SHIFT4™

API Specifications

Transit Transaction Processing

Version 2.0 | December 2023

The services are provided by Shift4 companies. For more information see: shift4.com/license

Contents

Introduction 3
Useful Documents / References 3
Publisher Information 3
General Information 4
Glossary 4
Transit Transaction Models 6
Mastercard Aggregation / Pay As You Go 9
Maestro Aggregation 12
Visa Mass Transit Transaction 12
Family ticket 15
Debt Recovery 16
Deny list 18
Tokens 19
Revenue Inspection 19
Appendix A: t1 Values 21
Appendix B: t2 Values 22
Change History 23
Support Information 24

Introduction

The purpose of this document is to provide an in-depth description of the operations available for processing transit transactions with Shift4.
Due to the immediate nature of transit transactions, where waiting several seconds for payment authorisation is not feasible, deferred authorisations are used to provide the best consumer experience. This document details how to handle such transactions across different scenarios.

Useful Documents / References

The following documents may also be useful in understanding the Shift4 transit specifications:

- **Shift4 Payment API Specifications** – an in-depth description of the Shift4 Gateway API specifications
- **Shift4 Card-Present Specification** – a supplement to the *Shift4 Payment Platform API Specifications* with detailed information on the API's use of Card-Present data

These documents can be found on the Shift4 Developer Portal.

Publisher Information

Copyright © Shift4 All rights reserved.

General Information

Mastercard and Visa have created a set of solutions for transit operators, by moving from proprietary ticketing technologies to globally standardised solutions. By supporting these, transit operators can offer greater convenience to passengers who can now purchase tickets upon entry using their card. By utilitising card accounts and contactless technology, you can deliver operational improvements, enhance passenger experience, and ensure fast and secure fare payments.

These transit transactions are limited to the following MCCs:

- 4111 : Transportation – Suburban and Local Commuter Passenger, including Ferries
- 4112 : Passenger Railways
- 4131 : Bus Lines
- 4784 : Bridge and Road Fees, Tolls

Glossary

The following terms are used throughout the document.

Term	Meaning
Aggregation	A mechanism where a single transaction is generated for multiple taps/fares.
AVR	Account Verification Request. A 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 Authorisation request and does not verify the financial standing of the funding account.
ATC	Application Transaction Counter. A counter residing on the chip card which is incremented by the card for each transaction.
CDA	Combined Data Authentication. A mechanism that uses dynamic data as well as transactional data to ensure that the card is not cloned and the transaction is genuine.
Chargeback Threshold	The maximum fare amount that can be submitted to clearing upon an initial decline response for first card use, or following any unsuccessful authorisation approval within the aggregation model.
CIT	Cardholder Initiated Transaction. A transaction in which the cardholder actively selects the card to use and completes the transaction using previously-stored credentials (card number or token).
Deferred Authorisation	A card-present environment authorisation that is requested after the cardholder has left the point of transaction.

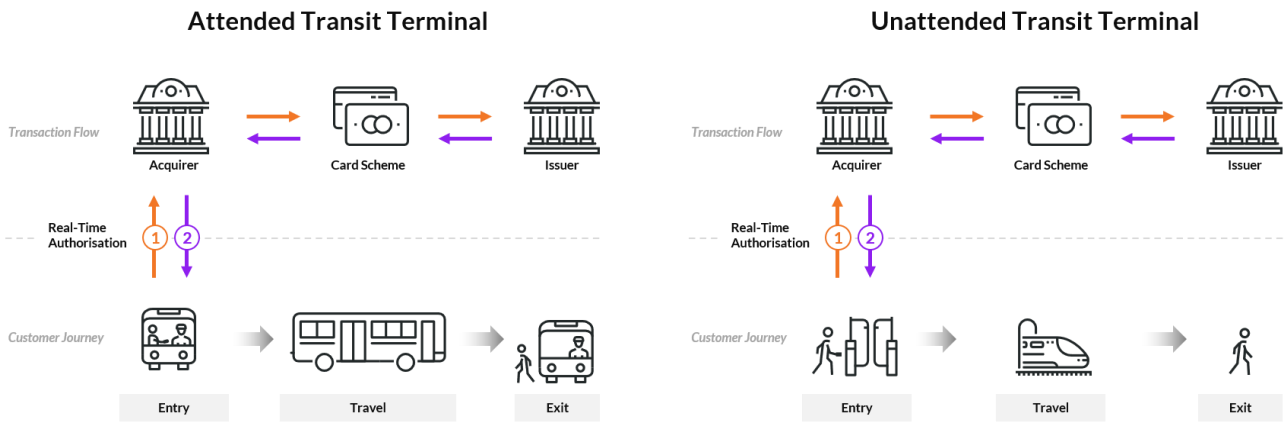
Term	Meaning
Deny List	A method for blocking cards that have not been accepted for travel within the transit merchant's system.
fDDA	Fast Dynamic Data Authentication. An optimised form of Offline Data Authentication.
MIT	Merchant Initiated Transaction. A transaction submitted by the transit merchant using previously-stored credentials (card number or token).
MTT	Mass Transit Transaction.
KFT	Known Fare Transaction
ODA	Offline Data Authentication. A method by which the transit reader requests and checks the authentication data received from the card to ensure it is genuine.
Transit Back Office	A component within a transit merchant's systems which processes taps received from transit readers, and performs any or all journey construction, fare calculation, risk management, and payment processing.
First Ride Risk	The initial risk taken on by the operator when using a deferred authorisation, allowing a cardholder to enter the transit system before the authorisation is confirmed.
Cardholder Device CVM (MC only)	Cardholder Device Cardholder Verification Method (CDCVM) is used to verify cardholders using mobile devices for payment transactions.

