Road transport and traffic telematics - Electronic fee collection - Interoperability application profile for DSRC

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

Käesolev Eesti standard EVS-EN 15509:2007 sisaldab Euroopa standardi EN 15509:2007 ingliskeelset teksti.	This Estonian standard EVS-EN 15509:2007 consists of the English text of the European standard EN 15509:2007.
Standard on kinnitatud Eesti Standardikeskuse 21.06.2007 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teatajas.	This standard is ratified with the order of Estonian Centre for Standardisation dated 21.06.2007 and is endorsed with the notification published in the official bulletin of the Estonian national standardisation organisation.
Euroopa standardimisorganisatsioonide poolt rahvuslikele liikmetele Euroopa standardi teksti kättesaadavaks tegemise kuupäev on 09.05.2007.	Date of Availability of the European standard text 09.05.2007.
Standard on kättesaadav Eesti standardiorganisatsioonist.	The standard is available from Estonian standardisation organisation.

ICS 35.240.60

Võtmesõnad:

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 15509

May 2007

ICS 35.240.60

English Version

Road transport and traffic telematics - Electronic fee collection - Interoperability application profile for DSRC

Télématique de la circulation et du transport routier - Perception de télépéage - Profil d'application d'interopérabilité pour DSRC

Straßenverkehrstelematik - Elektronische Gebührenerhebung - Anwendungsprofil für DSRC Interoperabilität

This European Standard was approved by CEN on 22 March 2007.

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

Management Centre: rue de Stassart, 36 B-1050 Brussels

Contents

Page

Foreword

This document (EN 15509:2007) has been prepared by Technical Committee CEN/TC 278 “Road transport and traffic telematics”, the secretariat of which is held by NEN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by November 2007, and conflicting national standards shall be withdrawn at the latest by November 2007.

This European Standard defines an Application Profile based on a set of base standards according to the concept of "International Standardised Profiles (ISP)" as defined in ISO/IEC TR 10000-1. The objective is to support technical interoperability between EFC DSRC-based systems in Europe. The principles of Application Profiling and relations to underlying base standards are defined in the Introduction.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, 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.

Introduction

CEN/TC278 (/WG1) has produced a set of standards that supports interoperable electronic fee collection (EFC) dedicated short-range communication (DSRC)-based systems (e.g. EN ISO 14906, a “toolbox” for defining EFC-application transactions). However, these standards are necessary but not sufficient to ensure technical interoperability. This European Standard provides for a coherent set of requirements of the EFC-application that may serve as a common technical platform for EFC-interoperability.

This European Standard defines an Interoperable Application Profile for DSRC-EFC transactions. The main objective is to support technical interoperability between EFC-systems within the scope of the standard (as defined in Clause 1 below). A basic description of the EFC-service and an EFC System can be found in CEN/ISO TS 17573.

This European Standard only defines a basic level of technical interoperability for EFC equipment, i.e. on-board unit (OBU) and roadside equipment (RSE) using DSRC. It does not provide a full solution for interoperability, and it does not define other parts of the EFC-system, other services, other technologies and non-technical elements of interoperability.

The elaboration of this European Standard is based on the experiences from a vast 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) as a part of the European EFC Directive (2004/52/EC) also calls for the definition of an interoperable EFC-service. This European Standard provides for effective support for the work on the definition of EETS.

Although there already are numerous existing base standards and specifications, there are specific needs that motivate this Interoperable Application Profile standard.

— Definition of the necessary and sufficient EFC-DSRC requirements to support technical interoperability.

— Provision of a crucial part of the EETS and hence support for the EFC Directive (2004/52/EC). Including structured management of revisions of the standard.

— CARDME/PISTA/CESARE dialects are used in many countries but they need to converge, as the present situation is not cost effective.

— Needed additional DSRC-requirements are made.

— Choice of data elements including vehicle data.

— Extended definition of the use of some data elements, including semantics and coding.

— Clear choices for security implementation.

— It facilitates a complementing test specification (with clear relations between the conformance requirements and evaluation tests).

— Good support for procurements.

The Application Profile is described using the concept of "International Standardised Profiles (ISP)" as defined in ISO/IEC TR 10000-1. The ISP-concept is specifically suited for defining interoperability specifications where

a set of base standards can be used in different ways. This is exactly the case in EFC, where a set of base standards allows for different choices that are not interoperable.

The principles of the ISP-concept can be summarised as follows.

— An ISP shall make references only to base standards or other ISPs.

