Visa Contactless
Transit Implementation Guide

August 2017

Version 1.0

Visa Confidential

Visa Confidential

The Visa Confidential label signifies that the information in this document is confidential and proprietary to Visa and is intended for use only by Visa clients and other third parties that have a current nondisclosure agreement (NDA) with Visa that covers disclosure of the information contained herein.

Changes are periodically added to the information herein. At any time, Visa may make improvements and/or changes in the product(s) and/or the programme(s) that are described in this document.

Every reasonable effort has been made to ensure the accuracy of information provided by Visa. Visa shall not be held liable for any inaccurate information of any nature, however communicated by Visa.

Document history

Version	Date	Author	Summary of Changes
1.0	August 2017	Nicolas Mackie Steven Orelowitz Stephen Beecroft Marc Ammundsen	Initial version

Referenced or related documents

References	Document	Author	Location
[VCPS]	Visa Contactless Payment Specification	Visa	Visa Online (VOL) or via acquirer for transit merchants.
[VMCPS]	Visa Mobile Contactless Payment Specification	Visa	Visa Online (VOL) or via acquirer for transit merchants.
[TTIG]	Visa Contactless Transit Terminal Requirements and Implementation Guide	Visa	Visa Online (VOL) or via acquirer for transit merchants.
[BOOK C-3]	EMV Contactless Specifications for Payment Systems Book C-3 Kernel 3 Specification	EMVCo	www.emvco.com
[PCI DSS]	Payment Card Industry Security Standards	PCI	www.pcisecuritystandards.org
[ISO27001]	Information technology, Security techniques, Information security management systems, Requirements	ISO	www.iso.org
[MIT]	Alignment of Authorization procedures for Merchant Initiated Transactions	Visa	Visa Online (VOL) or via acquirer for transit merchants.

Contents

Tables

Figures

1 About this document

1.1 Purpose

This document defines the requirements and provides guidelines for stakeholders involved in the acceptance and processing of Visa Contactless payments for automatic fare collection in mass transit systems.

1.2 Audience

This document is intended for the following clients:

- Transit merchants and their technology partners implementing contactless acceptance
- Financial institutions and payment service providers acquiring transactions for transit merchants
- Financial institutions issuing contactless-enabled cards (the definition of which includes mobile and other device form-factors).

1.3 Scope

This document provides requirements and recommendations to be considered when designing and building a mass transit system that accepts Visa Contactless cards as a method of automatic fare collection. It also introduces the principle activities that should be considered to prepare for a successful launch.

1.4 Document organization

This document has the following sections:

Table 1 - Document organization

Section	Description
About this document	Describes the purpose, audience, scope and organization of this guide.
Overview of Visa mass transit models	Describes the high level background and key features of each of the Visa mass transit models.
Mass Transit Transaction model	Describes the processes, rules, and potential impact to merchant, acquirer and issuer systems in accepting Visa Mass Transit Transactions.
Known Fare Transaction model	Describes the processes, rules, and potential impact to merchant, acquirer and issuer systems in accepting Visa Known Fare Transactions.
Transit merchant security requirements	Describes specific security requirements arising from the handling of transit transactions, and introduces lessons learned from current deployments.
Card personalization	Highlights the key personalization requirements for Visa Contactless cards (and other device form-factors).
Customer service	Describes the considerations that merchants and issuers should take into account when designing their customer service operations and systems.
Dispute resolution	Describes how disputes arising from contactless transit transactions should be handled.
Testing	Describes how testing should be carried out by clients for their respective host systems, terminals, or cards.
Deployment preparation	Provides a set of checklists to help prepare for launch.
MTT Custom Authorization model	This appendix describes an alternative model for custom processing of transit transactions for merchants who do not wish to Authorize every transaction at the end of each travel period, applicable in Europe region markets where floor limits for contactless transit transactions are not zero.
MTT handling of VCPS 2.0.2 cards	This appendix describes special processing required at a transit reader in order to accept cards compliant with previous generation Visa Contactless specification (i.e. VCPS 2.0.2).

1.5 Definitions

This document uses the following terms and abbreviations:

Table 2 - Definitions

Acronym or term	Description
AAC	Application Authentication Cryptogram
AD	Account Data (i.e. CHD and SAD), as defined in [PCI DSS].
Amount, Authorized	The data element included in a contactless transaction Authorization (Tag "9F02") that stores the amount for the current transaction, as transmitted to the card when it was tapped to the reader.
ARQC	Authorization Request Cryptogram
ATC	Application Transaction Counter
AVR	Account Verification Request. Request submitted to the issuer by the merchant to verify that the card has not been blocked as lost or stolen. AVR is not an Authorization request and will not verify the financial standing of the funding account.
Back Office	A component within a transit merchant's systems which process taps received from transit readers, and performs any or all journey construction, fare calculation, risk management, and payment processing.
CAP	Card Additional Processes. A data element within the payment application that indicates to the terminal the card's processing requirements and preferences.
Capping	A fare policy implemented by some transit merchants whereby the overall fare for a chargeable period (e.g. a day) may be limited to a threshold which gives the cardholder a favorable price compared to the sum of the individual journey prices.
Card Clash	May occur when more than one contactless card is presented to a transit reader. The outcome could vary depending on how it has been configured, but could include the reader denying entry to the transit system or the wrong card being debited.
CDCVM	Consumer Device Cardholder Verification Method
CHD	Cardholder Data, as defined in [PCI DSS].
Chargeback Threshold	The maximum fare amount that can be submitted to Clearing on an initial decline response for first card use or following any successful Authorization approval within the MTT model.

Acronym or term	Description
CoC	Conditions of Carriage. The terms under which a transit merchant accepts passengers for travel.
Contactless Card or Card	A cardholder payment device carrying the Visa payWave application. It may be implemented on a plastic card, a mobile phone, a wearable device, or an alternative form factor.
CVM (or CVL)	The Cardholder Verification Method (sometimes referred to as Cardholder Verification Limit) is used to evaluate whether the person presenting a payment device is the legitimate cardholder.
DDA	Dynamic Data Authentication. A cryptographic value generated by a chip on a card in an offline environment that uses transaction specific data elements and is verified by a chip-reading device to protect against skimming.
Deferred Authorization	A card present environment Authorization that is requested after the cardholder has left the point of transaction.
Deny List	Method for blocking cards that have not been accepted for travel within the transit merchant's system.
EMV	The international body that governs the standards used by chip-based payment cards and terminals.
ETM	Electronic Ticket Machine
fDDA	fast Dynamic Data Authentication. An optimized form of Offline Data Authentication.
GPO	Get Processing Options. A command used by the reader to request that a card performs a payment transaction.
Journey Construction	The process of analyzing individual taps received from transit readers and forming logical journeys performed by cardholders.
Known Fare Transaction (KFT)	A contactless transaction performed at the turnstile, gate, or point of boarding of a mass transit merchant where the fare amount is known prior to travel and tap of a Visa card.
Mass Transit Merchant	A Public Transport Operator or Authority (PTO) assigned MCC 4111, 4112, or 4131, which uses one or more of the models described in this document to accept Visa card payments.
Mass Transit Transaction (MTT)	A contactless transaction performed at the turnstile, gate, or point of boarding of a mass transit merchant where the final fare amount is calculated using data derived from one or more taps of a Visa card during a travel period.
MCC	Merchant Category Code

Acronym or term	Description
MIT	Merchant Initiated Transaction
MOTO	Mail Order/Telephone Order transaction
ODA	Offline Data Authentication. A method by which the reader requests and checks the authentication data received from the card to ensure it is genuine.
P2PE	Point to Point Encryption. P2PE is used to cryptographically protect Account Data (AD) from the point where the merchant accepts a payment card (the reader) until it reaches a secure decryption environment.
PAN	Primary Account Number
PAR	Payment Account Reference. A non-financial unique identifier assigned to each Visa payment account, in order to link payment activity across the ecosystem, and facilitate consumer identification without using sensitive cardholder data.
Passback or Pass-back	Merchant-specific processing to prevent a single card being used more than once in a given timeframe, to prevent cardholder misuse and potential revenue loss from period pass re-use.
Pay As You Go (PAYG)	Refers to a cardholder presenting a card at a transit reader to authorize travel without having previously paid for their journey.
PCI DSS	Payment Card Industry Data Security Standard. A standard that ensures that card and payment data are stored, processed, and transmitted in a secure manner.
Pre-purchase	Refers to a cardholder purchasing their ticket or other transit product as a right to travel before they present it at a transit gate or reader.
PTO	Public Transport Operator or Authority
QSA	Qualified Security Assessor, as defined in [PCI DSS].
RoC	Report on Compliance
STIP	Stand-In Processing. Service in which Visa will act on behalf of an issuer in the Authorization process.
SAD	Sensitive Authentication Data, as defined in [PCI DSS].
Tap	Refers to the act of presenting a contactless card at a transit reader. Sometimes referred to (outside of this document) as “touch”.

Acronym or term	Description
Tap Data	The data that is captured at a tap for future use by a mass transit merchant, which may include time and date of tap, mode of transport, and any additional data relevant to fare calculation.
TC	Transaction Certificate
Tokenized PAN	A secure value that replaces and uniquely identifies a PAN, using different representation from the original PAN.
Transaction Identifier	Also known as Tran ID. This is a unique identifier assigned to each transaction submitted by a mass transit merchant's acquirer as part of the Authorization and Clearing messages.
Transit Gate or Gate	A physical barrier which controls access to a transit system. Incorporates a transit reader.
Transit Reader or Reader	A Visa-approved contactless reader to which the cardholder presents their contactless card to gain access to a transit system.
Travel Period	A fixed period of time (typically 24 hours, but can be intra-day) within which a merchant performing Mass Transit Transactions accumulates journey data for a passenger.
Visa Contactless	Also known as "Visa payWave" or simply "contactless". It is a method of initiating a card-present transaction using a short-range radio communication from a card in compliance with Visa Mobile/Contactless Payment Specifications (VCPS/VMCPS).
VOL	Visa Online. A repository for Visa documentation and other stakeholder supporting materials.

1.6 Document conventions

The following table lists the conventions used in this document:

Table 3 - Document conventions

Convention	Description
Important	Highlights important text in the guide
Note	Provides more information about a topic
Italics	Indicates document titles or specific data elements

1.7 Requirement terminology

The terminology for requirements and recommendations are as follows:

- Use of the word "must" denotes a mandatory requirement
- Use of the word "should" denotes a recommendation
- Use of the word "may" denotes an optional feature

1.8 Visa requirements

Requirements derived from the *Visa Core Rules and Visa Product and Service Rules* ("*Visa Rules*") specific to mass transit are embedded in this document as requirements. Each requirement is included in the following format:

> ***Requirement Number: Rule Subject***
>
> ***(Rule: See ID# of the Visa Rules)***
>
> *An extract of the key elements of the rule*

The summaries of the rules for mass transit found throughout this document are provided for information only. Please refer to the current version of the *Visa Rules* for the full definition of the relevant rule.

