TECHNICAL SPECIFICATION

ISO/TS 21719-1

First edition
2018-02

Electronic fee collection — Personalization of on-board equipment (OBE) —

Part 1: Framework

Perception de télépéage — Personnalisation des équipements embarqués —

Partie 1: Cadre

Reference number
ISO/TS 21719-1:2018(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*.

A list of all parts in the ISO 21719 series can be found on the ISO website.

Introduction

On-board equipment (OBE) is an in-vehicle device that is able to contain one or more application instances in order to support different intelligent transportation system (ITS) implementations such as electronic fee collection (EFC). Examples of EFC applications are road toll collection/road charging, localization augmentation (LAC) or compliance checking (CCC).

To assign the EFC application in the OBE to a certain user and/or vehicle, personalization should be performed. This means that unique user and vehicle related data, needs to be transferred to the OBE.

The CEN/TR 16152 already assessed many aspects of the personalization process and it also defined the overall personalization assets, i.e. application data, application keys and vehicle data.

Different communication media may be used for transferring the personalization assets to the OBE; but for all media, common procedures may be applied such as an overall message exchange framework and necessary security functionality in order to ensure data protection and integrity.

By standardizing the personalization procedure, compatibility of personalization equipment is supported, and the entity responsible for the personalization, e.g. a toll service provider, will be able to outsource parts of, or a complete, personalization to a third party, another service provider or a personalization agent.

This document defines common functionality for personalization that is independent of the communication media and personalization equipment (PE) used, while the subsequent parts define in detail how the functions are realized on different defined communication media and interfaces.

Electronic fee collection — Personalization of on-board equipment (OBE) —

Part 1: Framework

1 Scope

This document describes:

— an overall description of the EFC personalization process;

— a description of EFC functionality that can be used for personalization.

The personalization process takes place within the domain of the entity that is responsible for the application in the OBE.

The scope of the EFC functionality is limited to the interface between the personalization equipment (PE) and OBE as shown in Figure 1. It is out of the scope of this document to define whether the personalization functionality resides completely in the PE or whether this functionality instead resides in a central system and where the PE is more or less "transparent".

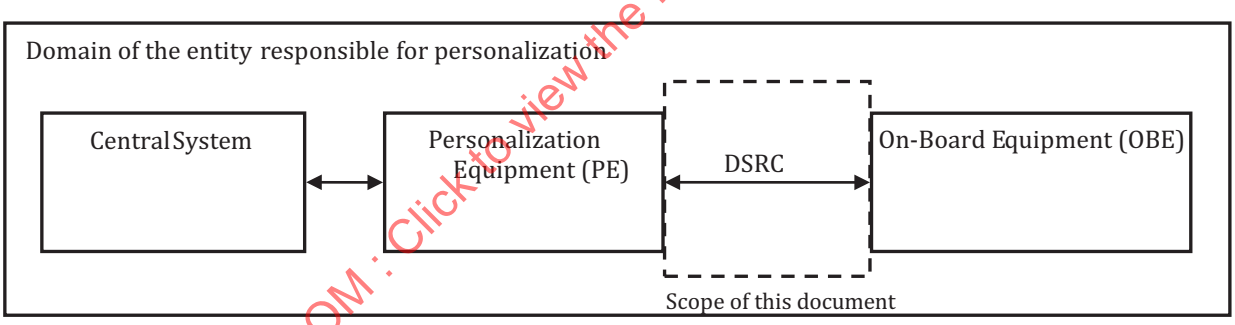

Figure 1 — Scope of this document (box delimited by the dotted line)

It is outside the scope of this document to define the following:

— exact application command or message structures for the EFC personalization functionality (these are dependent on the communication media and described in subsequent parts of the ISO/TS 21719 series);

— conformance procedures and test specification (this may be provided in a by separate set of standards that are referred to in the subsequent parts of the ISO/TS 21719 series);

— setting-up of operating organizations (e.g. Toll Service Provider, personalization agent, trusted third party, etc.);

— legal issues.

