TECHNICAL REPORT

ISO/TR 14806

First edition
2013-07-15

Intelligent transport systems — Public transport requirements for the use of payment applications for fare media

Systèmes intelligents de transport — Exigences pour les transports publics relatives à l'utilisation d'applications de paiement pour les moyens de perception du prix du voyage

Reference number
ISO/TR 14806:2013(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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. 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. 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.

The committee responsible for this document is ISO/TC 204, *Intelligent transport systems*.

Introduction

For several years, payment institutions have started to roll out worldwide contactless payment cards. These cards support a contactless interface in addition to a contact interface or magstripe.

Where made available by Payment Application Issuers, these cards might be used by the Public transport industry for accessing the transport networks for specific use cases and customer groups. To facilitate payment application usage, the Public transport industry will benefit from data storage within the payment application, but this data storage capability is not a compulsory prerequisite as some Public transport Operators (PTOs) will start accepting payment application without such data storage facilities.

This Technical Report describes the current state of the art in a fast changing subject domain. It should not be used as the primary basis for system procurements. It describes PTO requirements for the ways that payment cards, or more specifically, payment applications (see Notice below), can be used by the PTOs to serve specific customer needs. The PTO requirements expressed in this Technical Report aim at being applicable to all payment application scheme/brand specifications for, and only for, the listed use cases in this Technical Report. For the use cases primarily based on the contactless interface, this Technical Report describes the functions needed by the Public transport industry and provides requirements from PTOs to the payment industry. Note that not all PTO requirements are currently available and some will require further discussion between the payment industry and PTOs, possibly leading to further developments in the availability and use of payment application functions. This Technical Report will be updated according to ISO procedures to reflect the evolution of PTO requirements and the corresponding level of functionality afforded by the payment industry. It assumes that any available data storage space will allow the storage of limited information only but may not be able to host fare products as they are defined today for ticketing applications (e.g. it might not be sensible to store a season ticket in a record that might be overwritten).

This Technical Report has been designed to provide ticketing and payment system designers who wish to accept payment applications with a clear definition of what usage options are available from these payment applications. It describes the functional interface to the payment application, with the aim of facilitating the design and procurement of fare collection systems.

Annexes A and B also provide:

- a checklist of commercial issues that need to be addressed by Public transport (PT), usually under a contract with a bank providing merchant acquiring services;
- options for providing interoperability between fare payment schemes that use bank issued payment applications, including proposals for any concomitant changes to those payment applications and payment application scheme rules.

NOTICE: The term "Payment application" used in this Technical Report refers to both an application resident either in a conventional payment card or an application loaded into a multi-application customer media (as described in ISO/TR 24014-3[3]).

Intelligent transport systems — Public transport requirements for the use of payment applications for fare media

1 Scope

This Technical Report defines the requirements from public transport for payment application owners to specify their application to make payment application media accepted as a tool to access the public transport networks by means of either media centric or back-office centric fare management systems, for non-local and non-frequent users as well as regular users.

This Technical Report defines both technical and non-technical requirements needed.

Four main items have been identified:

— Discrepancies between the existing payment application scheme rules and PTOs expectations.

— Definition of a short lifecycle storage area (scratchpad) which may support Check-In/Check-Out access and inspection processes.

— Definition of a long life cycle storage area (product area) to store a transport and other products within the payment application.

— Condition for use in a multi-application context, when different payment and transport applications are implemented in the same medium.

This Technical Report describes the requirements for:

— Level of Security and associated trust model;

— Conditions for the use of the specific storage area and the overwriting of products or data.

This Technical Report does not describe commercial issues which have to be defined for an implementation and may differ from place to place, e.g.:

— From Media Owner to Customer;

— From Media Owner to Application Owners;

— From Payment Application owner to customer;

— From Payment Application Owner to Public transport;

— From Public transport to Customer.

The first cases addressed by this Technical Report are EMV contactless applications and those variants (not strictly EMV) with application storage. All other payment applications (e.g. contactless magstripe emulation) will be addressed potentially in a future version of this Technical Report.

2 Terms and definitions

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

2.1
acquirer (or acquiring bank)
payment institution having a contract with the merchant for handling the remittance and settlement of transit fares charged to customers using the transport network

Note 1 to entry: Merchant in this Technical Report is Public Transport Operator (PTO).

Note 2 to entry: The acquirer may accept payments using payment applications from one or more payment application issuers, and/or for one or more payment application schemes/brands.

2.2
cardholder
holder of the payment application

Note 1 to entry: The cardholder has a contract with the issuer of its payment application. The media hosting the payment application may not necessarily be a "card".

2.3
certification
certification applicable to payment application, payment media and payment terminals, as required by the banking industry stakeholders, e.g. EMVCo, payment schemes

2.4
card-not-present transaction
CNP transaction
payment transaction where neither the card nor its holder are present at the point of sale

EXAMPLE Orders by telephone, fax or the Internet.

2.5
EMV Contactless Application
payment schemed defined applications relying on EMV technology

Note 1 to entry: As opposed to a payment scheme application relying on magstripe emulation.

Note 2 to entry: This is the type of payment application.

2.6
issuer
payment application issuer
payment institution having a contract with the cardholder and issuing the payment application on a contactless media

Note 1 to entry: The issuer issues payment applications such as credit or debit cards and guarantees payment for properly authorized transactions using the payment application.

2.7
merchant
entity having the necessary terminal equipment for handling payment transaction at validation points

Note 1 to entry: In this Technial Report, merchants are Public Transport Operators (PTOs).

2.8
payment application
application resident either in a conventional payment card or an application loaded into a multi-application customer media

Note 1 to entry: As described in ISO/TR 24014-3.[3]

2.9
payment interoperability
acceptance of payment application at the merchant point of sales whatever the payment application issuer is and whatever the merchant acquirer is

Note 1 to entry: Payment interoperability is ensured by rules and certification process enforced at each payment application scheme level and by EMVCo.

2.10
payment application scheme
payment brands that establish industry operating regulations for acquirers and issuers to facilitate coordination with merchants and cardholders

Note 1 to entry: Payment application schemes can have international scope (VISA, MasterCard, JCB Intl) or a domestic one (ZKA, GIE Carte Bancaire).

2.11
public transport
general statement about the transit industry

2.12
public transport operator
local specific implementation, independently of any difference between the roles of authorities, operators or retailers in fare management systems as defined in ISO 24014-1

2.13
transit data storage
standard logical data storage within the payment application available for transit ticketing operations, even if this storage is open to other merchants

Note 1 to entry: Transit data storage can take two implementation forms that determine their life cycle: included in the payment transaction log; separate, and available for non-payment needs.