Some information found in this document refers to VisaNet transaction processing requirements, which are applicable only where Visa processing is used.

1.9 For further information

For further information about Visa mass transit models, or for questions about this document, issuers and acquirers may contact their Visa representative. Mass transit merchants should contact their acquirer.

2 Overview of Visa mass transit models

Transit merchants vary in terms of size and network complexity. The fares charged can be affected by:

- Single or multiple modes of transport (e.g. bus, metro, and trams)
- Distance or route travelled and/or time of journey
- Concessionary fares (e.g. the elderly, students, or staff)
- Fare capping policies that impose limits on the amount charged

Visa has developed four flexible models that enable the acceptance of "open-loop" payment cards based on contactless EMV technology for fast, convenient, and secure automatic fare collection within transit environments, as described in the following table.

Table 4 - Visa mass transit models

Model	Description	Examples
Mass Transit Transaction (MTT) model	The Visa Contactless card is used at points of access to the transit service on readers that accept contactless payments only. The final fare charged is not always known at the time of travel, but is calculated at the end of a travel period (typically 24 hours, but can be intra-day) by the PTO based on journeys made during that period.	The transit reader may be connected to a gate or turnstile. Some PTOs may require the card to be used at entry-only, while others may require use at entry and exit. The reader may charge flat, distance, or time based fares.
Known Fare Transaction (KFT) model	The Visa Contactless card is used at points of access to the transit service where the fare charged is always known by the reader, which accepts contactless payments only.	An on-vehicle transit reader which may either charge flat or distance based fares.
Visa Access Credentials model	Travel has been paid for in advance and the same Visa Contactless card is used as a credential or "authority to travel" in place of a ticket. This model is not discussed further here.	Pre-purchase ticket, then card is used as an authority to travel by tapping on a transit reader.
Retail model	A ticket is purchased using a card at a terminal which accepts all Visa card payments, and the ticket (paper or smart) is used to access the transit system. This model is not discussed further here.	A ticket vending machine, a ticket office, a bus contact and contactless ticket terminal.

2.1 At a glance – Comparing MTT and KFT models

The following table explores the key differences between the MTT and KFT models that are described in this document:

Table 5 - High-level comparison of MTT and KFT models

Characteristics	MTT	KFT
Designed for very high customer throughput	Yes	Yes
Fare amount always known at the time the journey is started	No	Yes
Transit reader accepts contactless payments only	Yes	Yes
Intended for complex fares, including "capping" or multi-modal	Yes	No
Allows accumulation of multiple journeys into a single transaction	Yes	No
Account Verification Requests performed on card's first use	Yes	No
Special liability model included (Chargeback Threshold)	Yes	No
Requires declined cards to be blocked using deny lists	Yes	No
Requires merchant back office for fare calculation	Yes	No
Intended Authorization model	Deferred	Real-time
Authorization resubmissions for debt recovery	Yes	Yes

3 Mass Transit Transaction model

3.1 MTT Overview

The Mass Transit Transaction (MTT) model is a "pay as you go" model where the fare for each journey may not be known at the point at which the card is tapped on the transit reader. Regardless of whether the fare is known or not, tap data is accumulated, and the total fare amount is calculated and charged by the transit merchant at the end of the travel period.

The key characteristics of this model are:

- Transit readers accept contactless payments only (no chip & PIN or magnetic stripe)
- When a card is tapped on a reader it is authenticated and tap data is generated
- Cards are checked against a deny list before the cardholder can be accepted for travel
- Taps are accumulated in a back office system (typically operated by the merchant) and the amount to be charged is calculated at the end of the travel period
- An MTT should be submitted online as a deferred Authorization at the end of the travel period where the amount charged is equal to the fare calculated
- Liability is shared between the merchant and issuer through a defined MTT liability framework

This shared liability framework – sometimes referred to as the "first ride risk" framework – provides limited protection to merchants for the first declined transaction on a Visa Contactless card up to a defined MTT Chargeback Threshold. Eligible transactions may be sent to Clearing, and may not be charged-back, even if the Authorization request is declined by the issuer. For transaction amounts above the threshold, liability is accepted by the merchant.

Financial risk is managed by:

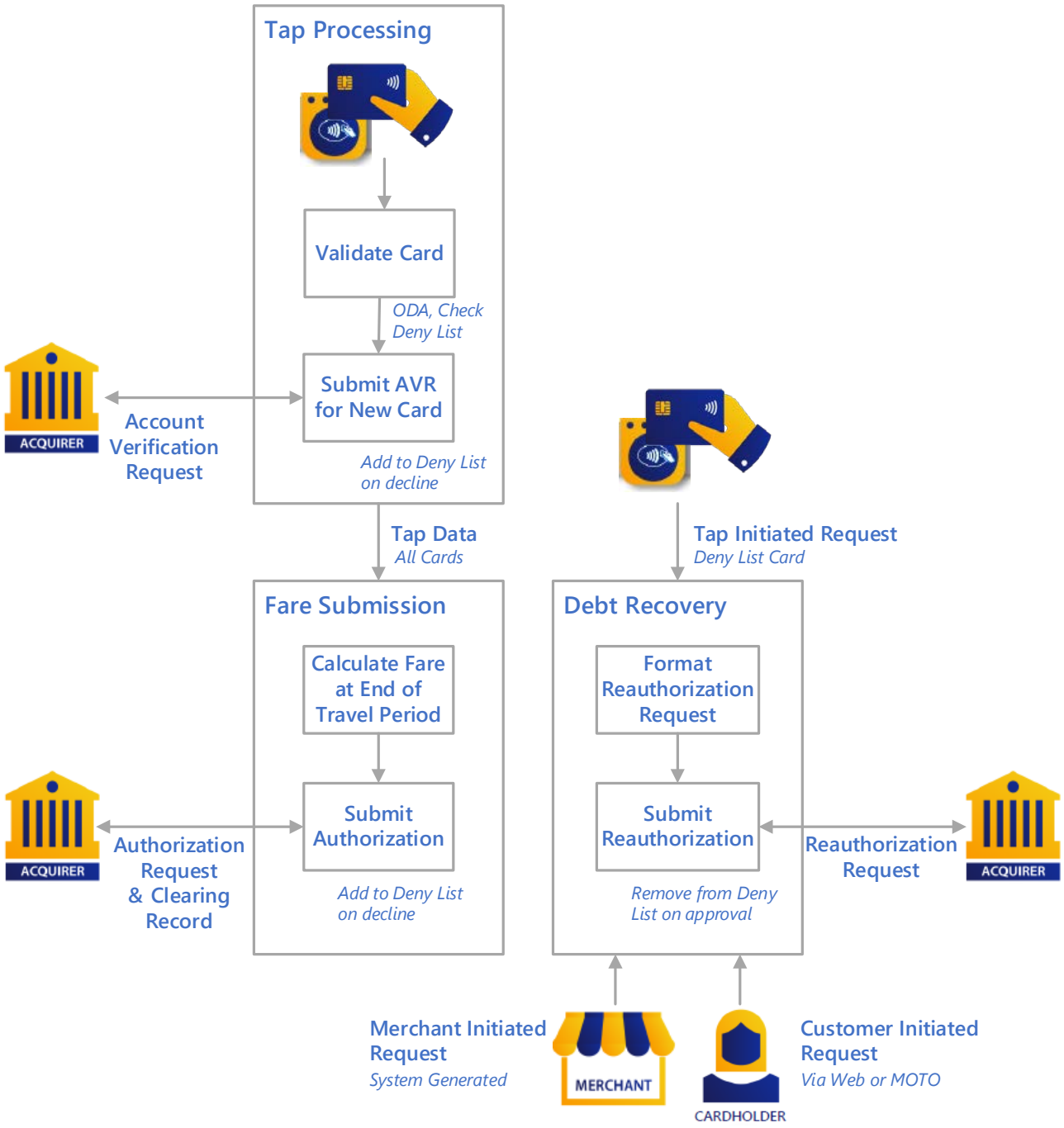
- Using Offline Data Authentication (ODA) to authenticate that the card is genuine when it is tapped on the reader. Cards which fail ODA should not be accepted for travel
- Performing an Account Verification Request (AVR) immediately after a contactless card is first used on a PTOs network, to quickly identify cancelled, lost, or stolen cards
- Centralizing tap data frequently (typically at *least* every hour)
- Authorizing and/or Clearing each transaction no later than the end of the travel period, to limit the total amount of any outstanding fares due to the transit merchant
- Maintaining and updating deny lists frequently to prevent cards from being used for further travel where an Authorization request has been declined by the issuer
- Resubmitting previously declined Authorization requests, in attempt to recover debt owed to the transit merchant (e.g. unpaid fares), and remove cards from the deny list if a subsequent Authorization request is approved

The MTT model is designed to be attractive to multi-modal metropolitan PTOs with the need for high passenger throughput and/or where complex fare calculation policies are operated.

3.2 Processing overview

A high-level overview of the MTT model is given in Figure 1.

Figure 1 – Overview of the MTT model



This section describes how the MTT model may be implemented, covering the following key areas of functionality as illustrated above:

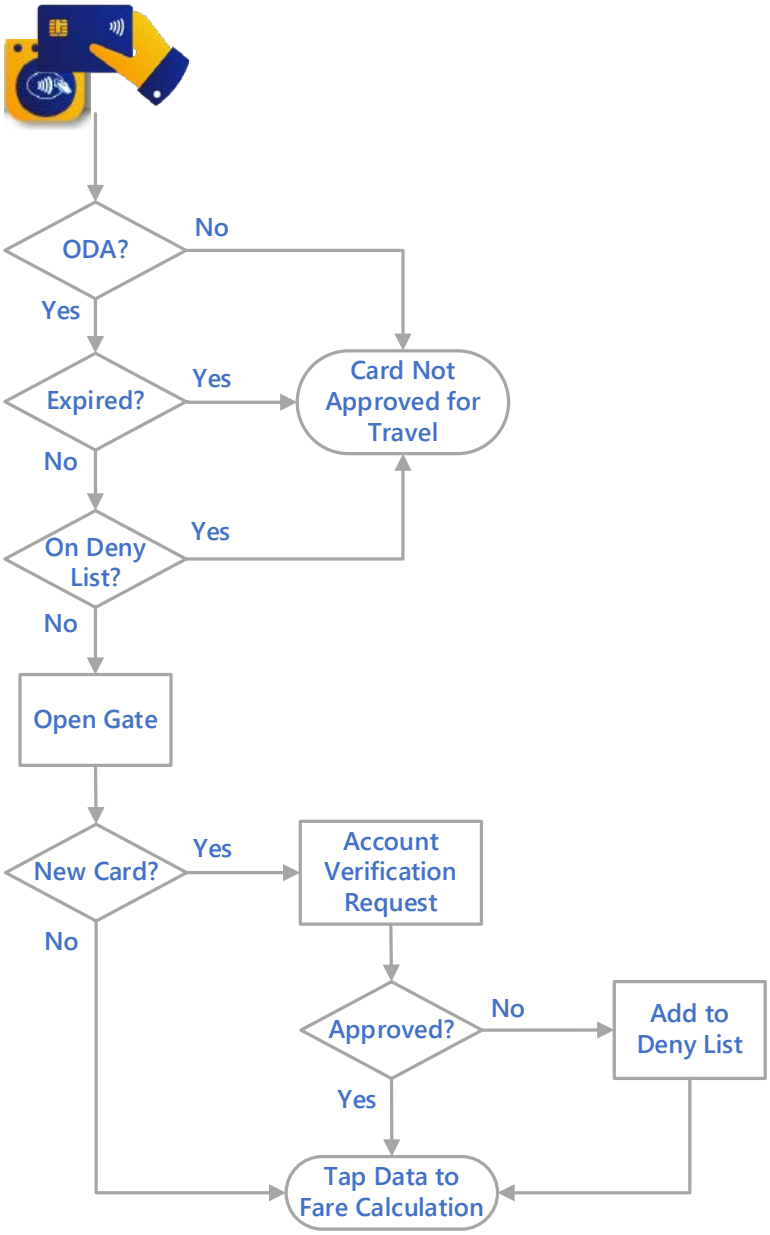
- Tap processing – describing how the tap and validation of the card is performed
- Fare calculation and submission – clarifying the functionality required to encode and submit transactions for Authorization and Clearing

