
**Intelligent transport systems —
Common Transport Service Account
Systems —**

**Part 1:
Framework and use cases**

Partie 1: Cadre et cas d'utilisation



STANDARDSISO.COM : Click to view the full PDF of ISO/TR 21724-1:2020



COPYRIGHT PROTECTED DOCUMENT

© ISO 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

Contents

	Page
Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	2
5 Common Transport Services Account overview	3
5.1 General	3
5.2 Common Transport Services Account definition	3
5.3 Common Transport Service Account concept	3
5.4 CTSA requirements	5
5.5 Transport service requirements	5
6 CTSA system framework model	6
6.1 General	6
6.2 Description of actors/entities	7
6.3 Framework data flows	9
6.4 Comparison to EFC and IFMS	12
7 Processes and use cases	16
7.1 General	16
7.2 Use case process and methodology	16
7.3 Transport service user use case process descriptions	17
7.3.1 General	17
7.3.2 Transport service user registration	17
7.3.3 SecureID registration including sharing agreement	18
7.3.4 Multimodal journey services	19
7.3.5 Point of sale	20
7.3.6 Fee/fare calculation and service rights validation for service operator	21
7.3.7 Service rights validation for interagency acceptance	22
7.4 Authentication of secureIDs	22
7.5 Open payment use case process descriptions	23
7.5.1 General	23
7.5.2 Open payment transaction process	23
7.5.3 Valid and hot list upload process	24
7.6 Multimodal use case process descriptions	24
7.6.1 Transport service usage rule sharing processes	24
7.6.2 Transport service usage rule sharing processes	24
7.6.3 Pricing rule sharing process	25
7.6.4 Commercial rule sharing process	26
7.6.5 Transport service user account information sharing process	27
8 Next steps	27
Annex A Informative Payment categories	29
Bibliography	32

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*.

A list of all parts in the ISO 21724 series can be found on the ISO website.

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

Many transportation services (e.g. public transport, tolled roads, parking, city bike rental etc.) require payment for use. This has previously caused each service provider (e.g. public transport authorities, toll authorities, public and private parking providers, etc.) to develop independent, stand-alone payment systems to enable users to pay for access to their service. Consequently, a traveller who traverses multiple transport modes had to purchase services at more than one point of sales location. If the payment systems are integrated, then the transport service user may possess more than one payment/ticketing media, application, and/or account. However, in public transport there have for many years been products that enable a traveller to benefit from a seamless journey from A to B using several transport means, modes and operators. These products have been available through cooperation between operators and regional and national tariff schemes.

The transportation industry has seen an evolution in the collection of fares and fees throughout its history. The main drivers of that evolution have been the pursuit of increases in customer convenience and system efficiencies. Automated Fare Collection has progressed from use of magnetic technology to contactless smart cards, and recently to open financial payments and mobile payment applications.

Automated Toll Collection began with the use of simple read-only tags and is now looking to new approaches and technologies for future payment system advancements. Examples are open road tolling, vehicle miles travelled methods, and technologies such as Dedicated Short Range Communications (DSRC), Global Navigation Satellite System (GNSS), and Cellular Networks (e.g., GSM). Agencies have used these high-technology systems not only to enable automated payment and speed throughput, but to capture data, improve system reliability, and perhaps most important, to improve customer service.

Historically, transportation payment systems have covered only one service provider. Therefore, public transport ticketing/payment systems have not typically been technically integrated with charging/payment systems for tolls or parking and vice-versa. The reasons for this isolated nature are twofold. The first is that the individual service providers had little interest, from a business case standpoint, in integrating their purpose-built ticketing-, charging- and payment systems. The second is that technically this is a difficult and costly exercise, owing to the fact that the systems are typically proprietary and were designed to enable payment for one transportation service. However, in public transport, more and more electronic ticketing systems are supporting communication in conformance with ISO/IEC 14443 or ISO/IEC 18092. This implies physical and technical interoperability, but also that the ticketing applications have to be interoperable as well, as there has to be a contractual interoperability.

Some integration has occurred, for example between commuter or urban rail and parking. A traveller can often pay for both parking and their train ride with a common medium. But these examples usually occur only when there is one transport service provider for both the parking and public transport.

Other examples exist for purpose-built integrations of payment systems across two or more transportation modes. In some Asian countries like Japan and Korea there are several implementations of integrated payment systems for public transport and tolling. Examples include the use of a toll transponder that allows the insertion of a public transport card. The integrated payment systems are mostly based on a common payment media, i.e., smartcard with stored electronic value on the card.

In the past 5 to 10 years, the public transport industry in particular has embraced the development of Common Transport Service Account systems. In this approach, transportation products are stored in a central account rather than on the payment media. This architecture allows the system front end to be very flexible to enable customers to use contactless credit and debit cards and contactless mobile payment and ticketing applications alongside transport smart cards.

The subject of this document is to study the convergence of toll fee collection and payment and public transport fare collection and payment through the integration of the systems' accounts rather than their fee/fare payment media. This concept is flexible and can also include payment systems for other transport services, such as parking, electric charging stations, rideshare, bikeshare, and other disruptive transportation modes. Using an account-based backoffice architecture (prevalent in the toll

industry), is becoming increasingly common in public transport and other transport service payment systems in the United States and Europe.

The technical approach is to link accounts used in multiple transportation modes to create a common transport service user account. For customers, this creates a seamless, end-to-end experience where they can easily access and pay for all transport modes for which they opt-in: public transport fares, toll fees, rideshare, etc. For operators, this common or linked account allows for additional customer benefits such as incentives, discounts or loyalty points strategies, and can add valuable customer usage data to inform their planning and operations, enhance mobility and reduce congestion in regions.

This document examines the concept, functional requirements, and benefits of converging payment systems for tolling, public transport and other transport services through a central account linkage. Readers interested in how this can be achieved by use of a common media are advised to access ISO/TR 19639.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 21724-1:2020

Intelligent transport systems — Common Transport Service Account Systems —

Part 1: Framework and use cases

1 Scope

This document describes the characteristics of a Common Transport Service Account System (CTSA). It presents the common transport service account framework and associated use cases. The objective of the CTSA role model is to cover relevant transport services, the payment methods, the account types where the user of the service is charged for the service and that requires a more overall role and responsibilities model. The model also defines external stakeholders that impact and border the model, that is, the general financial (banking) system. The framework assumes an account-based system where charges for services are calculated and charged in the account system. The main idea behind the CTSA framework is to provide a transport service user with the benefit of seamless acquisition of access rights to multiple transport services by multiple service / operator managers through a common transport account. This framework assumes a technology-agnostic front end with respect to the payment media and reading equipment. The focus of this framework is the back-office / account management system as a vehicle to integrate multiple transport services and managers.

A new set of terms are introduced in this document to distinguish the convergence of a common approach for payment for transportation services from more traditional models using “smart cards” or electronic tickets. The model describes a move towards common or linked mobility accounts for all traveller payment needs, whether for parking, tolls, public transport and other disruptive mode options (e.g., bikeshare, carshare, microtransit, micromobility), inclusive of commercial payment and benefit models.

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:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

3.1 actor

user playing a coherent set of roles when interacting with the system within a particular *use case* (3.6)

Note 1 to entry: A user can, for instance, be a human, an Organisation or another (sub)system.

3.2

secureID

evidence that a transport service user (customer) is entitled, at the Point of Entry (POE) to the transport service, to benefit from a transport service provided by a transport service manager

Note 1 to entry: A secureID may consist of a set of data elements defined in a standardized format stored on an electronic media, e.g. a smartphone, used for a secure storage of the information and a secure communication of the information to the media accepting devices installed either at the POE or at the Point of Sales (POS). The set of data elements and their content (values) can vary depending on the type of payment method, type of media and electronic identification application stored on the media and the type of transport service provided.

Note 2 to entry: A secureID may consist of a simple vehicle ID as given by the vehicle number plate and read by the roadside equipment (RSE) by means of Automatic Number Plate Recognition (ANPR).

Note 3 to entry: A secureID may also consist of a biometric identification, e.g. finger-print or facial recognition of the transport service user.

3.3

open interface

public standard (or generally accepted specification) for connecting hardware to hardware and software to software

[SOURCE: <https://encyclopedia2.thefreedictionary.com/open+interface>, 22 March 2016]

3.4

open payment

use of open industry interface standards and specifications for the electronic remuneration and provision of transport services

Note 1 to entry: See Reference [7] for more information on open payment architecture.

3.5

payment method

timing and location of remuneration for services including whether the payment is required prior to, at the time of, or post access to transport or related services

3.6

use case

description of typical interactions between the *actors* (3.1) and the (sub)system itself, capturing the functional requirements of the (sub)system by defining a sequence of actions performed by one or more actors and the system

4 Abbreviated terms

ANPR	automatic number plate recognition
EFC	electronic fee collection
IFMS	integrated fare management system
IFMSA	integrated fare management system architecture
PAYG	pay as you go
POE	point of entry

POS	point of sale
RSE	roadside equipment
TCRP	Transit Cooperative Research Program (a program sponsored by the United States National Academy of Sciences)

5 Common Transport Services Account overview

5.1 General

This clause presents the Common Transport Services Account System framework and architecture. This clause includes the definition, requirements, role model and role descriptions, modes, and flows of the system. These components are described in more detail in the following subclauses. The objective of the CTSA role model is to cover any transport service where the user of the service is charged for the service and that requires a more overall role and responsibilities model.