Note 2 to entry: In the context of this Technical Report, the word transit data area (TDA) designates such a dedicated storage.

2.14
ticketing interoperability
technical interoperability provided by the usage of the same format for writing transit data in the payment application

Note 1 to entry: In the context of this Technical Report, ticketing interoperability is considered an optional requirement.

2.15
validation
transaction made with payment transaction equipment for confirming the validity of a payment transaction product or for enabling access to the transport network by realizing a payment transaction

2.16
zero value (payment) transaction
offline transaction at the reader for a null amount

EXAMPLE Null amount, e.g. £0.00 or 0€ or 0USD.

Note 1 to entry: This transaction may not be possible on all cards now.

3 Symbols and abbreviated terms

For the purposes of this Technical Report, the following symbols and abbreviations apply:

3.1 CNP

Card-not-present

3.2 HHT

Hand-held Terminal (used for revenue inspection)

3.3 PAN

Primary Account Number

3.4 PT

Public Transport

3.5 PTO

Public Transport Operator

3.6 TDA

Transit Data Area

3.7 TR

Technical Report

3.8 ZVT

Zero Value Transaction

4 Objectives and general requirements for the PTO

PTOs motivations for using the payment applications as a fare media can serve different **objectives**:

- [Obj.1] To offer a solution for local transit product storage:
  - Using payment application as a fare media can, in some cases, remove the need (and cost) for PTO to distribute ticketing application and/or customer media.
- [Obj.2] To replace cash as a fare payment at the gate
  - Using payment application as a fare media can replace cash payment at the gate or at bus/tram entry by electronic payment.
- [Obj.3] To provide a seamless and universal way of providing access to the transport network for infrequent users
  - Using payment application as a fare media can offer PTOs a complement to their existing ticketing application covering the needs of frequent customers, which by nature don't hold their ticketing application,
- [Obj.4] To enable a third party application used for customer authentication in the fare management system
  - Using payment application as a fare media can allow customer authentication via their payment application in post payment fare management system and avoid the issuance of transport media for registered customers.

The corresponding use cases are described in (Clause 5):

The Public transport requirements that make them possible address the following elements:

- Requirements for payment applications used in transport ticketing (Clause 6)
- Application security in payment applications (Clause 8)
- Customer media requirements (Clause 9)
- Test and certification of payment applications (Clause 10)
- Customer data privacy (Clause 11)

These PT requirements are also completed by explanations about how payment applications can be used and what fare policy can be implemented according to the use cases and validation access rules applicable in a transport network (Clause 7).

Beyond the scope of this Technical Report, a first level of analysis is also given for guidance in annexes about:

- business rules checklist for using payment applications (Annex A);
- options for providing national and international ticketing interoperability (Annex B).

NOTE Where interoperability is achieved by means of the basic contactless payment application without transit data storage, there is no need for any ticketing data to be interoperable.

5 Use cases

Payment applications can be used in a number of ways for transport ticketing, as determined by the PTO and subject to suitable agreement in the merchant acquiring contracts.

The generic ways are defined in the following use cases which can eventually be complemented by national interoperable fare management applications.

In the description of the use cases, three possible validation access rules to the transport networks are considered:

- non validation rule:
  - customers should have an entitlement to travel, but are not required to validate at any stage of the journey although they may be subject to revenue protection control.
- entry validation rule:
  - customers are required to validate only on entry.
- entry/exit validation rule:
  - customers should validate both on entry and exit, and possibly at intermediate validation points.

These different validation access rules will structure the way payment applications can be used in transport networks as described in the following use cases and further analysed in Clause 7.

5.1 Use case 1: Product purchase for loading on customer media

5.1.1 Objective

This use case is the conventional one where a customer selects a product from a retailer and uses a payment application to pay for the product. The payment application can be used in contact mode, contactless mode or in cardholder not present mode. The payment options vary according to mode.

5.1.2 Customer path

- The customer selects a product.
- The customer pays with a payment application.
- The PTO product is not loaded to the payment application.
- The PTO product is loaded onto the PTO media and application.
- The customer travels and validates using the PTO’s entry or entry/exit ticketing system.

5.1.3 Comments

This use case is conventional and well defined and is therefore out of the scope of this Technical Report although included here for completeness.

5.2 Use case 2: Access with PTO product data in payment application

5.2.1 Objective

- [Obj.1] payment application as a solution for local transit product storage.

5.2.2 Customer path

- The customer should first purchase or request a product from his/her PTO at a suitable ticket machine or should purchase or request online for later collection at a ticket machine.
- Once the transaction is accepted, payment made if required, and the customer is at a suitable loading terminal, which can be the entry gate, the product is loaded from the terminal into the payment application.

- The customer uses the product held in the payment application at points of validation to gain entry and exit, according to the PTO's entry or entry/exit validation rule and presents the medium with the payment application when requested for revenue inspection.

5.2.3 Comments

The PTO product loading is commonly carried out on PTO equipment. It may also be carried out on bank equipment. This operation is out of the scope of this version of the Technical Report as there is no identified demand yet for standardising it.

PT systems, data and products are PTO-specific and may be interoperable.

Existing PTO product data format may need to be adapted to cope with the limited storage capacity provided by the TDA.

PT data can include PTO-specific personalisation data, travel ticket, discount entitlement or concession.

If the payment application holds a PTO-specific discount entitlement or entitlement, it will be used by PT system when the customer uses the payment application during ticket purchase or revenue inspection.

5.3 Use case 3: Pay single journeys on validation

5.3.1 Objectives

- [Obj.1] solution for local transit product storage,
- [Obj.2] replacement of fare payment at the gate,
- [Obj.3] seamless and universal way of providing access to the transport network for infrequent users.

5.3.2 Customer path

- Where the fare is not fixed/flat, validation prior to boarding may require the customer/cardholder to select zone of travel or customer engages with driver who selects product/fare. Travel is limited to single journeys only.
- The customer uses the payment application at points of validation to gain access and exit, according to the local PT entry or entry/exit validation rule and presents the medium with the payment application when requested for revenue inspection.
- The travel price may be flat or be calculated prior to travel depending on the route or distance or zonal or time-based pricing, or be a mixture of the five and depending on the tariff rules.
- For transport networks with entry validation rule:
  - The travel price is known or calculated on entry validation,
  - Contactless payment is made at the moment of entry validation,
  - The PT Operator requests settlement after validation for each individual journey.
- For transport networks with entry/exit validation rule:
  - The travel price is known or calculated at exit validation, the meaning of exit validation being determined by the PTO in its ticketing rules,
  - Contactless payment is made at the moment of exit validation,
  - The PT Operator requests settlement after validation for each individual journey.