- Debt recovery – explaining how merchants can attempt to recover any unpaid fares
- Transaction processing – describing how key Visa processing fields must be used
- Exception handling – outlining some of the most common exception events that should be considered and handled

3.3 Tap processing

Tap processing is how cards are handled at a transit reader to support an MTT. For a full technical description of contactless processing requirements, please refer to [VCPS], and for full details of the additional requirements for MTT acceptance please refer to [TTIG].

Figure 2 – Tap processing



Note A Visa card cannot "fall-forward" to a chip & PIN transaction at a contactless-only transit reader since such a terminal does not support a PIN entry device and is configured as such (see [TTIG] for details). According to [VCPS] it is not therefore possible for a Visa card to be rejected on the grounds that it attempted to fall-forward.

3.3.1 Offline Data Authentication (ODA)

In order to authenticate the card, the reader performs ODA (specifically *fast Dynamic Data Authentication*, fDDA) as part of a zero value local currency transaction. ODA must be performed successfully in order to consider the card eligible within the MTT model.

Note Successful completion of ODA means that the terminal can rely on the card details being genuine and unaltered since it was issued.

Important If ODA fails, or if ODA is not returned by the card, the reader should reject the card and regard it as not accepted for travel within the MTT model.

> ***Req 01: Mass Transit Merchant Requirements***
> ***(Rule: See ID# 0030050)***
> *An Acquirer must ensure that its Mass Transit Merchant performs Offline Data Authentication (ODA) using fast Dynamic Data Authentication (fDDA).*

3.3.2 Expiry date check

Transit merchants should reject expired cards since there is a risk that the deferred Authorization may be declined at the end of the travel period. Refer to [TTIG] for details.

Note Transit merchants should ensure that the reader date settings are accurate to avoid false acceptance or rejection of cards based on their expiry date.

Important Issuers must be aware that cards that have expired may be rejected by transit readers.

3.3.3 Deny list check

The transit merchant is required to block cards that receive a decline response to an Authorization or AVR. Most transit merchants operate a deny list that is stored on, or accessible to, the transit readers. The list comprises of card data (typically non-reversible hashed PANs). If a tapped card is on the deny list, the card should not be accepted for travel.

Important Any card data held on a deny list must be secured as described in section 5.

Note The deny list is normally managed in the transit merchant's back office system and shared with the transit readers. Depending on performance and throughput requirements, it may be possible for transit readers to lookup a deny list that is held centrally in the back office. However, typically, a copy of the deny list is held on the transit reader, and changes (or "deltas") are broadcast regularly to all readers in order to synchronize them.

3.3.4 New card check

The transit merchant must be able to identify if a card is being used for the very first time on its transit services or system.

If the card has not been used before on a PTOs network (i.e. it is a new card) an Account Verification Request (AVR) must be performed as soon as possible after the card is tapped at the reader and the cardholder is accepted for travel. This enables transit merchants to minimize financial loss from lost or stolen cards.

> ***Req 02: Mass Transit Merchant Requirements***
> ***(Rule: See ID# 0030050)***
> *An Acquirer must ensure that it's Mass Transit Merchant:*
> - *Submits an Account Verification when a Card is first used at the Merchant*
> - *Blocks a Card from being used for travel within 1 hour of receiving an Account Verification decline response from the Issuer*

If the card has been used previously then there is no need for the transit merchant's back office to perform an AVR, although transit merchants are free to use AVRs periodically in accordance with their risk appetite (e.g. some transit merchants might consider all cards as "new cards" every 14 days).

An AVR requires the following processing:

- AVR messages have a similar format to an Authorization, with key differences being that the transaction amount data (*Amount, Authorized*) is always set to zero and the POS Condition Code data in Field 25 is set to "51". Message formats are detailed in Table 7 of section 3.6 below
- Issuers will respond to AVRs in Field 39 with "85" (No Reason to Decline) if the account is in good standing and the card can be accepted for travel

Important If the issuer declines an AVR, the transit merchant is liable for any journeys using that card after the first hour. To minimize this risk, transit merchants should ensure no further acceptance of the card by immediately placing it on the deny list as described in sections 3.3.3 and 3.4.3.

- Where the issuer has declined the AVR, the transit merchant should still submit the transaction at the end of the travel period for Authorization and Clearing based on the charge for the journey(s) completed within the first hour after the AVR decline response was received. Acquirers have chargeback protection up to the MTT Chargeback Threshold

3.3.5 Deferred Authorization

Transit merchants that defer online Authorizations must submit the request in accordance with the *Visa Rules*.

3.3.6 Transit merchant proprietary processing

In addition to the transaction processing required at the transit reader by [VCPS] and [TTIG], merchants may implement their own specific processing based on their fare policies. For example, many transit merchants implement "pass-back" checks to prevent multiple passengers using the same card at the same reader, gate, or station within a given timescale, in contravention of the merchant's conditions of carriage.

Note Visa places no limit on proprietary processing, however transit merchants should be aware that if the PAN is used for establishing the card identity, it is only available at completion of the GPO command, and must be protected (see section 5).

3.3.7 Transit merchant revenue protection devices

Transit merchants may use readers, typically portable terminals, to verify passenger compliance with the PTO's fare policy. Such a device performs the same function as a conventional reader (i.e. it authenticates the card, checks the deny list, and generates tap data which is sent to the merchant's back office). As such, these devices are subject to the same requirements and certification as readers installed elsewhere on the transit network.

3.3.8 Previous generation cards

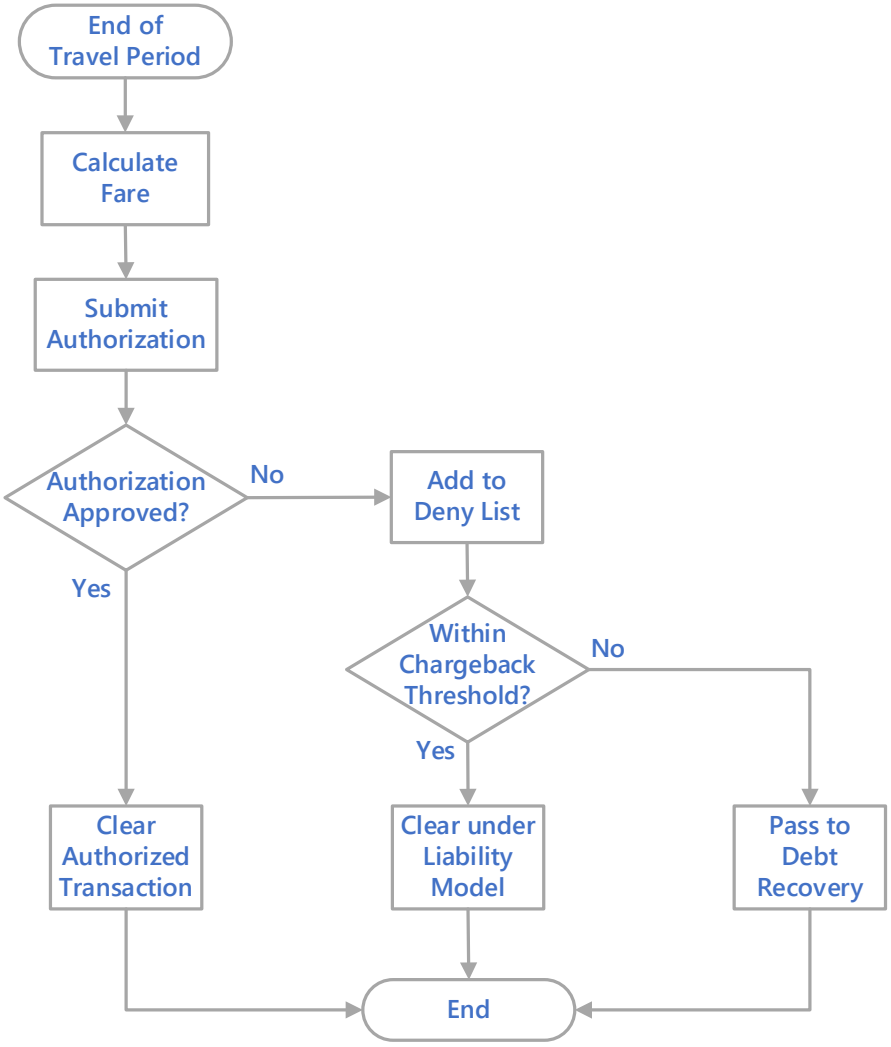
Transit merchants operating in markets with a large volume of previous-generation VCPS 2.0.2 cards may seek Visa approval to implement special transit reader processing to maximize acceptance of these cards. See Appendix B for details.

3.4 Fare calculation and submission

To implement the MTT model, the transit merchant requires a back office system to calculate the fare based on the taps from a card accumulated during the travel period, before a transaction can be submitted to Authorization and Clearing.

An overview of the typical processes is given in Figure 3.

Figure 3 – Fare calculation and submission



3.4.1 Fare calculation

For each card used for contactless travel during the travel period, the transit merchant will use tap data gathered from the readers to determine the journeys made and calculate the fare that will be charged. The methods used for journey calculation and fare pricing policies are outside the scope of this document, as the PTO may wish to operate a flat, distance, or time based (or multi-modal combination) fare structure to suit their needs.

Important Transit merchants must ensure that the methods and amounts used to calculate travel fares are clear and readily available to its customers.

