TECHNICAL SPECIFICATION

ISO/TS 21193

First edition
2019-10

Electronic fee collection — Requirements for EFC application interfaces on common media

Perception du télépéage — Exigences relatives aux interfaces d'application de télépéage sur média commun

Reference number
ISO/TS 21193:2019(E)

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

Published in Switzerland

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 of 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 www.iso.org/iso/foreword.html.

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Transportation network improvement, including road and railway, is essential to drive economic growth. Integrated transport service has been aimed at topics such as user convenience, transport safety, reliability, efficiency and availability. For example, a traffic manager can find which kinds of improvements are needed to relieve traffic bottlenecks by analysing user transport flows in a transport system considered as a whole.

It is usually necessary to use different transport services to transfer people or goods from origin to destination. Sometimes, using different transport services in the same trip becomes cumbersome when transport services are operated by different operators, e.g. bad interconnections between different transport modes due to user needs to search and compare transportation modes, need for separate charging or payment for the transport services used. The connections between different transport modes and the means to achieve seamless travel are improving with the use of information and communication technologies (ICT).

ISO/TR 19639 investigated case studies on the use of a common payment medium when combining public transport services and road services, based on the use of a common payment schema. This common payment schema is further categorised into integrated central accounts and integrated on-board accounts.

ISO/TR 19639 concluded by stating the need for new electronic fee collection (EFC) standards to support on-board integrated accounts, among which is an application interface between the common payment medium and the common service rights provider (CSRP). The background of on-board accounts in EFC are:

— Operational methods of EFC systems might be different due to regional and local circumstances. EFC systems can be classified into central accounts and on-board accounts, using a common payment medium, which are widely adopted in Asian countries.

— On-board account payment media are commonly used for public transport in several countries, e.g. Singapore, Malaysia and China.

— Central payment accounts are considered one of the common service rights methods explained in ISO/TR 20526, whereas the EFC standards are currently predominantly based on a central account.

— A convergence on the usage of on-board account for both EFC systems and public transport should be considered.

This document describes an EFC application as one type of transport service specific application and the application interface requirements for a common service rights application. A common service rights application is explained in informative Annex C of this document for understanding a common payment scheme based on this concept as shown in Figure 1.

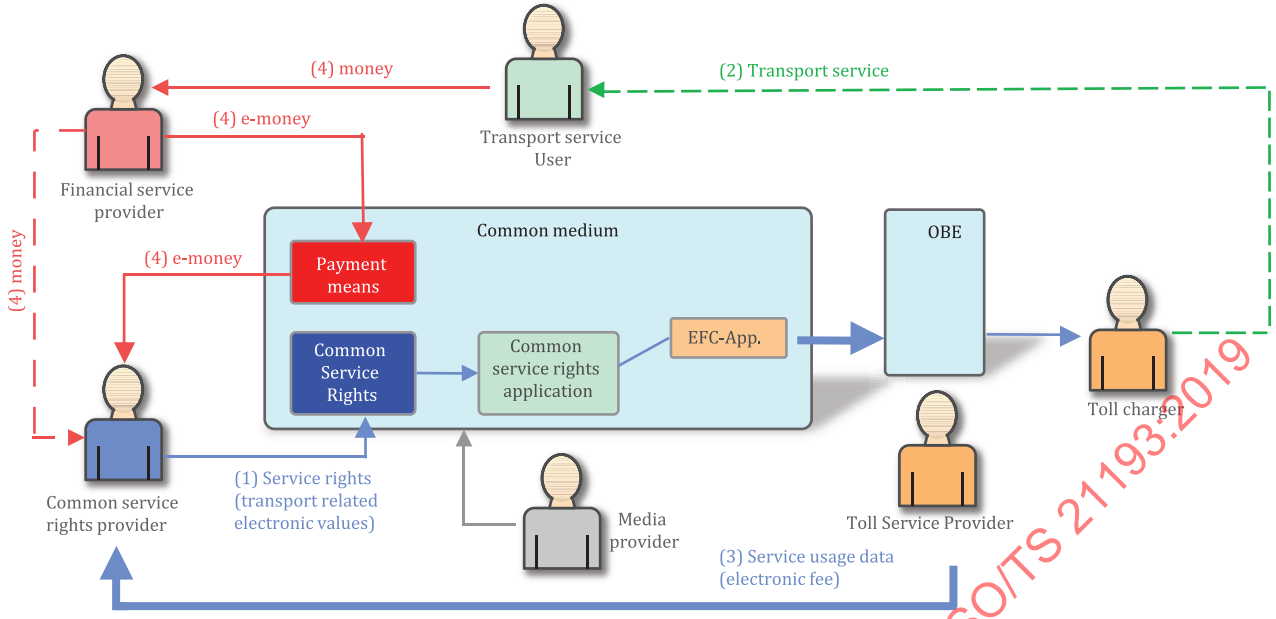


Figure 1 — Common payment medium concept for EFC scheme

Arrow lines (4) labelled 'money' and 'e-money' are monetary flows and out scope of this document.

Arrow line (2) labelled 'Transport service' is not an ICT interface but a physical transport service.

Other arrow lines are in the scope of ISO/TC 204 (EFC and public transport standards) and the thick arrow line between common payment medium and OBE is within the scope of this document.

This document will extend the set of EFC standards to allow provisions for multi-modal transport services by using a common payment medium.

This document defines among others, the role and responsibilities of a CSRP. The CSRP provides a common payment medium for enabling use of EFC, a public transport service and retail shopping service to service users with one account. CSRP may provide the usage record of user's multi modal transport trip as a form of customer service.

This document contains a number of annexes. Data type specifications are given in Annex A, an implementation conformance statement (ICS) proforma is given in Annex B. The common payment medium concept for any transport service is presented in Annex C. General kinds of application structure in a medium are presented in Annex D. General requirements from medium relating standards is presented in Annex E. A typical system migration method and technical solution supporting medium upgrading are presented in Annex F. Examples of reloading types and transactions are presented in Annex G. The EFC security requirements for a common payment medium are presented in Annex H based on EFC functional requirements.

The scope of this document includes an EFC application interface for a common payment medium as shown in Figure 2, as well as the role and responsibilities of a Common Service Rights Provider (CSRP).

NOTE Figure 2 explains the relation of CSRP among related sectors including EFC. E-money is exchanged between the Transport Service Provider (TSP) in the EFC sector and the CSRP. E-money is exchanged between retail in the commerce sector and the CSRP.

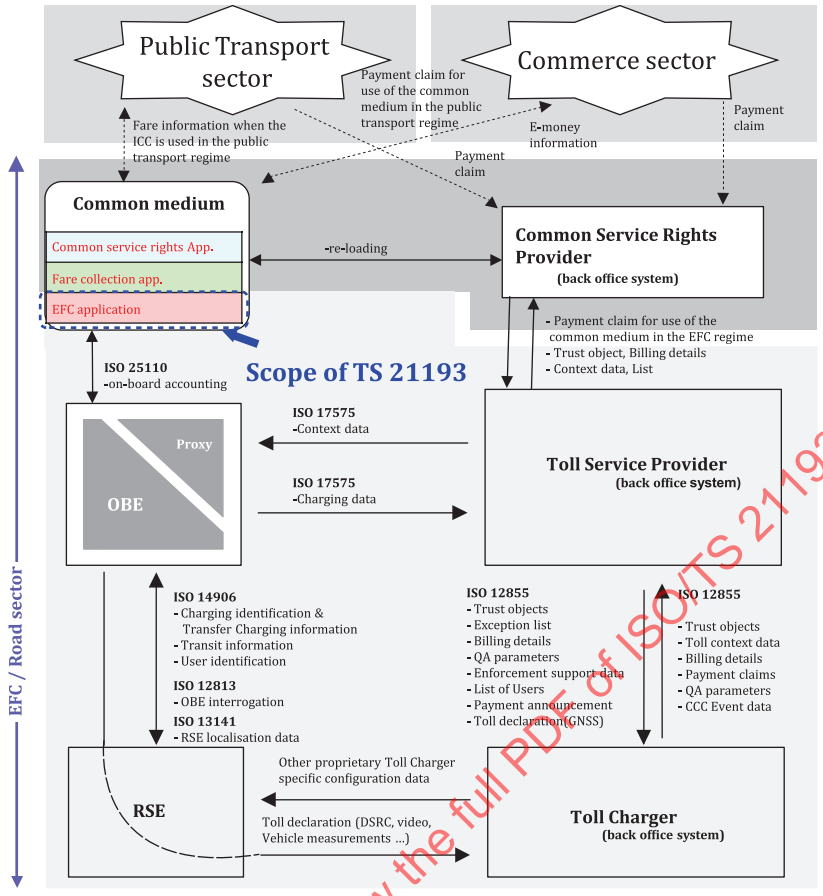


Figure 2 — Scope within the EFC computational architecture

Electronic fee collection — Requirements for EFC application interfaces on common media

1 Scope

This document defines requirements to support information exchanges among related entities of a common payment scheme. It defines:

a) electronic fee collection (EFC) functional requirements for a common payment medium;

b) an application structure in a common payment medium;

c) EFC application data in a common payment medium.