5.2 Common Transport Services Account definition

A CTSA system is characterized by the use of open interfaces for validating payment and a transport account management system ('back-office') for processing and managing secureIDs, transport service user products and value stores for multiple transport service and operator managers. The back-office processes ensure privacy, security and portability of secureIDs to support current and expanded integrated services offered by multiple transport service managers.

In general, a Common Transport Service Account system conducts the majority of the validation and authentication of user payment and access rights to service in the back-office; the secureIDs and media used by a traveller is typically used for identification purposes only. The value is not typically contained on the media, and under normal circumstances (when communications is available), the fee or fare calculations are not calculated in the media reader.

5.3 Common Transport Service Account concept

The concept of a CTSA is for a traveller to seamlessly travel from origin to destination while using the most convenient means of gaining service access rights. As depicted in [Figure 1](#), a traveller may join one or more transport service or operation managers and also link the most appropriate secureIDs to gain access to transport services via their account.

Service access rights processing is performed in the account back-office, which enables systems to be loosely integrated where they do not need to share the same equipment types, technologies, applications, or customer media form factors. The flexibility provides customers with choosing their preferred service modes, payment and secure identification methods, as well as the ability to migrate to new technologies as they are deployed. They are able to use the most convenient means to access services, provided their secureID is based on an open interface, and the operations manager is able to process the link that their secureID provides to the back-office customer account.

EXAMPLE 1 A toll operator can require that a traveller register a licence plate and establish a stored value purse to pay for travel on toll lanes; a bikeshare service can require a monthly fee and bank card of record for a guarantee; a parking vendor can provide discounts for rail travellers, and a commuter rail service can require tickets or passes for travel. With the CTSA, the traveller has a one-stop location to register all the appropriate secureIDs, create a single travel purse, store a single card for all transactions, and register for benefits or discounts that are available for using public or active transport alternatives. The customer can better manage their travel history. Meanwhile, service managers can better manage transportation alternatives for customers, offer discounts for changing travel choices, and coordinate network management scenarios to more effectively meet demand.

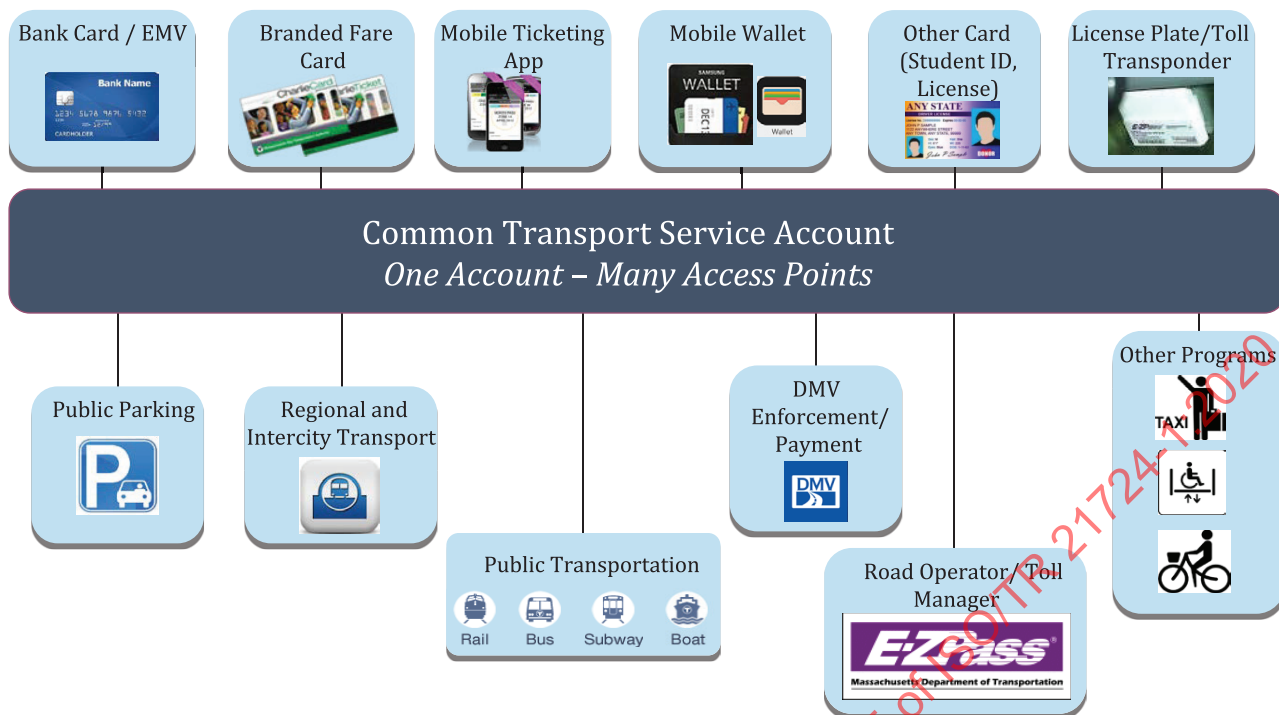


Figure 1 — Common Transport Service Account concept

Specifically, the idea behind the CTSA is to provide the transport service user with a framework where the transport service user benefits from many types of transport services without having several interfaces with different financial service providers, e.g., banks and credit card companies supporting the different transport service providers. The transport service user is able to receive one invoice with all the charging transactions for all the transport services used. Every time the transport service user benefits from a transport service, the validation of his travel service rights (secureIDs) is collected and transferred to the manager of the Common Transport Service Account. The CTSA manager settles the transport service user account based on the transport services consumed and the commercial rules relevant for the services or combination of services consumed. Hence, the whole concept is based on a transport related central account and an identification of the transport service user and his/her secureID. The following more complex example may describe the concept of CTSA:

A transport service user benefits every day from three types of transport services. The first one relates to the use of a tolled highway to a city. The second transport service is the use of parking services at a Park&Ride terminal and the third service is the use of a bus line from the Park&Ride terminal to the city centre. The transport service user uses an on-board equipment (electronic tag) with a post-paid central account for the electronic fee collection (EFC) on the tolled road, a smartcard with a pre-paid central account for access to the parking lot and a fare medium with a pre-paid period pass for riding with the bus. Every month, the transport service user receives an invoice from each of the three different transport service providers. There are no links or relationships between the three transport service providers enabling the user to benefit from the combination of transport services or to have one invoice covering all transport services.

The three transport service providers then agree to join forces, making the usage of transport services more user-friendly concerning charging and invoicing. They establish a joint venture association and enable the user to have a CTSA managed by the joint venture association. The CTSA manager (the joint venture association) receives the proof of usage (validation of secureIDs) from each of the three transport service providers and settles the user's CTSA once a month, enabling the user to have specific rates for his/her combined usage of transport services. The user then receives one invoice each month with the documentation of his/her transport service usage and one amount to be paid.

It should be noted that the CTSA manager does not act as a financial service provider, e.g., a bank or credit card company. The CTSA manager is primarily a clearing and forwarding entity that belongs to the transport domain and that clears and settles the CTSA linked to each of the transport service users that have a CTSA contract enabling them to have one common account for all their usage of transport services. The CTSA manager also settles financial accounts between different stakeholders in the transport domain involved in the CTSA concept. There are only a few disparate systems in place today that can support a CTSA. This framework will provide a blueprint for others to migrate to an account-based system that support multiple service and operations managers.

5.4 CTSA requirements

The CTSA system is characterized by the following requirements:

- 1) A CTSA system enables a transport service user to hold one account from which to pay for service rights to a variety of linked or unlinked transport services from one or more transport operators including vehicle, public transport, rail, taxi, electric charging, parking, shared use transport and other mobility providers.
- 2) A CTSA system enables a registered transport service user to use their most convenient secureID to pay on entry/exit or to acquire transport service rights from a variety of transport operators. Examples of a secureID may include licence plate, government identification cards, private label media that conform to open interface standard formats, bank cards or virtual bank cards stored in mobile phones, or payment services such as Apple Pay and PayPal, and emerging technologies.
- 3) A transport service user's registered secureID may be used on a transport service when a payment method or transport product is associated with the secureID.
- 4) A multimodal journey that may include travel across toll roads, public transport, parking, shared use mobility aids and systems may be linked across different service and operation managers to provide travel or other benefits or discounts to the transport service user.
- 5) A CTSA system enables a transport operator to act as a typical payment merchant with respect to a transport service user, wherein pay as you go (PAYG) for services model is used.
- 6) In a CTSA system, a payment is made using open interface standards.
- 7) A CTSA system allows point of entry and point of sales locations to co-exist at the same location.
- 8) A CTSA system allows information about transport service user accounts to be shared among other service providers based on a transport service user agreement (opt-in/opt-out) at any time during membership/registration to the service.
- 9) A CTSA system allows an entity/actor to extract data appropriate to revenue sharing and statistical requirements of transport service user usage, transactions and access to services.
- 10) The CTSA model should be capable of extending the use to different POE and POS technologies, including passive and active reader methods.
- 11) The CTSA model should be structured to accommodate current best practices to prevent internal and external fraud and to safeguard the revenue collection by the appropriate service providers.
- 12) The CTSA model should protect transport service user privacy.

NOTE Passive and active reader methods are based on whether a customer actively presents a secureID to a reader (active method) or a "reader" senses its presence (passive method).