— The profile shall restrict the choice of base standard options to the extent necessary to maximize the probability of interoperability (e.g. chosen classes, conforming subsets, options and parameter values of base standards).

— The ISP shall not copy content of the base standards (in order to void consistency problems with the base standards).

— The profile shall not specify any requirements that would contradict or cause non-conformance to the base standards.

— The profile may contain conformance requirements that are more specific and limited in scope than those of the base standards.

— Conformance to a profile implies by definition conformance to a set of base standards. Whereas conformance to that set of base standards does not necessarily imply conformance to the profile.

The use of the Application Profiling concept also provides for a flexible framework towards adoption, migration and use of the standard. Operators, Issuers and Manufacturers may use this Application Profile as a basis for interoperable use of their equipment, without having to disturb or otherwise affect any EFC-system used locally.

The Interoperable Application Profile is defined in terms of conformance requirements as given in Clause 5. To facilitate easy referencing, testing and look-up, these requirements are divided into two parts; On-Board Unit (OBU) requirements (5.1) and Roadside Equipment (RSE) requirements (5.2).

In addition the standard also includes various annexes that provide further detailed specifications as well as background, motivation and examples for the conformance requirements. The intention is that these enhance readability and understanding of the standard.

It is noted that the base standard EN ISO 14906:2004 is subject to a near standing review. The next edition of EN ISO 14906 will incorporate advancements made since its publication such as e.g. the definition of additional Euro classes (i.e. Euro-4 and Euro-5). Hence, such amendments have not been made in this standard as it would jeopardise the consistency with the base standard and violate the ISP-concept.

This European Standard is complemented by a set of standards defining Conformity Evaluation of the Conformance Requirements in this European Standard (not finalised when writing this European Standard).

1 Scope

The scope for this European Standard is limited to:

— payment method: Central account based on EFC-DSRC;

— physical systems: OBU, RSE and the DSRC interface between them (all functions and information flows related to these parts);

— DSRC-link requirements;

— EFC transactions over the DSRC interface;

— data elements to be used by OBU and RSE used in EFC-DSRC transactions;

— security mechanisms for OBU and RSE used in EFC-DSRC transactions.

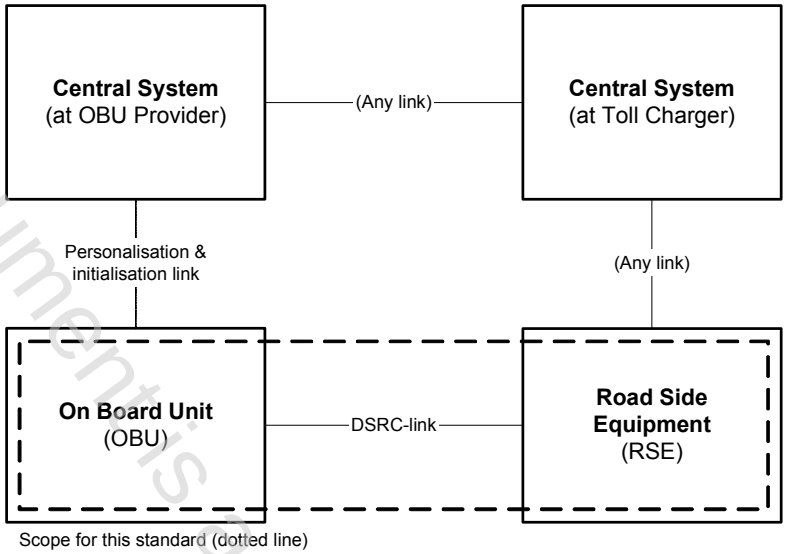

Figure 1 — Scope for this European Standard (within the box delimited with a dotted line)

It is outside the scope of this European Standard to define:

— contractual and procedural interoperability requirements (including issues related to a Memorandum of Understanding, MoU);

— conformance procedures and test specification (this is provided in a separate set of standards);

— setting-up of operating organizations (e.g. clearing operator, issuing, trusted third party etc.);

— legal issues;

— other payment methods in DSRC-based EFC (e.g. on-board accounts using integrated circuit cards);

— other basic technologies (e.g. GNSS/CN or video registration based EFC). However, this European Standard may be used for defining the DSRC-EFC parts for the use in applications that implement a mix of different technologies.

— other interfaces or functions in EFC-systems than those specified above (i.e. information flows and data exchange between operators or personalisation, initialisation and customisation of the OBU).

