

ICS

English Version

Electronic fee collection - Personalisation and mounting of first mount OBE

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

Elektronische Gebührenerhebung - Personalisierung und
Einbau von Fahrzeuggeräten der Erstausrüstung

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

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



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

Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

Foreword.....	3
Introduction	4
1 Scope	5
1.1 Background and expected benefits of first-mount OBE	5
1.2 Personalisation concept	5
2 Normative references	6
3 Terms and definitions	6
4 Symbols and abbreviations	6
5 Context Description	7
5.1 General.....	7
5.2 Actors and Roles	8
5.3 Overview of Assets.....	10
5.4 Use cases	12
5.4.1 Initialisation: Mounting of OBE	12
5.4.2 Initialisation: Assignment of individual data	12
5.4.3 Initialisation: Assignment of vehicle data	13
5.4.4 Contracting of the OBE with the Service Provider	14
5.4.5 Enabling long range mobile communication	15
5.4.6 Change of the vehicle for the same contract	16
5.4.7 Cancellation of an existing contract	17
5.4.8 Change of the contract for the same vehicle	17
5.4.9 Normal EFC use cases: charging and enforcement	18
5.4.10 Repair and upgrade of the OBE	19
5.4.11 Change of vehicle properties	20
5.4.12 Decommissioning and replacement of the OBE	21
6 Personalisation concept	22
6.1 Overall requirements	22
6.1.1 Functional requirements	22
6.1.2 Security Requirements.....	26
6.2 Vehicle interface requirements and constraints	34
6.2.1 Introduction	34
6.2.2 Installation principles	35
7 Personalisation data.....	35
7.1 EFC Attributes	35
7.2 OBE related data	37
7.3 Access protection information.....	37
7.4 Vehicle registration data	37
8 Recommendations.....	38
Bibliography	40

Foreword

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

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

Introduction

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

The issues addressed by the document include:

- 1) vehicle interfacing requirements and constraints
 - a) vehicle data buses
 - b) requirements and constraints from the automotive industry (e.g. in terms of electronic, mechanics...)
 - c) safety
 - d) security
- 2) personalization requirements and constraints
 - a) Access to the protected data inside the OBE e.g. ContractNumber
 - b) Where are the EETS and contract data located? (inside the OBE or in a smart card).
 - c) Activation and deactivation of the OBE

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

1 Scope

1.1 Background and expected benefits of first-mount OBE

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

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

1.2 Personalisation concept

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

- a) the personalisation procedure can be done "over the air". In such case, personalisation data can be encoded in the OBE by the Service Provider over a secure air-link, or
- b) personalisation data can be loaded directly by the driver into the OBE or Service Provider via a personal storage media.

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

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

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

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

- a) whether the EFC system is based upon DSRC, GNSS-CN, or a combination of both technologies;
- b) for permanently installed OBE;
- c) for both original equipment manufacturers (first mount) and after sales permanently attached to the vehicle by OBE manufacturers.

2 Normative references

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

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

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

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

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

3 Terms and definitions

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

3.1

on-Board Equipment (OBE)

equipment fitted within or on the outside of a vehicle and used for toll purposes

3.2

electronic fee collection (EFC)

toll charging by electronic means via a wireless interface

3.3

roadside equipment

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

3.4

Toll Charger

legal entity charging toll for vehicles in a toll domain

3.5

Toll Service Provider

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

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

4 Symbols and abbreviations

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