This document is a preview generated by EVS

Identification card systems - Surface transport applications - Interoperable Public Transport Applications - Framework

Identification card systems - Surface transport applications - Interoperable Public Transport Applications - Framework

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

Käesolev Eesti standard EVS-EN 15320:2007 sisaldab Euroopa standardi EN 15320:2007 ingliskeelset teksti. Käesolev dokument on jõustatud 18.12.2007 ja selle kohta on avaldatud teade Eesti standardiorganisatsiooni ametlikus väljaandes. Standard on kättesaadav Eesti standardiorganisatsioonist.	This Estonian standard EVS-EN 15320:2007 consists of the English text of the European standard EN 15320:2007. This document is endorsed on 18.12.2007 with the notification being published in the official publication of the Estonian national standardisation organisation. The standard is available from Estonian standardisation organisation.

Käsitlusala: This European Standard specifies sets of data presented at an interface, the card sub-system interface, in a structured form as well as the rules for dealing with that data to enable products such as tickets to be written to a Machine Readable Card in a manner which will minimise the amount of data to be held on the card while allowing an authorised party to be able to access and interpret the data easily and efficiently. This is the basis for practical interoperability and as such, this European Standard forms the foundation of interoperability across systems subject to commercial agreements and interchange of details concerning how this European Standard has been physically interpreted. As part of this capability, the design of the data environment allows for the addition of new sets of data to represent new or modified transport products without compromising the ability of existing terminals to continue to handle all sets of data held on the card, whether or not they are to be interpreted and possibly used. Associated with the data is the set of processes which applies to the data within the application. The inclusion of process in the standard means that similar data will be treated in a similar way by all external services and terminals leading to true interoperability that can be achieved and maintained through this European Standard.	**Scope:** This European Standard specifies sets of data presented at an interface, the card sub-system interface, in a structured form as well as the rules for dealing with that data to enable products such as tickets to be written to a Machine Readable Card in a manner which will minimise the amount of data to be held on the card while allowing an authorised party to be able to access and interpret the data easily and efficiently. This is the basis for practical interoperability and as such, this European Standard forms the foundation of interoperability across systems subject to commercial agreements and interchange of details concerning how this European Standard has been physically interpreted. As part of this capability, the design of the data environment allows for the addition of new sets of data to represent new or modified transport products without compromising the ability of existing terminals to continue to handle all sets of data held on the card, whether or not they are to be interpreted and possibly used. Associated with the data is the set of processes which applies to the data within the application. The inclusion of process in the standard means that similar data will be treated in a similar way by all external services and terminals leading to true interoperability that can be achieved and maintained through this European Standard.

ICS 35.240.15

Võtmesõnad:

The document is provided by EVS

Eesti Standardikeskusele kuulub standardite reprodutseerimis- ja levitamisõigus

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 15320

December 2007

ICS 35.240.15

English Version

Identification card systems - Surface transport applications - Interoperable Public Transport Applications - Framework

Systèmes de cartes d'identification - Applications pour le transport terrestre - Applications de transport public interopérables

Identifikationskartensysteme - Landgebundene Transportanwendungen - Interoperable Anwendungen für den öffentlichen Verkehr - Rahmenwerk

This European Standard was approved by CEN on 8 September 2007.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN Management Centre has the same status as the official versions.

CEN members are the national standards bodies of 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.

This document is a preview generated by EVS

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

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

© 2007 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. EN 15320:2007: E

Contents

Page

Foreword 6
Introduction 7
1 Scope 9
2 Normative references 10
3 Terms and definitions 10
4 Symbols and abbreviated terms 14
5 Basic structure of application components[)] 15
6 Data groups 17
7 The abstract interface 24
8 Application security 33
9 Profiles 40
Annex A (normative) Data group definitions 44
Annex B (normative) Identification and mapping of data groups 48
Annex C (normative) EN 1545 data elements enumerated for use in the application 72
Annex D (normative) ASN.1 Tag allocations 86
Annex E (informative) General requirements 95
Annex F (informative) Examples 103
Annex G (informative) Accessing the Interoperable Public Transport Application 140
Annex H (normative) Relationship between legacy systems and the Interoperable Public Transport Application 143
Annex I (informative) Supporting Legacy Systems 146
Bibliography 149