Transit Transaction Models

Each of the card schemes offers several transit transaction models with varying processes, however the overall logic is similar. Some models are exclusive to Mastercard or Visa. In the following sections we detail the specific transaction flow, best practices and process handling for each Visa and Mastercard transit model.

The transit model is indicated using the t1 (transit transaction type) parameter. In some cases, you might also need to indicate the transit transportation mode using the t2 parameter. The parameters' values are detailed in Appendix A: t1 Values and Appendix B: t2 Values.

Known Fare



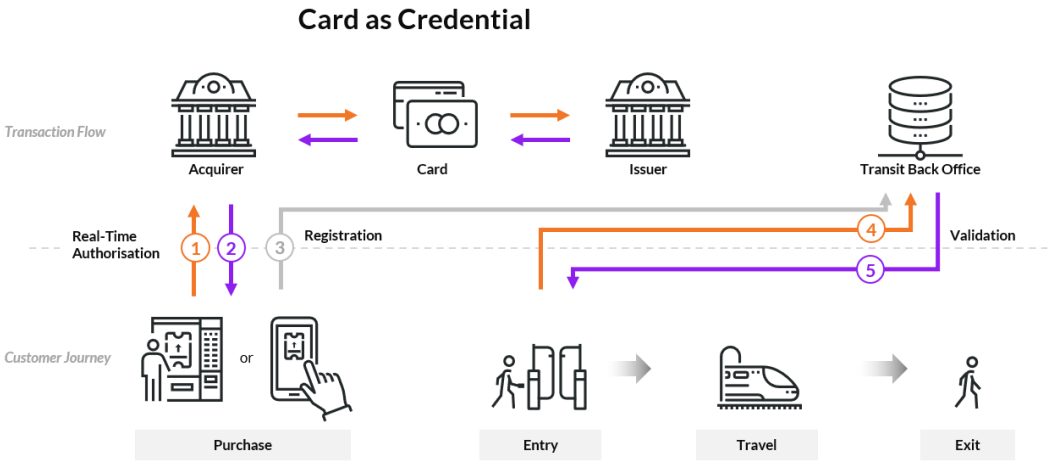
This model, supported by both Mastercard and Visa, is best suited for use when the fare is known, such as a EUR 2.50 single ticket.

The authorisation for this transaction can be performed in real-time or on a deferred basis. Preforming the authorisation in real-time may cause a delay in opening the gate or other frictions when the passenger alights. Deferring authorisation, on the other hand, imposes some risk on the transit operator because it allows the cardholder to enter the transit system before the operator receives authorisation for the transaction.

For Mastercard	t1=02 (refer to *t1 Values*) t2 must be sent For deferred authorization add the following: a10 = 3 (Deferred Authorization) a6=date of authorisation request a7=time of authorisation request

For Visa	The a4 parameter and EMV 9F02 tag should have the same value a6=date of authorisation request a7=time of authorisation request b9=07 If the transaction is deferred you can resubmit an authorisation for a previously declined authorisation request twice in a 14 day period as MIT.

