SLOVENSKI STANDARD
SIST EN 15320:2011

01-maj-2011

Sistemi z identifikacijskimi karticami - Aplikacije za prevoze po kopnem - Aplikacija za interoperabilni javni prevoz - Okvir

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

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

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

Ta slovenski standard je istoveten z: **EN 15320:2007**

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices
35.240.60	Uporabniške rešitve IT v transportu in trgovini	IT applications in transport and trade

SIST EN 15320:2011 **en**

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.

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

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

Ref. No. EN 15320:2007: E

Contents

Page

List of Figures

List of Tables

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.

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.

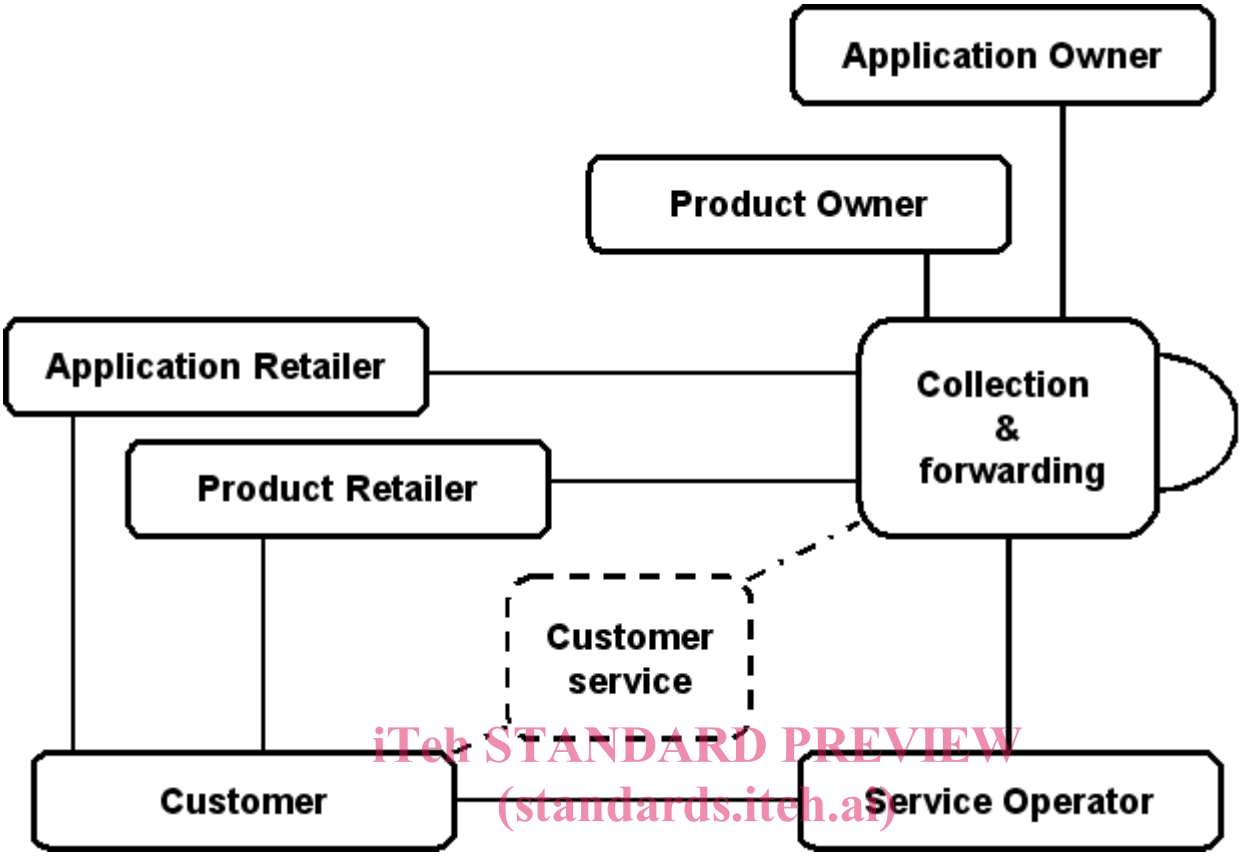

Figure 1 — Interoperable Fare Management system

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.

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.

— 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.

3.1
abstract syntax notation
form of notation used to describe data elements and processes, standard for CEN documentation

3.2
account
record of the current value and (truncated) transaction history of a product held on the 'back office' system of the 'product owner'

3.3
anonymous card
card which is not linked to a named holder, but which will still bear a traceable serial number

3.4
anti-tear
describes measures taken to ensure that any intentional alteration of data in the customer media during normal use does not lead to un-recoverable corruption of the customer media

3.5
application
instance of the Interoperable Public Transport Application resident on a Machine Readable Card or other customer media

3.6
application owner
entity which holds the application contract for the use of the application with the customer

3.7
application retailer
entity which sells and terminates applications, collects and refunds value to a customer as authorised by the application owner

3.8
Card Accepting Device
device which can interact with a card and exchange data with the card

3.9
card holder
person who owns the right to use the card

3.10
Charge to Account
facility/process for post-billing - rather than pre-payment or payment at the time of purchase (subtype of product)

3.11
check in – check out
holders actively validate cards when entering and leaving defined areas specified by a transport provider

3.12
concession
entitlement to a reduced (or zero cost) fare on the basis of age, condition or status

3.13
contract
expression of an agreement between two or more parties in the transport environment. It defines the conditions under which the user may use the services. Products such as tickets or entitlements represent a contract

3.14
customer media
entity which at least supports the same functionality as a Machine Readable Card but may be in a different form factor

3.15
data element
single store for an irreducible datum value (see EN 1545-1)

3.16
entitlement
entitlement or qualification for a service expressed as a product (a type of product template)

3.17
hot list
list of cards, applications, products or items of equipment where a transaction requires special attention

3.18
Interoperable Fare Management
encompasses all systems designed to manage the acquisition and use of fare products data in an interoperable public transport environment

3.19
interoperability
ability of systems to provide services to and accept services from other systems

3.20
journey
complete sequence of one or more journey legs (rides) required to achieve a specific purpose at a specific destination. This sequence may include the use of more than one vehicle and using more than one transport mode (see EN 1545-1)

3.21
key
binary string which is used to control access to an application or product, or which is used as the basis of encryption or during the calculation of Message Authentication Codes

3.22
loyalty
rewards for use of transport services

3.23
Message Authentication Code
computed field based on data in previous stated fields which allows a message to be verified as genuine

3.24
Machine Readable Card
token or entity that conforms to ISO/IEC 14443 Parts 1 to 3

3.25
profile
means to achieve interoperability between different card platforms

3.26
product
enables a customer to benefit from a transport service. It is an instance of a product template in the application. It is identified by a unique identifier. The Interoperable Public Transport Application distinguishes between four subtypes of a Product: CTA, STR, ticket and entitlement

3.27
product owner
entity which performs the functions of ownership (specifies pricing, usage rules and commercial rules), clearing and reporting

3.28
product retailer
entity which sells and terminates products, collects and refunds value to a customer as authorised by a product owner

3.29
product rules
product owner requirements (set of usage, pricing and commercial rules)

3.30
product specification
specification of function, data elements and security schema according to product rules

3.31
product template
technical master of the product specification for implementation. A unique identification (product template ID) is given to each product template by the registrar, triggered by the product owner

3.32
retailer
see: product retailer, application retailer

3.33
ride
component of a journey

3.34
route
reference to a single path through a transport network

3.35
seal
guarantee of authenticity