This document is a preview generated by EVS

List of Figures

Figure 1 — Interoperable Fare Management system 8
Figure 2 — Data element within a data object 15
Figure 3 — Data structure 16
Figure 4 — Data group 16
Figure 5 — Relationships between the data groups 17
Figure 6 — Data group contents 22
Figure 7 — Product data group with fixed and variable parts 22
Figure 8 — The application environment links the data groups together 23
Figure 9 — Relationships between the logical interfaces, the SSS and the card and terminal 24
Figure 10 — Logical interface 1: the card data interface 26
Figure 11 — Logical interface 2: the data group interface 27
Figure 12 — A representative application command flow 32
Figure 13 — Application states 33
Figure 14 — Data group Control Data Structure 39
Figure 15 — A Control Data Structure entry 39
Figure 16 — Profile ID structure 41
Figure 17 — Profile derivation 43
Figure E.1 — The Interopeable Public Transport Application 96
Figure E.2 — Products within the Interoperable Public Transport Application 96
Figure E.3 — Interoperable Public Transport Application product usage 97
Figure G.1 — Card and application activation 140
Figure H.1 — Application wrapper 144
Figure H.2 — Inter-environment operation 144
Figure H.3 — Interoperable Public Transport Application stub 145
Figure H.4 — Hierarchy of access 145
Figure I.1 — Interoperable Public Transport Compliant application 148

This document is a preview generated by EVS

List of Tables

Table 1 — Card data interface functions 26
Table 2 — Data group interface functions 27
Table 3 — Application activities and use cases 29
Table 4 — Access mode byte specification 40
Table A.1 — Data Group Identification 44
Table A.2 — Data structures within data groups 45
Table B.1 — Application environment specific mandatory data structures 48
Table B.2 — Event log specific mandatory data structures 50
Table B.3 — General mandatory data structures 51
Table B.4 — Type A optional data structures 55
Table B.5 — Type L data structures 64
Table B.6 — Cyclic event log data structure 70
Table C.1 — Application data elements fully specified in EN 1545 72
Table C.2 — Application data elements not fully specified in EN 1545 76
Table C.3 — Application data elements not included in EN 1545 83
Table F.1 — Example of a label 103
Table F.2 — Example of an instance identifier 103
Table F.3 — Example of a seal 103
Table F.4 — Concession; creation of holder ID and entitlement 104
Table F.5 — Concession: creation of validity 105
Table F.6 — Concession: use of concession 106
Table F.7 — Carnet: customer purchases the carnet 108
Table F.8 — Carnet: a journey is made 109
Table F.9 — Carnet: a further journey is made 110
Table F.10 — Carnet: top-up of rides 111
Table F.11 — Check in/ Check out: Stored Travel Rights availability 112

This document is a preview generated by EVS

Table F.12 — Check in / Check out: Check In 113
Table F.13 — Check in/ Check out: Check out 114
Table F.14 — Check in/ Check out: Stored Travel Rights usage 115
Table F.15 — Check in/ Check out: the journey continues 115
Table F.16 — Check in/ Check out: further Stored Travel Rights usage 117
Table F.17 — Be in/ be out: entitlement to ride 118
Table F.18 — Be in / be out: after boarding 118
Table F.19 — Be in / be out: the journey continues 119
Table F.20 — Streifenkarte: purchasing for cash 120
Table F.21 — Streifenkarte: boarding the vehicle 121
Table F.22 — Streifenkarte: further journeys 122
Table F.23 — Rail travel: reservation 124
Table F.24 — Rail travel: a journey is made 125
Table F.25 — RET: a ticket is purchased 127
Table F.26 — RET: Check in 129
Table F.27 — RET: Check out 130
Table F.28 — RET: Check in next leg 132
Table F.29 — RET: Check out next leg 133
Table F.30 — RET: Check in return journey 134
Table F.31 — RET: Check out return journey 136
Table F.32 — Zonal fare scheme: a ticket is purchased 138
Table F.33 — Zonal fare scheme: the ticket is used 139
Table G.1 — Responses of known cards types 141

This document is a preview generated by EVS

Foreword

This document (EN 15320:2007) has been prepared by Technical Committee CEN/TC 224 "Personal identification, electronic signature and cards and their related systems and operations", the secretariat of which is held by AFNOR.

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 June 2008, and conflicting national standards shall be withdrawn at the latest by June 2008.

This document builds on the following standards to define an Interoperable Public Transport Application:

— EN 1545-1:2005, *Identification card systems — Surface transport applications — Part 1: Elementary data types, general code lists and general data elements*;

— EN 1545-2:2005*, Identification card systems — Surface transport applications — Part 2: Transport and travel payment related data elements and code lists*.

This document describes a foundation for a technology neutral environment for an Interoperable Public Transport Application within the confines of the definition of identification card systems. Nevertheless, interoperability cannot be maintained if different interface technologies are used by Machine Readable Cards within such a scheme. Consequently this document specifies the adherence to ISO/IEC 14443 Parts 1 to 3 as a necessity to ensure interoperability.

Amendments and enhancements to this European Standard will be made from time to time and published on the CEN website.