3.4.2 Authorization requirements

No later than the end of the travel period, the transit merchant must request an online Authorization for each transaction.

This approach substantially simplifies the implementation within the transit merchant's back office systems, improving reconciliation, simplifying transaction dispute and chargeback processes, and ensuring full compliance with the MTT model.

Req 03: Mass Transit Transaction Authorization Requirements
(Rule: See ID# 0030049)
A Merchant performing a Mass Transit Transaction must submit an Online Authorization Request at the end of each travel period

For transit merchants based in Europe an alternative MTT Custom Authorization model is available as described in Appendix A. However, for new implementations this approach is not recommended by Visa.

3.4.2.1 Card sequence number

Important Although this data element (EMV data tag 5F34) is defined as optional within the [VCPS], this only means it is optional for an issuer to include it within their contactless-enabled card. It is essential that, if it is retrieved by the reader from the card presented by the cardholder, all transit acceptance and acquirer data processing systems must forward this data element unaltered as part of the Authorization message and Clearing record sent on to the issuer. This data element is used in the validation of the online authentication process, and if it is not returned correctly when present in the card, will cause the Authorization to be declined.

3.4.2.2 Authorization amount

A transit merchant must submit an Authorization request for the final transaction amount.

Req 04: Authorization Amount Requirements
(Rule: See ID# 0025596)
A Transit Merchant must submit an Authorization Request for the final transaction amount.

3.4.2.3 Transaction date

The transaction date must be the day of the last tap in the travel period.

Req 05: Transaction Date Limits
(Rule: See ID# 0005753)
For a Mass Transit Transaction, the Transaction Date must be the last day on which a journey took place.

3.4.2.4 Purchase date

The purchase date will be the day of the first journey made in the travel period, as this date should appear on the issuer statement.

Important Acquirers must ensure that the purchase date in the Clearing record is the day the cardholder took the first journey in that travel period. In cases where the merchant's transaction processing day is not on the same calendar day as the first journey was made, the purchase date must be set to the day the cardholder first used their card for travel.

3.4.3 Deny list management

Transit merchants must add cards to the deny list within one hour of receiving a decline response to an Authorization request (or AVR) in order to ensure the card is not accepted for travel.

> ***Req 06: Mass Transit Merchant Requirements***
> ***(Rule: See ID# 0030050)***
> *A Transit Merchant must block a Card from being used for travel within 1 hour of receiving either: a decline response; or an Issuer response to an Account Verification Request indicating that the transaction should not be completed with that Card.*

Transit merchants must remove cards from the deny list within one hour of receiving an approval response to an Authorization request, in order to ensure the card is accepted for travel as soon as possible after an issuer approval.

Important Merchants must prevent declined cards from entering the system until an Authorization approval has been received from the issuer.

It should be possible for a customer to establish if their card is on a deny list and the process for its removal. The PTO is responsible for this element of customer servicing.

> ***Req 07: Mass Transit Merchant Requirements***
> ***(Rule: See ID# 0030050)***
> *Upon receipt of an approval response to an Authorization Request, the travel block on a Card must be removed within 1 hour.*

3.4.4 Clearing

Transit merchants may submit a transaction to Clearing if the Authorization was approved by the issuer.

An MTT should be submitted for Clearing no later than the timeframe specified in the *Visa Rules*, which is typically within 8 days from the end of the travel period. Most mass transit merchants will aim to submit transactions to Clearing on the calendar day following the end of the travel period unless a "late data" scenario has occurred.

Req 08: Acquirer Processing Timeframes
(Rule: See ID# 0027796)
An Acquirer must process transactions within the timeframes specified in the "Acquirer Processing Timeframe Requirements" table in the Visa Rules.

With the exception of transactions that are eligible under the MTT Chargeback Threshold, merchants are liable for all transactions where the Authorization request is declined by the issuer.

3.4.4.1 MTT Chargeback Threshold

The MTT Chargeback Threshold, also sometimes referred to as "first ride risk protection" for mass transit merchants, aims to mitigate the risk and exposure and distribute liability for an MTT where the Authorization at the end of the travel period is declined by the issuer.

Req 09: Mass Transit Merchant Requirements
(Rule: See ID# 0030050)
If the Transit Merchant receives a decline response from an Issuer, it may submit a Clearing record for that MTT only if all of the following apply:
- *The transaction is a domestic transaction or an intraregional transaction*
- *Either: the transaction is the first transaction on the Card at the Merchant or the previous Mass Transit Transaction for which Authorization was requested received an approval response*
- *ODA using fDDA was performed*
- *The transaction amount is less than or equal to the market or region specific values specified in the MTT Chargeback Thresholds of the Visa Rules*

The transit merchant may therefore submit an MTT to Clearing if the issuer declined the Authorization request, providing:

- The issuer declined in response to the *very* first MTT Authorization request for this card
- The issuer declined in response to the first MTT Authorization request for this card *since a previous* MTT Authorization approval response
- The transaction amount is *less than or equal to* the MTT Chargeback Threshold

Transit merchants are not permitted to submit transactions to Clearing where the amount has been reduced to meet the criteria governing the MTT Chargeback Threshold. The practice, which is sometimes referred to as "part-clearing" represents a violation of compliance with the MTT rules.

Req 10: Mass Transit Merchant Requirements
(Rule: See ID# 0030050)
For a transaction that received a decline response, a Transit Merchant must not submit a Clearing record with a lower transaction amount in order to meet submission criteria.

Important Acquirers must ensure that an MTT that is cleared under the MTT Chargeback Threshold is correctly labelled with the value of "VFT000" in the Authorization response code of the Clearing record.

3.5 Debt recovery

A small proportion of transaction Authorization requests may be declined by issuers. In some cases, this may be for financial reasons, due to cyclical variations in an account balance (e.g. where a cardholder has insufficient funds before a salary payment is received).

To enable cards to be accepted for travel again once the account returns to good standing, a transit merchant may re-attempt to Authorize the transaction (i.e. to unblock the card for travel). If an approval response is given by an issuer to a debt recovery transaction, the transit merchant must remove the card from the deny list within one hour of receiving the Authorization approval.

In general, transit merchants will submit debt recovery transactions where the amount of the re-attempted Authorization request is equal to the outstanding debt (i.e. the unpaid fares amount).

Req 11: Mass Transit Merchant Requirements
(Rule: See ID# 0030050)
To obtain an approval response, a Transit Merchant must request online Authorization using either of the following amounts:

- *The amount of any outstanding fare*
- *If no fare is outstanding, the transaction amount that was cleared following the decline response, and the Authorization request must then be reversed*

Upon receipt of an approval response, the travel block must be removed within 1 hour.

3.5.1 Data fields in debt recovery

The methods of debt recovery re-attempted Authorization requests permitted on the following channels are identified by the values in specific data fields given in the table below. For MITs, these data fields are additional to those introduced in section 3.5.3 below.

Table 6 - Key fields used in debt recovery Authorizations

		Card Present	POS Entry Mode Field 22	POS Condition Code Field 25	Chip Data present	CVV2 present
Merchant Initiated Transactions		No	01	00	No	No
Cardholder Initiated	Tap	Yes	07	00	Yes	No
	MOTO	No	01	08	No	Yes
	E-commerce	No	01	59	No	Yes

Important Issuers must not automatically send a decline response based solely on a missing CVV2 for resubmitted MITs originating from a mass transit merchant.

3.5.2 Zero amount debt scenario

In some cases, the outstanding debt may in fact be zero, since a Clearing record may have been submitted under the MTT Chargeback Threshold, yet the card is blocked since the issuer declined the Authorization request.

In this scenario, the Authorization amount should be equal to the amount that was previously submitted to Clearing under the MTT Chargeback Threshold. In the event that the Authorization request is approved by the issuer, the merchant must immediately reverse this transaction, and ensure the card is removed from the deny list.

To facilitate an optimal cardholder experience, transit merchants should support the debt recovery mechanisms described below.

3.5.3 Merchant initiated

Merchants may resubmit a declined Authorization request under the *Merchant Initiated Transactions* framework, see [MIT]. This can be done automatically via a system generated submission process in the merchant's back office.

Req 12: Resubmission following a Decline Response to a Transit Transaction (Rule: See ID# 0030046)

An Acquirer that has received a Decline Response to a transaction that originates from a Mass Transit Merchant may enter that transaction into Clearing if the following applies:

- *The Merchant has received an approval response to a subsequent Authorization request that included the data from the original transaction*
- *The Merchant has not submitted either:*

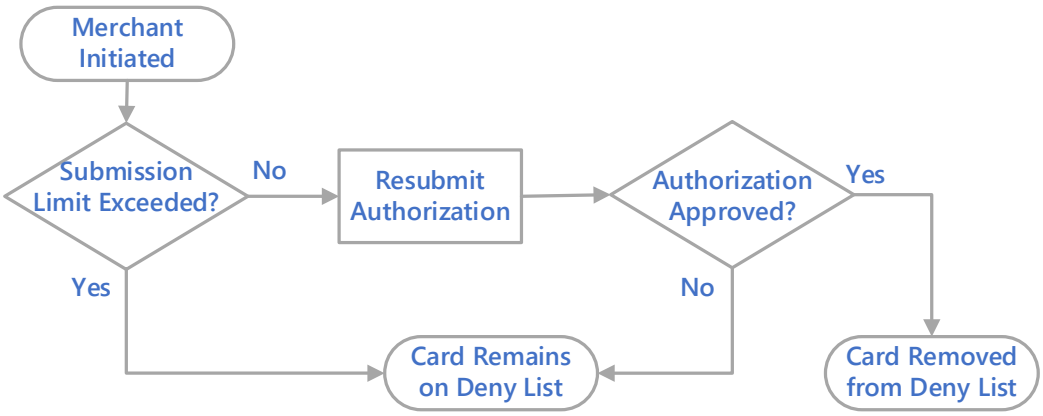
- For a KFT, more than 2 Authorization Requests within 14 calendar days of the initial decline response

- For an MTT, following the initial decline response, more than the number of permitted Authorization requests within the market or region timeframes specified in the MTT Decline Response Thresholds of the Visa Rules

For transit merchants operating within the MTT model, this policy typically allows up to four resubmissions to Authorize within a 14 calendar day period since the original contactless Authorization request was declined. The number of resubmissions within the MTT model can vary depending on the market or region as defined in the *Mass Transit Transaction Processing Requirements* table in the *Visa Rules*. Merchants should limit the response codes that they submit system generated re-attempted Authorization requests for to align with the [MIT] framework and mitigate further unnecessary decline responses.

A typical process for merchant initiated debt recovery is illustrated in Figure 4.

Figure 4 – Merchant initiated debt recovery



In this example for the *Europe* region, merchants operating within the MTT model are permitted up to *six* Authorization resubmissions within 14 days. The first resubmission could be attempted two days after the original Authorization request was declined, and if this is also declined, a second resubmission may be attempted after five days, and so forth.