5.3.3 Comments

The payment application is used for both travel validation and payment.

For transport network with entry validation rule, fare products proposal will be significantly limited for payment application holders unless a product selection is proposed at the entry validation (by the driver on bus/tram or by an interface on validation terminal).

For transport network with entry/exit validation rule, fare products proposal can be more comprehensive including distance or route based charging, but "negative" price adjustment on exit validation should be avoided as no offline refunds are possible via a contactless transaction. Depending on the payment application scheme, online authorization cards may not be accepted and where accepted will require extra risk mitigation via a specific deferred authorization processes.

Online real-time transactions should be avoided unless ground equipment or communication capacity is compatible with processing time demands.

Most payment transactions for EMV contactless payment application will be performed offline, provided that the charged price remains under the offline spend limit for the payment application.

The non-validation rule is not relevant for this use case and is out of scope.

5.3.4 Risk management

A customer may not know how close he is to his offline card limits when he travels and may face a decline at the point of payment (for example on boarding a bus).

When the counter limits of the payment application are reached, the PTO should be able to accept the transaction on the basis of additional risk management measures (e.g. whitelists, hotlists) and to present it for deferred authorization. This introduces a potential revenue risk for the PTO as the payment of declined/forced transaction is not guaranteed by current scheme rules and should be subject to PTO/Acquirer negotiation.

5.4 Use case 4: Pay after a period

5.4.1 Objectives

— [Obj.1] solution for local transit product storage,

— [Obj.2] replacement of fare payment at the gate,

— [Obj.3] seamless and universal way of providing access to the transport network for infrequent users

5.4.2 Customer path

— The customer uses the payment application at points of validation to gain entry and exit, according to the PTO's entry or entry/exit validation rule and presents the medium with the payment application when requested for revenue inspection.

— The PTO requests settlement for the total price of travel over a period of time.

5.4.3 Comments

The payment application is used for both travel validation and payment.

The use case may apply to transport networks with either entry or entry/exit validation rules.

The non-validation rule is not relevant for this use case and is out of scope.

The travel price of each journey can be flat fare or be calculated depending on the route or distance or zonal or time-based pricing, or be a mixture of the five and depending on the tariff rules.

The effective price charged to the customer is calculated at the back office for a period according to the tariff rules. Best value or capped fares over the period may be offered. There is also the possibility to take into account products pre-purchased with the same and associated payment applications during fare computation by the Back Office. In this case, only those journeys outside the pre purchased travel product are charged to the payment application account.

Depending on payment application scheme, on line authorization cards may not be accepted and where accepted will require extra risk mitigation via a specific deferred authorization processes.

5.4.4 Risk management

For an EMV contactless payment application, transaction amounts cryptographically certified by the payment application at entry or later exit validation will likely be different from the price amount computed by the back office that is used for the settlement after the period or for deferred authorization.

The hard-limit offline no-CVM maximum price limitation may not then necessarily apply, but other limits may be imposed subject to payment application scheme/ brand rules applied through the acquirer contract.

This introduces a potential revenue risk for PTO that should be covered by a deferred payment authorization and should be subject to PTO/Acquirer negotiation. It is strongly recommended to have deny lists at the check-in validators to manage this revenue risk. This will allow denying entry to payment applications that have failed a payment authorization for a previous journey.

5.5 Use case 5: Entitlement with payment application

5.5.1 Objectives

- [Obj.4] payment application used for customer authentication in the fare management system

5.5.2 Customer path

The customer:

- registers once to the PTO by providing some payment application data allowing him to be identified uniquely through his payment application and agrees being charged after usage; or
- pre purchases an entitlement product with its payment application and agrees having its payment application registered to a “white list”; or
- registers to a combination of pre-paid products and post-payment facility for journeys outside his pre-purchased product.

The customer uses the Payment application at points of validation to gain access and exit, according to the PTO’s entry or entry/exit validation rules and shows the medium with the payment application when requested for revenue inspection.

For customers who registered to post payment facility:

- The price is calculated after validation.
- The PTO requests settlement after validation either for individual journeys or for the total price of travel over a period of time. Settlement is made using the payment means registered by the PTO during customer enrolment and not necessarily done using the payment application data.

For customers who registered to pre-paid products:

- The entitlement validity is checked at each entry validation and access is declined in case of check failure.

5.5.3 Comments

All validation rules are permitted for this use case.

This use case for post-paid customers differs from use case 4 by the fact that the payment is not settled on the account linked to the payment application but on different means (such as a direct debit from customer account) making the type of payment instrument used in this process less prescriptive. However, payment application schemes forbid the use of their payment applications for this purpose.

6 Requirements for payment applications used in transport ticketing

The expectations of PT described in the use cases, mainly for revenue inspection and entry/exit validation system fare calculation, can more easily be satisfied in a simple way by fare management system with offline validation terminals if data can be stored in the payment application.

Therefore, PT benefits from the possibility to store public transport data in payment applications.

6.1 Payment application storage options

This subclause describes three levels of requirements according to the levels of data storage that can be guaranteed by the payment applications.

Note The transaction log approach (see 6.3 for detailed description) even if relying on existing features defined by EMVCo standards for contact payment, requires mechanisms not implemented in current payment scheme contactless payment applications. Hence, there is lack of likelihood to see transaction log become a universal solution, but it may remain an option for a domestic solution.

6.2 Payment application without any public transport data

6.2.1 State of the art

This is the current context with the usage of legacy payment applications.

6.2.2 Comments

In this context, there are no additional requirements for the payment application.

However it should be configured to support zero value transaction. It allows a payment terminal to authenticate offline a payment application without taking the risk of an amount authorization rejection or of an online authorization request (see [Req. 16] below).

This requirement also applies for payment application with transaction log and with TDA, as this transaction allows any terminal to write data in a payment application during entry validation when fare is calculated at exit validation.

6.3 Payment application with payment transaction logs

6.3.1 State of the art

The payment transaction log is a mechanism specified by EMVCo for contact payment transactions. Its supply is a payment application issuer decision that can be made at payment application issuance only.