5.5 Transport service requirements

This subclause describes the modes and services for which payment is charged for usage. Within the four basic transport modes, road, rail, sea, and air, we focus on the road, rail or sea. Due to their structure, these modes have different requirements that drive the secureID technology, media, transaction type,

and transmission performance. In this model, the traveller service discovery, reservations, sales and provisioning of secureIDs for access is also included in transport service requirements due to the choices available to travellers. For that reason, transport service requirements also includes a service called: Information and Reservation Service Provider. The transport modes and their requirements are listed in [Table 1](#).

Table 1 — Transport mode requirements

Mode/Service	Requirements
Road/Tolled infrastructure	Need for display/transmission of secureIDs at a distance from POE while vehicle is moving. Need to enforce vehicle secureIDs passively from vehicle or transmitted from vehicle (e.g., licence plate cameras or via transmission to RSE)
Road/Public transport services	Need for fast transaction times. Need to transact micropayments. Need to operate in a barrier or barrier-free mode.
Rail/Subway and metro services	Need for fast transaction times. Need to transact micropayments. Need to operate in a barrier or barrier-free mode.
Road/Parking, Shared-use mobile services (bicycle and car-sharing services)	Need for intermodal transfers and sharing secureID/access/benefit information (e.g., car park, bike sharing, bike storage, car share). Need to operate using different enforcement provisions such as lock, gate, or inspection.
Road/Long distance bus Road/Car sharing Road/Charging station electric vehicles Rail/Train services Sea/Ferry	Although limited real time need, Need for fast transaction times. Need for estimate of number of travellers/users per “trip”. (Optional) Need for payment inspection and enforcement.
Information and Reservation Service Provider	Although limited real time need, need for fast transaction times. Need for interfaces to product, service fee, fare, and service transfer rules. Need for reciprocity and discount/benefit rules.

6 CTSA system framework model

6.1 General

The CTSA system framework model overlaps with the IFMS framework (ISO 24014-1) and EFC models (ISO 17573 series), although the secureID Registrar role is replaced with a financial service provider. Details of the relationship between the CTSA and IFMS and CTSA and EFC are described in [6.3](#).

The framework model is shown in Figure 2. The framework is composed of six main actors or entities, as described in [Table 2](#). The enumerated data flows (e.g., 1. Display/Actuate), show the major data exchanges between actors. These flows are described in [6.2](#).

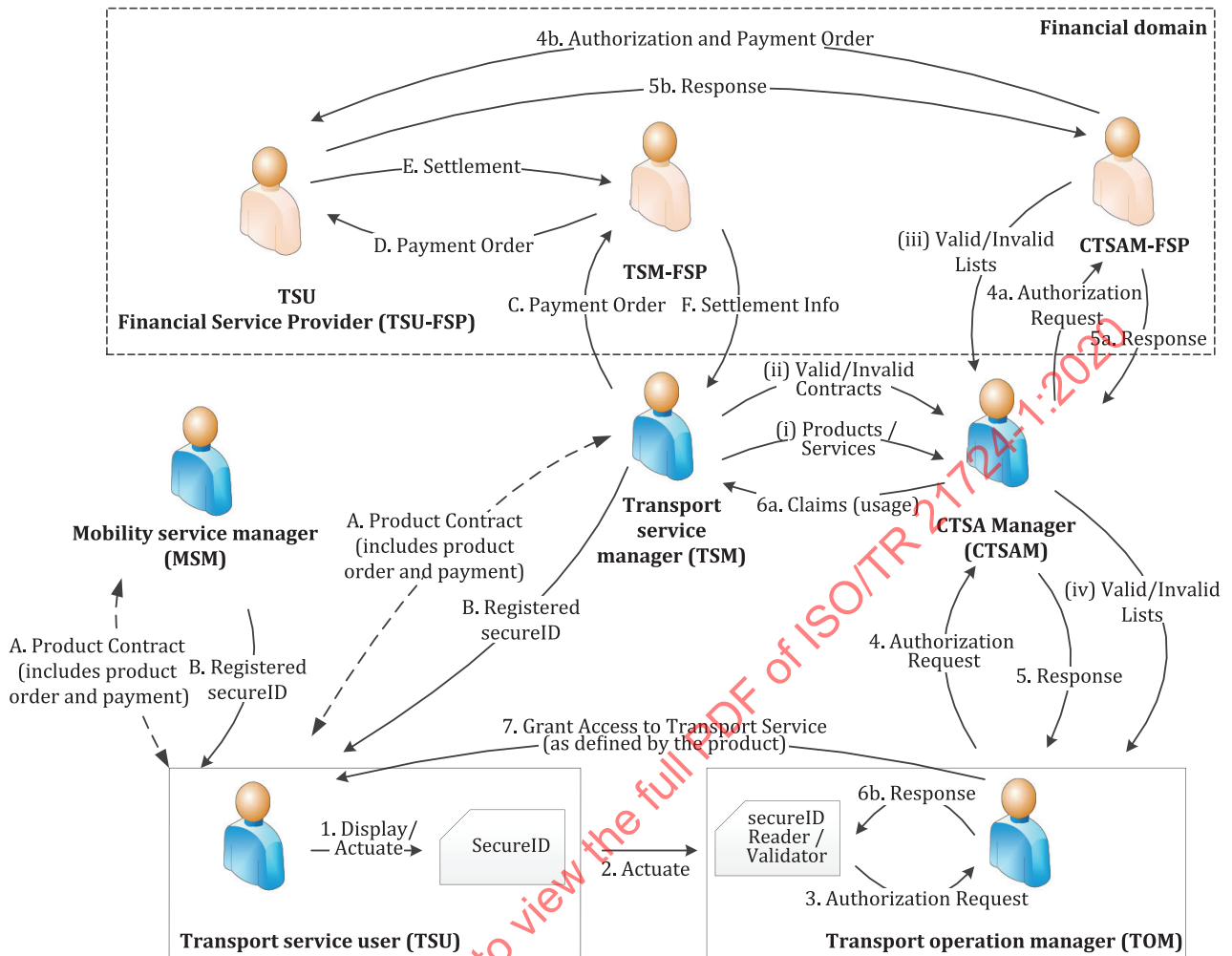


Figure 2 — Common Transport Services Account framework model

6.2 Description of actors/entities

The critical roles in a CTSA system are listed in Table 2. The model is compatible with the IFMS and EFC to ensure a seamless integration with legacy tolling and fare collection systems.

Table 2 — Common Transport Services Account framework role descriptions

Actors	Description
Transport service user (TSU)	The TSU (user) benefits from a transport service and pays for the service either before, during or after the transport service has been used. A transport service could for instance be the use of a tolled road, a bus or metro ride or a parking service. The TSU uses different types of transport services and for some of the services he/she is charged a fee or fare that covers parts of or the whole cost of the transport service provided. The TSU is denoted differently when consuming different transport services. In tolling and parking he/she may be called a Vehicle owner or Driver and in public transport he/she may be called a Customer. For shared bike services he/she may be called a Cyclist or Bike user and for Transport information services he/she may be called a Driver, Customer or Traveller. Any transport service where the user of the service has to pay for the service can be part of the CTSA concept and any transport service would very often have their own service specific names for the user of the transport service. The overall name in the CTSA concept is just TSU.

Table 2 (continued)

Actors	Description
Transport Operations Manager (TOM)	The transport service itself is provided to the TSU by the TOM. This means either transporting the user by the transport means operated by the TOM (e.g. bus, metro, ferry or train) or giving the TSU service rights (access) to the transport infrastructure operated by the TOM, e.g., a tolled bridge owner and operator. The transport services provided can include many different types of transport service, e.g., the use of road infrastructure, the use of a parking lot, the use of public transport means (e.g. buses, trams, metros and trains), the use of commercial vehicles for transporting goods and the use of transport information and individual route guidance. In these cases, the TOM is the road owner/operator, the parking lot owner/operator, the public transport means owner/operator (Service operator in the IFMSA role model), the commercial vehicle owner/operator, the transport information provider and the individual route guidance provider. The TOM requires that the TSU pays for the transport service that is provided. In the CTSA concept, the TSU will not pay at the time and place the transport service is used. The TOM accepts that the TSU has the right to the transport service based on the secureIDs the TSU is carrying with him/her and that are presented to the TOM whenever the TSU benefits from the service, e.g. when the customer enters the bus or when the driver enters the tolled road. The TOM requires some infrastructure for reading and validating the secureIDs carried by the user. In a tolling environment, this includes the required EFC physical architecture with OBES, Roadside and Central Equipment. Hence, the TOM will also be what is called the Toll Charger in the EFC role model. In the public transport domain, the infrastructure for reading and validating the secureIDs will include different types of media readers and validators and back-office systems usually operated by the IFMSA role model Service provider.
Transport Service Manager (TSM)	The TSM is the role that acts as the interface to the TSU including amongst others an explicit or implicit contract with the user, charging of the user for the transport services provided/to be provided and user support. The TSM is also responsible for paying the TOM for the transport services provided to the user. This is typically a public entity. The service rights (the secureIDs) are issued by the TSM. There is an explicit or implicit contract between the TSU and the TSM depending on the type of transport service. The contract describes the product (the transport service) and how and how much the TSU should pay for the product that the contract covers. In public transport the contract will typically include the Usage and Pricing rules as defined in the IFMSA standards. In a tolling environment, the product description will describe the road infrastructure the TSU will have access to, how he/she should identify himself when using the road infrastructure, e.g. by the use of On-Board Equipment (OBE), and how much the user have to pay for the use of the road infrastructure. The TSM will be the Toll Service Provider in a tolling environment. In the IFMSA role model the TSM will be the product retailer on behalf of the product owner.
Mobility Service Manager (MSM)	The MSM role provides bundled or unbundled transport information and reservation services, as well as registration of payment secureIDs to acquire the benefits of the available transport services.
Common Transport Service Account Manager (CTSAM)	The CTSAM is divided into two major roles: the manager that interacts with the TOM or TSM, and the settlement account manager that interacts with the banking sector (FSP). The CTSAM is responsible for the management of the registered CTSA.
Financial Service Provider (FSP)	The role that issues and validates electronic payment media, and authenticates and settles payment transactions. Each party involved in payment for public transport service may include their FSP in the process. For example, when a credit card is used for payment, the card may be issued by one brand, the payment may be authenticated through another merchant acquirer, and the settlement may be executed through a third provider.