Important All transit merchant system generated Authorization requests must be submitted as *Merchant Initiated Transactions*, see [MIT].

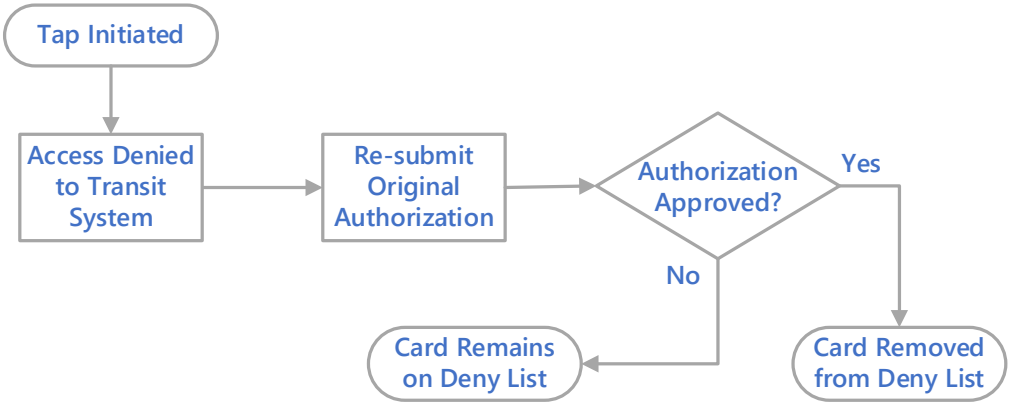
In the resubmitted Authorization request, the [MIT] framework requires the transit merchant to identify the transaction was initiated as an MIT and:

- Identify the intent of the MIT by specifying Reason Code 3901 (Resubmission) in the message Reason Code (Field 63.3) of the transaction
- Provide proof of a preceding transaction by using the Transaction Identifier (i.e. Tran ID) of the original transaction in the Tran ID data field (Field 62.2 or Field 125, Usage 2, Dataset ID 03). The same principle applies even if there is more than one resubmission. Please see Table 6 above for further information.

3.5.4 Tap initiated

A cardholder attempting to use a blocked card at the merchant's transit reader may create a fresh debt recovery Authorization request. While the card will not be accepted for travel, the tap may be used to trigger a fresh contactless Authorization request using the chip data from the tap.

Figure 5 – Tap initiated debt recovery

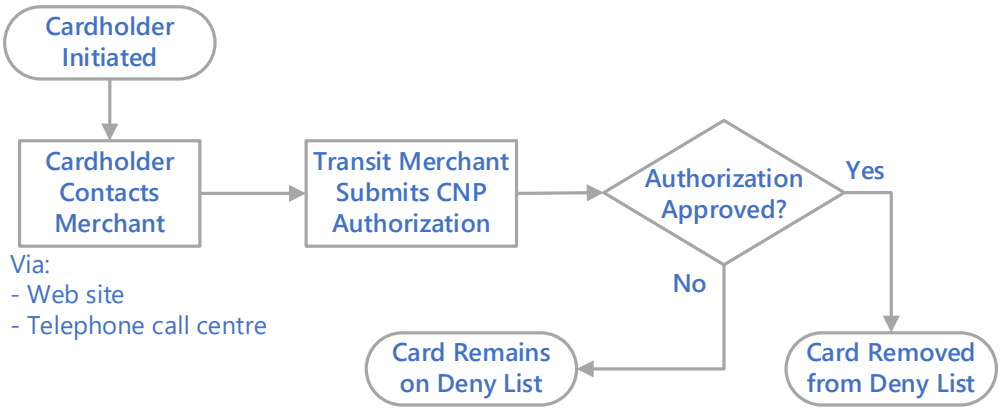


There are no specific limits on the number of Authorization re-attempts that a cardholder can initiate in trying to pay unpaid fares and/or unblock their card for travel.

3.5.5 Cardholder initiated

A Cardholder may also be invited by the merchant to pay unpaid fares (or unblock their card if the debt is zero) via a website, call center or other means. On receipt of approval of a re-submitted Authorization request, the transit merchant must remove the card from the deny list within one hour.

Figure 6 – Cardholder initiated debt recovery



There are no specific limits on the number of Authorization re-attempts that a cardholder can initiate in trying to pay unpaid fares and/or unblock their card for travel.

3.5.6 E-commerce initiated

E-commerce debt recovery transactions should be secured by Verified by Visa, as described in the relevant section of the *Visa Rules*.

3.6 Transaction processing

3.6.1 Transaction Identifier

Transactions originating from a transit reader operating under the MTT model must be identified correctly, as per the *Visa Rules*. The Tran ID that is generated during Authorization should be used for the corresponding Clearing record.

3.6.2 Transaction data fields

Important For an MTT, acquirers and issuers should not expect a match between the cryptogram amount in Field 55 and the transaction amount specified in Field 4.

The important data fields and values in the AVR, Authorization, and Clearing messages for an MTT are shown in the following table:

Table 7 - MTT data fields

Authorization	Clearing	Value	Remarks
Amount, Transaction Field 4	Source Amount TCR 0 Position 77-88	Variable	For an MTT, the values here will not match the value of tag 9F02 in Field 55.
Transmission Date and Time Field 7	N/A	Variable	The value here must contain the date and time at which the acquirer submits the Authorization message.
Merchant Category Code Field 18	MCC TCR 0 Position 133-136	4111 4112 4131	Indicates a transit merchant: 4111: Local and Suburban Commuter Passenger Transportation, including Ferries 4112: Passenger Railways 4131: Bus Lines
POS Entry Mode Field 22.1	POS Entry Mode TCR 0 Position 162-163	07	Indicates a contactless-read transaction.
Card Sequence Number Field 23	Card Sequence Number TCR 7 Position 7-9	Variable	EMV data tag 5F34, which if present in the card personalization and received by the reader, must be forwarded to the acquirer.
POS Condition Code Field 25	N/A	00	Authorization
		51	Account Verification Request

Authorization	Clearing	Value	Remarks
ICC Related Data Field 55 - Transaction Date Tag 9A (Field 146 for third bitmap issuers)	Terminal Transaction Date TCR 7 Position 10-15	Variable	Transaction Date
ICC Related Data Field 55 - Amount, Authorized Tag 9F02 (Field 147 for third bitmap issuers)	Cryptogram Amount TCR 7 Position 87-98	0.00 (or 0.01 only for VCPS 2.0.2 cards)	For an MTT, the values here compared to Field 4 will not match.
Terminal Type Field 60.1	Acceptance Terminal Indicator TCR 1 Position 124	3	The value here must be set to an Unattended Cardholder Activated Terminal (UAT). See [TTIG].
Terminal Entry Capability Field 60.2	POS Terminal Capability TCR 0 Position 158	8	Indicates that the terminal had a contactless reader only (i.e. no contact chip/magstripe capability).
Cardholder ID Method Indicator Field 60.9	Cardholder ID Method TCR 0 Position 160	3	Unattended Terminal, no PIN pad.
Local Transaction Date Field 13	Purchase Date TCR 0 Position 58-61	Variable	The values here should contain the date on which travel first took place.

3.6.3 Dates in Authorization and Clearing

The merchant's travel period can start and end on different calendar days even if operating a 24 hour one. For example, from 04:30am on (calendar) day 1 to 04:29 on (calendar) day 2. A journey that commences on day 1 and finishes on day 2 must be identified in Clearing (TCR0 Position 58-61, Purchase Date) with the date corresponding to day 1. This will appear on the issuer statement.

Table 8 below shows the dates used in Authorization and Clearing message data field for a typical MTT with a card used at a transit reader. Table 9 below shows the dates used in Tap initiated debt recovery transaction.

Table 8 - Dates used for an MTT

	Field 7	Field 55	TCR0 Pos 58-61	TCR7 Pos 10-15
Authorization	Date and time at which acquirer submits the request	Date of the last tap in the travel period	N/A	N/A
Clearing	N/A	N/A	Date of the first tap in the travel period	Date of the last tap in the travel period

Table 9 - Dates used for a tap initiated debt recovery transaction

	Field 7	Field 55	TCR0 Pos 58-61	TCR7 Pos 10-15
Authorization	Date and time at which acquirer submits the request	Date from the tap that initiated the debt recovery transaction	N/A	N/A
Clearing	N/A	N/A	Date of the first tap in the original travel period	Date from the tap that initiated the debt recovery transaction

3.6.4 Transaction Authorization amount

The transaction amount in Field 4 will indicate the actual amount calculated by the transit merchant's back office. This is the amount to be charged to the cardholder.

For an MTT, the cryptogram amount in Field 55 tag 9F02 (or in the case of a third bitmap issuer in Field 147) will be zero, or one minor currency unit.

3.6.5 Acquirer transaction processing

This section describes the impact of an MTT from the acquirer viewpoint.

3.6.5.1 Cryptogram and Cryptogram data

The cryptogram included in online Authorization and Clearing messages may be a Transaction Certificate (TC) or an (ARQC). The transit merchant must use the chip data from the most recent available tap they received from their terminals, and recorded in their back office system, for that travel period.

Important Acquirers must ensure that chip data in the online message is identical to the data received from the card during the last transaction tap performed at a transit reader.

The data fields forming the Authorization request are given in Table 7 above.

3.6.5.2 Merchant name and location

Cardholders are encouraged to contact the transit merchant for assistance with fare payments. To help passengers make contact, transit merchants must pass their contact details to issuers in the *Merchant Name and Merchant City* fields of Clearing messages. In

turn, issuers must reproduce these fields in limited characters on statements (e.g. "PTO travel charge, www.PTO.com/contactless").

Important Acquirers must transmit the *Merchant Name and Merchant City* fields unaltered in the Clearing records.

3.6.5.3 Authorization code in Clearing

Important Acquirers must ensure that any MTT sent to Clearing under the MTT Chargeback Threshold (i.e. ones that were declined by the issuer) is correctly labelled with the value of "VFT000" in the Authorization code (e.g. Sales Draft Data, TCR 0 Position 152–157, Authorization Code).

Otherwise, acquirers must ensure that standard values for the Authorization code are used.

3.6.5.4 Incorrect transaction processing

Visa reserves the right to assess penalties for acquirers in the Europe region who regularly submit incorrect or invalid transactions.

In the Europe region only, if an issuer suspects the transit merchant is not complying with the MTT model rules then they may raise a compliance case against the acquirer.

Important A Europe acquirer may be subject to a Visa non-compliance assessment of EUR 30 for each MTT processed incorrectly by its merchants.

3.6.6 Issuer transaction processing

3.6.6.1 Account Verification Requests

Issuer hosts should expect to receive a greater number of AVR from merchants implementing the MTT model. The transit merchant will send tap data corresponding to a card in the form of an AVR as soon as possible after a card is used for the first time in the transit network.

Issuer hosts should expect that AVRs will be identified with a zero amount from a contactless-only transit reader with POS Condition Code data field set to "51".