PTOs should however not expect all payment applications to have the transaction log enabled.

The payment transaction log (TL) is a cyclic FIFO (First In First Out) file on the payment application.

The transaction log is a file that can be only written by the payment application.

The transaction log data can be read by any off card application and do not require a secure connection.

When TL is active a record is expected to be filled automatically by the payment application itself for each successful payment transaction.

However, because a payment application doesn't authenticate the payment terminal, any device can emulate a payment terminal and perform a payment transaction, resulting in the payment application to generate a new transaction log entry in case of successful transaction.

The size of the records and their number in the TL file may differ from one implementation to another one.

The payment transaction log, if present, is likely to include the following fields as a minimum, but the content is at the discretion of the issuer:

< Transaction Amount >

< Transaction Currency Code >

< Transaction Date >

< Transaction Time >

< Application Transaction counter > (ATC)

Some payment application schemes specifications propose as an option the possibility for payment terminal to insert an acquirer-defined field in the record.

< Merchant Custom Data > : an area which contents is defined by the Merchant terminal.

However, this option is not implemented in any of the current EMV payment applications and requires a dedicated tag to be defined.

6.3.2 Comments

The TL can be used by PT without requiring any PTO specific adaptation of the payment application. This feature offers a convenient way for PT:

- to manage revenue inspection by retrieving the entry validation transaction into the transaction log file;
- to compute payment at exit gate by retrieving the entry and connecting validation transactions into the transaction log file.

However, PT should have equipment that ensures that the log of the entry transaction will not be erased before the end of the single journey.

The card/reader transaction time to select the appropriate record in the TL file should also remain compliant with the need for fast validations (see [Req. 34].

Furthermore, the appropriate level of security can only be achieved if the transaction log does include some PT authenticated data. PTOs are therefore requesting the ability to log their own data into the < Merchant Custom Data > for logging their own data such as their Merchant ID, the PTO terminal ID and a PTO signature based on some elements of the payment transaction. It is the responsibility of each PTO to maintain the topology of all its Payment Terminals allowing it to map each PTO Terminal ID with a physical location when using distance, route or zonal fare calculation.

6.3.3 Requirements

[Req. 1] The sequence of commands (APDUs) used for a given payment application to read the transaction log data may be payment application scheme dependent but should not be Payment Application Issuer dependent.

[Req. 2] The transaction log file should have a minimum size of 15 records to guarantee a minimum resilience of the data.

[Req. 3] The < Merchant Custom Data > in the Transaction Log file should have a size of 20 bytes.

[Req. 4] The contents of the field < Merchant Custom Data > should be provided by the PTO terminal (Merchant defined) and can be different for each payment transaction.

[Req. 5] The field < Merchant Custom Data > should be assigned a dedicated tag. This tag should be the same for all PTOs.

[Req. 6] The field < Merchant Custom Data > should be coded as follows:

- The Merchant ID is based on ISO standard and is the RID of the PTO Ticketing application AID.
- The terminal ID has a format which remains PTO specific and should have a fixed length of 8 bytes.
- The PTO signature area has a minimum length of 4 bytes and remains PTO specific.

[Req. 7] It should be possible for the PTO to compute its authentication signature by using data of the payment transaction including ATC, Transaction Amount, Transaction Date, Transaction Time and PTO specific data. The specification for computation of the PTO authentication data can remain PTO specific and is out of scope of this Technical Report.

[Req. 8] The PTO terminal should be able to retrieve from the payment application the current < ATC > value prior to having to send to the payment application the contents of the Merchant Custom Data field.

6.4 Payment applications with transit data areas (TDAs)

6.4.1 State of the art

Payment application schemes have defined specifications for their payment application that provide merchants with Transit Data Areas (TDAs), the life cycle of which is separate from the payment TL mechanism.

PTOs should however not expect all payment applications to be TDA-equipped.

Magstripe emulation payment applications may not have TDAs.

TDA data can be written and read by all payment application terminals by using the payment application commands/API provided by the reader's payment application software supplier [= vendor] (i.e. no direct read/write access to the medium by the PTO. The payment application on the medium should be first selected to write and read TDA data.)

TDA writes and reads can use either contact or contactless interface.

The format of the data written in the TDA is PTO specific, but interoperable TDA contents could be defined later.

Two types of TDAs are available: Transient TDA and Permanent TDA.

Permanent TDA can be PTO write-protected TDA or Issuer write-protected TDA

The three classes of TDAs are defined as follows:

Transient TDA

Transient TDAs need no credentials stored in the payment application and they can be written and overwritten without authentication.

Available Transient TDAs are attributed to PTOs when the need occurs and identified with a PTO TDA ID.

Data in a Transient TDAs will not be protected against overwriting by a different PTO. Protection will only rely on terminal rules that may be part of Acquirer contractual agreement.

Permanent TDA

PTO write protected TDA

PTO write protected TDAs have PTO credentials (secret keys, one time password, …) stored in the payment application on the request of the PTO by the payment application Issuer either at personalisation or during an online transaction post issuance. Subsequent operations on the TDA can be carried out by the PTO offline and without reference to the Issuer.

Issuer write protected TDA

Issuer write-protected TDAs depend on the Payment Application Issuer credentials which are always stored in the payment application.

They require an online transaction for writing which shall use the contact interface to communicate with some service that has access to relevant keys. On the request of the PTO the TDA is written by the issuer during an online transaction. As a consequence, issuer write-protected TDA can only be available for payment application hosted on contact and contactless media.

6.4.2 Comments

TDAs may provide PT with better guarantees that their data will be secured and/or will remain available for a longer period of time. They can therefore address all use cases.

PTOs should however obscure data using their own methods if their data are sensitive, confidential or private.

Transient TDAs are suitable for use by PTOs where the importance or duration of the PTO data are higher or longer than guaranteed by the Transaction Log and its loss would not disproportionately imperil its fare collection.

PT should however allow for the case where no Transient TDA on a TDA-equipped medium is available.

PTO Write protected TDAs are suitable for use by PTOs where the importance of data to the PTO is high and its loss would prejudice fare collection so that the PTO needs to be certain none of his data will be lost.

A TDA is then assigned to this PTO by the Payment Application Issuer to store PTO data.

This approach requires the PTO to establish beforehand a business agreement with selected Payment Application Issuers. Such a solution therefore remains specific to each PTO/Payment Application Issuer pairs, which restricts the advantage of universality for occasional customers.