To the best of their knowledge the authors of this European Standard do not believe it infringes any commercial copyright, intellectual property rights or patents. However, CEN cannot guarantee this and shall not be responsible for any such infringements or claims, which will be dealt with according to CEN rules and regulations.

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.

This document is a preview generated by EVS

Introduction

The Interoperable Public Transport Application defines the foundation and basic structure of a transport application primarily for ticketing for implementation on a Machine Readable Card that makes use of the Data Elements defined in EN 1545 and which may be made interoperable subject to commercial agreements between the parties involved and an exchange of specific implementation details. This has the effect that different operators will be able to read, interpret and handle Machine Readable Cards containing the application produced by others. Moreover, again subject to commercial agreements between the parties, it should be possible for a transport operator to write its ticket products to Machine Readable Cards issued by others that contain the application. Annex H discusses how legacy systems can interface with the application such that some level of interoperability may be achieved through a migration path to it.

This European Standard describes the basis of a public transport application resident on a Machine Readable Card as presented at the interface to a suitable terminal. In many cases where the card contains a processor, this interface will be between the card and the accepting device. In other cases, additional logic within the terminal application will be included in order to provide the necessary support. This is accomplished by mandating a logical abstract interface. The actual format of the data held on the card is not described by this European Standard. This format may be derived from a mapping of the data described in this European Standard to the card using an ASN.1 encoding rule.

This European Standard forms one part of a series relating to public transport which define the interoperable fare management system as shown in Figure 1.

This document is a preview generated by EVS

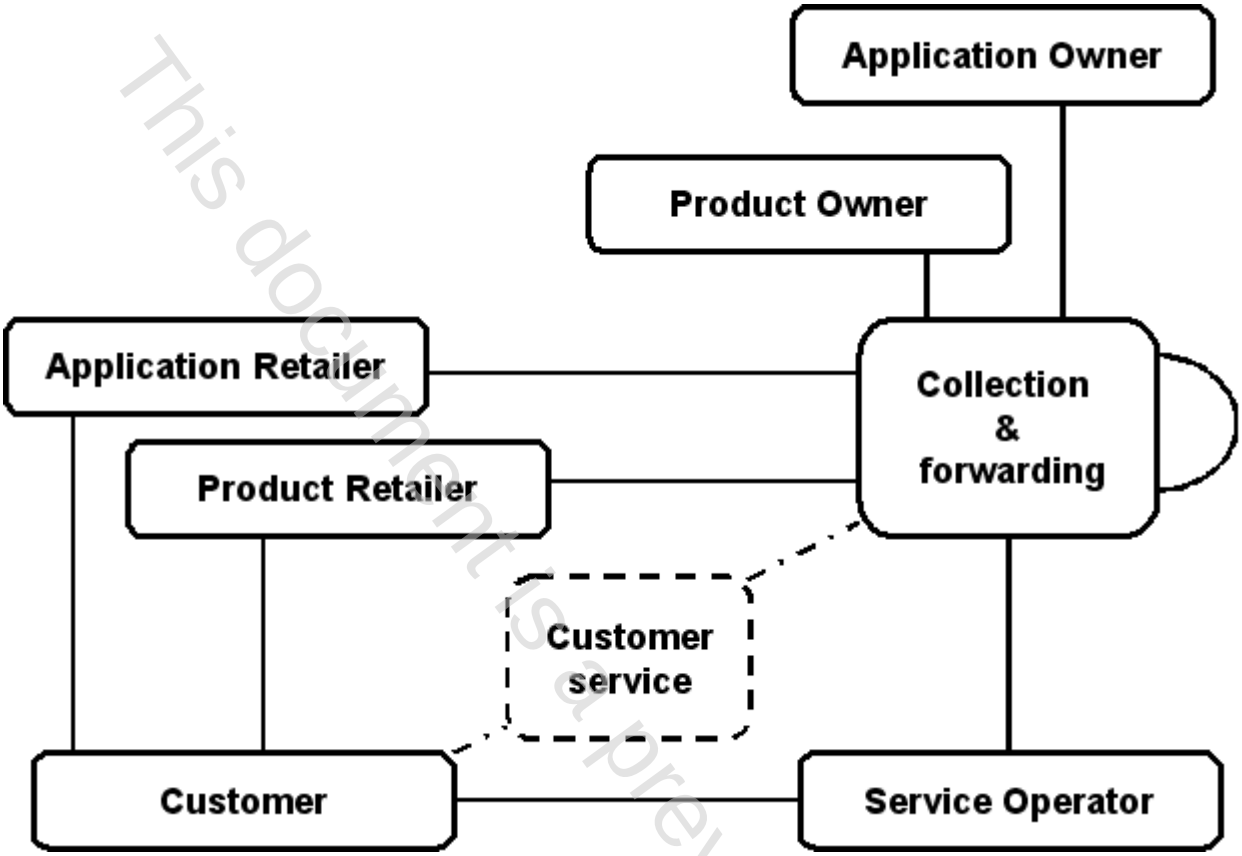

Figure 1 — Interoperable Fare Management system

This European Standard describes the basis of an environment which aims to achieve the following objectives:

— to provide a basis for offering machine readable interoperable tickets across the public transport network in Europe;

— to satisfy the demand for securing a seamless journey for the passenger allowing them travel with all participating operators, possibly in different networks and countries, using a single card while in the context of not inhibiting commercial competition.