6.3 Framework data flows

There are several data flows that are described by the CTSA Framework. They include:

- Validation/Authentication secureIDs flow
- Account and secureID registration and settlement: for TU flow
- Account to account exchanges

Descriptions of the collaboration flows are provided in [Table 3](#), [Table 4](#), and [Table 5](#) below.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 21724-1:2020

Table 3 — Validation / authentication secureIDs flow

Validation and authentication of secureID flow	Origin	Target	Description
1. Display/Actuate	TSU	TOM	TSU displays or activates secureID to TOM's reader or sensor.
2. Actuate	SecureID	Reader	The reader processes the secureID including validating it and generating a request to the CTSAM to authorize the secureID holder's right to access the transport service.
3. Authorization request	Reader	TOM	The TOM transmits the request to the CTSAM.
4. Authorization request	TOM	CTSAM	The CTSAM determines access value for use of service and processes the secureID to determine priority product to use to gain access to service. See 7.3.6 for use case.
4a. Authorization request	CTSAM	CTSA FSP	For open payment (see 7.4, specifically bullet point 1 for use case), the CTSAM sends an additional request to its merchant to authorize the payment.
4b. Authorization and payment order	CTSAM FSP	TSU FSP	The merchant may send a request to the TSU's bank for authorization.
5. Response	TOM	Reader	When the reader receives the authorization message, it provides or denies access to the secureID holder.
5a. Response	CTSAM	TOM	CTSAM generates a message to the TOM that authorizes or denies access to the secureID holder after it enters the transaction.
5b. Response	TSU FSP	CTSAM FSP	TSU FSP responds to the CTSA FSP request with an approval or denial of authorization request.
6a. Claims (usage)	CTSAM	TSM	The CTSAM reports to the TSM on the transaction, including status (approval/denial), value/ product use, and appropriate TSU information
6b. Response	TOM	Reader	TOM directs reader to provide or deny access to secureID holder.
7. Grant access to transport service	TOM	TSU	TOM grants or denies access to TSU.

Table 4 — Account and secureID registration and settlement: for TU

Account and secureID flow	Origin	Target	Description
A. Product contract	TSU	CTSAM	For a CTSAM centric account management. The CTSAM provides a customer registration and point of sales process. See 7.3.2, 7.3.4 and 7.3.5 for use cases. (Separate flows are identified between the CTSAM and TOM/TSM for acquisition of access rights.).
B. Registered secureIDs	CTSAM	TSU	For a CTSAM centric account management. The CTSAM may allow registration secureIDs for a TOM or TSM. See 7.3.3 for detailed use case. NOTE The CTSAM requires validation by the owner of the secureIDs; for a bank card, it is the bank merchant and for transport service or operator manager, by their registrar.
A. Product contract	TSU	TSM	For a TSM centric account management, the TSM provides a customer registration and point of sales process. See 7.3.2 and 7.3.5 use cases. (Separate flows are identified between the TSM and TOM/a different TSM for acquisition of access rights.)
B. Registered secureIDs	TSM	TSU	For a TSM centric account management. The TSM may allow registration secureIDs for a TOM or other TSM. See 7.3.3 for detailed use cases. NOTE The CSM requires validation by the owner of the secureIDs; for a bank card, it is the bank merchant and for transport service or operator manager, by their registrar.
C. Payment order	TSM (MSM)	TSM FSP (MSM FSP)	A payment order entails validating a bank card on record or authorization request/response to the organization's FSP. The flow travels from the point of sale (TSM or MSM) to the manager's FSP.
D. Payment order	TSM FSP	TSU FSP	The merchant's (TSM or MSM) FSP forwards the authorization request to the TU's FSP for authorization (or validation) who then responds.
E. Settlement	TSU FSP	TSM FSP	Once authorized, a settlement sent from the TU's FSB to the merchant's (TSM or MSM) FSP.
F. Settlement information	TSM FSP	TSM	Information on the settlement is sent to the merchant.

These flows will support reload, autoload and other payment services.

Table 5 — Account to account exchanges

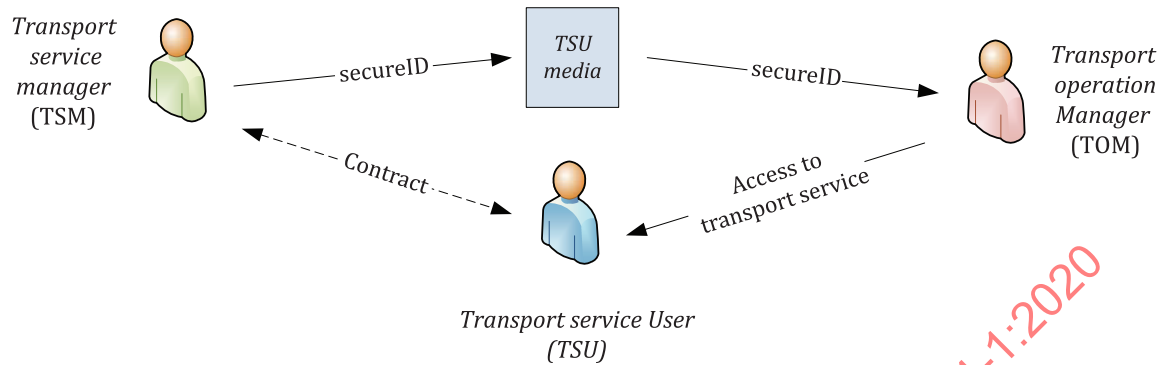
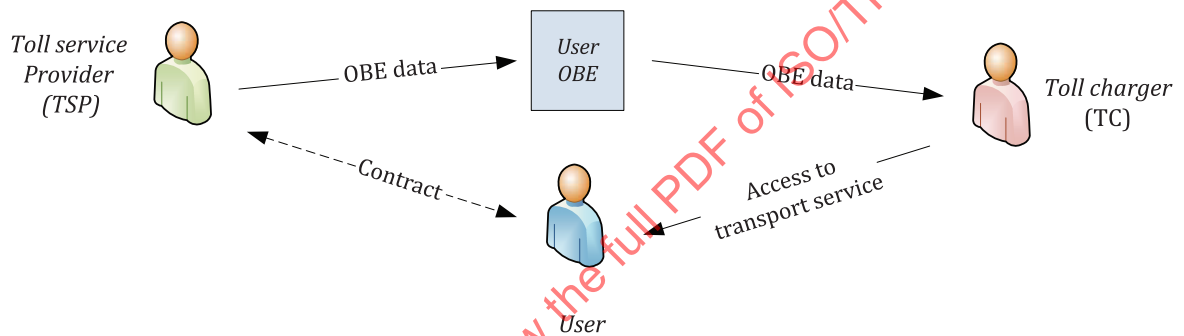
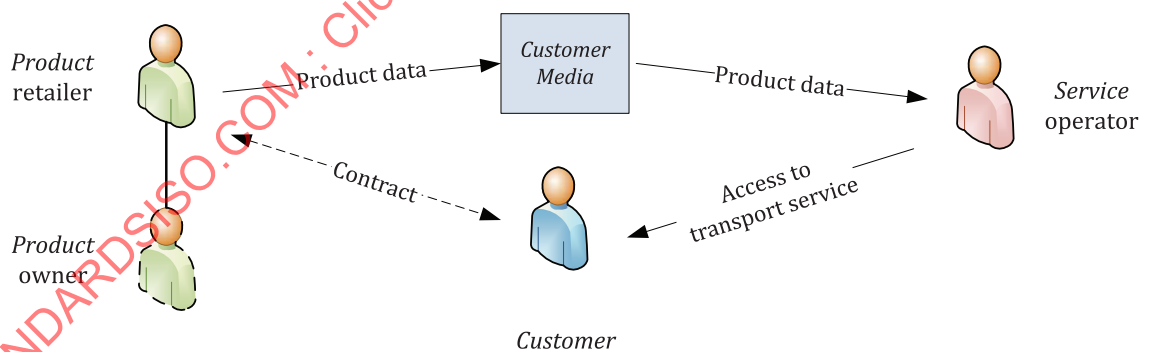
Account to account exchanges	Origin	Target	Description
i. Product Services	TSM	CTSAM	Product owner shares a catalogue of products and values, access rights and related information. Details may be found in use cases found in 7.5.2 through 7.5.3 . Additionally, an additional use case in 7.4.4 describes the exchange between a TSM/CTSAM and CTSAM when a customer agrees to allow a customer account owner to share information with a selected TOM.
ii. Valid / invalid contracts (secureIDs, tickets, access rights)	TSM	CTSAM	Product owner shares list of valid / invalid products and rules (contracts) with CTSAM. The exchange of customer account status and purchases occurs when a customer agrees (“opts-in”) to share personal and account information between the TSM/CTSAM and CTSAM. The TSM informs the CTSAM about updates to an account for example product purchases, uses, cancellation, secureID changes, and other material changes to the account information. These details are discussed in the 7.5 use cases.
iii. Valid / invalid lists (a and b)	FSP (CTSAM)	CTSAM (TOM)	Payment method owners share list of valid / invalid payment methods (i.e., bank card numbers) with point of sale actors (TOM, TSM, MSM, CTSAM, for open payment systems, the POS is at the reader and it requires provisioning of an invalid card list). See 7.4 for detailed use case.