National agreements could be facilitated by national payment application associations or even possibly at wider levels, e.g. EU, within each payment application scheme.

Issuer write protected TDAs have the same features as PTO protected, but writing can only be done by a terminal under control of the Payment Application Issuer.

As long as not all payment applications will include TDAs, those with TDA or terminal accepting only payment application with TDA should be clearly branded to let the customer know if he can use the access facilities to the transport networks.

The requirement for a dedicated branding of TDA media may need to be agreed with payment application schemes.

6.4.3 Requirements

[Req. 1] A terminal should be able to identify whether the payment application is TDA enabled or not at the beginning of the payment transaction.

[Req. 2] A dedicated branding for TDA enabled payment application should be agreed with and defined by the payment application schemes and should be visible to cardholder on the media.

[Req. 3] Transient TDAs should not be used by a PTO that already owns a PTO write protected TDA in the same payment application.

[Req. 4] TDA records provide 160 bytes of free-format data for use by PTOs. Some Payment Application Issuers may provide TDAs with larger TDAs, eventually for permanent TDA following Payment Application Issuer and PTO specific negotiations but a minimum size of 160 bytes should be warranted on all issued payment applications which are TDA enabled.

[Req. 13] Each TDA enabled payment application will have minimum of 3 Transient TDAs. Payment Application Issuers will determine the number of each other type of TDA available on their issued payment applications.

[Req. 14] Once affected to an operator, Transient TDAs should not be overwritten by any other operator before the end of the following day. After that, the cyclic buffer rule applies.

[Req. 15] PTOs will be assigned a 4 byte PTO TDA ID by each payment application scheme. Assignment should not need PTO to have direct agreement with payment application schemes and should be managed through the Acquirer agreement. PTO may not be assigned the same PTO TDA ID value from different payment application schemes.

[Req. 16] It should be possible for a PTO to request its data from the TDAs via the payment application by a single request specifying its PTO TDA ID.

[Req. 17] Payment application should provide a mean for interoperability between PTOs. This should be provided in a manner to be determined. Some options for providing interoperability are presented in Annex B.

6.5 Supported transaction types

According to the different use cases mentioned above, several types of transactions by the contactless payment application are needed

6.5.1 Legacy Payment transaction types

- The price charged to the customer is known at the time of the transaction.
- A contactless payment transaction is performed.
- An online authorization can be requested by the payment application based on issuer risk management policy set in the payment application. Unless the terminal has communication capacity to proceed with an online authorization transaction, the transaction between the terminal and the payment application should be executed off line.

This means that either:

- an authorization is sent by the terminal to the issuer authorization server as part of the payment transaction and the contactless transaction will complete, or
- the terminal declines to make an online authorization, the payment transaction may be postponed and the back office should take care to manage a deferred authorization request based on information collected from the terminal (see 6.5.2 for deferred authorization requirements).

In both cases, there is a revenue risk for the PTO when the authorization is declined.

6.5.2 New types of transactions

Payment application schemes should provide support for the new following types of transactions.

Zero Value Transaction (ZVT)

- The price charged to the customer may or may not be known at the time of the transaction.

- PTO should be able to use a Zero Value Transaction (ZVT) when price is not known at the time of the transaction, to avoid any risk for a declined transaction because of reaching a risk counter limit.

[Req. 18] PT requires the support of the offline authorization for Zero Value Transaction (ZVT).

Deferred payment authorization

- For terminal not having communication capability allowing them to process an online authorization request in due time, a deferred payment authorization should be able to be initiate from the back office at a later time.
- The period until which a payment transaction can be presented for a deferred authorization may be agreed between PTO and its acquirer on a case by case.
- To support deferred authorisations, the PTO should implement a deny list check at validators, so that declined cards can be blocked.

[Req. 19] PTO back office should be able to submit deferred authorization requests based on a single or aggregated previous payment transactions.

[Req. 20] A deferred authorization can be requested for a different amount than the one used for the payment transaction appended to the authorization request.

[Req. 21] The deferred payment authorization should be applicable to all types of payment applications, including prepaid cards and online authorization cards.

Payment application authentication

This transaction is only used to authenticate the payment application of the customer.

Authentication should be based on a unique and public identifier of the payment application retrieved from the transaction data.

A ZVT transaction should be conducted as the way to authenticate the payment application.

Permanent TDA handling

The transaction is used for storage and validation and reading of products into a TDA.

[Req. 1] Selection, Read and Write commands of permanent TDA should be available for PTO terminals.

Read and write TDA journey information

This transaction is used for storage and validation and reading of journey data into a TDA.

[Req. 2] Read and Write commands of selected transient TDA should be available for PTO terminals.

The following transaction types should be available for the following use cases:

Transaction types	Possible Applicable Use Cases
Payment	**Use case 3:** Pay on validation **Use case 4:** Pay after a period
Deferred Payment authorization (new)	**Use case 3:** Pay on validation **Use case 4:** Pay after a period
ZVT (new)	**Use case 4:** Pay after a period **Use case 5:** Authenticate customer with payment application
Permanent TDA handling (new)	**Use case 2:** Access with PTO product in payment application **Use case 3:** Pay on validation **Use case 4:** Pay after a period
Transient TDA handling (new)	**Use case 3:** Pay on validation **Use case 4:** Pay after a period

7 Matching between use cases, validation access rules and payment application types

This Clause describes for each type of transport network, according to its network validation rules and according to the type of payment application (without any public transport data, with Payment Transaction Logs enabled or with TDA) how the different use cases can be implemented and what the fare policy limitations are.

The current separation mainly apply to EMV Contactless Application, as currently, magstripe emulation payment application does not enable transaction logs or TDA and then should be considered in the same case as for EMV Contactless Application without public transport data.