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

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at www.electropedia.org

— ISO Online browsing platform: available at www.iso.org/obp

3.1
attribute
addressable package of data consisting of a single data *element* (3.3) or structured sequences of data elements

[SOURCE: ISO 17575-1:2016, 3.2]

3.2
electronic fee collection
EFC
fee collection by electronic means

[SOURCE: ISO 12855:2015, 3.6]

3.3
element
DSRC directory containing application information in the form of *attributes* (3.1)

3.4
OBE personalization
process of transferring *personalization assets* (3.6) to the *on-board equipment* (*OBE*) (3.5)

3.5
on-board equipment
OBE
required equipment on-board a vehicle for performing required *electronic fee collection* (*EFC*) (3.2) functions and communication services

[SOURCE: ISO 12855:2015, 3.9]

3.6
personalization assets
specific data stored in the OBE related to the user and the vehicle

3.7
personalization equipment
equipment for transferring *personalization assets* (3.6) to the *OBE* (3.5)

3.8
toll domain
area or part of a road network where a certain toll regime is applied

[SOURCE: ISO 17573:2010, 3.18, modified — “certain” has been added.]

4 Abbreviated terms

CCC Compliance check communication (see ISO 12813)

EFC Electronic Fee Collection (see ISO 17573)

IAP Interoperable Application Profile (see EN 15509)

LAC Localization augmentation communication (see ISO 13141)

OBE On-board Equipment

PE Personalization Equipment

5 Personalization overview

5.1 Process

To prepare an OBE for use, it has to be prepared with the EFC applications and data required for the toll domain(s) where the OBE shall be used.

Before personalization, one or more initial non-personalized data structures for the EFC applications should be present in the OBE and it is out of scope of this document how these structures are entered into the OBE. The personalization process deals with how this existing EFC application structures are populated with personalization data (personalization assets), such as payment related data, vehicle data or security keys. It is also assumed that necessary security functionality and initial keys to perform the personalization already are present in the OBE at time of personalization.

According to ISO 14906, application data shall be stored in attributes that are addressed in Elements corresponding to specific EFC applications as shown in Figure 2.

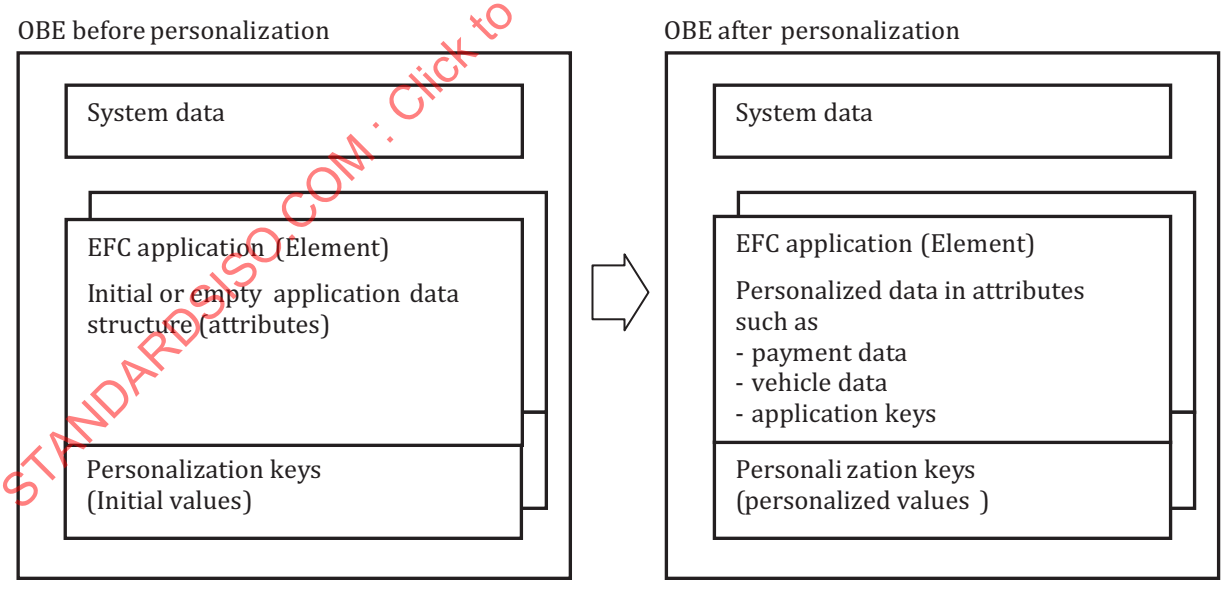

Figure 2 — Scope of personalization

The entity that is responsible for the EFC application defines the exact data content in the application and also the access rights to this data.