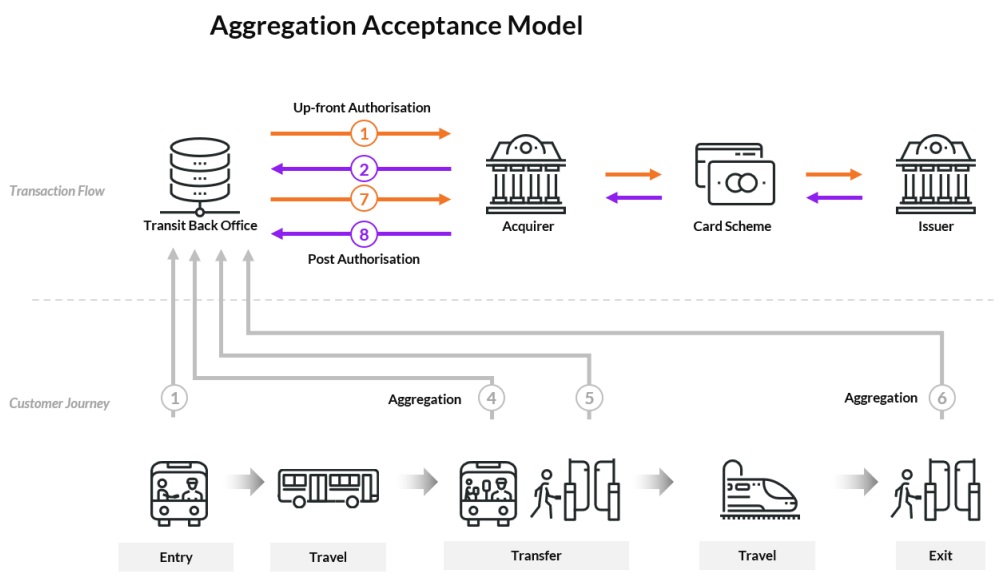
Card as Credential – Mastercard only



In this model the passenger tops up his card and uses it as credentials for travelling. Topping-up can be performed as a Card-Not-Present transaction, where the passenger makes the payment using a mobile app or website, or as Card Present transaction where the payment is made via a kiosk at the station. This transaction takes place prior to travelling and is not part of the travelling cycle. This model is supported by Mastercard only.