3.6.6.2 Cryptogram types

Issuer hosts should expect to receive Authorization requests that can either contain TCs (offline cryptograms) or ARQCs (online request cryptograms) which are sent online. This is because the chip data present in the deferred online Authorization will correspond to the last tap performed by the cardholder, as explained in section 3.6.5.1. For the same reason, issuer hosts should expect to receive Clearing records that can either contain TCs or ARQCs.

Issuers in markets that operate zero floor limits for contactless transit transactions should expect to receive only ARQC online cryptograms.

3.6.6.3 Application Transaction Counter (ATC) checking

Issuer hosts should expect to receive Authorization requests where the value of the ATC is out of sequence, or even equal to, a previously received ATC value. The same ATC value can occur, for example, when an Authorization request is reversed.

ATC values can occur in any sequence, as the number and order of the MTT is unpredictable.

Important Issuers must not automatically decline an MTT based on an unexpected sequence of ATC received in the online Authorization.

Req 13: Issuer Processing of Mass Transit Transactions
(Rule: See ID# 0030051)
An Issuer must be able to correctly process an Authorization request for a Mass Transit Transaction and must:

- *Not send a decline response based solely on the value of the Application Transaction Counter (ATC)*

3.6.6.4 Issuer Stand-In Processing (STIP)

Issuers should be aware of the peak volumes of transactions which will be processed by transit merchants at the end of each travel period (typically during evening hours). Visa recommends that issuers review their STIP settings to ensure that these are appropriate for potentially high volumes of Authorizations that may be received during times where the issuer host systems are unavailable.

3.7 Exception handling

3.7.1 Late or lost data scenario

Accurate fare calculation relies on a complete set of tap data being available in the transit merchant's back office for processing at the end of the travel period. However, for various operational reasons (e.g. station loses connectivity for a period of time), some tap data may fail to arrive into the back office in time.

Transit merchants may wish to defer fare calculation processing until a complete set of tap data is available. This would avoid the application of charges for incomplete journeys where the merchant is aware of a technical issue or condition with its systems.

3.7.1.1 Tap data arrives after online Authorization (before Clearing)

If the revised amount, after fare calculation, exceeds amount previously Authorized (e.g. the late tap data resulted in a higher fare), the transit merchant must reverse the original Authorization and submit a fresh Authorization for the correct amount.

Otherwise, if the revised amount is lower (e.g. an incomplete journey charge was corrected to a lower fare), the transit merchant may submit the lower transaction amount in the Clearing record (i.e. lower than the amount in the original Authorization).

3.7.1.2 Tap data arrives after Clearing

If the revised amount, after fare calculation, is less than that in the original Clearing record, the transit merchant should issue a refund to the customer as soon as possible (see below).

If the revised amount, after fare calculation, is greater than that in the original Clearing record the transit merchant must Authorize the difference between the original and revised amount

before submitting a Clearing record for the difference. If the Authorization is declined, it must be treated the same as any other declined Authorization.

3.7.2 Refunds

A refund transaction must be initiated if the cardholder has been overcharged (e.g. because of late data).

Important Refunds should be initiated as soon as possible after discovering the overcharging.

3.7.3 Revenue protection charges

A transit merchant's fare policy may include a provision to impose specific penalty charges if a passenger is found to be travelling in contravention of their conditions of carriage (e.g. customer did not tap their card when accessing the transit service).

Any charges that are processed in connection with violation of fare policy by a transit merchant must be processed as a separate charge on the cardholder account. That is, the merchant should Authorize and Clear these charges as separate transactions from the MTT travel charges and provide the following information that should be placed on the issuer statement:

- A clear reason for the charge
- How the cardholder may challenge the charge

Important Conditions under which inspection charges may be imposed and the amount(s) should be clearly stated in the transit merchant's conditions of carriage which should be freely available to cardholders.

4 Known Fare Transaction model

4.1 KFT overview

The Known Fare Transaction (KFT) model is a "pay as you go" model where the fare for each journey or ticket is known at the time the payment card is presented to the transit reader.

The key characteristics of this model are:

- Transit readers accept contactless payments only (no chip & PIN or magnetic stripe) and must be capable of completing online Authorizations (in real-time or deferred)
- The amount of the fare charged is always known before the card is tapped
- Transactions can be Authorized online or handled offline at the terminal according to Authorization rules and where market specific floor limits allow
- Transaction amounts are likely to be restricted to the market specific contactless *Cardholder Verification Limit* (CVL), since the reader has no PIN entry device
- There is no special liability framework available like there is with the MTT model. All transactions must be Authorized before they may be submitted to Clearing

4.2 Tap processing

The interaction of the card and reader for the KFT model is exactly the same as for any retail contactless transaction. However, a transit reader does not support chip & PIN or produce receipts.

4.2.1 Real-time Authorization

The transaction processing flow is the same as for standard retail contactless transactions:

- The card is tapped on a transit reader and a transaction for the known amount is processed. The PTO can operate a flat or distance based fare structure to suit their needs
- The transaction will be Authorized online or handled offline at the terminal depending on the type of card used and market specific floor limit requirements
- The Authorization decision will be shown on the reader once the transaction completes
- Only if the Authorization is approved may the transaction may be sent to Clearing

It is acknowledged that online Authorizations over cellular data connections (e.g. GSM 3G or 4G) typically take 2-5 seconds to complete. While this may be faster than cash boarding, it may not be fast enough to satisfy the needs of all transit merchants, so should be considered during the planning of any implementation.

4.2.2 Deferred Authorization

Transit merchants may, at their risk, defer online KFT Authorizations in order to maintain service continuity where online Authorizations cannot be completed (e.g. a temporary loss of cellular connectivity) or where a higher rate of customer throughput is required (e.g. long queue at a vehicle stop).

Transit merchants that choose to defer online Authorizations should be aware of the following:

- Transit readers should successfully perform ODA on accepted cards to remove risk of counterfeit card use (see previous section 3.3.1 for further detail)
- Transit readers should check the expiration date of the card and reject expired cards (see previous section 3.3.2 for further detail)
- Transit merchants are permitted to employ additional proprietary processing (see previous section 3.3.6 for further detail)
- Transit merchants must submit the request in accordance with the *Visa Rules*

Transit merchants operating within the KFT model may resubmit an Authorization for a previously declined Authorization request twice in a 14 day period, under the [MIT] framework (please see section 3.5.3 and Table 6 for further detail).

Note Merchants, payment service providers, and acquirers must ensure that storage, processing, transmission of PAN, or other account data complies with [PCI DSS].

4.3 Transaction processing

4.3.1 Transaction Identifier

Transactions originating from a transit reader operating under the KFT model must be identified correctly, as per the *Visa Rules*. The Tran ID that is generated during Authorization should be used for the corresponding Clearing record.

4.3.2 Transaction data fields

Important For a KFT, acquirers and issuers should expect a match between the cryptogram amount in Field 55 and the transaction amount specified in Field 4.

The important data fields and values in the Authorization and Clearing messages for a KFT are shown in the following table:

Table 10 - KFT data fields

Authorization	Clearing	Value	Remarks
Amount, Transaction Field 4	Source Amount TCR 0 Position 77-88	Variable	For a KFT, the values here must match the value of tag 9F02 in Field 55.
Transmission Date and Time Field 7	N/A	Variable	The value here must contain the date and time at which the acquirer submits the Authorization message.

Authorization	Clearing	Value	Remarks
Merchant Category Code Field 18	MCC TCR 0 Position 133-136	4111 4112 4131	Indicates a transit merchant: 4111: Local and Suburban Commuter Passenger Transportation, including Ferries 4112: Passenger Railways 4131: Bus Lines
POS Entry Mode Field 22.1	POS Entry Mode TCR 0 Position 162-163	07	Indicates a contactless-read transaction.
Card Sequence Number Field 23	Card Sequence Number TCR 7 Position 7-9	Variable	EMV data tag 5F34, which if present in the card personalization and received by the reader, must be forwarded to the acquirer.
POS Condition Code Field 25	N/A	00	Identifies transaction conditions at the point of sale. For use in the Authorization message.
ICC Related Data Field 55 - Transaction Date Tag 9A (Field 146 for third bitmap issuers)	Terminal Transaction Date TCR 7 Position 10-15	Variable	Transaction Date
ICC Related Data Field 55 - Amount, Authorized Tag 9F02 (Field 147 for third bitmap issuers)	Cryptogram Amount TCR 7 Position 87-98	Variable	For a KFT, the values here compared to Field 4 must match since the fare amount was known at the time the card was presented to the reader.
Terminal Type Field 60.1	Acceptance Terminal Indicator TCR 1 Position 124	3	The value here must be set to an Unattended Cardholder Activated Terminal (UAT). See [TTIG].
Terminal Entry Capability Field 60.2	POS Terminal Capability TCR 0 Position 158	8	Indicates that the terminal had a contactless reader only (i.e. no contact chip/magstripe capability).

Authorization	Clearing	Value	Remarks
Cardholder ID Method Indicator Field 60.9	Cardholder ID Method TCR 0 Position 160	3	Unattended Terminal, no PIN pad.
Local Transaction Date Field 13	Purchase Date TCR 0 Position 58-61	Variable	The values here should contain the date on which travel took place.

4.3.3 Payment processing

Transit readers operating the KFT model must be configured as per Table 10 above.

The KFT model does not require any specific risk management logic to be implemented by the merchant in its back office.

For payment processing, the transit merchant back office may:

- Perform online Authorization requests for transactions in real-time or deferred
- Perform Settlement for Authorized transactions (i.e. submit them to Clearing)
- Receive and process chargebacks

4.3.4 Acquirer transaction processing

Acquirers must ensure that transit merchants operating the KFT model configure their readers as per Table 10 above. The processing of transactions from merchants operating the KFT model is otherwise identical to contactless retail transactions.

Acquirers must not submit any transactions to Clearing that have not been Authorized (online or offline). Acquirers that resubmit Authorization requests must follow the processes defined in the [MIT] framework, as explained in the previous section 3.5.3.

4.3.5 Issuer transaction processing

Issuers can identify a KFT based on the configuration of the transit reader (i.e. a UAT capable of contactless payments only from MCC 4111, 4112 or 4131) where the fare was known at the point the card was tapped (i.e. Field 4 is equal to *Amount, Authorized*).

4.3.5.1 Application Transaction Counter (ATC) checking

As with MTTs in section 3.6.6.3, issuer hosts should expect to receive Authorization requests where the value of the ATC is out of sequence, or even equal to, a previously received ATC value. The same ATC value can occur, for example, when an Authorization request is reversed.

ATC values can occur in any sequence, as the number and order of the KFT or retail transaction is unpredictable.

Important Issuers must not automatically decline a KFT based on an unexpected sequence of ATC received in the online Authorization.