When using the interoperable applications profile (IAP) for charging, compliance checking communication (CCC), or local augmentation communication (LAC), data sets and access conditions are already defined in the corresponding standards.

5.2 Personalization assets

Personalization assets are, as in CEN/TR 16152, application keys, application data and vehicle data.

The application keys consists of

— access keys that are used to grant access to application data, and

— authentication keys which are used to secure the authenticity of the OBE and the data integrity of the application data assets at time of use in the toll domain(s).

The application data consist of data that is required to support one or several a services. Application data is defined, e.g. in ISO 14906, EN 15509, ISO 12813 or ISO 13141.

Vehicle data defines the characteristics of the vehicle in the case that the application in the OBE is bound to a specific vehicle.

5.3 System architecture

The overall system architecture required to perform personalization according to the described process is shown in Figure 3.

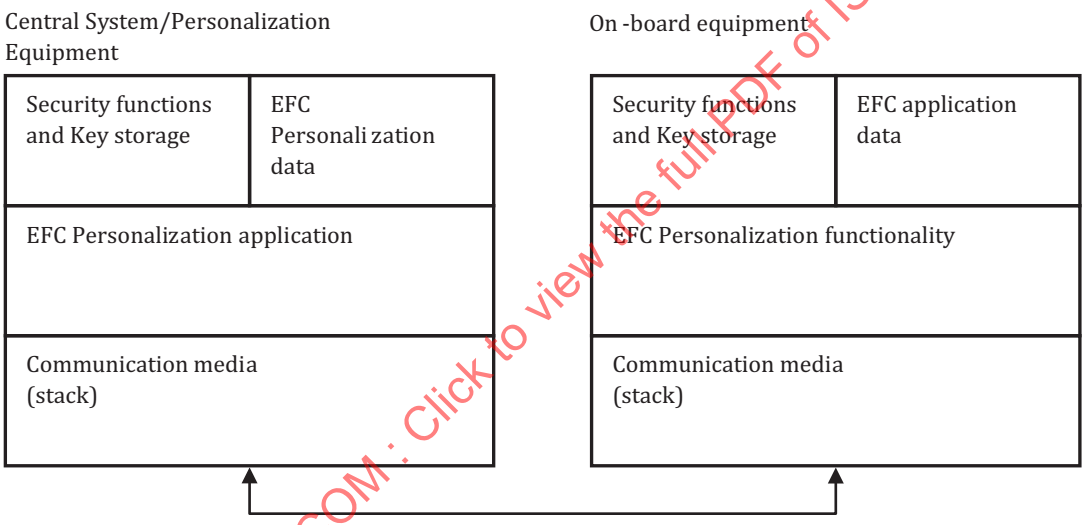

Figure 3 — Personalization system architecture

6 EFC personalization functions

6.1 Overview

In order to support personalization over different types of media and in different environment, a number of personalization functions or primitives have been identified and are described in this clause.

How the personalization functions are implemented in a specific system will depend on the type of communication interface and it is defined in the subsequent parts of the ISO/TS 21719 series.

6.2 Write function

6.2.1 Basic functionality

The basic function of personalization is to write personalization assets like, e.g. contract identifier, vehicle data or security related data, into data elements within an EFC application in the OBE.

The Write functionality defined as a Write_request-command that is provided by the PE to the application layer in the OSI communication stack. The OBE will receive the command, execute it, and respond with a Write_response-command.

The exact definition and coding of the commands for the Write command depends on available write and addressing functionality provided by the communication interface. The command, however, shall support the security functions that are defined below.

All security calculation are performed with keys present before the Write_request command. This means, for example, that if security keys are updated, the old keys are used for security calculations.