For Mastercard	t1=01 (refer to *t1 Values*) t2 must be sent

Daily Aggregated / Tap in – Tap Out

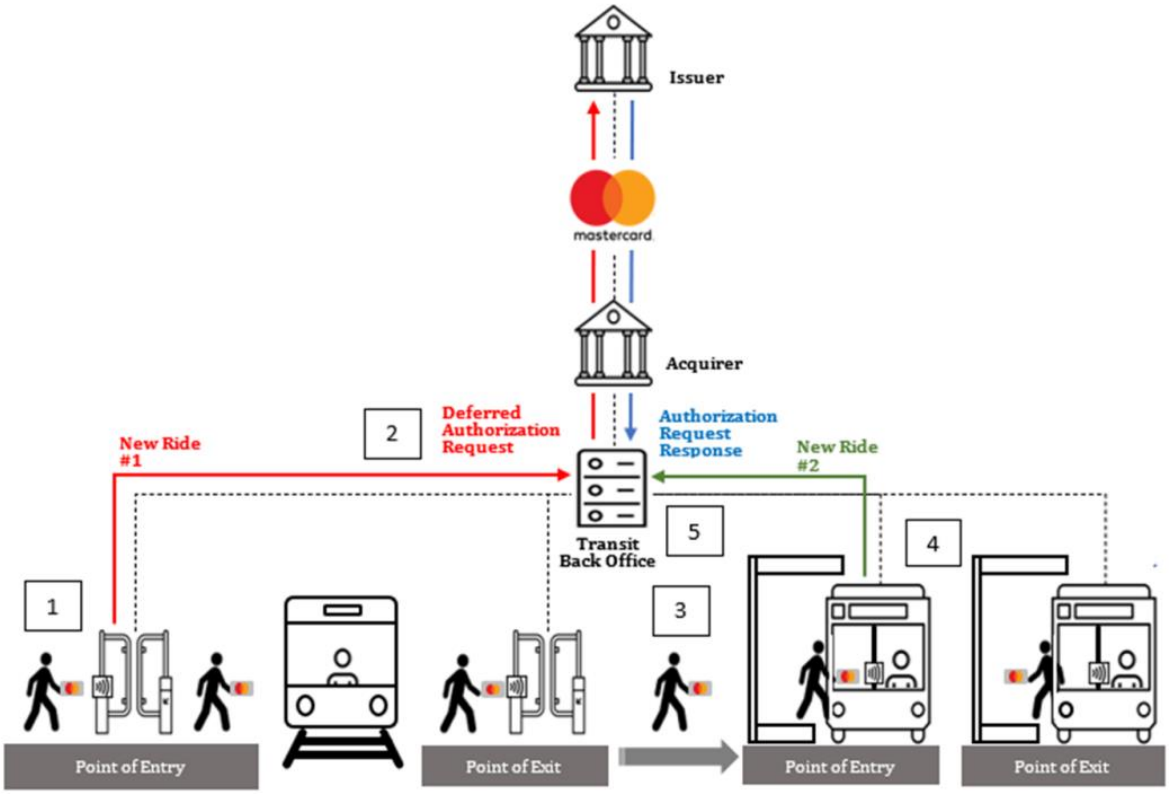


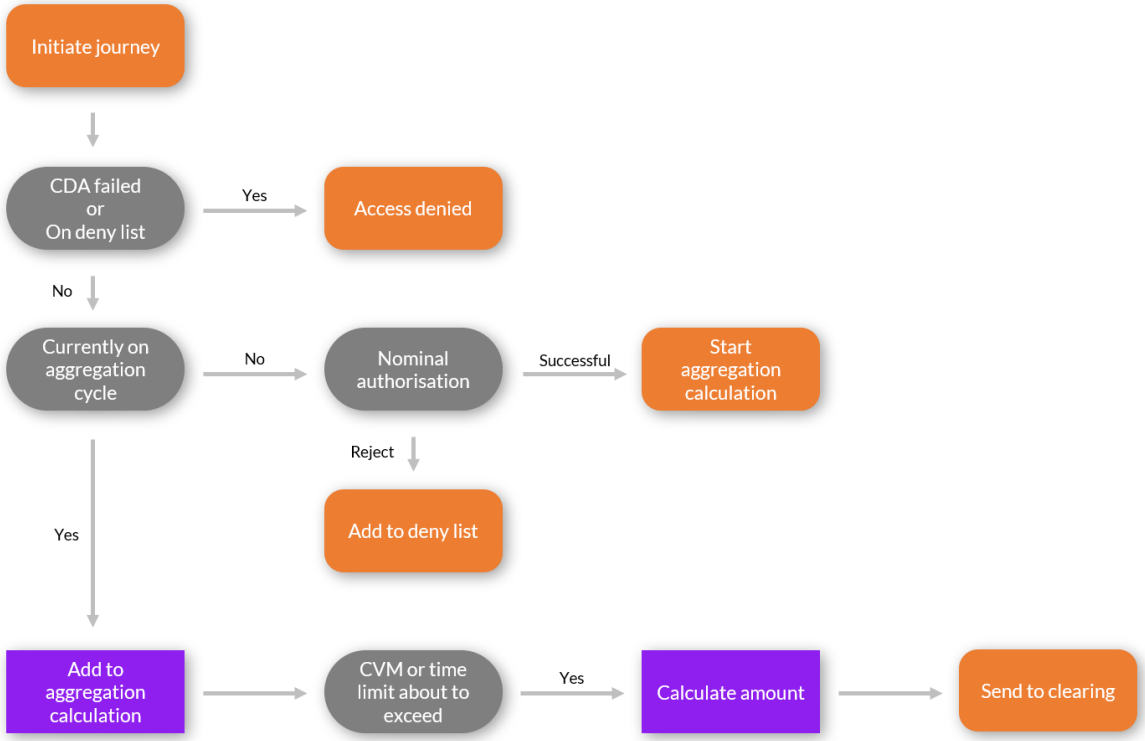
This model, supported by both Mastercard and Visa, is called by different names depending on the scheme, but is well known as Tap in – Tap out. This model is useful when the fare is not known at the time of entry, and is not fixed but rather needs to be calculated dynamically according to the number of trips or stations the cardholder used. The total fare amount is calculated and charged by the transit operator at the end of the travel period.

This is the most complex of the models and is handled differently by each of the card schemes, using different terminology.

Mastercard Aggregation / Pay As You Go

This model applies to all EU and EEA member countries, excluding the UK, Ireland and the Netherlands.





Flow

1. The cardholder initiates the journey by tapping their card on a dedicated device, usually a ticketing gate or a point of entry into the transit network.

Perform CDA (combined data authentication) to check whether the card is on the deny list.

a. If the card is on the deny list, access is denied.

b. If the card is not on the deny list, check whether the card is on an aggregation cycle.

i. If the card is not on an aggregation cycle, the gate opens and simultaneously a nominal authorisation is sent.

a. If the nominal authorisation is successful, a new aggregation cycle is initiated.

b. If nominal authorisation fails, the card is added to the deny list.

i. If the card is on an aggregation cycle, add the journey fare to the calculation.

Check whether the CVM or the time limit is about to be exceeded.

c. If the CVM or the time limit are about to be exceeded: calculate the amount, send the transaction for clearing, and reset the aggregation to start a new cycle.

d. If neither the CVM nor the time limit is about to be exceeded, no action is taken and the cycle continues upon the next tapping of the card on a dedicated device, such as when exiting or passing through a transit gate.

Note:

- Nominal authorisation should be sent as deferred-authorisation (a10=3)
- Nominal authorisation should be sent with t1=03 (refer to t1 Values)
- Nominal authorisation must be sent with t2
- Nominal authorisation can be any value from EUR 0.1 up to the Contactless transit aggregated limit (CVM limit). Usually the amount is EUR 0.1 in order to improve the approval rate.
- Make sure you update your CVM limits for your countries of operation.
- You have up to 14 days to clear the transaction after sending the nominal authorisation.

Nominal authorisation example

```
M=<gw_mid>
K=<signature>
O=2
```

```
a1=<request_id>
a2=6
a4=10
a5=EUR
a10=3
b1=<card_number>
b3=<card_expiration_month>
b4=<card_expiration_year>
b5=<cvv>
b9=07
b10=2
b17=<terminal_id>
b19=2
b55=<chip_card_data>
d1=<ip_address>
t1=03
t2=00
```

ATC Update

The Application Transaction Counter (ATC) is a sequential counter managed by the contactless card to ensure the cardholder's security using unique cryptograms, this only applies to Mastercard transactions.