The following are outside the scope of this document:

— requirements and data definitions for any other transport services such as public transport;

— a complete risk assessment for an EFC system using a common payment medium;

— security issues arising from an EFC application among all transport services;

— the technical trust relationship between a CSRP and a service user;

— concrete implementation specifications for implementation of security for an EFC system;

— detailed specifications required for privacy-friendly EFC implementations;

— any financial transactions of the CSRP.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

ISO 14906:2018, *Electronic fee collection — Application interface definition for dedicated short-range communication*

ISO 17573-1:2019, *Electronic fee collection — System architecture for vehicle-related tolling — Part 1: Reference model*

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:

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

— IEC Electropedia: available at http://www.electropedia.org/

3.1
central account
payment means (3.11) or common service rights in an electronic fee collection (EFC) system, stored in a central system

3.2
common service rights
rights to use services offered by several toll domains or more than one transport mode

EXAMPLE Usage allowance for a number of trips or for a certain time span.

3.3
common service rights provider
CSRP
entity providing *common service rights* (3.2) to the service user

3.4
EFC architecture
description of the key elements of an electronic fee collection (EFC) system, their functions and interrelationships

3.5
electronic money
e-money
value having its equivalence in real money, electronically stored, e.g. in a bank account or an IC-card, which can be used by the user for payments

3.6
fare collection regime
set of rules, including enforcement rules, governing the fare system in the public transport domain

3.7
integrated circuit card
IC card
ICC
card with electronic components performing processing or memory functions with the capability to communicate with an interrogator

Note 1 to entry: Contact IC cards are specified in the ISO/IEC 7816 series of standards, contactless proximity IC cards are specified in the ISO/IEC 14443 series of standards, contactless near-field communication IC cards are specified in ISO/IEC 18092 and ISO/IEC 21481, whereas contactless vicinity IC cards are specified in the ISO/IEC 15693 series of standards.

Note 2 to entry: All references to an IC card are understood to be references to the IC of the card and not to any other storage on the card (e.g. magnetic stripe).

3.8
issuer
entity responsible for issuing the *payment means* (3.11) to the user

3.9
multi-modal transport
the transportation performed with at least two different means of transport

3.10
on-board account
payment means (3.11) or *common service rights* (3.2) in an electronic fee collection (EFC) system, stored on-board either in a *payment medium* (3.12) (e.g. IC card) or in an on-board equipment

3.11
payment means
value in an *on-board account* (3.10) (e.g. cash, tokens or stored electronic values) or a reference to a *central account* (3.1) (e.g. a fleet card, bank account, credit card number or a contract ID) that gives the user access to available services

3.12
payment medium
carrier of *payment means* (3.11)

EXAMPLE Paper ticket, IC-card, smart phone.

3.13
public transport services
shared passenger transport service which is available for use by the public

EXAMPLE Bus, tram, train.

3.14
sensitive EFC data
EFC related data, either the data itself or combined with other EFC related data, that could be used for identifying an EFC user

3.15
toll regime
set of rules, including enforcement rules, governing the collection of a toll in a toll domain

[SOURCE: ISO 17573-1:2019, 3.18]

3.16
transaction model
functional model describing the structure of electronic payment transactions

[SOURCE: ISO 14906:2018, 3.17]

4 Symbols and abbreviated terms

CSR	Common Service Rights
CSRP	Common Service Rights Provider
DSRC	Dedicated Short-Range Communications
EFC	Electronic Fee Collection
ETC	Electronic Toll Collection
OBE	On-Board Equipment
PCI DSS	Payment Card Industry Data Security Standard
PT	Public Transport
RSE	Roadside Equipment
RSU	Roadside Unit
SAM	Secure Access Module
SLA	Service Level Agreement
SU	Service User
TC	Toll Charger
TSP	Transport Service Provider

5 Requirements for a common payment medium

5.1 Requirements for EFC architecture

Any EFC architecture using a common payment medium shall comply with the EFC Roles model defined in ISO 17573-1. The relation of role and responsibility of the "Provision of common service rights" and the EFC role model described in ISO 17573-1 is shown in Figure 3 when enabling interoperability with any transport services. The role of a common service rights provision includes a part of EFC function for EFC regime. As an example, the EFC transaction data described in ISO 14906 and ISO 17575-1 include account information stored in the common payment medium. The EFC role model belongs to the tolling domain and the "Provision of the common service rights" role belongs to another domain, but the two domains are linked together by the use of common service rights in EFC.

NOTE ISO 17573-1 also explains how any EFC-specific common payment medium is used when there is no interoperability with other transport services.

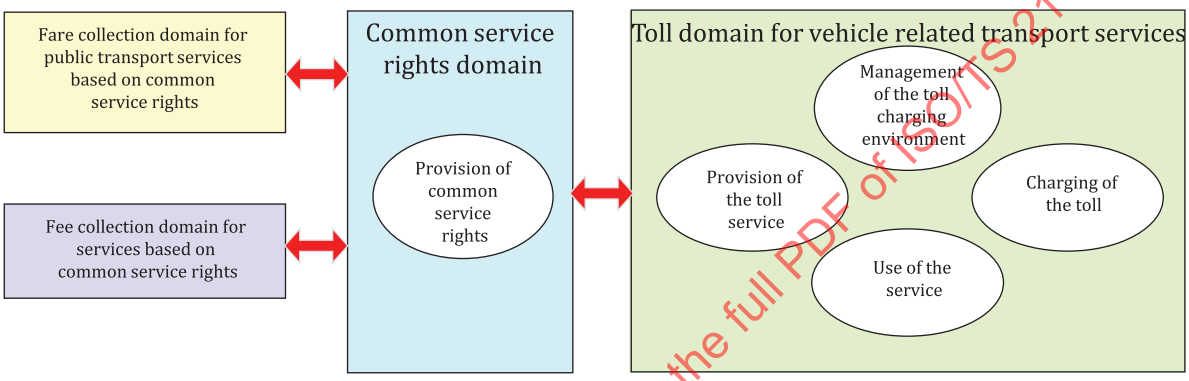


Figure 3 — EFC role model with provision of common service rights

The role related to CSRP is responsible for providing the basic artefacts, mechanism, organizational structure, and information transfer tools needed to integrate an interoperable EFC system into a multi-modal transport system.

Responsibilities related to this role are only restricted to CSRP and include:

— providing basic provision, including

  — providing a common payment medium,

  — guaranteeing that the entity performing the charging of the transport service rights role will be paid for it,

  — providing the common service rights to the user or accepting an existing one,

  — collecting the money from the signer of the EFC service contract and performing reloading transaction for common payment medium,

  — collecting all transport service transactions, clearing and distributing the money to the Transport Service Provider (TSP),

  — managing the customer relationships related to the use of the transport service concerning information, claims, questions and answers, error handling and any contractual or financial matters,

  — implementing and adhering to the security and privacy policies for the transport systems, and

  - monitoring the actual operational quality relative to agreed service level agreements (SLAs);
- acting as a contract agent, including
  - offering contractual relations according to defined conditions to interested users and concluding contractual agreements, and

    The user needs to contract both use of OBE and use of common payment medium for EFC service.
  - providing and managing the transport service contract including the service rights for the toll service user;
- customizing the common payment medium, including
  - customizing the common payment medium in a secure way;
- maintaining the common payment medium, including
  - maintaining the functionality of the common payment medium,
  - maintaining the hot listing of the common payment medium, and
  - performing the refund of values stored on the common payment medium.

A common service right provider may make requirements to the TSP such as protecting some data, security keys and so on for the TSP, toll service provider in an EFC environment.

5.2 EFC functional requirements

While an OBE is generally related to a vehicle, a common payment medium can be carried by the owner/user also for use outside a vehicle. This means that the common payment medium should be considered from the following points of view:

- Enabling the use in all transaction models, for payment modes (pre-pay and/or post pay) and applying security requirements;
- Enabling the use of the EFC service with an OBE.

  NOTE Enabling flexible EFC operation both with OBE and without OBE.
- Enabling confirmation of account information and usage record of service as basic user services.

Based on these viewpoints, requirements are derived for support of a common payment medium, as shown in Table 1.

Table 1 — Basic EFC functional requirements

Functional areas	EFC function item	Functional requirement for a common payment medium
Transaction types	Closed Toll - Entry Transaction Closed Toll - Exit Transaction Open Toll Transaction Transit Transaction Checking Transaction Purse Reloading Transaction	— Common payment medium shall be usable for all transaction types with OBE — Common payment medium shall store EFC contract information — Common payment medium shall securely store a minimum of 3 usage log entries including transaction type and date and time for use of a service — Common payment medium shall store the entry data for closed tolling system with OBE[a]
Payment types	Central Account On-Board Account Pre-Payment Post-Payment Electronic Purse Based Payment Token Based Payment 'Open'(multiple service) Payment System 'Closed'(single service) Payment System No/Zero Payment Refunding	— Common payment medium shall be usable for all payment types — Common payment medium shall be usable for common payment among transport services — Common payment medium shall be usable for reloading transaction if user signed a contract
Contract types	Area Dependent Contract Time Dependent Contract Vehicle Dependent Contract Person Dependent Contract Group of Persons Dependent Contract Anonymous Contract	— Common payment medium shall be usable for all contract types — Common payment medium shall be usable with OBE for vehicle dependent contract since vehicle information is stored in OBE. Otherwise RSE shall detect vehicle information for this contract when only common payment medium is used.
Contract handling	Contract Selection Implicit Contract Explicit Contract Multiple Simultaneous Contracts	— Common payment medium shall be able to store multiple contract information if necessary[b]

[a] This also enables performing flexible EFC operations both with OBE and without OBE.