5 Transit merchant security requirements

5.1 Introduction

Transit merchants are required to meet the relevant security requirements of the payments industry including:

- [PCI DSS] due to the storage, processing and transmission of account data
- Additional security requirements for readers within the Visa specifications (e.g. the protection of scheme public keys)
- Good security practice, such as that specified in [ISO27001]

5.2 PCI DSS requirements

The [PCI DSS] documentation provides comprehensive security requirements which apply to any organization involved in the storage, processing, or transmission of payment card transaction data.

[PCI DSS] defines account data as consisting of cardholder data and sensitive authentication data. If account data is stored, processed, or transmitted by a transit merchant or their processor, appropriate measures must be taken to protect the data.

Important The best practice tips are intended to provide stakeholders with learnings they may apply where appropriate. They do not replace a thorough risk analysis against [PCI DSS] or the engagement of a Qualified Security Assessor (QSA).

5.3 Security best practice

When defining their security architecture, a transit merchant should take particular care to consider:

- The management of card lists
- The implementation of point to point encryption (P2PE), to protect account data in transmission
- Processing of account data in the back office
- The need for mutual authentication, to protect against unauthorized access to account data

To ensure compliance is achieved with minimal impact, it is important that a transit merchant engages with a QSA early in the lifecycle of a deployment project.

5.3.1 Cardholder data protection during list processing

A transit merchant's approach to cardholder data protection can impact the management of card lists.

The use of suitably protected card lists, held at readers and/or centrally in a transit system, is expected to be a common design solution to meet Visa's requirements for risk management.

Lists may be used for a number of possible reasons, for example:

- Deny lists – to prevent further travel by cards deemed not accepted for travel (e.g. following an online Authorization decline)
- Pass-back lists – to prevent the same card being used multiple times at the same time on a reader. This feature is one that a number of transit merchants use to ensure compliance with their conditions of carriage
- Accept lists – a list that positively identifies cards that have been pre-approved as accepted for travel

A common requirement across the processing of these lists is the need to match a PAN presented at a reader with the secure PAN data on the list.

It should not be necessary to recover the plain text PANs for matching purposes.

Important Due to the risk of unauthorized third parties attempting to discover PANs through the use of a pre-computed "rainbow" table of non-reversible hashed PAN values, [PCI DSS] requires the use of a "salt" with a one-way hash. Please refer to [PCI DSS] or a QSA for details.

5.3.2 Account data in back office systems

The arrival of account data in the back office may be the trigger for a number of processes, such as:

- Fare calculation
- List management
- Authorization and Clearing requests
- Customer servicing

Multiple back office systems may need access to account data, which potentially extends the scope of [PCI DSS] to these systems. This is something that most transit merchants seek to minimize, and their systems should be designed to avoid PAN data (or any other sensitive account data) being stored in multiple locations, which increases risk.

Important Transit merchants may wish to consider securely storing just one copy of the PAN, and design their solution such that either the PAR or an unreadable representation of the PAN is available for use by other systems.

5.3.3 Mutual authentication

Mutual authentication is a requirement in the context of configuration and management of devices in [PCI DSS] and requires that the reader and the back office system with which it is communicating can trust the integrity of the data exchanged. This is to prevent an attacker from placing software in a reader that could be used to circumvent security by giving access to unprotected account data.

Important Mutual authentication should be considered as part of the overall design between all types of transit readers and back office systems to ensure that exchanges of data, whether transactional, management or otherwise, are protected against attack.

5.3.4 Using the Payment Account Reference

A Payment Account Reference (PAR) is a unique identifier associated with a specific payment account. This reference is used with a Visa token in place of sensitive cardholder data such as PAN, and transmitted across the payments ecosystem to facilitate consumer identification regardless of payment device form factor. PAR allows acquirers and merchants to link all activity related to the underlying payment account across multiple tokens without relying on the PAN.

The cardholder taps the Visa Contactless card to a transit reader where it initiates a transaction, and the token and PAR are transmitted via EMVCo tag 9F24. The merchant identifies the tokenized payment and processes an Authorization request including the token and PAR. The merchant will then receive an Authorization response including both of these references in Field 56.

The PAR may also be useful for customer services in using a replacement for the PAN across systems and reducing PCI compliance requirements. For example;

- Real time cardholder identification
- Deny list management
- Risk / fraud / management
- Omni-channel CRM
- Enhanced loyalty / rewards programs
- Better account lifecycle management

Req 14: Security of Account Numbers and Payment Account References (Rule: See ID# 0029276)

An Acquirer must ensure all of the following:

- *That the Account Number associated with a payment Token in a transaction is not disclosed to the Merchant*
- *That a Payment Account Reference (PAR) is not stored with its associated full Account Number(s) or payment Token(s)*
- *That a transaction is not initiated with a PAR*
- *That a PAR is used only for the following:*
  - *Providing or managing only customer service*
  - *Performing fraud and risk control activities*
  - *Supporting value-added services in which the Cardholder has opted to participate*
  - *Aiding compliance with applicable laws or regulations*

Important While PAR is not identified as sensitive data in PCI, PAR data should be used and protected in accordance with national, regional, and local laws and regulations, including privacy laws.

6 Card personalization

Visa's MTT and KFT models are designed to accept contactless cards that are capable of performing ODA (specifically fDDA). However, there are two personalization settings that issuers should be aware of, and verify, to ensure their cards are accepted at all transit merchants.

6.1 Support ODA

Issuers should personalize cards for ODA as defined in [VCPS].

Important Cards should allow ODA during online Authorizations. This is done by correctly personalizing cards to ensure the "Disable Offline Data Authentication (ODA) for Online Authorizations" (CAP byte 2 bit 6) is zero. If CAP byte 2 bit 6 is set, the card will not return ODA data and it will be rejected by transit readers.

6.2 International use

Issuers should personalize cards to allow international transactions, as defined in [VCPS].

7 Customer service

Transit merchants and card issuers must consider how they are going to support cardholders using a mass transit system, especially how support is shared between organizations. This section discusses the key considerations.

7.1 Transit merchants

7.1.1 Conditions of carriage

The charges applied when using contactless cards in transit, including inspection, penalty or "maximum" fare charges, are subject to the transit merchant's conditions of carriage. At a minimum, the following must be satisfied:

- Conditions of carriage must be readily available to cardholders
- If entry to the transit system is deemed to imply acceptance of the conditions of carriage, then prominent notices must be present at points of entry to the network as well as communicated on the transit network itself

7.1.2 Handling customer queries

Cardholders using a transit system after presenting their card may query the charge. This may be for a number of reasons, particularly in the MTT model where the fare calculation may be relatively complex (e.g. due to distance travelled, peak/off-peak, use of different transit modes, or capping).

Although a transaction may appear on a statement, the issuer will not have access to the data necessary to respond to a query. Transit merchants should offer the following support to their customers:

- Clear messaging to avoid known issues (e.g. card on deny list)
- Advice for customers on how to get support, preferably through self-service

7.1.3 Online access to transaction data

Since transit readers operating under the MTT model do not generally provide transaction receipts, information must be made available to cardholders via alternative means as the following requirement states:

> ***Req 15: Mass Transit Merchant Requirements***
> ***(Rule: See ID# 0030050)***
>
> *An Acquirer must ensure that its Mass Transit Merchant, upon completion of a transaction, provides the Cardholder with access to all of the following information for a minimum of 120 days following the Transaction Processing Date:*
>
> - *Merchant name*
> - *Total transaction amount in the transaction currency*

- *Details of each individual journey completed during the travel period, including the start and end time of each journey*
- *Final Transaction Date*
- *Any discounts applied*

Many queries can be answered by providing the cardholder with online access to their travel history, including information from tap data captured and charges made to the card. This can help avoid the need for customers to contact customer services, and can reduce transit merchant and issuer customer service costs.

Transit merchants can make online receipts available for cardholders using either a standard contactless card or a tokenized form of payment. A web interface can be used to capture, for example, the last 4 digits of the PAN or token, date of travel and the fare amount, and optionally also along with a unique reference number placed on the issuer statement.

Some transit merchants will already provide web based portals for customers to log in to and may wish to provide this information within that.

- For standard card users, the cardholder would register an account with the merchant and link their card by completing a secured e-commerce transaction (to prove the card is in possession of the cardholder). Once linked, the transaction history for that card can be shown
- For tokenized device users, the cardholder would register and link their card in the same way, and the Payment Account Reference (PAR) may be used to associate the linked card (the PAR value is returned in the authorization response when the card was linked) with the tokenized transactions (the same PAR value is provided in the tap data)

7.1.4 Customer education

Some of the more common questions that cardholders may raise regarding card usage can be mitigated by the provision of clear, timely and consistent information before and during travel. For example:

- Reminding the cardholder of the need to present only the card they wish to use in the reader field to avoid "card clash"
- Reminding the cardholder of the need to tap in and out using the same card for the entire journey to get the best fare. PTOs should be contacted for assistance with any query
- Reminding mobile users to provide cardholder authentication in advance of travel to avoid the need to enter their passcode as they pass through a gate

7.2 Issuers

7.2.1 Handling customer queries

To handle customer queries effectively, issuers should ensure their customer service systems and staff can identify transit transactions, and manage them in an appropriate way.

Issuers should prepare analysis and resolution paths for the most common queries. For example, the following may be some of the types received:

- Card being declined at the reader – issuers should be able to identify that a card transaction has recently been declined at the transit merchant, resolve any outstanding account based issues, and then advise the customer to contact that transit merchant
- Charges being applied – issuers should handover or direct the cardholder to the transit merchant who can answer specific transit fare queries

7.2.2 Statement data

The transit Merchant Name and transit Merchant City fields are populated in Clearing records and should contain merchant contact information for cardholders (e.g. a website address or telephone number).

Merchants may wish to place a unique reference in these fields so issuers can use it as a means for their cardholders to identify the transaction if they query a charge directly.

Important Issuers should include the merchant contact information in statements.

7.3 Cardholder verification

As cardholder verification on the transit reader is not possible for mass transit, transaction amounts are restricted to the contactless CVL.

Mobile-capable devices may be set up to require the entry of a CDCVM on the handset, such as a fingerprint or passcode for all transaction types, including mass transit. To ensure fast throughput at transit readers and to improve the cardholder experience, transit merchants and issuers should explain that cardholders should pre-Authorize the tap prior to arrival at the reader.

8 Dispute resolution

8.1 Transit merchant

Where a cardholder has a dispute about a transit transaction, they should in the first instance contact the transit merchant, as described in section 7.

In order to answer such disputes, the transit merchant must be able to make purchase information and accumulated transaction information available to a cardholder for at least 120 days after the processing date of the transaction, please refer to section 7.1.3.