Use Cases	**Payment Application**	**Type of fares**	**Type of transaction**			
			Entry Validation	**Intermediate Validation**	**Exit Validation**	**Revenue Inspection**
Use case 2: Access with PTO product in payment application	No TL & no TDA	Not supported	Not supported			
	With Transaction logs	Not supported	Not supported			
	With TDA	Single journey/daily tickets for transient TDA. Any ticket for Permanent TDA.	Read TDA	Read TDA	Read TDA	Read TDA
Use case 3: Pay on validation	No TL & no TDA	For entry validation rule transport network: Ticket with fixed or time based charging (unattended terminal). Ticket with fixed time or distance based charging (semi-attended terminal). For Entry/exit validation rule transport network: Ticket with fixed, route, time or distance based charging	Payment + deferred authorization	ZVT	ZVT	ZVT + back office checking
	With Transaction logs					Read Transaction log
	With TDA					Read TDA
Use case 4: Pay after validation	No TL & no TDA	Same split as Use Case 3 with possible capped or best value fare computation over the period by the back office.	ZVT or Payment + deferred authorization	ZVT	ZVT	ZVT + check in back office
	With Transaction logs					Read Transaction log
	With TDA			ZVT + Read TDA	ZVT + Read TDA	Read TDA
Use case 5: Authenticate customer with payment application	No TL & no TDA	Any fare policy can be applicable including concession fares, seasons tickets and a mixture of prepaid product and “Pay As You Go”	ZVT	ZVT	ZVT	ZVT + check in back office
	With Transaction logs					
	With TDA					

NOTE The use case 2 “ Access with PTO product in payment application” can only be applicable for payment application with TDA. A branding distinction should be defined to enable cardholders to know whether or not their payment applicable has TDA and therefore can be used for storing a PTO product.

7.1 Revenue protection and inspection

The validation terminal may be online but it is proposed that all transactions be performed off-line. The terminal online capability is used to maintain the live deny list distribution.

In use cases 3, 4 and 5, the use of the payment application without TDA may produce no evidence of validation.

Revenue inspectors can use HHT with contactless capability to connect with the payment application.

Several solutions can be envisaged:

1. The HHT accesses the payment application's details via a ZVT and attempts to query the back office for evidence of use and fare payment. This approach assumes that the HHT will have the ability to communicate with the back office (GPRS, WLAN, other). Where proof of use is negative (no fare paid), the revenue inspector has the option to issue a penalty fare or standard fare (standard fare may be issued if the customer was unable to transact with the terminal(s)). Note that there are some legal issues related to automatic charging of penalties. Different regulations may apply in different countries/regions.

Issues:

- Entry validation transaction latency with respect to the back office;
- Reliability/availability of the HHT/back office communication link;
- Issuing a penalty fare or standard fare may hit the card's limit(s);
- Issuing of penalty fares necessitates compliance with country/regional legislation or accepted codes.

2. The HHT performs a zero value transaction for later consumption and processing by the back office. The HHT may operate in an off-line (no live communications with the back office) mode although this will limit the receipt of updated deny list.

Issues:

- The customer is given an extra charge once the ZVT is processed in the back office (this extra charge is for travelling without a valid permit to travel);
- Consider issuing a paper ticket/reference as proof of validation action;
- Need to identify merchant equipment for later cardholder statement;
- Issuing of penalty fares necessitates compliance with country/regional legislation or accepted codes.

3. A visual check from a list of last four digits of used payment application PANs printed from the terminal can also be performed in case of bus/tram inspection.

4. Where present, the TDA or transaction log may be interrogated by the HHT in order to determine whether data relevant to the process of revenue protection and inspection is present.

8 Security of payment applications

Security of the payment application is defined by the payment industry. The PTO needs to be protected against security flaws that may expose their customer data (in the TDA) or generate some fraud concerns. Liability for security flaws will be specified in the merchant acquiring contract.

The level of security for the contents of permanent and transient TDA should be PTO defined.

Each transport operator should be free to define and use additional levels of security when writing its own data into TDA, for example:

- checksum for data integrity;

- signature for data origin authentication;
- encryption for data privacy;
- counter implementation for anti-replay protection.

The security applied by the transport operator only aims at protecting data between writing operations done through issuance or at an entry gate and reading operations done during inspection or at a connecting or exit gate. Both read and write operations are under the sole control of PT organization and only rely on the cryptographic capabilities of their terminal application implemented in their front end equipment.

As a consequence, the additional level of security that may be selected by the transport operator should have no impact on payment application specifications.

9 Condition for use in a multi-application context

9.1 Using payment application in a multi-application media

In order to facilitate the acceptance of customer media hosting a payment application by the PT front end equipment, customer media may rely on ISO/TR 24014-3[3] when payment application is issued on multi-application customer media.

[Req. 24] When issued on a multi-application media, payment application and hosting customer media may comply with ISO/TR 24014-3[3] requirements.

9.2 PTO Participation in the life cycle management of payment applications

Transport operators may be involved in the issuance process of payment applications to store for example a customer profile in the permanent TDA.

The personalisation process of the permanent TDA during issuance process should comply with the following requirements:

[Req. 25] In case of PTO protected TDA, the keyset(s) used for securing the permanent TDA personalisation is managed by the transport operator and should not need to be known by the issuer.

[Req. 26] The issuer should be able to force termination of the permanent TDA under agreement of the owning PTO.

9.3 Payment application selection

Multi-application customer media may host several applications: ticketing and payment applications but also multiple payment applications.

Rules for determining which application is selected first by a transit validation terminal should remain a PTO choice.

Rules for selecting payment application when several payment applications are present should be managed according to payment industry rules and consistently with others payment terminal implementations. Notice that this selection may be subject to regional competition regulations.

The public transport industry does not intend to specify those rules but are awaiting clear specifications from payment application schemes or banking standardization organisations on this subject.

Additionally, when several payment applications are present in a payment application (or any medium without a user interface) and supported by the POS terminal, some regulation rules may impose to offer a choice to the cardholder. In the context of payment at the gates, there may be no user interface to propose a choice to the end user and PTO don’t want to implement a validation terminal user interface simply for handling payment application selection.

[Req. 27] Each PTO should be able to define the sequence used for application selection by its validation terminal when several (payment and non-payment) applications are supported.

[Req. 28] When multiple payment applications are present, the payment application should be selected by the validation terminal according to the priority rules defined by the payment industry (for example according PPSE priority list for EMV applications) and the applicable regulations.

[Req. 7] When multiple payment applications are present in a customer medial without any user interface, the payment application should be selected by the validation terminal without requiring for any end user interaction.

10 Test and certification of payment applications

10.1 Ease of integration into front end equipment

Transport operators are not keen on multiplying the number of payment applications to be integrated in their front end equipment to offer the largest acceptance of payment products. So far, contactless payment applications are payment application scheme specific, and hence only require having one integration (and certification) process per payment application scheme (American Express, Discover, JCB Intl, MasterCard, VISA).

Transport operators are therefore expecting that the payments industry provides them with a unique front end terminal set of functions able to cope with all of the available scheme-based contactless payment applications, whatever the payment application issuer is. Logically, transport operators are also expecting a unique certification process for payment application integration to replace the current contactless payment application scheme specific processes.