[b] Multiple application access method is defined in ISO/IEC 7816-4.

Table 1 *(continued)*

Functional areas	EFC function item	Functional requirement for a common payment medium
Security mechanism	One Way Authentication Two Way Authentication Data Integrity Mechanism No Specific Security Segment Integrity Mechanism Signature Based Mechanism Time/Event Based Mechanism Password-based Access Mechanism Encryption Mechanism	— Common payment medium shall implement the required security function(s) — Common service right provider as a common payment medium issuer shall provide secure processing environment to toll service provider
Operational issues	Different gantries configurations Different lane configurations OBE components addressing Alert/Warning information to the customer Dynamic classification Declared classification OBE Transaction Release OBE Remote Switch Off Version Handling Mechanism OBE Capability Handling Mechanism Multi-Application Handling	— Operational requirements when a common payment medium is used in EFC shall be considered before implementation — Common payment medium shall store Version Handling Mechanism — Common payment medium shall be able to be used for Multi-Application Handling — Common payment medium shall store a minimum of 3 usage log entries including transaction type and date and time for the use of a service — Common payment medium shall prevent manipulating the road usage data by user
Tariffing schemes	Distance Dependent Time Dependent Vehicle Dependent Event Dependent Fixed Combined tariffing Scheme	— Tariffing schemes shall be considered whenever a common payment medium stores parameters corresponding to the tariff
[a] This also enables performing flexible EFC operations both with OBE and without OBE. [b] Multiple application access method is defined in ISO/IEC 7816-4.		

The requirements on the common payment medium relating to Payment Card Industry Data Security Standard (PCI DSS) should also be considered as a part of EFC functional requirements. PCI DSS is the security standard of the card industry that was developed for cardholder data protection including technical requirements. Technical requirements relating to an EFC system using a common payment medium are derived from a part of the 12 categories of requirements in PCI DSS. These are described in Table 2.

No actor in an EFC system needs to be certified as PCI DSS compliant.

Table 2 — Requirements of PCI DSS for EFC function requirements

Functional areas	PCI DSS requirement	Functional requirement for common payment medium
Data protection	— Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes — Do not store sensitive authentication data after authorization (even if encrypted) — Mask primary account number (PAN) when displayed (first six and last four digits are the maximum displayed) — Render PAN unreadable anywhere it is stored (including on portable digital medium, backup medium, and in logs) by using any of the approaches	— Primary account number (PAN), shall be secured with strong encryption — EFC system shall store necessary and minimalized personal account data for operation, not store it if not used — EFC system shall not store sensitive authentication data after used
Cryptographic key management	— Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse — Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: — Generation of strong cryptographic keys — Secure cryptographic key distribution — Secure cryptographic key storage — Cryptographic key changes for keys — Retirement or replacement of keys — If manual key management operations are used, keys must be managed using split knowledge and dual control — Prevention of unauthorized substitution of cryptographic keys — Requirement for cryptographic key custodians	— Key lifecycle management, kind of key and key generation — Key updating method, on-line and off-line, secure transmission, key switching during operation — Secure key storage in hard and soft — List management, quantity of list, updating method, ensuring real-time
Transmission of sensitive EFC data	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: — Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission — Never send unprotected PANs by end-user messaging technologies	— Sensitive EFC data such as cardholder data and PAN shall be encrypted using strong cryptography at air interface such as WAN and contactless card interface

The following security measures derived above functional requirements shall be implemented in an EFC system. These abstracts are described in Annex H and a detail of a security specification is provided by medium issuer under contract.

— Key management, kind of key and key generation.

— Secure key storage in hardware and software.

— Key updating method, on-line and off-line, secure transmission, key switching during operation.

— List management, quantity of list, updating method, ensuring real-time.

— Sensitive EFC data.

— Secure data protection.

The business process requirements, derived from CEN/TR 16092 shown in Table E.1, should be considered during developing of the specification of and EFC system.

6 Application structure in a common payment medium

This clause explains the application framework including EFC application in a common payment medium.

The common payment medium for usage in several transport services is a portable device such as an IC card or a mobile device. For common use of a medium, this medium shall store either individual applications provided by each TSP or an application that enables usage among all TSPs. In this latter case the issuer of the medium is required to know all application details to support all service providers.

The common media can support three types of application structures:

— Type 1: Multi application. The common payment medium is configured with individual transport service applications and an application containing the CSR for use by all other transport service applications.

— Type 2: Shared data. The medium is configured with individual transport service applications and application with shared data used for CSR by all other transport service applications.

— Type 3: Single application. The medium is configured with one common application that stores all data for the use of corresponding transport services including CSR.

Explanations of these types are given in Annex D.

7 EFC application data in a common payment medium

7.1 General

This clause deals with the minimum set of EFC application data in the common payment medium necessary only to serve the interface data according to ISO 14906 for carrying out all EFC schemes described in 5.2, the EFC functional requirements.

NOTE 1 According to the additional threats and security measures listed in ISO 19299, some attribute data are added to those defined in ISO 14906 when a common payment medium is used for a closed toll system to prevent swapping a common payment medium in a toll road network for abusing and juggling the toll charge.

NOTE 2 Data elements defined in EN 1545 can be used when more transport-related data are necessary to be stored in the medium.

The EFC attribute data defined in 7.2 are required for the integrated use of a common payment medium within an EFC system. These additional attributes are only stored in the common payment medium.

7.2 EFC attribute data for a common payment medium

Table 3 shows the storage location of EFC attribute data in the case of a one-piece OBE (OBE built as a single unit) and two-piece OBE (OBE built as a couple of units, one of which is the common payment medium):

1) A one-piece OBE, shown as case 1, stores all attribute data required to operate EFC service defined in ISO 14906 and attribute data defined in this document;

2) A two-piece OBE, shown as case 2, stores attribute data for EFC service between an OBE and a medium defined in ISO 14906 and attribute data defined in this document. OBE stores vehicle relating data and a medium stores personal relating data.

NOTE In Table 3, the double check indicator means "mandatory", the single check indicator means "option" as explained in the following sentence.

According to the additional threats and security measures listed in ISO 19299, an additional attribute data ReceiptEntryVehicle shall be added to those EFC attributes defined in ISO 14906 when a common payment medium is used for a closed toll system to prevent swapping of a common payment medium in a toll road network for abusing and juggling the toll charge.

On a common payment medium for pre-payment service(s), the user can select an option for reloading stored values when EFC charging is performed at a toll station. An additional attribute data group named ReloadingParameter is included as a general data group for the reloading function of stored values on a common payment medium for pre-payment service(s) (see Table 5). This data group consists of some parameters for on-site reloading such as validity of reloading, threshold value for low balance and value for reloading.

This document does not inhibit the OBE from storing data stored in the common payment medium.

When the common payment medium is present, the stored EFC attribute data from the common payment medium shall be used.

When the common payment medium is not present, the stored EFC attribute data in OBE shall be used.

This is an option for user convenience service as indicated by a single check in Table 3. Another example, there are two parameters for ContractAuthenticator, one is stored inside the OBE and another is stored on the common payment medium, and toll charger and toll service provider can check whether these are authorised or not.

Table 3 — Additional attribute data for medium

EFC attributes defined in ISO 14906			Data location			Additional attribute for medium
			Case1	Case 2		
Data group	Attr. ID	Attribute	One-piece OBE	OBE	Medium	
Contract	0	EFC-ContextMark	✓✓	✓✓	✓✓	
	1	ContractSerialNumber	✓✓	✓✓	✓✓	
	2	ContractValidity	✓✓	✓✓	✓✓	
	35	ValidityOfContract	✓✓	✓✓	✓✓	
	3	ContractVehicle	✓✓	✓✓		
	4	ContractAuthenticator	✓✓	✓✓	✓✓	

Table 3 *(continued)*

EFC attributes defined in ISO 14906			Data location			Additional attribute for medium
Data group	Attr. ID	Attribute	Case1	Case 2		
			One-piece OBE	OBE	Medium	
Receipt	5	ReceiptServicePart	✓✓	✓	✓✓	
	6	SessionClass	✓✓	✓	✓✓	
	7	ReceiptServiceSerialNumber	✓✓	✓	✓✓	
	36	ReceiptFinancialPart	✓✓	✓	✓✓	
	9	ReceiptContract	✓✓	✓	✓✓	
	10	ReceiptOBEId	✓✓	✓	✓✓	
	11	ReceiptICC-Id	✓✓	✓	✓✓	
	12	ReceiptText	✓✓	✓	✓✓	
	13	ReceiptAuthenticator	✓✓	✓	✓✓	
	14	ReceiptDistance	✓✓	✓	✓✓	
	33	ReceiptData1	✓✓	✓	✓✓	
	34	ReceiptData2	✓✓	✓	✓✓	
Vehicle	15	VehicleIdentificationNumber	✓✓	✓✓		
	16	VehicleLicencePlateNumber	✓✓	✓✓		
	17	VehicleClass	✓✓	✓✓		
	18	VehicleDimensions	✓✓	✓✓		
	19	VehicleAxles	✓✓	✓✓		
	20	VehicleWeightLimits	✓✓	✓✓		
Equipment	24	EquipmentOBEId	✓✓	✓✓		
	25	EquipmentICC-Id			✓✓	
	26	EquipmentStatus	✓✓	✓	✓✓	
Driver	27	DriverCharacteristics	✓✓	✓	✓✓	
Payment	32	PaymentMeans	✓✓		✓✓	
	29	PaymentMeansBalance	✓✓		✓✓	
	30	PaymentMeansUnit	✓✓		✓✓	
	31	PaymentSecurityData	✓✓		✓✓	
Receipt					✓✓	ReceiptEntryVehicle
Payment					✓✓	ReloadingParameter

7.3 Additional EFC attribute data

7.3.1 Data group RECEIPT

This data group consists of some optional data elements. Typical data elements for a closed EFC system is shown in Table 4.