This European Standard describes those components of the application necessary to support an interoperable environment including:

— accessing the Interoperable Public Transport Application;

— data structure and presentation;

— sizing and enumeration of data;

— data access methodology;

— security and access considerations;

— dealing with legacy systems.

This document is a preview generated by EVS

1 Scope

This European Standard specifies sets of data presented at an interface, the card sub-system interface, in a structured form as well as the rules for dealing with that data to enable products such as tickets to be written to a Machine Readable Card in a manner which will minimise the amount of data to be held on the card while allowing an authorised party to be able to access and interpret the data easily and efficiently.

This is the basis for practical interoperability and as such, this European Standard forms the foundation of interoperability across systems subject to commercial agreements and interchange of details concerning how this European Standard has been physically interpreted. As part of this capability, the design of the data environment allows for the addition of new sets of data to represent new or modified transport products without compromising the ability of existing terminals to continue to handle all sets of data held on the card, whether or not they are to be interpreted and possibly used.

Associated with the data is the set of processes which applies to the data within the application. The inclusion of process in the standard means that similar data will be treated in a similar way by all external services and terminals leading to true interoperability that can be achieved and maintained through this European Standard. In addition, acknowledgement that the application specifies both data and process also implies that it needs to consider security both at the level of access rights to data and the security of the overall environment in which it operates.

The security related clauses in this European Standard define the minimum requirement of functionality necessary such that interoperability may be supported while protecting information stored within the application from unauthorised access and accidental or malicious damage. This European Standard defines an abstract card to card accepting device application interface which may be implemented, entirely at the card edge, or may include some logic in the card accepting device dependent upon the capability of the card. The view of security is similar in terms of an external system accessing, via the abstract interface, Machine Readable Cards, which may be just a card or a card – card accepting device combination. This means that security controls may exist in the card, the card accepting device or a combination of both. Additional descriptions of security architecture and expected implementation issues are described in Clauses 7 and 8.

This European Standard describes the minimum requirements for an interoperable transport application that may exist on a Machine Readable Card, either alone or together with other applications, and it is therefore a description of data sets and formats at the logical level. The abstract interface needs to support many Machine Readable Card varieties that conform to a contactless interface compatible with ISO/IEC 14443. ISO/IEC 14443 Parts 1 to 3 need to be supported. While this European Standard applies specifically to Machine Readable Cards, others may wish privately to use it with other customer media such as key fobs, subject to the customer media being able to interface with card acceptance devices supporting this European Standard where interoperability is required.

In terms of file structures, the data sets and data formats described in this European Standard are perfectly capable of being mapped onto a card conforming to ISO/IEC 7816-4. However, this European Standard does not define the card architecture, and the data formats and structures it defines are equally capable of being implemented on a pure memory card or a more complex multi-application card conforming to some other file format, subject to the card acceptance device supporting any required functionality that the card lacks in order to support the interface requirements of this European Standard.

This European Standard describes a generic logical model in ASN.1 format which may be mapped into a real environment using ASN.1 encoding rules such as BER and PER. However, it is recognised that certain overriding factors may affect the manner in which data is mapped onto real cards.

— Performance represented by transaction time is a critical issue in many transport applications. The PER encoding rules allow the physical data structure to be fixed and minimised in size using external Tag lists. For this reason it is expected that PER or some similar encoding rule will be used in practical implementations.

— Card data space limitations also mitigate towards the use of PER or similar encoding rules.

This document is a preview generated by EVS

— Need to maintain compatibility, limited or full, with existing legacy systems and systems currently in development implies that specifically derived encoding rules may be specified to map the logical structures into the required format.

As a foundation for interoperability, this standard provides the basis for interoperability across instances of the application supplied by different parties subject to commercial agreement and exchange of details of the physical interpretations of the 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.

EN 1545-1:2005, *Identification card systems — Surface transport applications — Part 1: Elementary data types, general code lists and general data elements*

EN 1545-2:2005, *Identification card systems — Surface transport applications — Part 2: Transport and travel payment related data elements and code lists*

ISO/IEC 7816-4:2005, *Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange*

3 Terms and definitions

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

This document is a preview generated by EVS