SLOVENSKI STANDARD
SIST-TP CEN/TR 16152:2011

01-maj-2011

Elektronsko pobiranje pristojbin - Personalizacija in montaža OBE za prvo vgradnjo

Electronic fee collection - Personalisation and mounting of first mount OBE

Elektronische Gebührenerfassung - Personalisierung und Montage der ersten bordeigenen Ausrüstung

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

Ta slovenski standard je istoveten z: CEN/TR 16152:2011

ICS:

03.220.20	Cestni transport	Road transport
35.240.60	Uporabniške rešitve IT v transportu in trgovini	IT applications in transport and trade

SIST-TP CEN/TR 16152:2011 **en**

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 16152

March 2011

ICS

English Version

Electronic fee collection - Personalisation and mounting of first mount OBE

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

Elektronische Gebührenerhebung - Personalisierung und Einbau von Fahrzeuggeräten der Erstausstattung

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

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

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

Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

Foreword

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

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

Introduction

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

The issues addressed by the document include:

1) vehicle interfacing requirements and constraints

   a) vehicle data buses

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

   c) safety

   d) security

2) personalization requirements and constraints

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

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

   c) Activation and deactivation of the OBE

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

1 Scope

1.1 Background and expected benefits of first-mount OBE

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

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

1.2 Personalisation concept

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

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

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

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

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

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

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

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

b) for permanently installed OBE;

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

2 Normative references

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

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

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

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

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

3 Terms and definitions

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

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

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

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

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

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

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

4 Symbols and abbreviations

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

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

5 Context Description

5.1 General

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

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

5.2 Actors and Roles

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Table 1 — Possible assignments of actors to roles

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

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

5.3 Overview of Assets

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

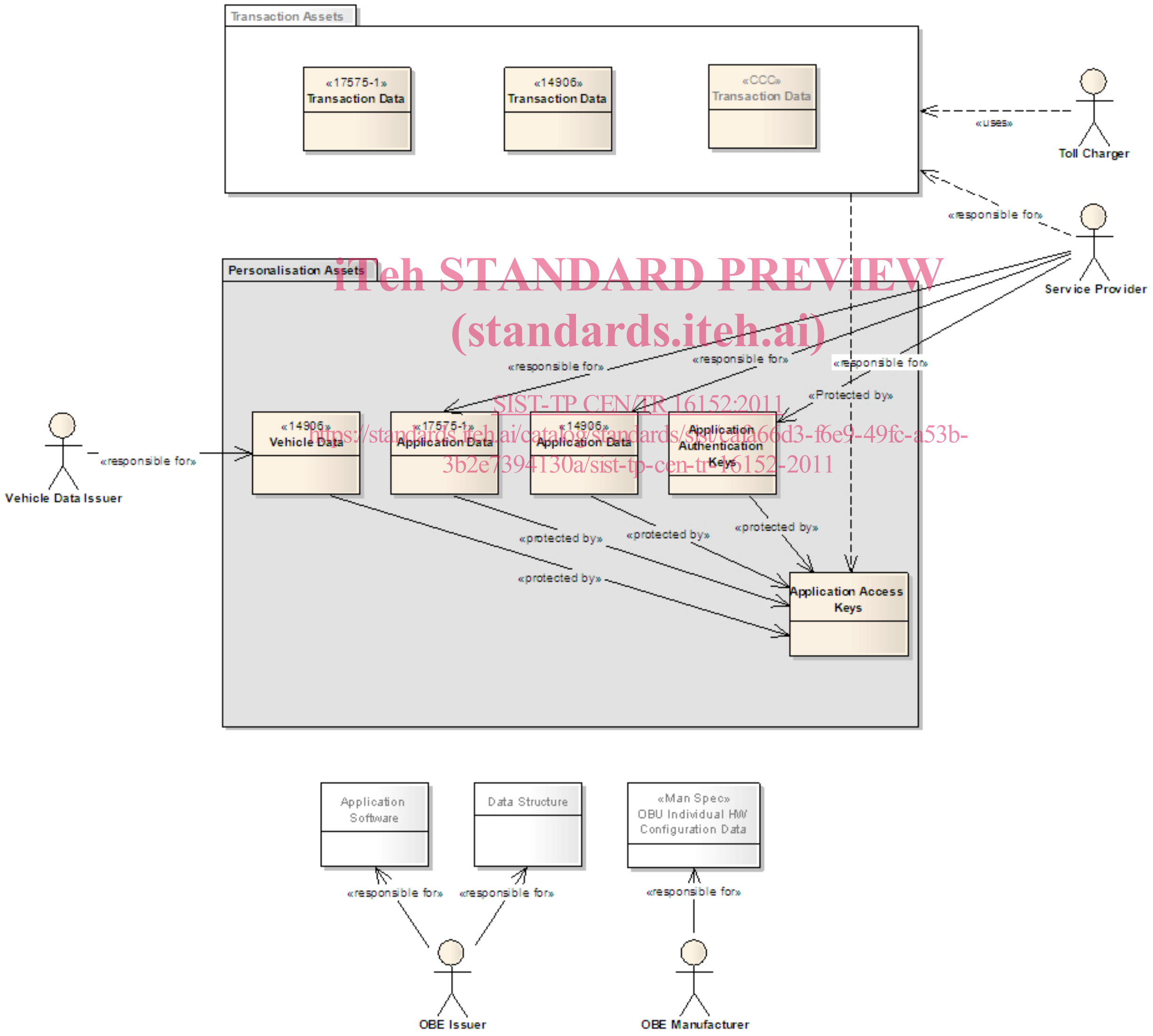

Figure 1 — Overview of Assets

The following assets exist:

a) Transaction Data Assets

b) Personalisation assets

c) OBE Manufacturer Specific Assets

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

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

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

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

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

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

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

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

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

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

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

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