Table 4 — Receipt data

EFC attribute	Data element	Definition	Type	Informative remarks
ReceiptEntryVehicle	VehicleLicencePlateNumber	Vehicle licence plate number recognized and stored at entry toll gate. e.g. enabling to detect swapping common payment medium at Service area and/or Parking area for devious toll payment.	LPN	
	EquipmentOBEId	OBE ID copied and stored at entry toll gate. e.g. enabling to detect swapping common payment medium at Service area and/or Parking area for devious toll payment.	OCTET STRING	
	VehicleClass	Vehicle class classified and stored at entry toll gate	INT1	
	EntryAuthenticator	Authenticator for this attribute.	OCTET STRING	

NOTE Specification of calculation of authenticator is provided by medium issuer.

7.3.2 Data group PAYMENT

This data group consists of some optional data elements. Typical data elements for pre-payment values stored on a common payment medium is shown in Table 5.

Table 5 — Payment data

EFC attribute	Data element	Definition	Type	Informative remarks
Reloading Parameter	ReloadingValidity	End date of the validity of the reloading contract option.	DateAndTime	
	ThresholdBalance	Threshold value of balance in medium for reloading activation at EFC transaction.	SignedValue, INT3	
	ReloadingValue	Value to add balance in medium at reloading transaction.	SignedValue, INT3	
	DepositValue	Amount of a deposit for checking when auto-reloading transaction is performed.	SignedValue, INT3	Described in EN 1545-2, as Amount.
	Dynamic Reloading ValueFlag	Flag for reloading value equal to charging value when insufficient balance.	Flag	
	Reloading Authenticator	Authenticator calculated by the Contract-Provider called Common Service Right Provider when issuing the Contract, to prevent tampering with contract data.	OCTET STRING	Authenticator of all data element in ReloadingParameter
	Autoload StartDate	Start date of the period of the reloading option service for checking when EFC transaction is performed.	DateAndTime	Described in EN 1545-2, as DateStamp.
	AutoloadEndDate	End date of the period of the reloading option service for checking when EFC transaction is performed.	DateAndTime	Described in EN 1545-2, as DateStamp.
	AutoRenewFlag	A flag indicating whether auto-renew is enabled. Valid flag for automatic reloading at EFC transaction.	Flag	Described in EN 1545-2, as Flag.

NOTE Specification of calculation of authenticator is provided by medium issuer.

Annex A
(normative)

Data type specifications

The EFC data types and associated coding related to the EFC attribute data, described in Clause 7, are defined using the Abstract Syntax Notation One (ASN.1) technique according to ISO/IEC 8824-1. The unaligned packed encoding rules according to ISO/IEC 8825-2 are applied.

The actual ASN.1 module is contained in the attached files "ISO21193(2019)EfcCsrv1.asn", which can be directly imported in a compiler.

The syntax and semantics of the ASN.1 types in the attached file "ISO21193(2019)EfcCsrv1.asn" that are imported shall comply with ISO 14906.

NOTE 1 The above referenced files (i.e. "ISO21193(2019)EfcCsrv1.asn") are available for download via a hyperlink at www.itsstandards.eu/index.php/efc#EFCstandards and at http://standards.iso.org/iso/ts/21193/ed-1/en.

Table A.1 provides the SHA-256 cryptographic hash digests for the referenced files, offering a means to verify the integrity of the referenced files. The SHA-256 algorithm is specified in NIST 180-4.

Table A.1 — SHA-256 cryptographic hash digests

File name	SHA-256 cryptographic hash digest
ISO21193(2019)EfcCsrv1.asn	ec436359369c65a8203ef4b7f5829d1ccdb5ab5dbb-5555c7f3e75690f8efd22a

NOTE 2 Pasting the text of the file into one of the hash digest computation pages available on the web can result in a non-matching hash digest due to changes in the underlying coding.

Annex B
(normative)

Implementation conformance statement (ICS) pro forma

B.1 General

To evaluate the conformance of a particular implementation, it is necessary to have a statement of those capabilities and options that have been implemented. This is called an implementation conformance statement (ICS).

This Annex presents the pro forma to be used for the attributes defined in Clause 7 and Annex A, with ICS templates that are to be filled in by equipment suppliers.

B.2 Purpose and structure

The purpose of this ICS is to provide a mechanism whereby a supplier of an implementation of the attribute in medium defined in this document can provide information about the implementation in a standardised manner.

The ICS is subdivided as follows corresponding to categories of information:

— identification of the implementation;

— identification of the protocol;

— global statement of conformance;

— ICS tables.

B.3 Instruction for completing ICS

B.3.1 Definition of support

A capability is said to be supported if the implementation under test (IUT) can

— generate the corresponding operation parameters (either automatically or because the end user requires that capability explicitly), and

— interpret, handle and, when required, make available to the end user the corresponding error or result.

A protocol element is said to be supported for a sending implementation if it can generate it under certain circumstances (either automatically or because the end user requires relevant services explicitly).

A protocol element is said to be supported for a receiving implementation if it is correctly interpreted and handled and also, when appropriate, made available to the end user.

B.3.2 Status column

This column (see Tables B.1 to B.8) indicates the level of support required for conformance. The values are as follows:

m mandatory support is required;

o optional support is permitted for conformance to the standard. If implemented, it shall conform to the specifications and restrictions contained in the standard. These restrictions may affect the optionality of other items;

c the item is conditional (support of the capability is subject to a predicate);

c: m the item is mandatory if the predicate is true, optional otherwise;

— the item is not applicable;

— the item is outside the scope of this ICS.

In the ICS tables, every leading item marked “m” shall be supported by the IUT. Sub-items marked “m” shall be supported if the corresponding leading item is supported by the IUT.

B.3.3 Support column

This column (see Tables B.6 to B.8) shall be completed by the supplier or implementer to indicate the level of implementation of each item. The proforma has been designed such that values required are the following:

Y Yes, the item has been implemented;

N No, the item has not been implemented;

— the item is not applicable.

All entries within the ICS proforma shall be made in ink. Alterations to such entries shall be made by crossing out, not by erasing or making the original entry illegible, and by writing the new entry alongside. All such alterations to records shall be initialised by the person who made them.

B.3.4 Item reference numbers

Each line within the ICS which requires that implementation details be entered is numbered at the left-hand edge of the line. This numbering is included as a mean of uniquely identifying all possible implementation details within the ICS. This referencing is used both inside the ICS, and for references from other test specification documents.

The means of referencing individual responses is done in the following sequence:

a) a reference to the smallest individual response enclosing the relevant item;

b) a solidus character (“/”);

c) the reference number of the row in which the response appears;

d) if, and only if, more than one response occurs in the row identified by the reference number, implicit labelling of each possible entry as “a”, “b”, “c”, etc., from left to right, with this letter appended to the sequence.

B.4 ICS for medium

B.4.1 Identification of the implementation

The following pro forma are to be used to identify the implementation on the medium side.

Table B.1 — Identification of ICS

Item no.	Question	Response
1	Date of statement (DD/MM/YY)	
2	ICS serial number	
3	System conformance statement cross-reference	

Table B.2 — Identification of the implementation and/or system

Item no.	Question	Response
1	Common service right provider name	
2	Version number	
3	Other information	

Table B.3 — Identification of the medium supplier

Item no.	Question	Response
1	Organization name	
2	Contact name(s)	
3	Address	
4	Telephone number	
5	E-mail address	
6	Other information	

Table B.4 — Identification of the medium

Item no.	Question	Response
1	Brand name	
2	Type, version	
3	Manufacturer ID	
4	Serial numbers of supplied units	
5	Other information	

Table B.5 — Identification of this document

Item no.	Question	Response
1	Title, reference no., publication date of the document	
2	Document edition number	
3	Other information	

B.4.2 ICS tables

This part of the ICS identifies the supported application context, communication services and attributes for the medium side.

Table B.6 — Data requirements regarding Receipt

Item no.	Element	Reference	Status	Support
1	VehicleLicencePlateNumber	7.3.1	o	
2	EquipmentOBEId	7.3.1	o	
3	VehicleClass	7.3.1	o	
4	EntryAuthenticator	7.3.1	o	

Table B.7 — Data requirements regarding reloading

Item no.	Element	Reference	Status	Support
1	ReloadingValidity	7.3.2	o	
2	ThresholdBalance	7.3.2	o	
3	ReloadingValue	7.3.2	o	
4	DepositValue	7.3.2	o	
5	DynamicReloadingValueFlag	7.3.2	o	
6	ReloadingAuthticator	7.3.2	o	
7	AutoloadStartDate	7.3.2	o	
8	AutoloadEndDate	7.3.2	o	
9	AutoRenewFlag	7.3.2	o	

Table B.8 — Security measures

Item no.	Element	Reference	Status	Support
1	Key management, kind of key and key generation	7.3.2	o	
2	Secure key storage	7.3.2	o	
3	Key updating method	7.3.2	o	
4	List management	7.3.2	o	
5	Sensitive EFC data	7.3.2	o	
6	Secure data protection	7.3.2	o	

Annex C
(informative)

Common payment medium concept

This document explains EFC application as one of transport service specific application and application interface requirements for Common service rights application.