ATC update requests notify the issuer that multiple "taps" have occurred and incremented the ATC; however, these requests do not generate an authorisation request or clearing record. The transit merchant must, therefore, send an ATC update operation at least once every 20 times a card was used since the last issuer-approved transaction.

The operation should be sent according to the following format:

Parameter	Description	M/C/O	Notes
M	*Shift4* assigned gateway Merchant ID	M	
O	Operation Code	M	
T	Transaction processing timestamp formatted as MM/dd/yyyy HH:mm:ss	M	
a2	Payment Source Type as sent in the request	M	
a4	Requested Billing Amount as sent in the request	M	The value must be 0 (zero)
a5	Transaction Currency Code	M	

Parameter	Description	M/C/O	Notes
a6	Transaction local date	M	
a7	Transaction local time	M	
b1	Primary Account	M	
b3	Card expiration month as sent in the request	C	
b4	Card expiration year as sent in the request	C	
b7	Track 2 data	M	
b9	Card entry mode	M	
b10	PIN entry capability	M	
b55	Smartcard Specific (chip card) Data	M	
i2	Billing Descriptor - Card Acceptor Name/Location	C	

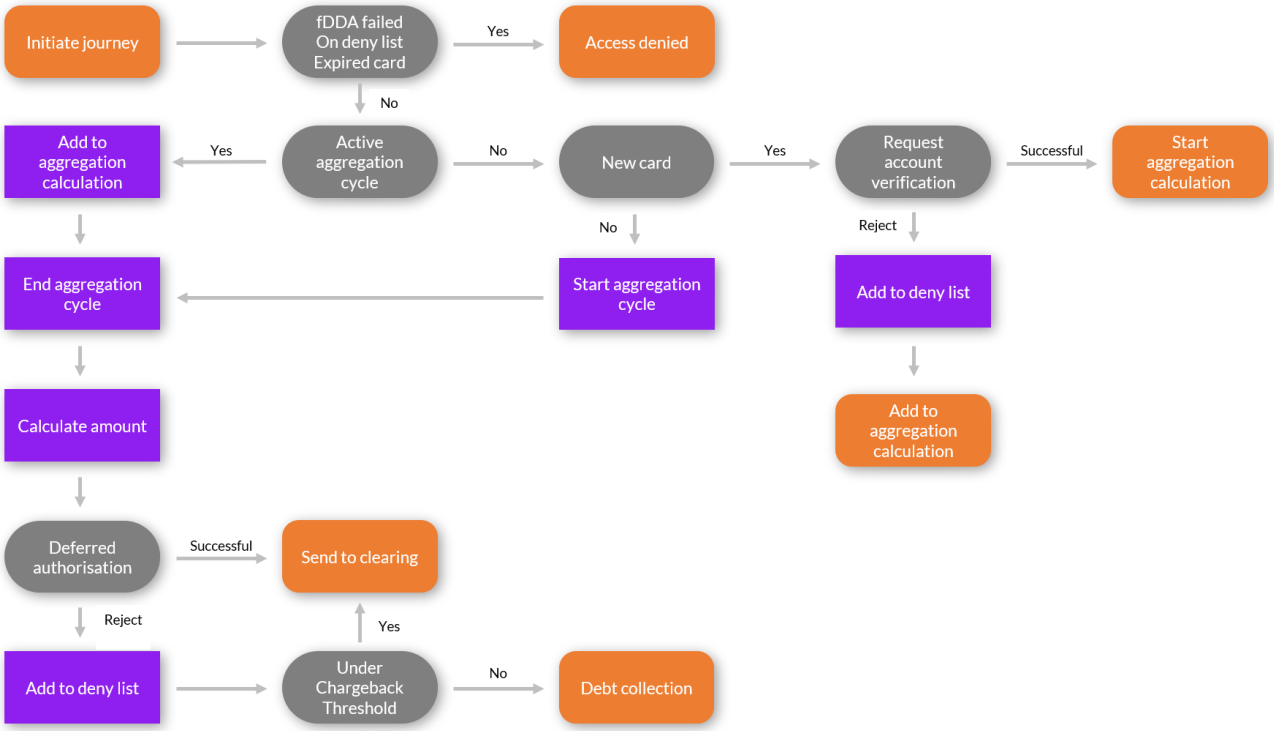
Maestro Aggregation

Maestro aggregation implementation is slightly different than Mastercard aggregation implementation.

This has two implications:

- The first authorisation amount sent, should be sent on estimated value: any value up to the contactless transit aggregated limit (CVM limit). It is recommended that the amount be equal to 2*single ride fare.
- At the end of the aggregation cycle (when the limit reached or after 3 days):
  - If you had sent an estimated authorisation, and the amount at the end of the aggregation is lower than the amount that was authorised, capture the final amount, and void the difference.
  - If the capture amount is equal or higher than the estimated authorisation amount, there is no need to void any amount. Simply capture the amount, as long as the daily limit was not exceeded.