6.4 Comparison to EFC and IFMS

This section maps the CTSA role model to the role models used in Electronic Fee Collection (EFC) and Interoperable Fare Management (IFM) systems showing how the CTSA role model covers the essential roles in EFC and IFM. The reader should have in mind that EFC and IFM are charging systems for just two transport services. As mentioned earlier, the objective of the CTSA role model is to cover any transport service where the user of the service is charged for the service and that requires a more overall role and responsibilities model.

The TSM, TSU and TOM, and the TSU media (or secureIDs) as described in [Table 2](#), share the equivalent roles in the EFC and IFMSA role models.

[Figure 3](#) shows three of the five basic roles in the CTSA concept and their most important relationships. The figure also shows the equivalent roles in the EFC and IFMSA domains.

Common Transport Service Account (CTSA) concept**Electronic Fee Collection concept****Interoperable Fare Management Concept****Figure 3 — The CTSA basic roles compared to EFC and IFM basic roles**

The mobility service manager (MSM) provides the TSUs with products that include two or more transport services bundled together, e.g., Park&Ride products. Another example could be multimodal products like the combination of road infrastructure usage — parking — public transport — bike sharing where the secureIDs could be carried in an OBE for road usage (and parking) and for the other services the secureIDs could be carried by a smartcard or a smartphone. [Figure 4](#) shows the last example.

The mobility service manager is not a role in the EFC or IFM role models as none of the role models covers combined services with different transport modes.

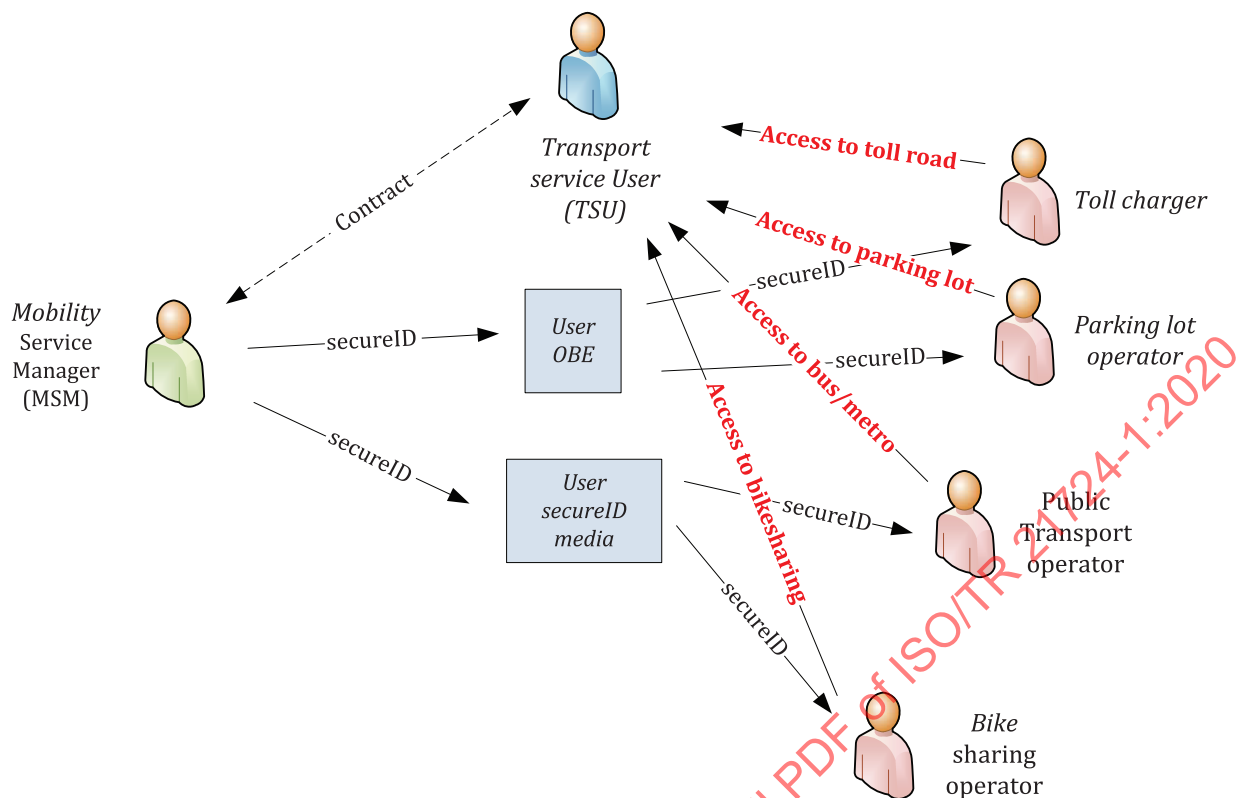


Figure 4 — The mobility service manager

The common transport service account manager (CTSAM) is a crucial element in the CTSA concept. The CTSAM has interfaces to the TOMs, the TSMs and the MSMs. The TSM and MSM send information on valid/invalid contracts and/or secureIDs to the CTSAM. The TOM sends information on the services provided to the CTSAM (see Figure 5). In those cases where the TOM does not authenticate the secureIDs he may send an authentication request to the CTSAM who does the authentication or forwards the authentication request to the FSP that issued the secureIDs. The authentication is described in a later clause. The CTSAM also sends white lists to the TOMs enabling the TOMs to have a simple and off-line local authentication. In some cases, this will be acceptable, at least for transport services where the fee or fare is so low that the TOMs can accept the loss due to a manageable amount of fraud.

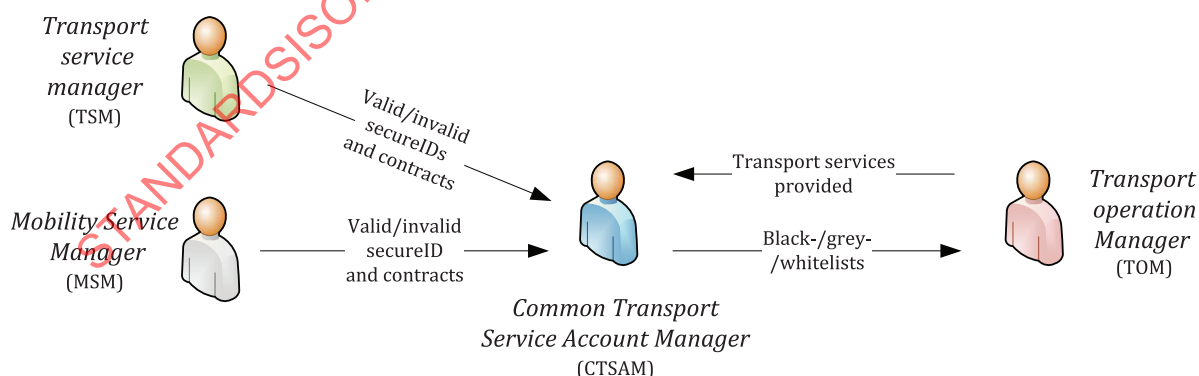


Figure 5 — The Common Transport Service Account manager

The CTSAM is responsible for the management of the registered CTSA. This includes the management and maintenance of the CTSA but also the settlements of the accounts and the clearing between the TSMs and TOMs concerning the products and services purchased and the products and services provided. The CTSAM is comparable to the Collection and Forwarding role in IFM systems.

The TSU wishing to benefit from the CTSA concept has to register a CTSA. This can be done at a TSM or a MSM. The CTSA includes a user profile, his/her transport service preferences, his/her preferred/agreed payment method and the secureIDs to be used for getting access to the transport services. The secureIDs are stored on the TSU secureID medium, e.g. an electronic tag or on different media, e.g. an electronic tag and a wireless communication smartcard. The TSU then presents his/her secureIDs at the access to the transport service provided by the Transport operation manager. The secureIDs are checked/authenticated in the validation process and the TSU is granted access to the transport service by the TOM. The data collected by the TOM at the use of the transport service is forwarded to the CTSA manager (CTSAM) who settles the user CTSA.

The CTSA concept is an add-on service to TSUs requesting a simplified and user-friendly way of paying for transport services. The concept does not block or prevent users without a CTSA from using the same transport services, but the user with multiple accounts does not benefit from the seamless synergy.

The TSU, the TOM, the TSM, the MSM and the Common Transport Service manager belong to the transport domain and form together the kernel roles in the CTSA concept. The EFC role model includes an Interoperability manager that is not included in the kernel roles of the CTSA concept. The responsibilities of the Interoperability manager are also needed in the CTSA concept and the responsibilities could either be allocated to the CTSA Manager or an external body outside the kernel roles or even split between the CTSA Manager and an external body. The IFM role model includes the Registrar and the Security manager and their responsibilities are also required in the CTSA concept. The responsibilities could either be allocated to the CTSA Manager or there could be external bodies like in the IFM model dealing with the registration of the different roles, products, secureIDs etc. and the information security and privacy in the CTSA concept. [Figure 6](#) shows the three domains and their roles.