Service rights are stored in an electronic transport related e-purse (stored value) installed with a Common service right application. The application is owned and operated by a CSRP whose functions could be compared with those of a financial service provider. The CSRP belongs to the transport domain and is within the scope of this document. The financial service provider belongs to the financial domain and is outside the scope of this document.

The payment means are used to purchase the service rights from a CSRP, see Figure C.1. The service rights in the form of a transport specific e-purse (stored value) are again used for purchasing other service rights from TSPs, e.g. passages through toll stations in a tolled road network or single trips in a PT network.

The CSRP needs to collect requirements from the financial service provider and TSPs to issue the common payment medium.

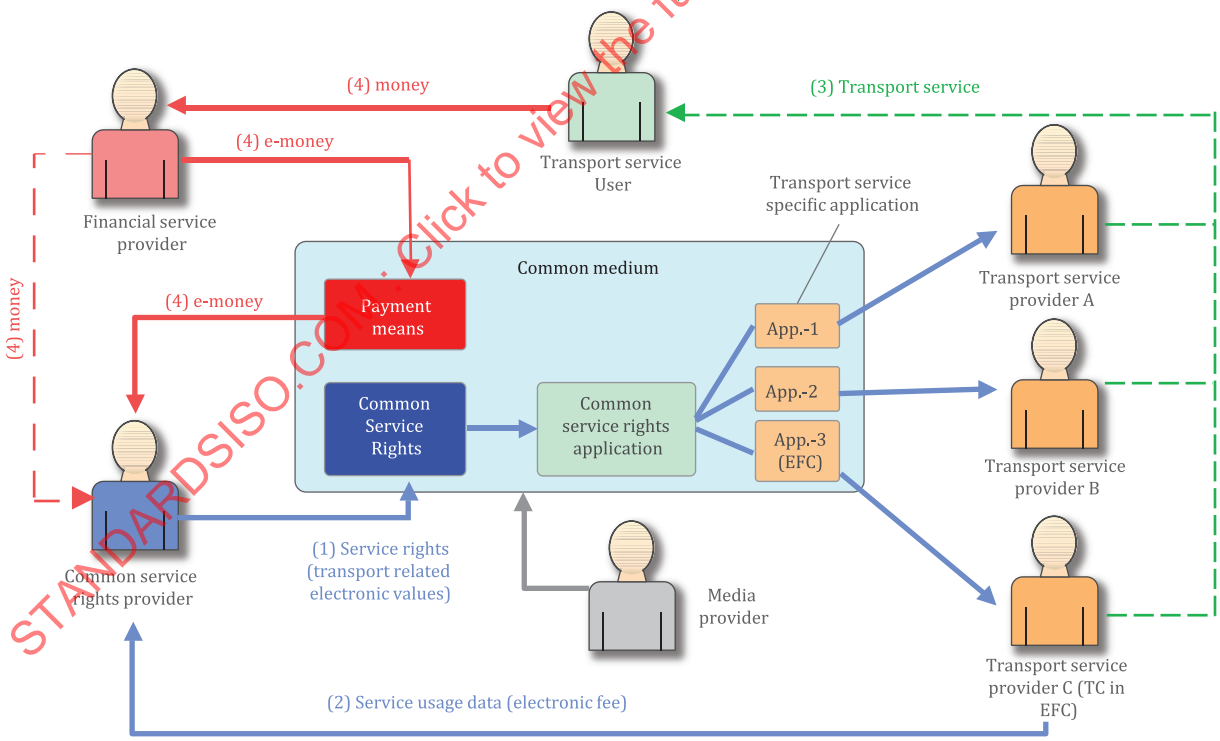


Figure C.1 — Common payment medium concept

NOTE 1 Interfaces (4) for e-money are monetary flow in financial and out of scope and 'Transport service' lines (3) are not interfaces but just an illustration that the TSP provides a transport service to the user.

NOTE 2 Interfaces between Application in medium and TSP are in scope.

In some cases, the TSP is split into two sub-roles. These are the Transport service manager dealing with the user contracts and payments and the Transport operation manager delivering/carrying through

the transport service. It should be noted that the division of the TSP role into two sub-roles is always used in interoperable fee or fare collection systems.

The user has a contract with a transport service manager, e.g. a toll service provider (EFC) or a product owner via a product retailer (public transport).

The service rights provided by the transport service manager enable the user to benefit from transport services provided by any transport operation manager having an agreement with the transport service manager.

For EFC this concept is defined in ISO 17573-1. For public transport this concept is defined in ISO 24014-1.

As the medium may exist in many different forms the medium providers could for instance be a credit card company, a smartphone provider, an On-Board Equipment provider and an RFID tag provider.

The CSRP could be a Trusted Third Party, e.g. an external entity or a co-operation between all or a sub-set of the TSPs involved in the common payment medium scheme.

An example of such an application could be an EFC application for common payment medium and on-board equipment. Figure C.2 shows the proposed application hierarchy and some application structures with security functions are shown in Annex D.

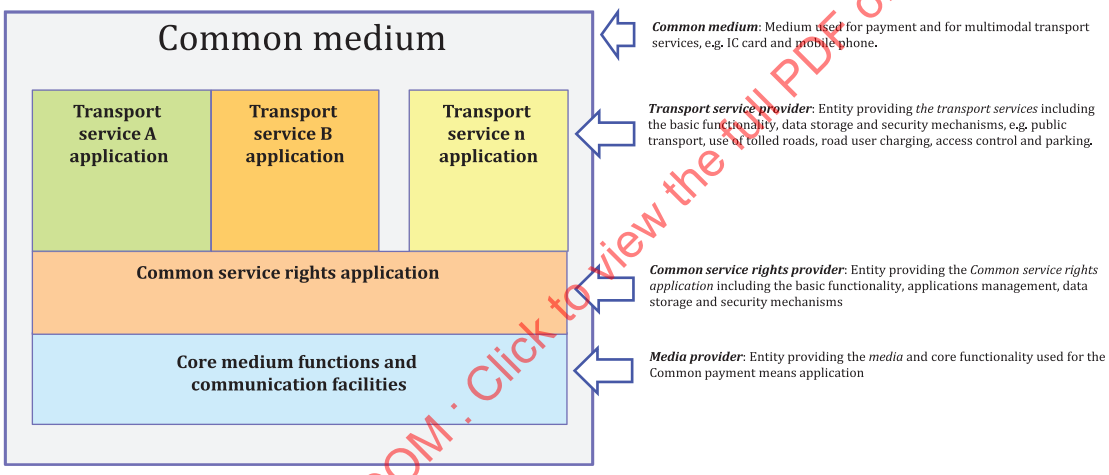


Figure C.2 — Proposed common payment medium application hierarchy

Annex D
(informative)

Application structure examples in common payment medium

D.1 General

This annex explains three types of typical application structures of common payment medium for multi-modal transport usage examples based on integrated-circuit card standards.

Three transport applications such as Public transport, Parking and EFC are appeared for instance in this annex. This means that this document does not constrain implementing these transport applications but allows implementing any transport service application in medium.

Common use data elements of transport service rights are stored in "common TrSR" memory area. This memory area is located not only in a purpose-built one application but also in a co-existence one application.

D.2 Application structure type 1

The common application structure is shown in Figure D.1. The medium is configured with individual transport service applications and an application containing the CSR for use by all other transport service applications.

The security objects are controlled individually by each transport system and only cryptography keys for "common TrSR" for enabling common use among all transport systems. When a service user uses a transport service, the transport service system accesses both the transport service application and the common TrSR application in sequence. This type needs to perform two or more access control processes such as application authentication at every switching application. This means a relatively significant amount of time is necessary for execution of the transaction.

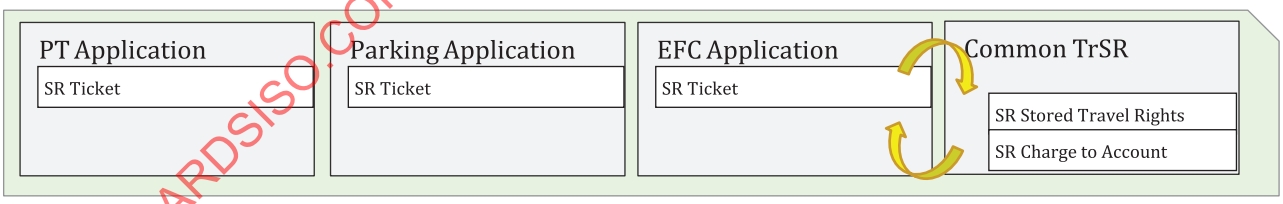


Figure D.1 — Multi-application

D.3 Application structure type 2

Application structure with shared data is shown in Figure D.2. The medium is configured with individual transport service applications and shared data used for CSR by all other transport service applications.