Visa Mass Transit Transaction



Flow

1. The cardholder initiates their journey by tapping their card on a dedicated device, usually a ticketing gate or a point of entry into the transit network.

Perform fDDA to check whether the card is expired or on the deny list. If the card is expired or on the deny list, access is denied.

2. If the card is neither expired nor denied, check whether the card is on an aggregation cycle.
   a. If the card is not on an aggregation cycle, the gate opens.
   b. if the card is a new one (not been used in the past 14 days), send an AVR.
      i. If the AVR is successful, initiate a new aggregation cycle.
      ii. If AVR fails, the card is added to the deny list.
   c. if this is not a new card, initiate a new aggregation cycle.
   d. If the card is on an aggregation cycle, add this tap to the calculation.

At the end of the aggregation period as defined by the transit operator, calculate the amount.

Send a deferred authorisation for the calculated amount.

   a. If the deferred authorisation is successful, request capture.
   b. If the deferred authorisation fails, add the card to the deny list.
      ii. Check whether the amount is under the chargeback threshold
         a. If yes, request clearing
         b. If not, continue to debt recovery

Note:

- You can choose to send the AVR for each aggregation cycle, whether this is the first time this card is used or not.
- The account verification request should be set as authorization with a4=0 and t1=03 (refer to appendix A: t1 values
- Deferred authorisation should be sent with t1=04 (refer to appendix A: t1 values)
- The capture transaction date should be the day of the first journey.
- Deferred authorisation should be captured within 3 days of the transaction date.

Clearing request example

```
M=<gw_mid>
K=<signature>
O=1
a1=<request_id>
a2=6
a4=1000
a5=EUR
a10=1
b1=<card_number>
b3=<card_expiration_month>
b4=<card_expiration_year>
b5=<cvv>
b9=07
b10=2
b17=<terminal_id>
b19=2
b55=<chip_card_data>
d1=<ip_address>
t1=04
t2=00
```

Chargeback Threshold

The MTT (Mass Transit Transaction) 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 whose authorisation at the end of the travel period is declined by the issuer. This applies only to Visa Mass Transit Transactions.

If a transit operator receives a decline response from an issuer, the operator 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
- One of the following:
  - The transaction is the first transaction for this card and this transit merchant, or
  - The previous Mass Transit Transaction for which authorisation was requested, had received an approval response
- ODA using fDDA was performed
- The transaction amount does not exceed the market or region specific values as specified by the card schemes.

Eligible transactions may be submitted to clearing and may not be disputed, even if the issuer declines the authorisation request. For transaction amounts above the threshold, liability is accepted by the merchant.

Note:

- To send a capture for declined deferred authorisation use g3=VFT000.
- For a transaction that received a decline response, do not submit a capture with a lower transaction amount in order to meet submission criteria.

Family ticket

This mechanism applies to both Mastercard and Visa aggregation transit transactions. In this scenario one card is used for simultaneous travel by multiple passengers (aka 'Pass Back').

You can support family tickets in any of the following ways:

- A nominal authorisation per each family member. In this case, the transit operator must wait before sending the nominal authorisation in order to find out if the card will be tapped only once or multiple times.
  The recommendation is to wait 30 seconds from the first tap to see whether any additional taps occur during those 30 seconds, and then to conclude that each of the additional taps is for a particular family member.
- A single nominal authorisation covers the entire family. In this case, the transit operator should work with multiple tap-ins against multiple tap-outs.

Note:

- A family ticket supports up to 10 passengers, as specified by the card schemes.

- Your transit operator engine has to be well configured in order to manage tap-in/tap-out for multiple travelers.
- Instruct passengers to stay together for ticket inspection purposes or tap-out fare calculation. Clear terms and conditions need to be properly communicated in advance to passengers.
- A family ticket exposes you to a larger first ride risk, which is the usual first ride risk multiplied by the number of passengers