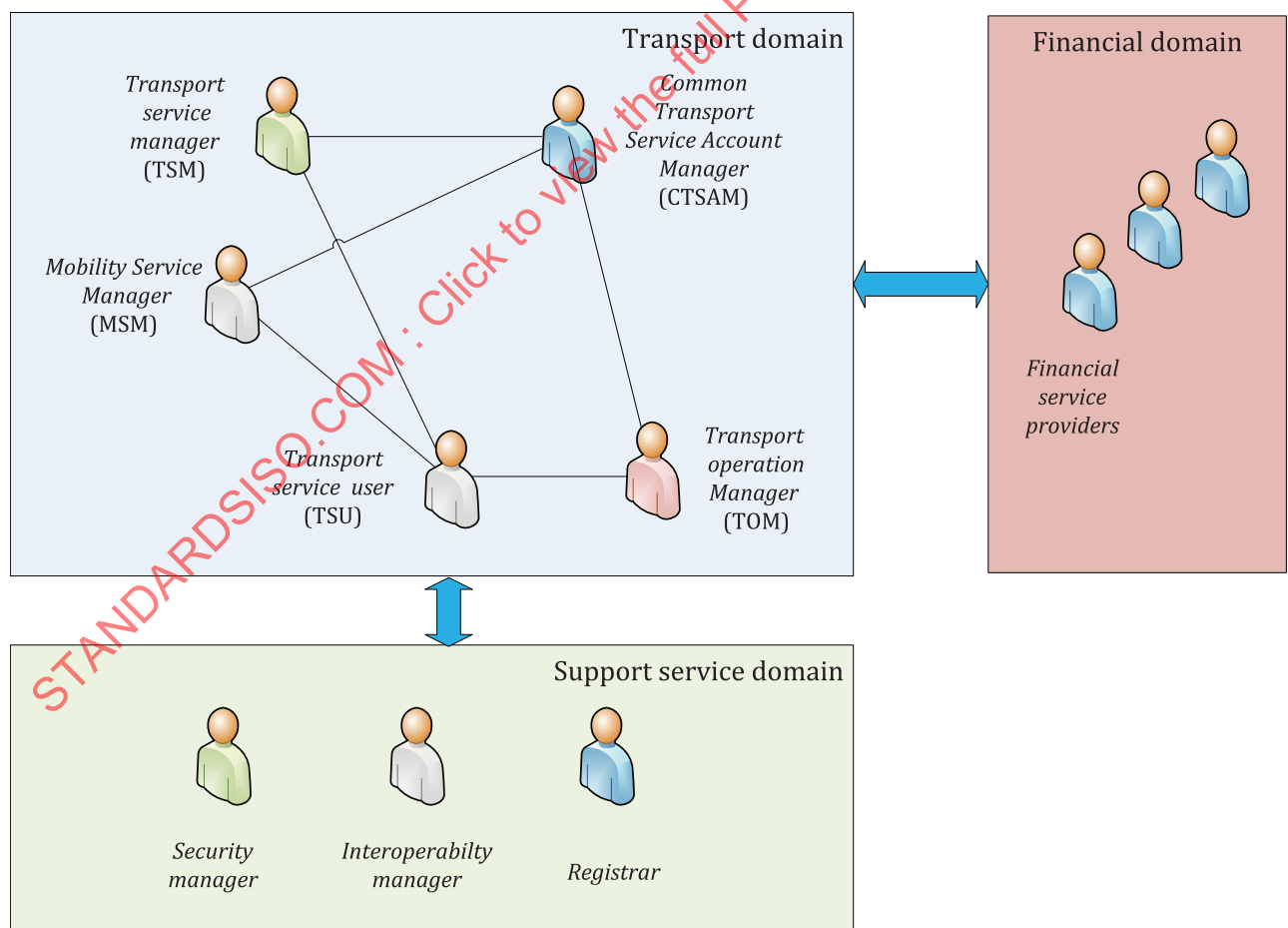


Figure 6 — The three involved domains and roles

7 Processes and use cases

7.1 General

The processes associated with each actor differ slightly depending on the mode and method used to pay for a service. In [Annex A](#), eight types of payment methods were identified as feasible for CTSA systems. The methods may be defined by four payment scenario categories:

- Prepaid Electronic Value
- Prepaid Tokens (e.g., tickets, passes)
- Postpaid Electronic Value
- Pay As You Go

These scenarios are described in [7.2](#) and [7.4](#) (as identified in [Table 6](#)).

Another set of scenarios deal with “centre to centre” or back-office exchanges of customer account and usage information and product / commercial and payment rules, transactions and settlement exchange. These use cases address the use of a common account among multiple organizations, such as the provision of transport services operated, managed or merchandized by different TOM, TSM and CTSAM. This set of use cases are described in [7.6](#) Multimodal Use Case Process Descriptions.

Table 6 — Use case process by secureID (TSU Perspective)

#	Use case process \ Payment method-product types	Section
1	Transport service user registration	7.3.2
2	SecureID registration including sharing agreement	7.3.3
3	Point of Sales	7.3.5
4	Service Rights validation for service operator	7.3.6
5	Service Rights validation for interagency acceptance	7.2.7
6	Multimodal journey services	7.3.4

7.2 Use case process and methodology

The method used to document the use case process is summarized in a table as shown in [Table 7](#). The table introduces the name, short summary, actors who instigate or trigger the use case process, actors who participate in the process and the basic description and list of actions and flows that occur in the use case. A more detailed discussion is described following the table along with a collaboration diagram to show the information and control flow.

Table 7 — Use case description table

Use case name	Use case process name
Description	A short description of the use case
Actor(s)	The actors who are involved in the use case
Assumptions	Any pre-requisites or issues related to this use case
Triggers	The user (actors or systems) interactions that trigger the use case
Interactions	A list of system actions and flows that occur in the use case.
Results	The outcome of the process

7.3 Transport service user use case process descriptions

7.3.1 General

The high-level TSU focussed use cases cover the actions of the customer from account registration, secureID (product and/or payment method) assignment, through reservations, fare/fee sales, and access to service including validation of payment secureIDs (see [Figure 7](#)). The processes are presented in this section.

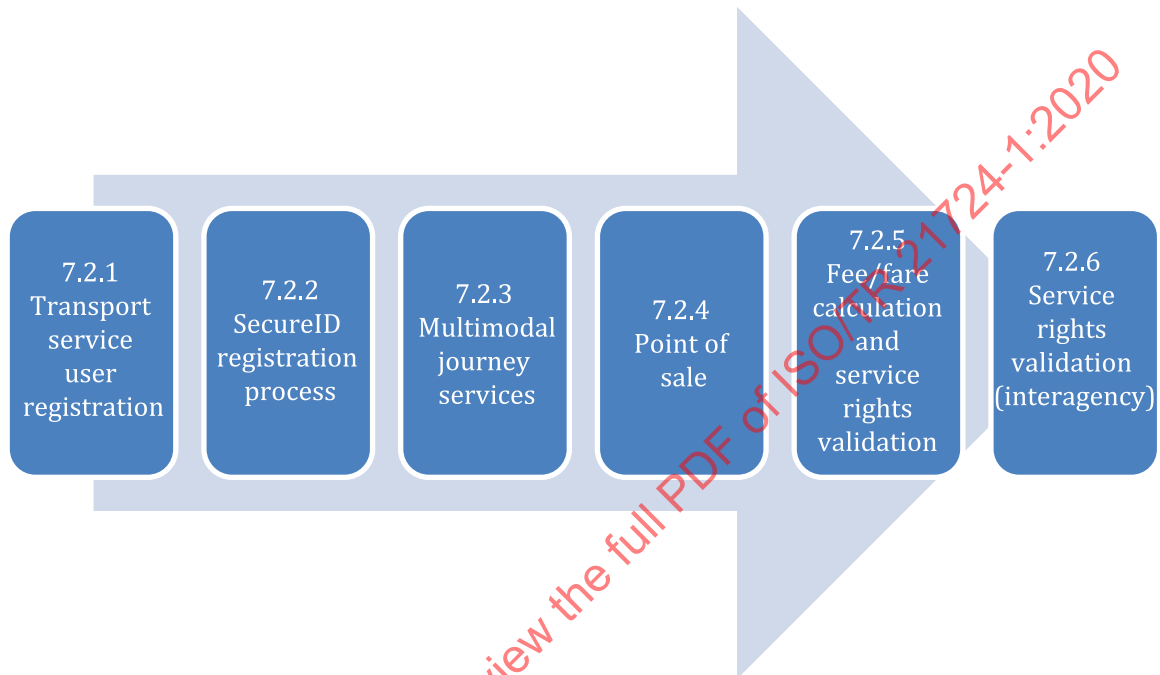


Figure 7 — High-level customer use cases

7.3.2 Transport service user registration

Use case name	Transport service user registration
Description	A transport service user sets up an account and registers payment methods and/or products.
Actor(s)	Transport service user, Common Transport Service Account Manager (or Mobility Service Manager), (optional Financial Service Provider).
Assumptions	Application has loaded without errors.
Triggers	Transport service user opens application to register for an account.
Interactions	— User opens an account. — User inserts contact information including email and related information. — User opts in/out of sharing contact information with other transport accounts (that have agreements with service provider, CTSAM or MSM).
Results	System verifies contact information and Transport service user successfully opens an account.