6.2.2 Security functions

In order to ensure that personalization assets are transferred without being exposed or altered during the personalization, a number of security functions will support the process. These are described in the following subclauses as separate primitives but these can be combined within the same Write command in order to fulfil required security. Exactly what security functions that are required depends on the personalization process, the communication media and the environment.

It is presumed that initial values of the personalization security keys that are needed to perform the personalization security functions are already present in the OBE at the time of personalization.

In all examples below, there might be additional steps where random numbers and key diversifiers are exchanged and used in the calculations in order to increase the system security.

6.2.3 Access protection

The OBE shall only write data into the OBE EFC application if a correct value of access credentials is received together with the personalization data in the Write_request command. This is a way for the OBE to validate that the personalization command originates from an authorized Personalization Equipment as shown in Figure 4.

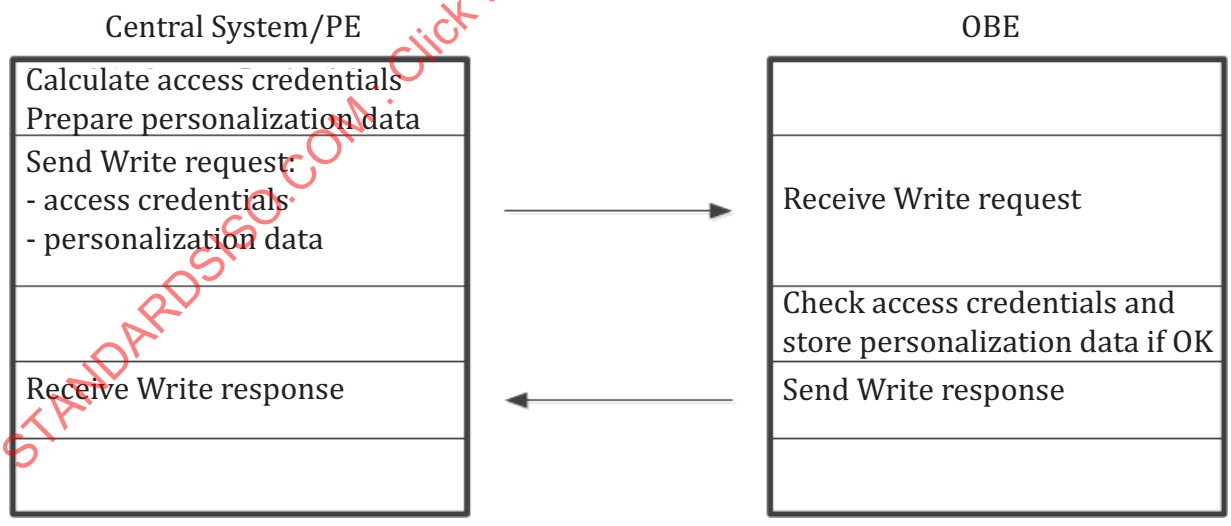

Figure 4 — Principle of access protection

6.2.4 Application data encryption

Personalization data that is sent to the OBE in Write_request command may be encrypted in the central system or PE in order to protect the data from eavesdropping or unintended disclosure. The OBE shall decrypt the data before writing it into the EFC application.

The encryption option shall always be used for data that cannot be exposed during the transfer due to privacy aspects or regulations and it shall also be used when updating security related parameters as security keys as shown in Figure 5.