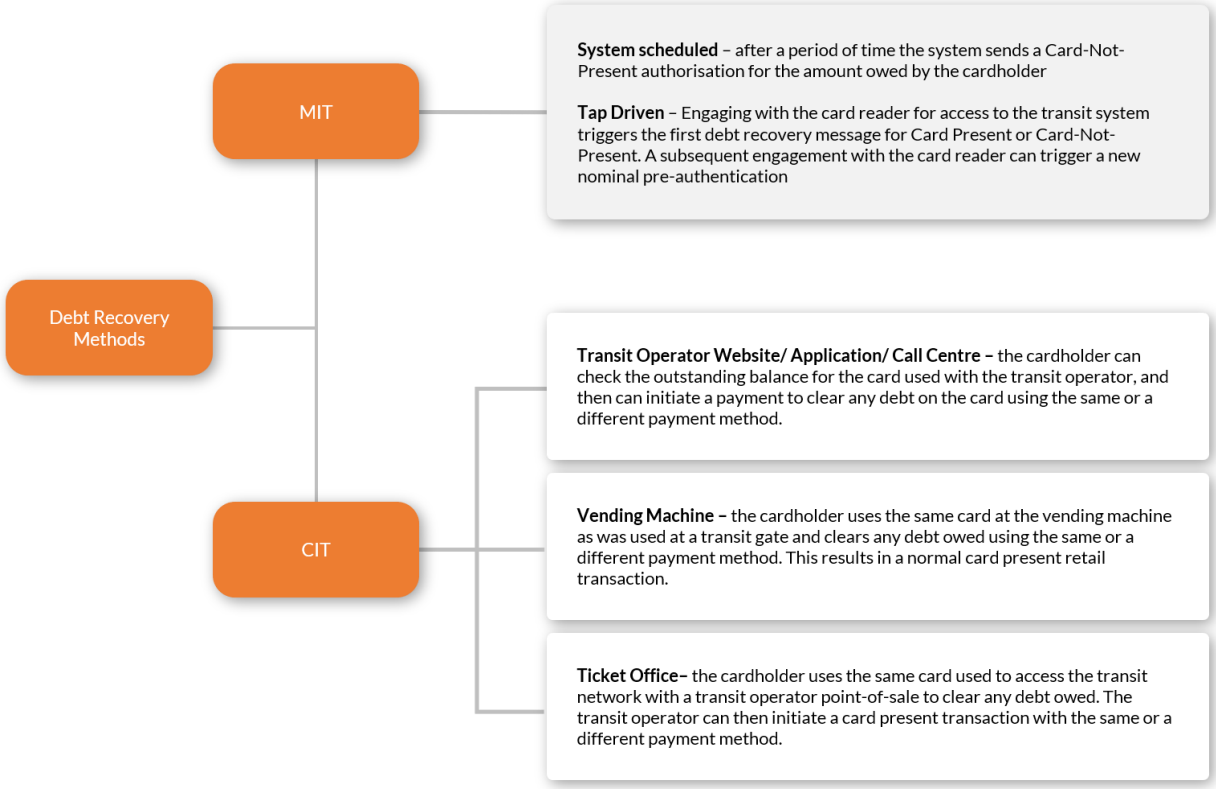
Debt Recovery

Debt recovery is a transaction through which the transit operator regains the cardholder's outstanding debt. As mentioned above, the transit operator takes some credit risk (aka first trip risk) by allowing a cardholder to travel before knowing whether the account linked to the tapped card is in good standing.

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

In general, the transit operator submits debt recovery transactions where the amount of the re-attempted authorisation request is equal to the outstanding debt (i.e., the unpaid fares amount).

The debt recovery transaction might be MIT or CIT.



MIT

A transit operator may resubmit a declined authorisation request under the MIT framework. This can be done automatically via a system-generated submission process in the merchant's back office. For a transit operator using the Visa MTT model, this policy typically allows up to 4 authorisation resubmissions within a 14-calendar days period since the original contactless authorisation request was declined.

CIT

Tap - A cardholder attempting to use a blocked card at the merchant's transit reader is allowed to create a fresh debt recovery authorisation request (even if the debt is zero). While the card will not be accepted for travel, the tap may be used to trigger a fresh contactless authorisation request using the chip data from the new tap, along with the fare amount of the previous declined authorisation. In this scenario there are no limits on the number of authorisation resubmissions.

Website, call centre or dedicated mobile application - 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 centre or other means.

Note:

- Debt recovery can be used when the transit operator is initially unable to collect the payment for the fare spent. Note that not every reject should trigger future debt recovery; for example, the transit operator should not perform debt recovery when the response code indicates an expired card, stolen card, etc.
- Debt recovery is a card-not-present transaction for a system scheduled method (MIT). In cases of Ticket Office and Vending the debt recovery is a card-present transaction.
- A debt recovery transaction for Mastercard must be sent with FPAN.
- A debt recovery transaction for Visa must be sent as an MIT transaction with reference for initial transaction.
- When a passenger tries clearing their debt with a different card, the transaction should be sent as a regular retail transaction (with no transit indication).
- For debt recovery the transit operator should include the operator name in the dynamic descriptor (i2). This only applies to Mastercard transactions
- A debt recovery transaction can be sent either as a Sale or as an Authorisation operation + Capture operation
- Debt recovery should be sent as a final authorisation (a10=1)
- Debt recovery should be sent with t1=05 (refer to appendix A: t1 values)
- For Visa the transaction should be sent as either a:
    - Mail Order/Telephone Order transaction where a2=3, OR

- eCommerce transaction where a2=2

Debt recovery example

```
M=<gw_mid>
K=<signature>
O=1
a1=<request_id>
a2=6
a4=6000
a5=EUR
a10=1
b1=<card_number>
b3=<card_expiration_month>
b4=<card_expiration_year>
b5=<cvv>
b9=07
b10=2
b17=<terminal_id>
b19=2
b55=<chip_card_data>
d1=<ip_address>
t1=05
t2=00
```

Deny list

The deny list is a mechanism for stopping certain cards from using the transit system.