7.3.3 SecureID registration including sharing agreement

Use case name	SecureID registration including sharing agreement
Description	A transport service user uses his/her account to purchase and/or register secureID media and register payment types that may be used for validating access rights. This use case also includes registering or linking accounts from other service or operator managers where commercial rules are established between managers.
Actor(s)	Transport service user, CTSAM or MSM, (optional: Financial Service Manager).
Assumptions	Transport service user has a registered account in good standing. The transport service user has a payment method, product, or both.
Triggers	Transport service user logs in to account, and selects option to register payment type, secureID media.
Interactions	<i>Scenario 1: Request secureID media assignment</i> — Transport service user select media assignment function. — Transport service user submits <i>media identification</i> with which to associate his/her user account and purchased products or stored value. — System validates authenticity of media by user: — If managed by system, then through media inventory management system; check if associated with another account. — If managed by another system, then a request for validation is sent and received by external system (e.g., banking card to bank, external media to appropriate account). — System assigns media to transport service user's account. <i>Scenario 2: Request secureID media purchase and assignment</i> — Transport service user selects media purchase function. — Transport service user purchases media through "store". — System assigns media to transport service user's account. <i>Scenario 3: Request payment type registration (for autoloan, reload or quick product purchase options)</i> — Transport service user selects payment type registration. — User submits payment type including bank card (credit/debit/prepaid/electronic funds transfer). — System sends a request/response for validation to external system (e.g., banking card to bank, external media to appropriate account). — Stores information in a secure location (per security policy, may provide a token for use).
Results	SecureID is assigned to transport service user account. Payment type is assigned to transport service user account.

7.3.4 Multimodal journey services

Use case name	Multimodal journey services
Description	A transport service user selects an end-to-end trip plan, reserves and purchases product(s) that provide access rights to the transport and related services in the journey. The products are registered to his/her account, and assigned to the transport service user's secureID. The secureID may be a one-time or multiple use pass for services.
Actor(s)	Transport service user, CTSAM, MSM
Assumptions	The transport service user has opted in to share or use payment method for multiple CTSAMs.
Triggers	Transport service user uses MSM to plan trip
Interactions	— Transport service user selects origin/destination, travel mode choice(s) and other journey selection criteria. — System generates one or more legs using appropriate modes for user to review. — Transport service user selects journey and class of travel by leg/service provider. NOTE There are many different ways to implement these functions depending on the "owner" of the transport service account and the agreements among the key actors. The two most general approaches are described in the alternatives below. — <i>Alternative 1:</i> MSM sends transport service user to every service provider's account management system to purchase product to travel on operator; each CTSAM/Service manager implements a POS individually (see 7.3.5). — <i>Alternative 2:</i> MSM sends request/response for reservation or product from each CTSAM/Service Manager to purchase product to travel. — If Transport service user is account holder with registered secureIDs and products, then MSM issues journey plan using existing products and identifies additional payments and/or secureIDs needed. MSM requests/ responds on behalf of user to each CTSAM/service provider requesting additional products based on applicable transfer rules. — If Transport service user is not an account holder, MSM requests/ responds on behalf of user to each CTSAM/service provider requesting journey products based on applicable transfer rules. — MSM issues receipt and itinerary. Logs transactions.
Results	A transport service user through a MSM generates, (reserves), pays and associates travel products with their secureIDs for an end-to-end journey plan.

7.3.5 Point of sale

Use case name	Point of sale
Description	The method and mode associated with payment for a sale of a product. The payment mode will drive the type of product and the service rights allowed.
Actor(s)	Transport service user, CTSAM or MSM, Transport Operations Manager (for PAYG), Financial Service Provider.
Assumptions	Transport service user has a payment type to purchase product(s).
Triggers	Transport service user initiates purchase transaction function.
Interactions	<i>Scenario 1: Purchase product and assign to secureID (Transport service user with existing account and registered secureID)</i> — Transport service user signs in or identifies account and selects product and purchase function. — User reviews and selects one or more products to purchase. — User associates product with available list of secureIDs assigned to account (see Scenarios 1 and 2 above); Note: a pass may only be associated with one secureID while stored value/single use products may be associated with multiple secureIDs. — User selects one or more payment types or available stored value associated with his/her account to pay for product(s). (Or, user can input information for a different payment type). — User reviews information and executes product purchase transaction. — System validates payment type with external system; executes purchase transaction; logs product information with account and associates it with the secureID media. — Receipt is generated for transport service user. <i>Scenario 2: Purchase product and assign to secureID (Anonymous transport service user)</i> — Transport service user selects product and purchase function. — User reviews and selects one or more products to purchase. — User selects secureID media with which product will be associated or identifies media that will be used for service access (inputs media identification information). — User provides payment type (e.g., bank card) for product purchases. — User reviews information and transacts product (and secureID) purchase. — System validates payment type with external system; executes purchase transaction; logs product information with anonymous account and associates it with the secureID media. — If secureID media was purchased, media inventory manager function updates status, assigns to anonymous account and logs the information. — Receipt is generated for transport service user.

Use case name	Point of sale
	<i>Scenario 3: Pay as you Go</i> (e.g., bank card, mobile app such as Android Pay, Apple Pay, etc.) — Transport service user communicates secureID information to “reader”. — System validates media and payment type (e.g., bank card, mobile app such as Android Pay, Apple Pay, etc.); reviews account system for registration. — If secureID is registered, the request is treated as a proof of entry (POE) — If the secureID is not registered but validated as a financial instrument, send request/receive authorization from financial service provider. — System purchases and assigns single use service rights to anonymous account associated with the transport service user’s financial instrument.
Results	Product is purchased and associated with a secureID.

7.3.6 Fee/fare calculation and service rights validation for service operator

Use case name	Fee/fare calculation and service rights validation for service operator
Summary	When the Transport service user exposes (through passive or active means) his/her transport secureIDs, the Transport Operations Manager reads and relays the information to its central account manager for fee/fare calculation, validation and authorization.
Actor(s)	Transport service user, Transport Operations Manager, CTSAM
Assumption	Transport service user has purchased one or more products and associated it with secureID media. Transport Operations Manager (secureID reader) reader is ready to read exposed secureID.
Triggers	Transport service user exposes secureID to TOM reader (e.g., reading licence plate, NFC transmission/card emulation, ISO 14443 a/b RF read, etc.)
Interactions	— Reader recognizes and reads exposed secureID; verifies secureID; relays information to central account management (CTSAM) for processing. — Checks to verify secureID registration (or associate CTSAM/MSM registration) in CTSAM. — Depending on fee/fare policy (pre- or post-paid, PAYG), CTSAM collects information on usage and secureID account and calculates value of service (fee or fare). CTSAM checks if associated products meet fee/fare price; calculates based on price rules (for example). — If distance/time-based fee, calculates based on available entrance/exit and time in/time out information (and user profile) deducts from stored value. — If pass, registers usage. — If requires additional fee, CTSAM charges account payment type (e.g., deducts from stored value or charges credit card). — If flat fee on entrance or exit (based on time of day /day of week), checks for single use product or deducts from stored value. — If associate CTSAM/MSM, request/respond whether product is available to pay for service (if product is not currently registered). — Once transaction is approved, reader signals secureID/product verification. — If secureID/product is not registered or approved, then access to service is rejected NOTE For PAYG, POS and fee/fare calculation are conducted together (see POS for alternative scenario).

Use case name	Fee/fare calculation and service rights validation for service operator
Results	Payment/product is verified and access to service is granted (rejected).

7.3.7 Service rights validation for interagency acceptance

Use case name	Service rights validation for interagency acceptance
Description	When secureIDs are parsed for payment, the CTSAM identifies the entity that is responsible for validating and authorizing payment for services. The entity may be a Financial Service Provider for bank cards or another Common Transport Service Account Manager.
Actor(s)	Common Transport Service Account Manager(s), Financial Service Provider, (Mobility Service Manager).
Assumptions	SecureID is registered with authorizing provider/manager. CTSAM/ MSM has an agreement with an associate CTSAM/MSM and provides an option for its account holders to register associate secureIDs in its user accounts. When registering secureID. — Transport service user registers with a CTSAM or MSM. — Transport service user selects to request use of secureID with an associate CTSAM / MSM (hereafter referred to as associates CTSAM).
Triggered by	Transport service user exposes secureID in an associate Central Account Manager to request service rights. CTSAM reads the associate secureID and contacts associate CTSAM for secureID verification.
Interactions	— CTSAM requests verification of secureID and fee amount from associate CTSAM. — Associate CTSAM responds with verification of secureID and authorization of payment amount. — Information is sent to the Transport Operator to allow access to service. — (Settlement is made to appropriate provider/manager).
Results	Transport Operator provides access to service for an associate secureID and payment.

7.4 Authentication of secureIDs

There are several options for authentication of the secureIDs enabling the Transport service user to have access to the transport service. The acceptable level of risk may differ between the actors involved in the CTSA concept and some actors may require a higher level of risks than other actors, e.g. due to the data in the secureIDs and/or the price for the transport service provided. The following alternatives may be used for authentication:

- 1) No authentication by the Transport operation manager, i.e. the TOM takes the whole risk by not authenticating the secureIDs. This could be the case where the equipment reading the user secureID medium is temporarily out of order, the fee or fare is very low and the fraud level is low.
- 2) Authentication by white lists stored in the user secureID medium reader operated by the TOM.
- 3) One-way authentication by the TOM at the point of entry to the transport service, i.e. the TOM verifies the user secureID medium by security mechanisms.
- 4) Mutual authentication, i.e. the TOM verifies the user secureID medium and vice versa by security mechanisms at the point of entry to the transport service.
- 5) Authentication by the CTSAM where the equipment of the TOM is nothing but a transparent on-line communication channel. The authentication could be as described for points 2–4 above.
- 6) Authentication by a role either in the Support service domain or the Financial domain where the TOM equipment and CTSA Manager equipment forms a transparent communication channel

between the user secureID medium and the authenticating role, e.g. a credit card company or a Trusted Third Party (Security manager).