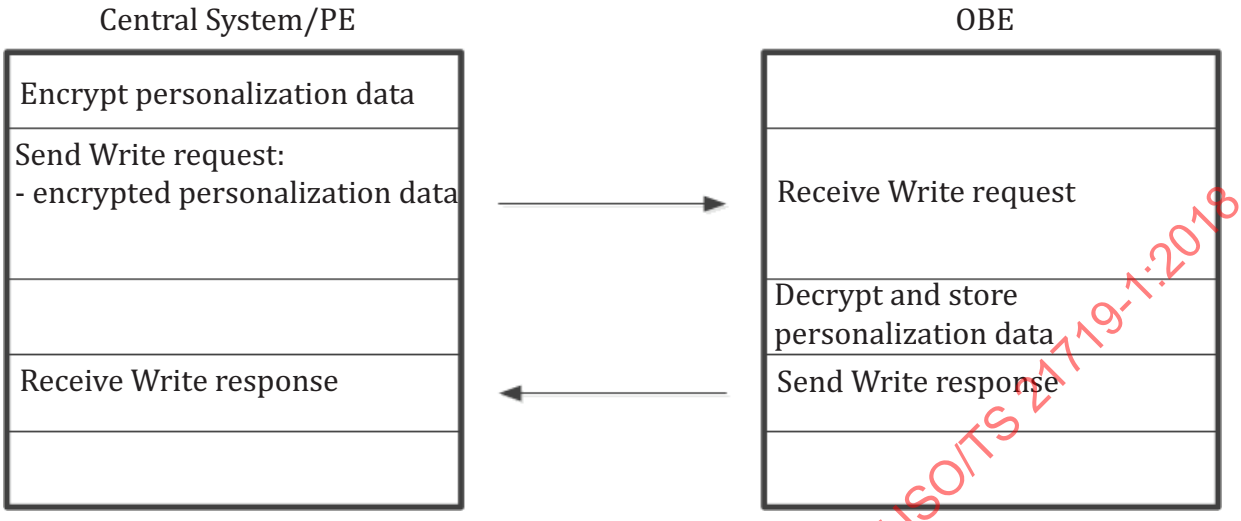

Figure 5 — Principle of personalization data encryption

6.2.5 Write_Request authenticator

The OBE shall only write or update data in the EFC application, if an authenticator, received together with the personalization data and calculated over the data, is correct. This authenticator is calculated by the Central System or PE and it will ensure the integrity of the data during the transfer to the OBE. This is shown in Figure 6.

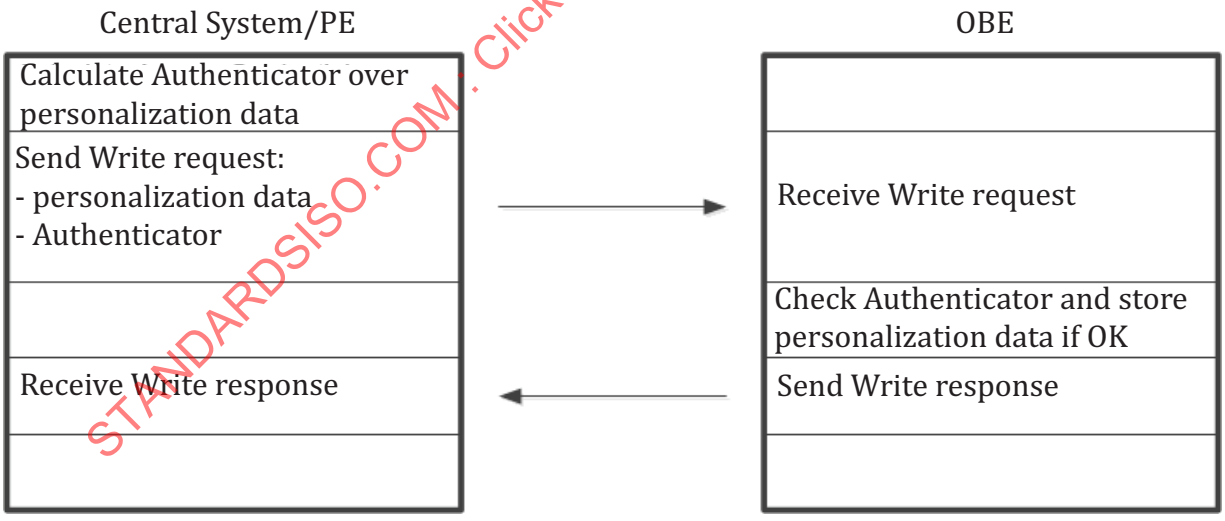

Figure 6 — Principle of Write request authenticator

6.2.6 Write_Response authenticator

The OBE will, after writing the personalization data into the EFC application, calculate an authenticator over the data and transmit this authenticator back to the Central System or PE in the Write response. This is a way for the entity that prepared the personalization data to check the integrity of the OBE and to receive a proof that correct data was written into the correct OBE. This is shown in Figure 7.