You must add cards to the deny list upon receiving a decline response to an authorisation request or AVR to ensure that the card is not accepted for travel:

- Within 1 hour for Visa
- Within 24 hours for Mastercard

You are also required to remove or delete cards from this list when the debt has been settled.

One component of this mechanism is a database of cards which must be checked each time a card is presented to the reader.

Deny List

Date	Account	Reason
02/18	5111 1111 1111 1111	Lost
06/18	4111 1111 1111 1111	Stolen
01/19	5111 1111 1111 1111	Insufficient funds
06/17	4111 1111 1111 1111	Cryptographic failure
03/19	5111 1111 1111 1111	Invalid tap

There are two main database approaches that can be used with a deny list:

- A single central database for all terminals
  This approach requires strong network connectivity as each terminal must establish a connection each time a card is tapped. If there are any issues or loads on the network, bottlenecks may occur, leading to less than optimal performance.
- A local database for each terminal
  Each terminal hosts a local clone of the central database, which replicates the changes from the server incrementally. This allows for quicker performance as a connection isn't required each time a card is tapped and the replication can be done when network performance is at peak.

Best practice:

- Even though the country might have a local industry card hot list or a Mastercard Warning List, the recommendation is not to append them to your own deny list since the benefits are marginal when considering the speed performance requirements.
- The cards on the deny list should be registered & tracked by **PAN number only** so that only that specific card is affected
- The deny list may also include BINs of card products not accepted by the transit system
- When mobile/wearables are used, the deny list should keep the mapping between the value of the contactless Token PAN (DPAN) and the Funding PAN
- Passengers should have the ability to ascertain whether their card is on the deny list; according to the card schemes, it is the operator's responsibility to provide this service

Tokens

A passenger can tap not only his contactless card, but also a smart watch or smartphone. When this payment method is used you should send the DPAN as the credit card number. Mastercard response will include the FPAN together with the PAR (Payment Account Reference). You will then be able to continue with the processes of the various transit models, including checking the deny list.

Revenue Inspection

Revenue inspection, when the bus/train inspector is checking that all passengers have valid tickets, should support transit transactions. It is suggested that inspection be conducted using the following flows:

Online Capable

1. Inspector taps the card on their dedicated device

The salted hashed PAN or PAR is sent to the back office

The back office validates and sends a response to the inspection device

Offline Only

1. Inspector connects to or downloads a database kept on the vehicle

Inspector taps the card

The salted hashed PAN or PAR is checked against the local database

The check outcome is sent to the inspection device

M/Chip Advance - When entry terminal uses a Merchant Custom Data

1. M/Chip Advance cards store data in the transaction log

Inspector taps the card

Inspection device checks the transaction log and verifies that an entry log exists with timestamp and custom data

Note

In cases where the inspector decides to charge a penalty, you should send a penalty transaction. The penalty can be part of the aggregation transaction, but usually the penalty fare is greater than the CVM limit.

The recommendation is therefore to send the penalty as a separate, additional retail transaction.

Appendix A: t1 Values

This section lists the t1 (transit transaction type) possible values

Value	Description	Best Practice
01	Prefunded	Use in card-as-credential model
02	Real-time authorisation	Use in known fare model
03	Authorisation for start aggregation cycle	Use in the first authorisation
04	Authorisation for end aggregation cycle	Use in the last authorisation
05	Debt recovery authorisation	Use in debt recovery cases / penalty

Appendix B: t2 Values

This section lists the t2 (transit transportation mode) possible values.

Value	Description
00	Unknown - Can be used for cases of multi transportation mode
01	Urban Bus
02	Interurban Bus
03	Light Train Mass Transit (Underground Metro, LTR)
04	Train
05	Commuter Train
06	Water Borne Vehicle
07	Toll
08	Parking
09	Taxi
10	High Speed Train
11	Rural Bus
12	Express Commuter Train
13	Para Transit
14	Self Driving Vehicle
15	Coach
16	Locomotive
17	Powered Motor Vehicle
18	Trailer
19	Regional Train
20	Inter City
21	Funicular Train
22	Cable Car

Change History

Version	Subject/Date	Description
2.0	November 2023	• Rebranding to Shift4 • Adding the option to send deferred authorization for MC also for transit operators
1.0 rev 1	October 2020	Edits to debt recovery transaction requirements and token transaction requirements.
1.0	September 2020	Release

Support Information

Contact the Shift4 Support 24/7 for any information request or technical issue.

US: +1.617.715.1977

UK: +44.20.3608.1288

EU: +356.2778.0115

Email: support.europe@shift4.com