The security objects are controlled individually by each transport system and only cryptography keys for "common TrSR" need to be shared among all transport systems.

When a service user uses a transport service, the transport service system accesses both the transport service application and the shared data file in sequence. This type needs to perform one access control process such as application authentication for accessing both transport service application and common TrSR without switching applications.

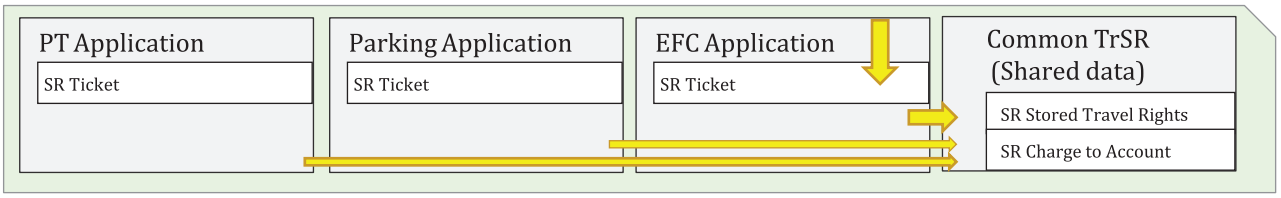


Figure D.2 — Multi application with shared data file

D.4 Application structure type 3

A single application structure is shown in Figure D.3. The medium is configured with one common application that stores all data for all uses of the corresponding transport services.

This type allows the use of one security object among all transport systems.

When the service user uses a transport service, the transport service system accesses both transport service data and common TrSR data in sequence. This type performs one access control process such as application authentication for accessing both transport service data and common TrSR data.

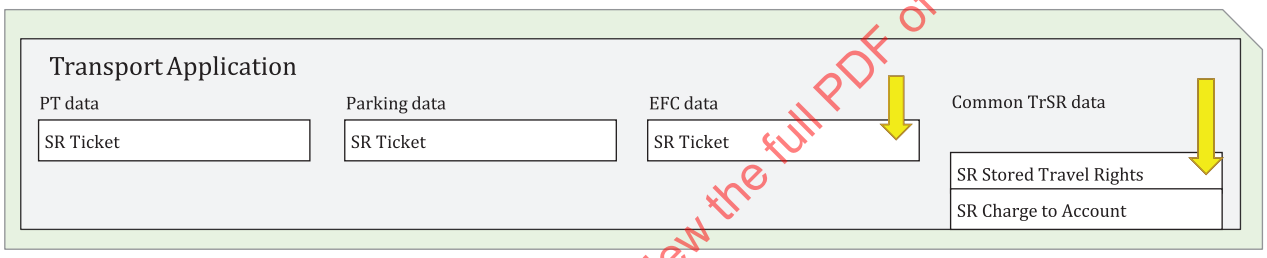


Figure D.3 — Single application

Annex E
(informative)

General information for common payment medium and OBE

EFC related transport service specific application will consist of:

— Application data elements necessary to build an EFC transaction according to ISO 14906. This is explained in Clause 7 of this document.

NOTE 1 EN 1545 defines application data elements for transport applications.

— Application interface accessing method is explained in ISO 25110.

— Business process requirements is explained in CEN/TR 16092

  — Issuing

  — Personalization

  — Loading; the example of Reloading transaction is shown in Annex G.

  — Charging; the example of Charging transaction is shown in ISO 14906

  — Clearing

  — Hot listing

  — Invoicing

  — Refund

— Technical requirements are explained in CEN/TR 16092 (and ISO/IEC 7810, ISO/IEC 7816, ISO/IEC 14443, ISO/IEC 18092, ISO/IEC 15693)

  — General requirements

  — Specific requirements for contact/contactless

  — Specific requirements for OBE

— Logical and Physical interface are explained in ISO/IEC 7816, ISO/IEC 14443 and ISO/IEC 18092.

— Command and response are explained in ISO/IEC 7816 and ISO/IEC 14443.

NOTE 2 Any interface such as Bluetooth and Wi-Fi of Mobile Phone can be applied for use of common payment medium also.

Table E.1 shows the essential to consider the business process in EFC system using medium. Details derived from these requirements are contained in the specification of EFC system using medium.

Table E.1 — The business process

Process name	Abstract
Issuing	First process for use of common payment medium is the issuing of common service rights from CSRP to service user (SU) and the issuing of transport service application. SU choose some options, such as stored-value with automatic-reloading or without automatic-reloading or credit.

Table E.1 *(continued)*

Process name	Abstract
Personalization	Any common payment medium except anonymous option such as stored-value without auto-reloading is personalized with contract. The link between the ID of the pre-personalized common payment medium and the centrally held account needs to be established before the first use of the common payment medium. Typical personalization method and transaction in EFC scheme is explained in ISO 21719 series.
Loading	The loading of value into a stored value in common payment medium is done at initial before first use and at periodicity. Reloading related EFC data definitions are described in chapter 7.3.2 and typical loading method and transaction in EFC scheme is explained in Annex G.
Charging	The charging of the toll for the TC allows using medium with OBE and without OBE. Typical DSRC based charging method and transaction in EFC scheme is explained in ISO 14906 and typical autonomous charging is explained in ISO 17575.
Auto-reloading	The auto-reloading of value into a stored value in common payment medium is done when low balance is detected under contract. Reloading related EFC data definitions are described in chapter 7.3.2 and typical automatic loading method and transaction in EFC scheme is explained in Annex G.
Clearing	The clearing of transactions takes place between the CSRP and the TSP and is identical to the claiming.
Hot listing	Hot listing as enforcement procedures is considered and operated as usually.
Invoicing	The invoicing of the service user is considered who create the invoice and do the user service.
Refund	If a SU closes the EFC contract with a CSRP, he must return the associated common payment medium.

Annex F
(informative)

System migration

This annex describes a general method for seamless upgrade EFC system and medium. Upgrading information security in the EFC system, new medium issued by newly medium provider and any medium except card type also can be assumed to use these methods.

At the first implementation of the EFC system on road, the requirements of the medium provider are taken into account to design the EFC system easily since the EFC system environment using medium is completely new as shown in Figure F.1.

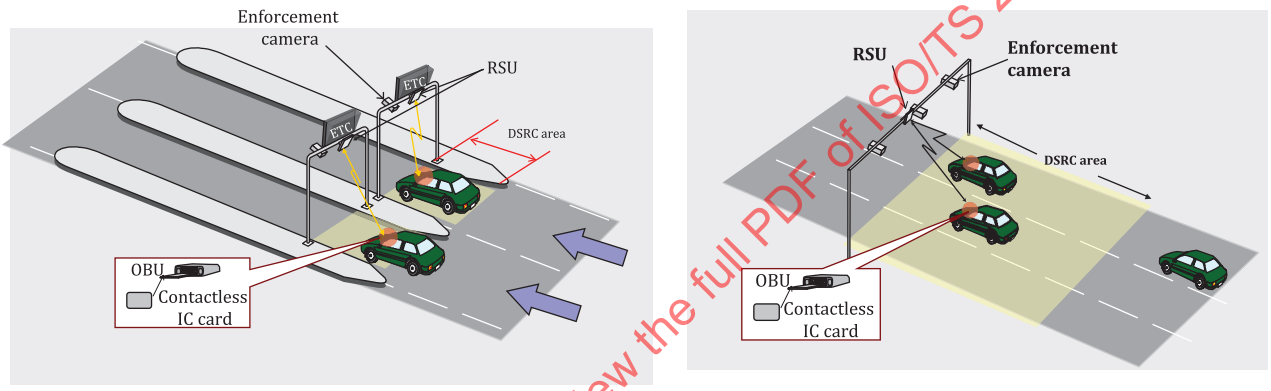


Figure F.1 — First installed EFC system image of single lane and multilane

On EFC system upgrading, when renew EFC system is implemented on toll road with present EFC system, the parallel operation method with the new and old EFC systems is required with parallel operation period. Additionally, there is selectable option described as follows.

1st is new roadside infrastructure supporting new and old EFC system; Both old and new EFC systems are installed at the same toll station in both multilane tolling and single lane tolling as shown in Figure F.2. Furthermore, separate old and new EFC single lane is selectable in single lane tolling also. After all OBE are replaced with new OBE during parallel operation period, old RSU will be replaced with new RSU.

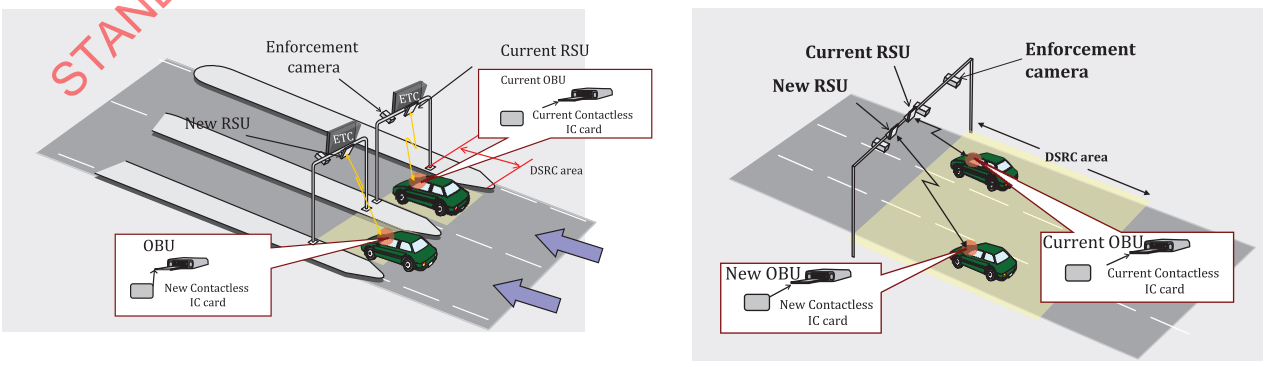


Figure F.2 — Dual EFC RSU tolling station image during parallel operation period

2nd is new OBE supporting new and old EFC system; OBE applies with the old and new EFC system as shown in Figure F.3. After all OBE are replaced with new OBE during parallel operation period, old RSU will be replaced with new RSU.