7.5 Open payment use case process descriptions

7.5.1 General

The open payment use cases are characterized as a merchant service. A transport service user uses a financial payment instrument such as a contactless bank card or mobile wallet to pay for service “on-the-go” or PAYG (see [Figure 8](#)).

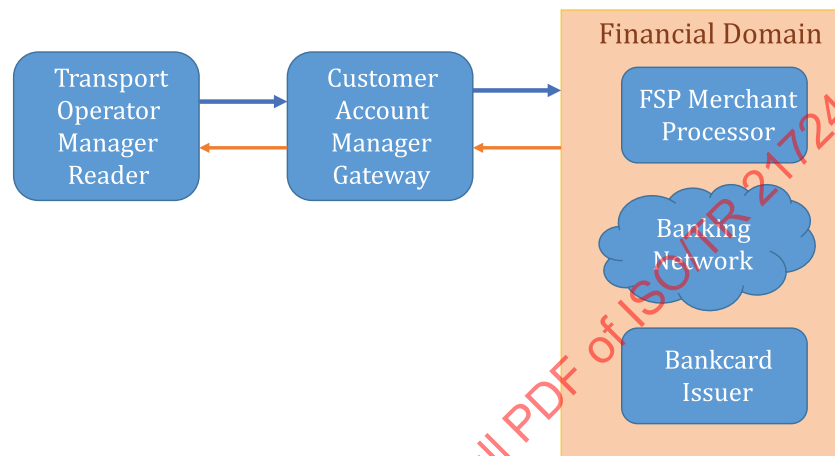


Figure 8 — Typical open payment process for pay as you go (PAYG) type

In the PAYG model, a TSU will “tap” a bankcard or handset using a transmission technology such as NFC by a payment reader. As in any merchant transaction, the reader will check the validity of the instrument, send a request for account verification and payment authorization to the CTSAM gateway (store and forward function) to determine whence the transaction should be forwarded (e.g., Central Transport Service Account Manager or Financial Service Provider). The CTSA manager will have its own gateway to forward the request to the customer’s bank (TSU FSB) for authorization. Once authorized (or denied authorization), the response will be directed back to the issuing reader.

7.5.2 Open payment transaction process

Use case name	Open payment transaction process
Description	Describes the process for a pay as you go (PAYG) transaction process
Actor(s)	Financial Service Provider (FSP), CTSAM
Assumptions	A contactless bankcard or mobile handset emulating a bankcard transmits bankcard information to the TOM reader. The ISO 8583 series on Financial transaction card interchange is used for the round trip request — response.
Triggered by	Bankcard transmission to reader (point of sale device).
Interactions	Request for authorization. Response to request for authorization.
Results	Accepted or denied authorization.

7.5.3 Valid and hot list upload process

Use case name	Bankcard list upload
Description	Describes the process for managing hot and valid bankcard lists from card issuers and financial service providers
Actor(s)	CSTAM Financial Service Provider (FSP), CSTAM
Assumptions	CSTAM procures services from a FSP to frequently update a list of the most current valid or hot listed bankcards (credit, debit, prepaid) user identification numbers.
Triggered by	On a subscription basis, this information is continuously updated.
Interactions	Upload all lists. Refresh current list.
Results	Current list of valid and hotlisted financial instruments.

7.6 Multimodal use case process descriptions

7.6.1 Transport service usage rule sharing processes

The multimodal use cases include exchange of product and usage information, account “opt-in” and “opt-out” requests and contact information, product and their usage rules, issuance and management, and services to support secureID validation and authorization, and settlement processes. These scenarios describe the interaction between managers.

The product is defined by three sets of rules according to ISO 24014, IFMSA: Usage, Pricing and Commercial rules. Each of these rule sets are handled in different ways when implemented in a multiagency (multiple transport service, transport operation, and/or customer service managers), multimodal environment. Because there are similar customer usage rules related to sharing and implementing information exchange, we will designate these rules as Transport Service rules.

- Transport Service Usage rules describes the transport service itself and how it should/may be used.
- Transport Service Pricing rules describes how fee/fares are calculated, and transactions are validated and authenticated by the appropriate product owner.
- The Transport Service Commercial rules describe how the involved roles will be paid, e.g., the split of the price paid (by the user) between the Transport service manager and the Transport operation manager.

A similar set of rules and data exchange flows apply to transport managers exchanging user account information. These rules cover the request to link accounts, the request for benefits, the request to pay for multimodal, and multiple transport services. For example, when a transport service user links his public transport account (and secureID) information to pay for or receive discounts for bikesharing or parking services near a rail station.

7.6.2 Transport service usage rule sharing processes

Transport service usage rules describes the transport service itself and how it should/may be used. For example, it includes sharing places, products, payment methods, valid secureIDs, and information about the services and transfer services associated with each. Typical scenarios include:

- Exchange of information related to the services offered and products accepted. These include product catalogue information, valid secureID types (or secureIDs if they do not contain personal information). Rules may differ for registered secureIDed versus anonymous products.
- Exchange of service information including places and transport services (modes) operated, transfers and discounts.

The product catalogue includes information on offered products such as those described in Table A.1. The product may be constrained by time or place. The product catalogue also includes information on valid services and service places where the products are accepted and may also include cross transport service/operation manager acceptance or transfer policies. This information is dependent on service place and transport service information which may have different version time periods or update frequencies.

NOTE The format for these interchange messages will be defined in the future ISO 21724-2.

Use case name	Transport service usage rule sharing
Description	Describes the process for common transport service account and mobility service managers to share information on Transport Services (of their transport service and/or operation managers).
Actor(s)	CSTAM, MSM TSM, TOM
Assumptions	An agreement has been made between two managers to share information on services and products followed by implementation of integration programming interfaces (or web services) between two CTSAMs or between a CTSAM and MSM.
Triggered by	CTSAM or MSM request or time-based update.
Interactions	Transport Manager Information — Request or subscribe to product catalogue, service place list and/or transport services. — Respond with new items or updates to product catalogue, service place list or transport services. — Cancel request or subscription for product catalogue, service place list and/or transport services.
Results	Receipt of messages with valid information.

7.6.3 Pricing rule sharing process

These processes consist of identifying the price and charging for a service or combined set of services. These rules are more critical for a card-based system than for an account-based system. The charges for the account-based system may request information on prices in real time, or apply a discount based on combined usage in a post-calculation. For example, a transport service user may pay less for parking when connecting with a public transport service. Additionally, some services may require a hold on the value of an account until the transport means is returned, for example in the case of distance-based fares or sharing services (e.g., bike and car share). There are several scenarios that may be implemented:

- Scenario 1: A CTSAM/MSM uses a pricing table which estimates and validates payment for access to service based on product acceptance and the latest Multimodal customer account exchange information. Later the actual charge is validated/authenticated when confirmed. (Scenario #2).

NOTE This approach is often used when communication from the reader to the CTSAM is not available.

- Scenario 2: A request is sent to a “partner” CTSA Manager or MSM for pricing information, verification and authentication of secureIDs / product.
- Scenario 3: A web service or protocol is provided by a partner CTSAM/MSM which calculates, validates and/or authenticates a product against service access (including applying discounts for one or more linked services).

Use case name	Transport service pricing rule and charging protocol
Description	Describes the approach to calculating price, validating and authenticating the charge for service access between managers.
Actor(s)	CTSAM, MSM (for TOM, TSM)
Assumptions	An agreement has been made between two managers to share information on pricing rules and charging protocols followed by implementation of integration programming interfaces (or web services) between two CTSAMs or between a CTSAM and MSM.
Triggered by	Request by travel user via MSM or CTSAM for access to service. Subscription request (for Scenario #1).
Interactions	Scenario #1: — Request/subscribe to fare/fee table including transfers (by product). — Request for pricing rules and notes (for table). — Update fee/fare table and/or pricing rules and notes. Scenarios #2 and 3: — Request for price for access to service based on customer secureID (e.g., registered or anonymous product and travel user type). — Response to price request query.
Results	Receipt of messages with valid information.

7.6.4 Commercial rule sharing process

The transport service commercial rules describe how the involved actors are to be paid, e.g., the split of the price paid (by the user) between the Transport service manager and the Transport operation manager.

Use case name	Transport service commercial rule sharing
Description	Describes the rules and exchanges related to settlement for linked trips, common secureID usage, and other account-based services.
Actor(s)	MSM, CTSAM (for TOM and TSM), FSP (for TSM, TOM or MSM).
Assumptions	An agreement has been made between two managers to share settlement for shared product usage by travel users. The agreement is followed by implementation of integration programming interfaces (or web services) between two CTSAMs or between a CTSAM and MSM.
Triggered by	Travel user transactions when using CTSAM and products from involved managers.
Interactions	Commercial Usage Information sharing — Request/subscribe to product usage history. — Request/subscribe to travel user transaction and travel history. — Transmit travel user access to service transaction/travel history. — Transmit product usage and status history. Reconciliation and Settlement Processes — Reconcile user transactions based on purchase and usage. — Allocate revenue based on actual usage. — Produce settlement reports. — Audit revenue processes.
Results	Receipt of messages with valid information