black list can be used as shown below:



Internet copy
www.easygo.com

7 Requirements to certification

7.1 Certification of RSE

EN 14907 is a test procedure worked out by the EFC standardization activities in ISO/TC204/WG5. The intention of EN 14907 is to prove conformance to EN ISO 14906, which is a standard for the Application interface definition for DSRC.

EN 14907 has 2 parts. Part 1 is intended to prescribe procedures and conditions for tests of EFC-related equipment. It specifies the test procedures of RSE and OBE with regard to the conformance to standard and requirements for type approval. EN 14907-1 defines the following tests and related parameters:

- Functionality
- Quality
- Referenced pre-test

Depending on the implemented services, additional certification procedures can apply (Reference is made to documents listed in chapter 0.

7.2 Certification of OBEs

The certification procedures for OBE are divided in three main phases, the conformity to specification declaration, the suitability for use tests and a monitoring phase during the initial operation phase.

a) The **Conformity to Specification Declaration** is to be delivered by the OBE manufacturer. The presented test- and evaluation reports shall prove conformity to the EFC standards and additional requirements. The following functionalities are to be verified:
   - Layer 1 and 2 requirements
   - Basic DSRC Layer 7 functionality
   - EFC application functions
   - EFC attributes
   - Physical requirements defined by the TSP

b) The **Suitability for Use Tests** covering functional and system compatibility test, End to End tests and pilot operation shall prove the proper functionality and minimum performance of the OBE under operational conditions using the TC's system components and system

c) These phases a) and b) will lead to a preliminary certification of an OBE model, necessary for first use by ordinary customers for a limited period, called **monitoring phase**. In the monitoring phase the average operating performance and quality requirements will be judged and after that the final certification can be reached.

Internet copy www.easygo.com

8 Security requirements

8.1 What are the security issues in interoperable toll collection?

Toll collection based upon DSRC technology has been in operation in more than 20 years. From the beginning little effort was put into security. The reason for this was:

- The systems were proprietary (not interoperable) and OBEs from one supplier could be not be used in a system supplied by another
- Equipment to read and program OBEs were expensive and technically complex
- The toll collection systems were not connected to open networks and thereby not vulnerable to electronic burglary
- Most systems were based on the principle of "one OBE – one contract – one central account". This meant that the OBE was mainly used for identification of a contract and each OBE was represented in a white list / status list at the toll station computer

The need for interoperability has made the systems more vulnerable to fraud and errors, and mechanisms to protect the systems have gradually been developed. Much of this development is similar to what has taken place in the banking sector but with some additional requirements. One example: a card issuer can ask the card holder to throw away his old card when it is replaced with a new one. An OBE is too expensive to be discarded in such a manner and instead the OBE must be updated or exchanged.

The following requirements for security are the most important:

- The TSP which issues the OBE must be certain that the OBEs cannot be copied or that roadside equipment at any TC can be manipulated so that invalid transactions are debited the OBEs account
- The User must be guaranteed that only his intentional use of the OBE is debited his account
- The TC must be certain that he will receive payment for all transactions registered through the use of approved OBEs

In addition to these three actors: TSP, User and TC a fourth actor is often nominated as a "Trusted Third Party" – TTP, to make sure that security keys etc. are handled in a secure way. Below the security aspects related to EasyGo and to interoperable toll collection in general are described.

8.2 General security aspects related to OBE

The main requirements for security for the OBE relate to:

- Identification of the OBE
- Authentication of the OBE
- Integrity of the data stored in the OBE
- Integrity of the data transmitted by the OBE
- Confidentiality of critical data (i.e. cryptographic keys) stored in the OBE

Internet copy www.easygo.com

8.3 General security aspects related to RSE

The main needs for security for RSE are:

- Identification of the RSE
- Authentication of the RSE
- Integrity of the data and software stored in the RSE
- Integrity of the data transmitted and received by the RSE
- Confidentiality of the critical data (i.e. cryptographic keys) stored in the RSE
- Availability of the RSE
- Availability of the data stored in the RSE
- Secure recording of all transactions performed by the RSE
- Secure manufacturing, storage, initialisation, personalisation and distribution of critical components (any equipment, device or component used to store, process or transfer critical data) of the RSE
- Secure protocols for update of critical and sensitive information in the RSE
- Identification and authentication of the staff and audit of the operations performed with and by the equipment
- Privacy of personal data stored in or transmitted by the RSE