Some of these issues are subject to separate standards prepared by CEN/TC 278, ISO/TC 204 or ETSI ERM.

The following figure shows the scope of this European Standard from a DSRC-stack perspective.

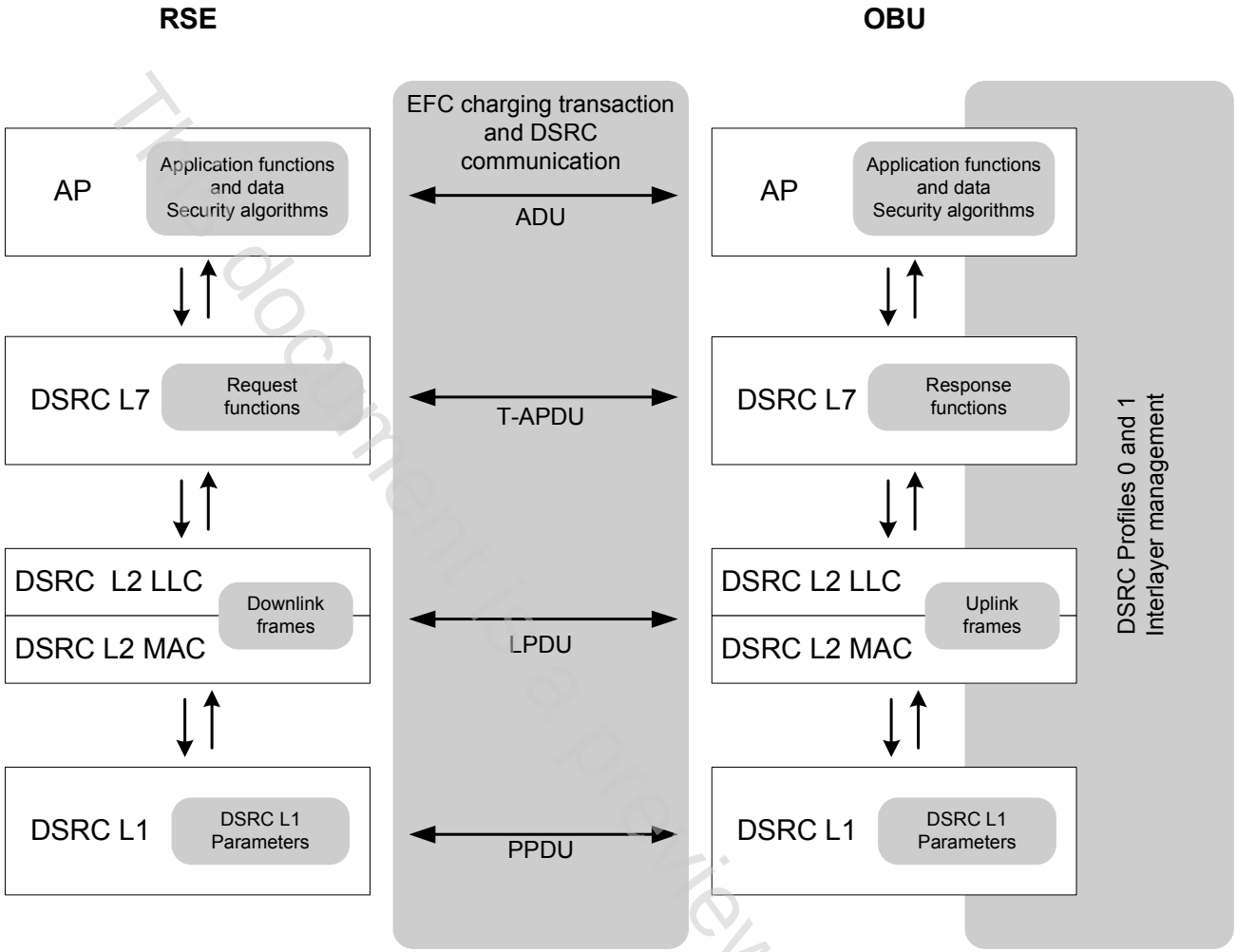

Figure 2 — Relations between this European Standard and DSRC-stack elements

This European Standard defines an Application Profile based on the ISP-concept. The base standards that this Application Profile is based upon are*:*

— EN ISO 14906 on EFC application interface definition for DSRC (this implies indirect references to EN ISO 14816 on Numbering and data structures);

— EN 12834: on DSRC application layer (L7).

— EN 13372 on DSRC profiles (this implies indirect references to the DSRC L1, L2 and L7 standards: EN 12253, EN 12795 and EN 12834).