8.2 Issuers

Issuers may chargeback for some of the following principle reasons:

- Where a transaction amount above the MTT Chargeback Threshold is submitted for Clearing after the issuer has declined an online Authorization request (Reason Code 71), as follows:

> ***Req 16: Chargeback Rights and Limitations***
> ***(Rule: See ID# 0029876)***
> *A Chargeback of a Mass Transit Transaction is valid for the full transaction amount if a decline response was sent and the transaction amount was greater than the MTT Chargeback Threshold, see Reason Code 71.*

- Where a card that did not support ODA was accepted for travel on the transit network (Reason Code 72)
- Where subsequent declined transactions are submitted after a declined Authorization request. This condition remains in place until the issuer approves an Authorization request for a transaction made with the card (Reason Code 72)

However, issuers may not chargeback Authorized transactions on the grounds of the transaction not being recognized or cases of fraud:

> ***Req 17: Invalid Chargebacks***
> ***(Rule: See ID# 0007579 and 0007642)***
> *Reason Code 75 and 81 are invalid for Mass Transit Transactions.*

8.3 Acquirers

Acquirers may receive chargebacks related to transit transactions for any of the three principle reasons detailed in section 8.2 above. Acquirers have the same re-presentment rights as for other disputes for these reason codes.

8.4 Dispute resolution summary

It is recommended that the resolution of cardholder disputed transactions should first be attempted through the PTO. Any chargebacks presented by issuers or acquirers must be provided with relevant evidence of a breach of the *Visa Rules*. Some of the more common dispute scenarios, both valid and invalid for transit transactions, are summarized in the following table (please refer to the dispute reason codes of the *Visa Rules* for full details):

Table 11 – Dispute resolution reason codes

	Valid	Invalid
Reason Code	**Description**	**Description**
71	Declined Authorization: Can be used for when transactions above the market or region values specified in the MTT Chargeback Thresholds table in the Visa Rules are submitted for Clearing.	
72	No Authorization: Can be used for when transactions on cards that did not support ODA are accepted for travel, or are submitted after a declined Authorization request.	
75		Transaction Not Recognized
80	Incorrect Transaction Amount or Account Number: The fare has been miscalculated.	
81		Fraud (Card-Present Environment)
82	Duplicate Processing: The PTO's system has caused the cardholder to be charged twice for the same service.	
85	Credit Not Processed: The PTO acknowledges that a refund is due and attempts to credit the cardholder, but it is not received.	
86	Paid By Other Means	

9 Testing

9.1 Transit merchant responsibilities

Merchants must ensure transit readers comply with all Visa requirements defined for the MTT and KFT models, including relevant tests detailed in EMVCo. For information about EMV certification, contact www.emvco.com. The Visa EMV Level 3 Test Tool can be used to complete Visa terminal testing. For guidance on this terminal testing process or obtaining terminal keys (including those required for transit cloud-based payments), mass transit merchants should contact their acquirer, and any other technology partner should contact the Visa Technology Partners team.

9.2 Acquirer responsibilities

To avoid implementation problems, acquirers should work closely with both Visa and transit merchants as soon as they begin to implement an MTT or KFT project. Acquirers do this to ensure that transit merchants understand the requirements and are able to implement them successfully. Acquirers should share terminal keys (including those required for transit cloud-based payments) with their mass transit merchant, and may contact their Visa representative to obtain these.

Req 18: Mass Transit Merchant Requirements
(Rule: See ID# 0030050)
An Acquirer must ensure that its Mass Transit Merchant does all of the following:

- *Registers with Visa*
- *Deploys contactless-only acceptance devices*
- *Meets all of the requirements of this guide and the Visa Rules*

9.2.1 System testing

Acquirers of transit merchants must test their processing systems to ensure compliance with the Visa requirements, and ensure passengers are charged the correct amount for their travel.

In addition to this, the acquirer host system certification testing process is managed by Visa's Client Support Services and Global Client Testing teams, who will provide guidance on the implementation process and the required test scripts for certification.

9.2.2 System audit

In cases where transit merchants are suspected of operating the MTT model incorrectly in the Europe region, Visa may perform, or require acquirers to perform, an audit of the transit merchant's systems and processes to ensure compliance with Visa Rules.

Req 19: Mass Transit Transaction Processing Non-Compliance Assessments
(Rule: See ID# 0030055)
A Europe Acquirer may be subject to a non-compliance assessment for each Mass Transit Transaction processed incorrectly by its Merchants.

10 Deployment preparation

Successful mass transit implementations require careful planning. The checklists which follow in this section provide a high level overview of the key factors which should be taken into consideration when implementing either the MTT or KFT models. In addition, stakeholders should engage with Visa directly for assistance with specific questions or clarifications.

10.1 Technical readiness checklist

Key technical readiness elements:

- Technical requirements described in this document have been correctly implemented
- Terminals have been correctly configured as described in the [TTIG] document
- Terminals read all required card data from the correct location(s)
- The required certification, such as EMV and PCI has been achieved
- Hardware testing with Visa, such as Visa EMV Level 3 testing, has been completed
- All required cryptographic keys have been successfully installed on terminals
- Deny lists have been correctly configured including update procedures
- Middle-office functionality is correctly set up to receive and transmit data
- Acquirer functionality has been integrated into the overall system
- Host system certification testing completed with Visa to ensure issuer or acquirer systems are capable of receiving and transmitting all required transaction data fields
- Messaging between the acquirer and third parties (e.g. PSPs) is correctly handled
- Back office is correctly configured to implement the required transit rules
- Back office is capable of providing customer service interface
- Revenue inspection devices have been correctly set up
- Limited pilot testing (e.g. friends and family) is successfully completed
- Soft launch (e.g. limited use in live environment) is successfully completed

10.2 Operational readiness checklist

Key operational readiness elements:

- Transit operators' business rules have been correctly integrated into the system
- All key customer journey scenarios can be successfully handled (e.g. "happy path" journey as well as unsuccessful or incomplete journeys)
- Issuers have reviewed their STIP settings
- Debt recovery processes have been tested and are managed according to the Visa requirements (e.g. *Merchant Initiated Transactions*)
- Understanding transit merchant and issuer responsibilities for customer support
- Implementing FAQ's for customer support staff
- Understanding call center requirements (scripts and handover)
- Incorporating market specific regulatory and "conditions of carriage" requirements

- Understanding testing and launch schedules
- Planning rollout of training to internal teams

10.3 Market communications readiness checklist

Key communication elements:

- Ensuring communication in local media prior to launch to raise awareness
- Press release and communication on the day of the launch
- Local station communication advising passengers that they can use contactless as a method of payment
- Local environment publicity (e.g. posters and regular announcements)
- Station announcements to advise cardholders to avoid "card clash"
- Ensuring coordination with all stakeholders
- Contributing towards creating a "platform of awareness"

Appendix A MTT Custom Authorization model

For transit merchants operating in the Europe region where contactless transactions at transit MCCs are not subject to a floor limit of zero, an alternative Custom Authorization model may be used.

This model will reduce the number of Authorizations submitted at the end of each travel period, so instead of all transactions being Authorized (the default model described in the main body of this guide) transactions are Authorized on a periodic basis.

Implementation of the Custom Authorization model requires complex additional processing in the transit merchant's back office to identify where transactions may be submitted directly to Clearing at the end of the travel period. This added complexity, which is not insignificant, combined with the increased complexity of disputes processing will make this option more challenging for transit merchants.

A.1 Custom Authorization

Instead of sending all transactions for online Authorization at the end of the travel period, transit merchants may submit transactions directly to Clearing in some cases. However, if certain conditions are met the transaction must then be Authorized online, as the requirement below describes.

Req 20: Mass Transit Transaction Authorization Requirements
(Rule: See ID# 0030049)
A Europe Region Merchant performing a Mass Transit Transaction must submit an online Authorization request at the end of a travel period if any of the following apply:

- *The Card was used for the first time at the Transit Merchant or more than 14 calendar days have elapsed since Online Authorization was last requested for the Account Number by the Transit Merchant*
- *The chip on the Card requested online Authorization at any point during the travel period*
- *The cumulative value of a Mass Transit Transaction since the last Online Authorization Request by the Merchant for the Account Number is equal to or greater than the Mass Transit Transaction cumulative offline limit. This limit is set to the same value as the Contactless Floor Limit in that country*

Under the MTT Custom Authorization model, transit merchant's systems must ensure that Authorizations are sent online often enough for issuers to have effective control over the risk of misuse of their cards, while allowing many transactions to be Authorized offline at the terminal and submitted directly to Clearing.

The MTT Custom Authorization model does not have any impact on other required MTT processes such as AVR checking, deny list management, debt recovery, or the MTT Chargeback Threshold.

Custom Authorization requires the transit merchant's back office system to include the following risk management checks at the end of the travel period:

- **New card check**
  Where a card was used for the very first time, the transaction must be sent for online Authorization. This applies even if the AVR for that card was previously declined (earlier in the travel period)
- **Maximum time between online Authorizations check**
  Where a card was used and the previous online Authorization was more than 14 days ago. See the below table for details
- **Card cryptogram type check**
  Where a card requested online Authorization (generating an ARQC) at any point during the travel period. This ensures that transactions from online-only cards are always Authorized online at the end of the travel period
- **Cumulative offline spend check**
  Where a card has been used and the total amount spent on the card at the transit merchant since the last online Authorization exceeds GBP 15 or EUR 20. If the transaction takes the cumulative amount above the limit, the transaction must be online Authorized

Table 12 - MTT Custom Authorization risk management parameters

Parameter	Description	Merchant outlet location	
		United Kingdom	All other Markets
Maximum time between online Authorizations	If the number of days since the last online approved Authorization exceeds the maximum time between online Authorizations, the transaction must be sent for online Authorization.	14 days	14 days
Cumulative offline spend check	For each card, the transit merchant records the total amount spent on the card since the last approved Authorization. If a transaction takes the cumulative amount above the cumulative amount limit defined by Visa, that transaction must be Authorized online.	GBP 15	EUR 20

If any of the checks above are true, the transaction at the end of the travel period must be sent for online Authorization.

On receipt of an approved Authorization at the end of the travel period, the transit merchant may reset the Custom Authorization counters as described in Table 12 above. Debt Recovery transactions may not be used to reset these counters.

Appendix B MTT handling of VCPS 2.0.2 cards

This document has been developed around current generation [VCPS] version 2.1 cards or higher.

However, Visa recognizes that in some countries there will be cards in issue that are compliant with the previous-generation [VCPS] version 2.0.2. Such cards cannot perform ODA when attempting to process a zero value transaction amount. This means that VCPS version 2.0.2 cards would always be rejected at a transit reader under the MTT model.

In the event that a transit merchant wishes to accept these previous generation cards, they may optionally implement alternative reader processing.

B.1 Transit merchant acceptance

Instead of using the value of zero (0.00) for the *Amount, Authorized* field for all cards, the transit reader should be configured to use a value of one minor currency unit for all cards.

Important Acquirers must obtain written permission from Visa to configure transit readers as above, to enable acceptance of VCPS version 2.0.2 cards.

For full details of all other card processing, please refer to [TTIG] available on VOL or via the transit merchant acquirer.