Front end equipment should be able to recognize when selecting a payment application whether or not permanent and transient TDA are available and need to be able to respond appropriately if a TDA is required but not there.

10.2 RF protocol testing

All the applications present in the PT front end equipment may likely share the same HW platform (RF coupler) for handling the RF communication.

The RF protocol implementation on the PT front end equipment accepting payment application should fulfil the following requirements:

[Req. 30] Front end equipment should support ISO/IEC 14443 types A and B RF communication protocols ([4],[5],[6] and[7]) to enable contactless access with the secure element (SE) payment application.

[Req. 31] Additional payment industry requirements about RF protocol implementation should not restrict RF protocol interoperability and deprecate performance of RF data exchanges.

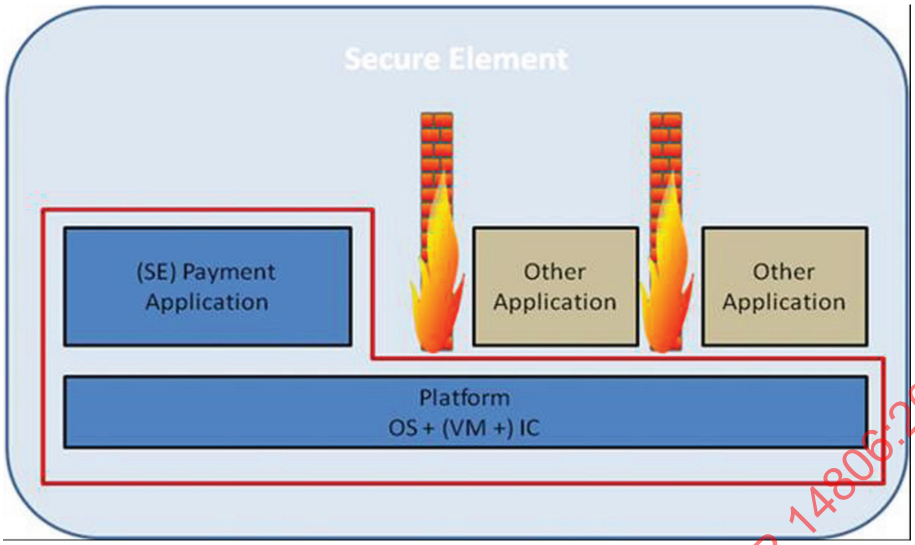
10.3 (SE) payment application certification

The SE of a customer media may host one or several applications.

In case of SE hosting multiple applications, PT organizations expect that:

[Req. 32] Each application environment should be isolated from each other. No access to application data are possible from another application except for application offering a shared interface.

[Req. 33] Certification from the bank or payment application scheme remains valid when other applications are added to, modified or removed from the SE.



10.4 Terminal payment application certification

A terminal payment application should be hosted in the front end equipment of PT organizations next to existing ticketing applications.

PT organizations expect vendors to design PT front end equipment accepting payment applications such that the following requirements are met:

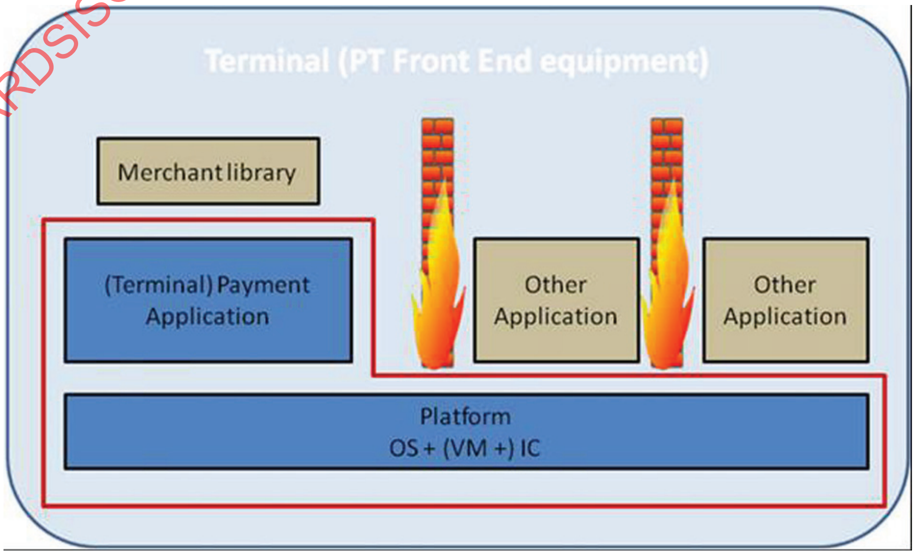
[Req. 34] The PT specific business logic associated to R/W into the TDA should be built up independently from the terminal payment application. See example diagram with a dedicated library module, called merchant library.

[Req. 35] Each application environment should be isolated from each other. No access to application data are possible from another application except for application offering a shared interface.

[Req. 8] Certification from the payment institution or payment application scheme should remain valid when:

— Other applications are added to, modified or removed from the terminal.

— The TDA library is modified by PT organization.



10.5 Transaction time

The target given in this Technical Report is that payment application/reader interactions should be completed within 350 ms at validation point with high passenger throughput and in no more than 500 ms in all other cases.

Two types of performance requirements are then defined, according to passenger throughput requirement defined by the PTO at the point of validation.

The payment application (on a given customer media) and the validation equipment should jointly meet the required performance requirement. The split of the processing time between the customer media hosting the payment application and the validation terminal will be defined in the next version of this Technical Report.

[Req. 9] The transaction time when using a payment application at a validation terminal with critical throughput requirement should be limited to a maximum of 350 msec inclusive of:

— Payment application processing time with eventual TDA handling.

— Terminal processing time including security list verification.

[Req. 38] Transaction time when using a payment application at a validation terminal with non-critical throughput requirement should be limited to a maximum of 500 msec inclusive of:

— Payment application processing time with eventual TDA handling.

— Terminal processing time including security list verification.

But exclusive of any eventual user interaction time with the validation terminal.

11 Customer data privacy

The architecture should be designed so that the national privacy laws can be enforced.

Data storage and data exchanges between transport operators and payment institutions should comply with the applicable privacy legal requirements and should enable:

— The possibility to get an anonymous accessibility and usage of the transport network,

— A protection against the abusive usage and dissemination of personal data.