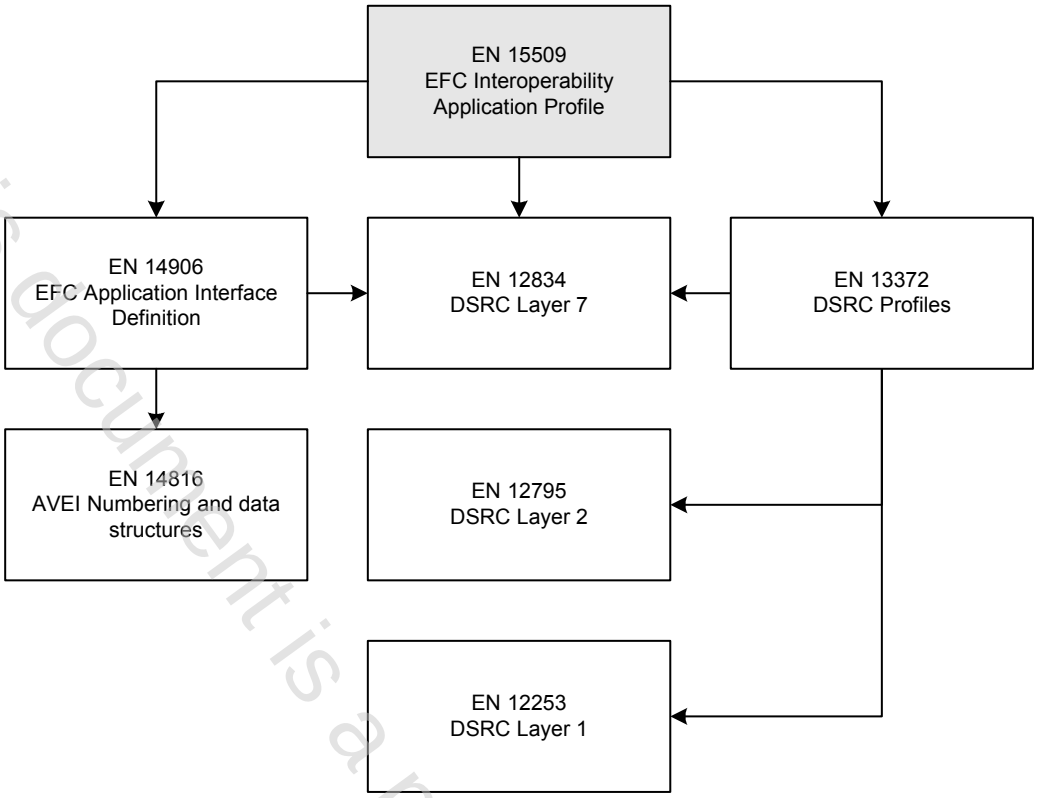

Figure 3 — Relation and references between base standards and EN 15509 (this European Standard)

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.

ANSI X3.92:1981, *American National Standard for Information Systems — Data encryption algorithm*

ISO/IEC 9646-7, *Information technology — Open Systems Interconnection — Conformance testing methodology and framework — Part 7: Implementation Conformance Statements*

ISO/IEC 9797-1:1999, *Information technology — Security techniques — Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*

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

EN 13372:2004, *Road transport and traffic telematics (RTTT) — Dedicated short-range communication — Profiles for RTTT applications*

EN ISO 14906:2004, *Road transport and traffic telematics — Electronic fee collection — Application interface definition for dedicated short range communication (ISO 14609:2004)*

ETSI TS 102 486-1-1, *Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 1: DSRC data link layer: medium access and logical link control; Sub-Part 1: Protocol Implementation Conformance Statement (PICS) proforma specification*

ETSI TS 102 486-2-1, *Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 2: DSRC application layer; Sub-Part 1: Protocol Implementation Conformance Statement (PICS) proforma specification*

3 Terms and definitions

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

3.1
access credentials
data that is transferred to *on-board equipment (OBE),* in order to establish the claimed identity of a roadside equipment (RSE) application process entity

[EN ISO 14906:2004]

NOTE The access credentials carry information needed to fulfil access conditions in order to perform the operation on the addressed element in the OBE. The access credentials can carry passwords as well as cryptographic based information such as authenticators.

3.2
action
function that an application process resident at the *roadside equipment* can invoke in order to make the *on-board equipment* execute a specific operation during the *transaction*

[EN ISO 14906:2004]