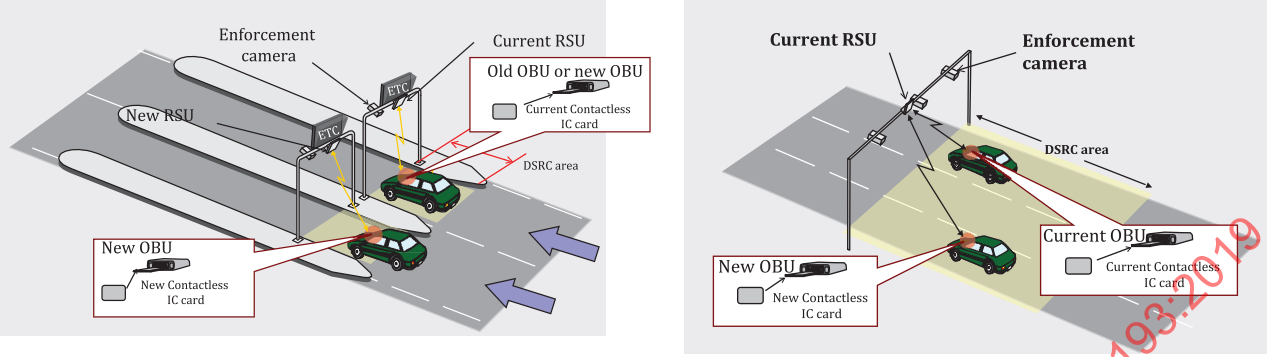


Figure F.3 — Dual EFC OBE tolling station image during parallel operation period

In addition to above general migration, following further study is necessary for EFC system with medium. There is different migration approach where the module for corresponding transaction and security processing with medium is equipped on OBE or RSU for OBE with medium.

In case of module equipped OBE; OBE perform transaction and security processing by using module and apply with old and new medium. Figure F.4 shows the medium migration study case with multiple applications in OBE.

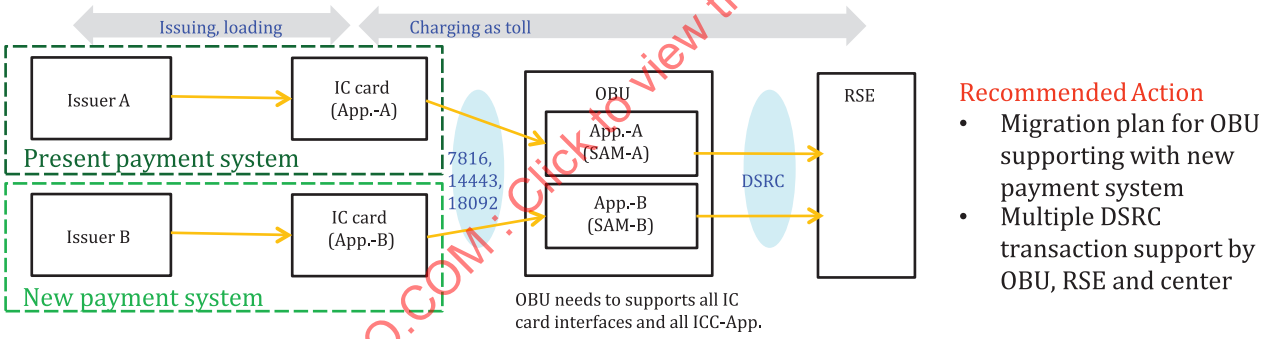
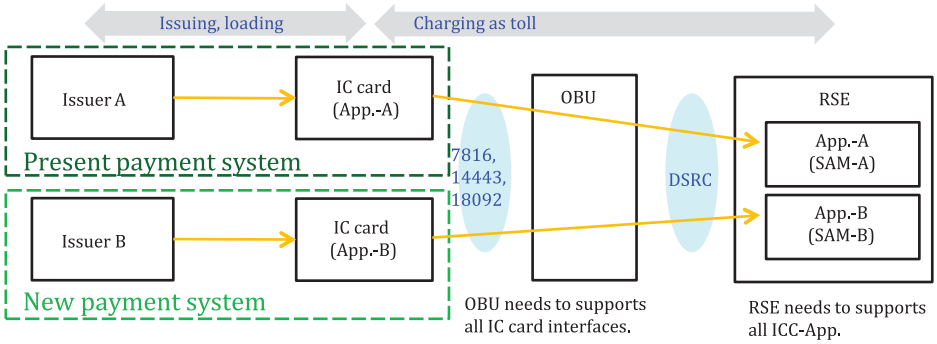


Figure F.4 — Multiple applications in OBE

Additionally, if OBE is not equipped the interface with new medium. OBE need to be upgrade for equipping new medium interface.

In case of module equipped RSU; RSU perform transaction and security processing by using module and apply with old and new medium. OBE apply with the both interface old and new medium and OBE works as transparent model described in ISO 25110. Figure F.5 shows the medium migration study case with multiple applications in RSU.



Recommended Action

- Migration plan for RSE supporting with new payment system
- Multiple DSRC transaction support by RSE and center

Figure F.5 — Multiple applications in RSU

The following items, among others, may also be relevant to consider for EFC system migration.

— Matching processing between a DSRC transaction data from old or new EFC system with an enforcement data.

— Enough migration periods with parallel operation from old EFC system to new EFC system.

— Wide announcement in advance for all service users about the migration plan.

Annex G
(informative)

Reloading system for pre-payment medium in Korean ETC

G.1 General

The EFC in Korea was started with a prepaid card. After 2009 post-paid card was adopted to the EFC system.

The toll fee is collected from the IC card called a “hi-pass card” which is inserted into the on-board equipment, and the same IC card can also be used in the manual lanes (booth). This is called "Touch & Go”.

Reloading is an especially important function in the same manner as charging. The prepaid card is reloaded with the value at the same time or before the charging transaction.

There are three types of reloading system on the Korean EFC of the prepaid card as follows and shown in Figure G.1.

— (case 1) direct reloading type in the toll booth;

— (case 2) on-line reloading type with POS device;

— (case 3) auto-reloading type in EFC during DSRC wireless communication.

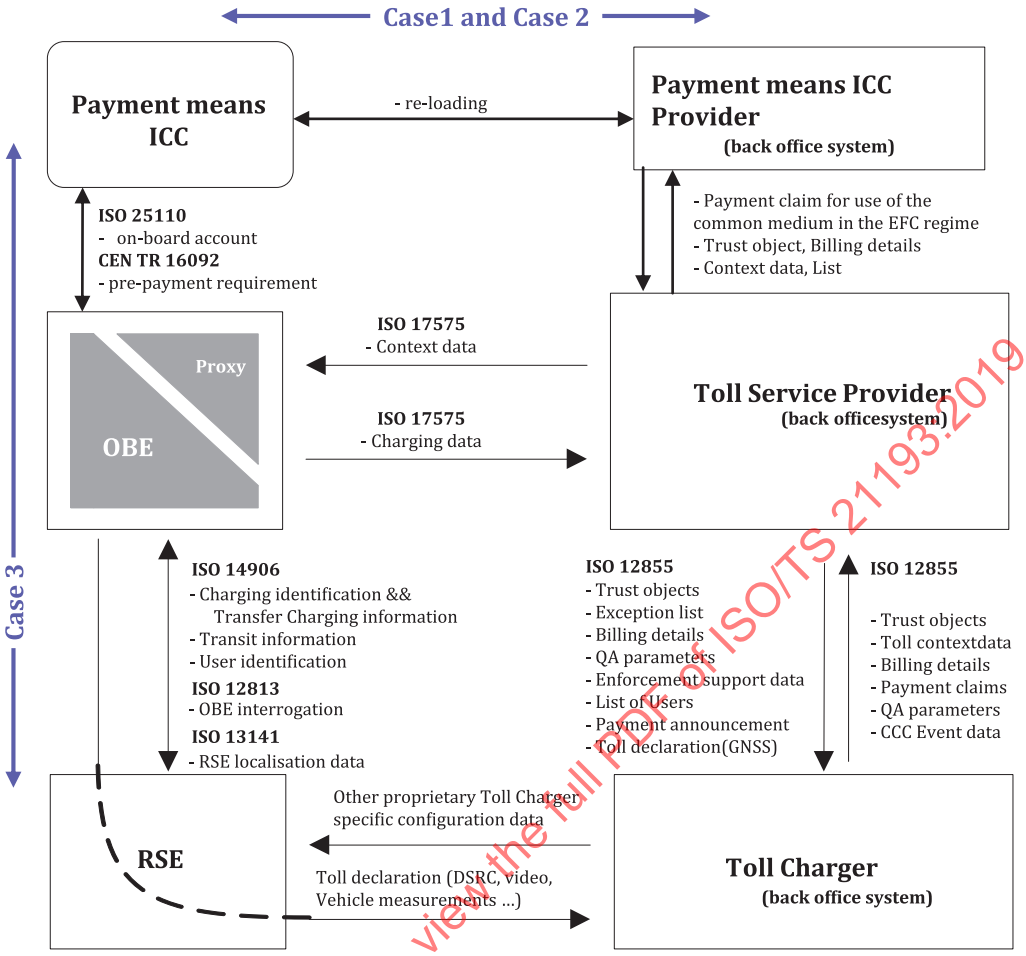


Figure G.1 — Korean EFC reloading model based on ISO/TR 19639

G.2 Direct reloading type

G.2.1 Overview

A certain amount is automatically loaded to the loaded security application module (LSAM), which is installed to the booth controller through a local network. If the user wants to reload to a prepaid card in the manual lane, the value from LSAM could be charged to the prepaid card.