That means that, unless the customer gives his explicit consent, all customer personal data collected by any entity should remain confidential and not accessible by other entities.

For example, as a consequence, when payment application ID or customer age is requested by the PT organization, the PT organization has to ask the customer to retrieve this information.

Annex A
(informative)

Business rules checklist for using payment applications

This Annex deals with topics that are not in the scope of the present Technical Report. This can provide useful background information for those PTOs considering using contactless payment applications either on their own or in combination with a PTO issued application:

— Commercial negotiations between PTOs and issuer/acquirer partners;

— Options for providing interoperability between PTOs using payment application as a fare media.

A.1 Outline of the payment industry model

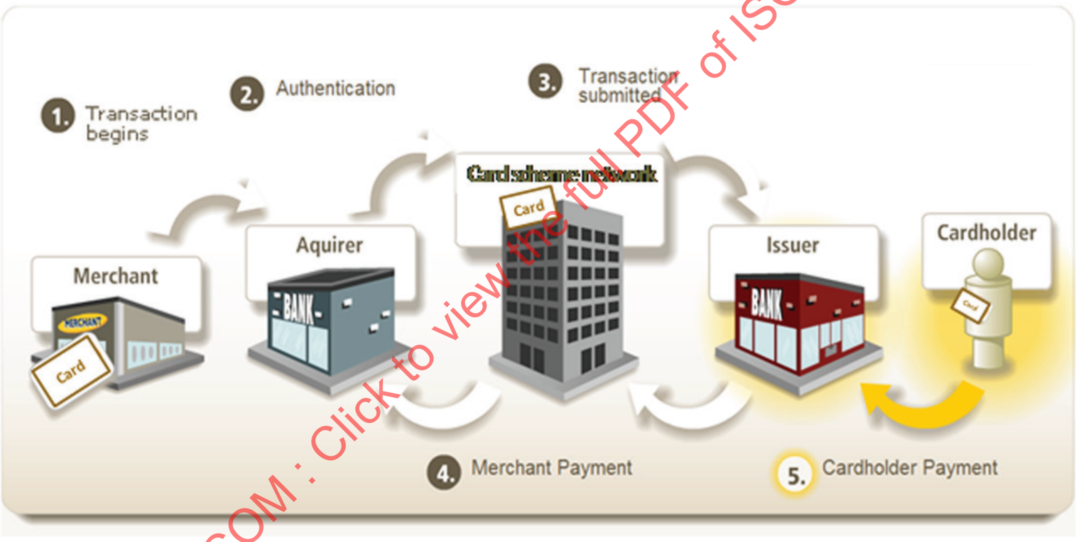


Figure A.1

[with thanks to MasterCard]

The payment industry uses a number of models to characterize payment processes. The process that generally underpins the use of payment applications for transport payment is shown in Figure A.1.

It is known as the “Four party domain” model, the domains being the merchant (the PTO in our case), the acquirer, the issuer and the cardholder. In this model, the merchant has a contract with and conducts all its payment business through its acquirer, irrespective of the issuer of the payment application or the type of payment application scheme used. This includes all commercial terms, evidences of equipment certification, requests for authorization, requests for payment, enquiries and chargebacks. The payment application scheme imposes its rules on the acquirer which may reflect them in the contract it has with a merchant.

The cardholder has a contract solely with the issuer. Payment application scheme rules that affect that relationship will also be included in that contract. Separately to his issuer contract, cardholder may also be required by the PTO to accept their conditions of carriage via a separate agreement.

On presentation of a payment application, the Merchant may request payment authorization from the Issuer via the Acquirer (“online authorisation”). In some cases, and especially in transit systems, payment may be made offline based on an authorization from the payment application itself. In either case a process of authentication is required to ensure that the payment application presented was genuine. Subsequently the Merchant makes a request for payment. The payment application scheme network links the Acquirer and the Issuer. It is the Issuer who produces the authorization response based on data generated by the payment application and its own secret keys. The Acquirer pays the Merchant on the basis of a settlement request and claims an equivalent payment from the Issuer. The Issuer will take payment from the Cardholder according to the contract terms, either immediately (with a debit card) or after a period of time (with a credit or charge card).

It is possible for Merchants and Issuers to have agreements to co-branded cards which carry both payment application scheme and Merchant branding and this is foreseen in the area of payment for transport. In this case, although the card has a Merchant brand on it, it is treated in exactly the same way as any other payment application, in terms of use, authorization and payment.

These co-branded/co-issued cards may be valid for more than one bank and/or one or more payment application schemes. In some cases however, the merchant (PTO) may even only accept these co-branded/co-issued cards, and issuer and acquirer roles may be ensured by the same payment institution.

So each PTO, as a merchant, may then partner directly with an issuer, an issuer/acquirer or just an acquirer.

A.2 Considerations of special cases of payment applications

There are certain types of payment applications that need consideration in the design of a scheme for transport payment based on payment institution-issued cards or co-branded cards.

A.2.1 Online authorization cards

The first type is cards that require online authorization, such as those magstripe emulation payment applications issued in the USA. If these are presented at a gate or validator then they can be treated the same as payment application that support offline authorization where the PTO allows "deferred authorisation" (see 6.5.2) and as long as the payment scheme requirements for authentication are met. In this case, PTO should accept the risk that payment authorization is declined after having given access to the cardholder. If PTO does not want to endorse such risk and wants to take transport payment at the point of access, an unusually fast (at least for 2011) communication network will be required to support online authorization. Otherwise, it will not be possible to use these online authorization cards because of the excessive time for the online authorization.

A.2.2 Prepaid cards

The second special case is cards that are not associated with a named bank account. Pre-paid cards are sometimes but not always provided to offer payment application functionality to those not normally able or entitled to hold a bank account, for example minors. These cards can be personal or anonymous and sometimes require online authorization. Similarly as for online authorization cards, PTOs should either use "deferred authorisation" after access and accept the risk to face a declined authorization or implement an usually fast (at least for 2011) communication network to support online authorization if they want to take transport payment at the point of access.

A.2.3 Purse cards

The third special case is where the card holds a purse that defines the amount of money that can be spent. For a transport network with back office centric fare computation, it is difficult to consider allowing this purse application to be used as there will always be a problem to keep the purse on the media in synchronisation with the amount of money left to spend, unless as for NFC phones there may be a means to remotely update the purse balance. Additionally, knowing that most purse applications are issuer specific, their acceptations will require a single integration into the validation terminals per issuer rather than per payment application scheme.