8.4 General security aspects related to OBE – RSE interface

The main needs for security of the EFC transactions and the OBE-RSE interface are:

- Identification of the communicating parties
- Authentication of the OBE (to prevent impersonation of devices or equipment)
- Integrity of the data exchanged by the OBE and the RSE (to prevent modification of the messages (i.e. OBE ID number), taking into account that the RSE can belong to the native TC (the one who issued the OBE) or to another TC
- Timeliness (to prevent replays)
- Availability of the interface (to prevent jamming of the communication link)
- Non-repudiation of the data exchanged through the interface (to prevent disputes)

8.5 Description of security architectures in EFC applications

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

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

Internet copy
www.easygo.com

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 14096:2004. 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 also supports the calculation of Access Credentials for protection against non-authorised access to sensitive user data and against use of OBE by non-authorised TCs. 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.

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.

BroBizz

Like PISTA.

8.6 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 must conform to the CEN ISO /TS 17574 – EFC security services framework – guidelines for security protection profiles.

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

Internet copy
www.easygo.com

- 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 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 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: TC's own cryptographic keys, cryptographic keys belonging to other 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

Internet copy
www.easygo.com

- 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

Internet copy
www.easygo.com

9 Directives, standards and regulations

- EFC Directive 2004/52/EC on the interoperability of electronic road toll systems in the community
- Commission Decision on the definition of the EETS and its technical elements (October 2009)

Other:

- Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment
- EMC Directive 89/336/EEC, 1992 - Electromagnetic Compatibility
- Council Directive 74/60/EEC of 17 December 1973 on the approximation of the laws of the Member States relating to the interior fittings of motor vehicles.
- ECE- R21 – Uniform provisions concerning the approval of vehicles with regard to their interior fittings

Standard	What	Year	Document name
EN 12253	Layer 1 OSI-model for DSRC	2004	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	2003	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	2003/ 2007	Road Transport and Traffic Telematics (RTTT) – Dedicated Short-Range Communication (DSRC) – Application Layer
EN 13372	DSRC Profiles	2004	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 14906:2010	EFC Application Interface	2010	Road Traffic and Transport Telematics (RTTT) – Electronic Fee Collection – Application interface definition for dedicated short range communication

Internet copy www.easygo.com

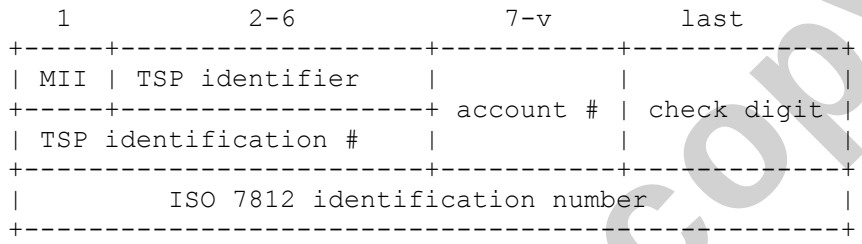
Standard	What	Year	Document name
EN 15509	Application profile for a DSRC standard	2007	EN 15509:2007 Road Traffic and Transport Telematics (RTTT) – Electronic Fee Collection – Interoperability application profile for DSRC
EN 14907	EFC Application Interface test		Part 1: To prescribe procedures and conditions 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

Internet copy
www.easygo.com

10 Annexes

10.1 Annex A – PAN / OBE ID notations in EasyGo

PAN /OBE ID'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:



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

Internet copy www.easygo.com

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

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-kode:	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).

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.

Internet copy
www.easygo.com

10.2 Annex B – Additional EasyGo documentation

EasyGo Document No	Document title	Reference shortcut
201	Requirements for central systems and EasyGo HUB	
202	Roadside equipment and on board units (this document)	
203	Technical requirements data format and interface specifications	
204	General requirements for data and information exchange	
205	Key distribution	
202-A	EASYGO+ OBE Functional Requirements for OBE	[OBE_req]
202-B	EASYGO+ OBE Data description (EASYGO+ OBE Personalization, Configuration and Operating Parameters)	[OBE_data]
202-C	EASYGO+ DSRC Transaction for Tolling and Enforcement	[DSRC]
202-D	EASYGO+ RSE Functional Requirements	
202-E	EasyGo+ OBE Compatibility Tests	

Internet copy
www.easygo.com