G.2.2 Data transfer process

In this type, there are two reloading procedures, the first is between LSAM and the prepaid card, and the second is between the reloading operator and LSAM as shown in Figure G.2. Mutual authentication between the prepaid card and LSAM is processed directly before the application data is exchanged and the value data is accessed. Both the result data and the balance amount of LSAM are sent to the reloading operator.

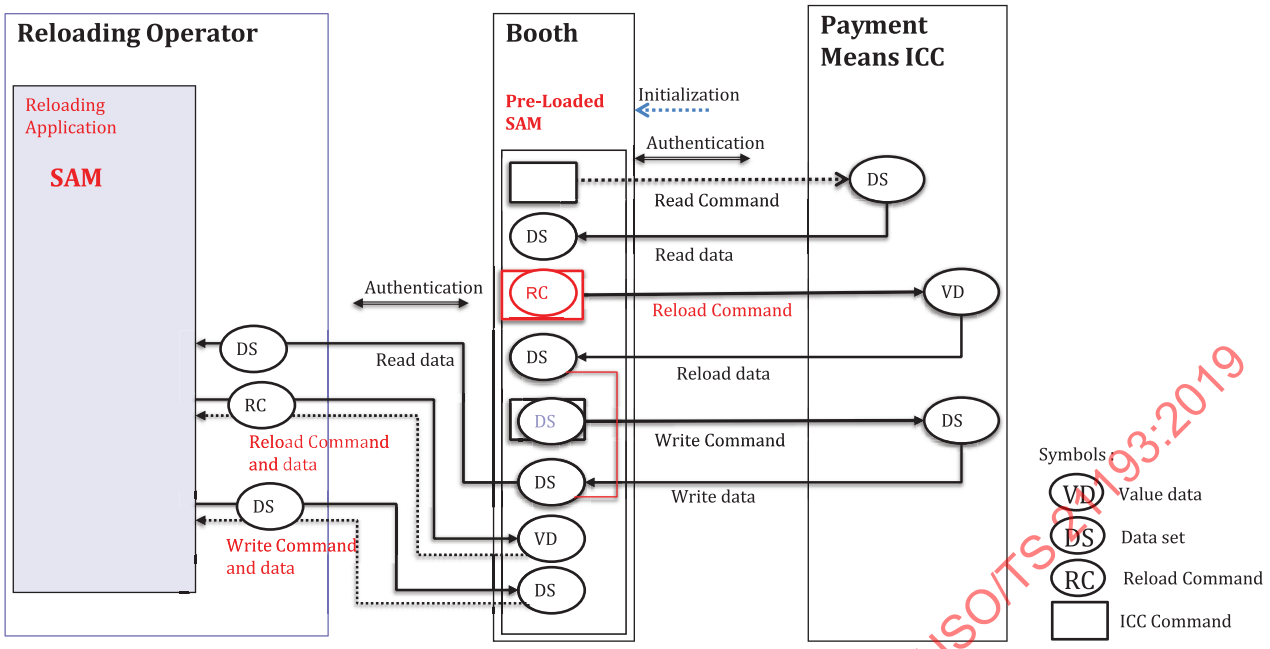


Figure G.2 — Direct reloading data transfer process according to ISO 25110

G.2.3 Interface definition

G.2.3.1 Functional configuration

In this type, the LSAM in the booth sends reloading command to a prepaid card. Then, the SAM of the reloading operator reads and checks both the result of reloading and the balance of LSAM. If the balance of LSAM is below the set-up amount, the SAM of the reloading operator would send the reload command to LSAM and charge the value to LSAM.

G.2.3.2 Command and response

Using DSRC-EID('0') and 'action parameter (based on ISO 14906), the LSAM commands access to the prepaid card directly with designating Channel ID=ICC(3)[according to ISO 14906].

Table G.1 — TRANSFER_CHANNELrequest (between the LSAM and prepaid card)

Parameter	ASN.1 Type	Value	Remarks
Element Identifier EID	DSRC-Eid	0	
Action Type	INTEGER(0..127,..)	8	Transfer Channel
AccessCredentials	OCTET STRING		

ActionParameter	ChannelRq ::=SEQUENCE {
	channelIdChannelId,
	apdu OCTET STRING
	}
			Always to be present
			Channel ID=ICC (3)

Mode	BOOLEAN		TRUE

Table G.2 — TRANSFER_CHANNELrequest(between SAM in the Reloading Operator and LSAM)

Parameter	ASN.1 Type	Value	Remarks
Element Identifier EID	DSRC-Eid	0	
Action Type	INTEGER(0..127,..)	8	Transfer Channel
AccessCredentials	OCTET STRING		

ActionParameter	ChannelRq ::=SEQUENCE {
	channelIdChannelId,
	apdu OCTET STRING
	}
			Always to be present
			Channel ID=SAM (1)

Mode	BOOLEAN		TRUE

Table G.3 — TRANSFER_CHANNELresponse(between SAM in the Reloading Operator and LSAM)

Parameter	ASN.1 Type	Value	Remarks
ResponseParameter	ChannelRs::=SEQUENCE { channelIDChannelID, apdu OCTET STRING}		Always to be present
Return Code(Ret)	Return Status		Optical use

G.3 On-line reloading type

G.3.1 Overview

Users can reload by themselves to access the reloading Operator Server through the Reloader such as an ATM or a card reader device.

G.3.2 Data transfer process

The data exchanged between the reloading operator and the prepaid card are processed directly after authentication between security application module (SAM) in the Reloading Operator is processed directly before the application data is exchanged and value data is accessed as shown in Figure G.3.

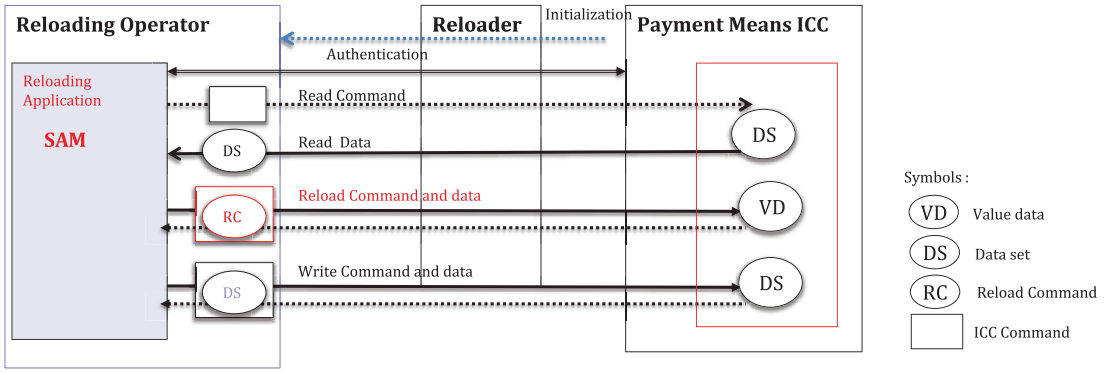


Figure G.3 — On-line reloading data transfer process according to ISO 25110

G.3.3 Interface definition

G.3.3.1 Functional configuration

In this type, the SAM of the reloading operator sends the reloading ICC command in its APDU to execute the ICC read/reload/write operation directly.

G.3.3.2 Command and response

Using DSRC-EID('0') and Action parameter (based on ISO 14906), the SAM of reloading operator commands access to ICC directly with designating Channel ID in the action parameter as channel ID=ICC(3).

Table G.4 — TRANSFER _CHANNELrequest(between SAM in the reloading operator and prepaid card)

Parameter	ASN.1 Type	Value	Remarks
Element Identifier EID	DSRC-Eid	0	
Action Type	INTEGER(0..127,..)	8	Transfer Channel
AccessCredentials	OCTET STRING		

ActionParameter	ChannelRq ::=SEQUENCE {
	channelIdChannelId,
	apdu OCTET STRING
	}
			Always to be present
			Channel ID=ICC (3)

Mode	BOOLEAN		TRUE

Table G.5 — TRANSFER _CHANNEL.response

Parameter	ASN.1 Type	Value	Remarks
ResponseParameter	ChannelRs ::= SEQUENCE { channelIdChannelId, apdu OCTET STRING }		Always to be present
Return Code(Ret)	Return Status		Optional use