Mastercard Global Transit Implementation Guide

January 2018

mastercard

Copyright

Trademarks

Trademark notices and symbols used in this manual reflect the registration status of Mastercard trademarks in the United States. Please consult with the Customer Operations Services team or the Mastercard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

Mastercard® is a registered trademark and Mastercard contactless™, M/Chip™ and Tap & Go™ are trademarks of Mastercard International Incorporated.

Disclaimer

Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this guide. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to the guide and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information).

Without limitation, Mastercard specifically disclaims all representations and warranties that any practice or implementation of the guide will not infringe any third-party patents, copyrights, trade secrets or other rights. Without limitation, Mastercard specifically disclaims all representations and warranties in relation to the guide, including but not limited to any and all implied warranties of suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result.

Any implementation decisions made should be taken with care and Mastercard cannot be held responsible for any action you take (or any third party takes on your behalf) as a result of this document, or any inaccuracies, inconsistencies, errors, formatting errors, or omissions in this document.

Mastercard is under no obligation to update this guide.

Classification

This document has been classified as Proprietary and Confidential.

Contact Information

Mastercard

www.Mastercard.com

Mastercard Contactless Branding

As from 31 August 2015 Mastercard contactless text, imagery, and branding is replaced by the EMV Co contactless marks plus the core Mastercard® or Maestro® brand marks.

Issuers should monitor Mastercard publications and announcements for further information regarding this and any other branding changes.

References to Rules and Mastercard Documentation

This document makes references to various Mastercard documentation, including rules and announcements. The cross references are correct at the time of publication. It is the duty of the reader to ensure that they always refer to the current Mastercard rules and documentation and the cross references in this guide should therefore not always be relied upon to be correct

Preface

Objectives

This document provides implementation requirements, guidelines, and Standards (as defined in the *Mastercard Rules* manual) for entities considering or developing contactless transit technology – for fare payment and/or system entry.

Scope

This document covers a variety of ways in which Mastercard Contactless media may be used for transit purposes, e.g.:

- Aggregating multiple journeys in one payment transaction or treating each trip/ticket as a separate transaction
- Performing real-time authorizations or deferred authorizations to a point in time after the device has been used
- Leveraging the bank card as a system access credential or using the card for payment

Audience

This document is intended for the following audiences:

- Acquirers
- Issuers: Financial Institutions currently issuing or planning to issue Mastercard Contactless credit, debit, or prepaid cards and/or Contactless devices
- Transit operators, transit authorities, and transport agencies responsible for providing transportation services to the general public
- System integrators
- Hardware and software suppliers

Assumptions

- The following assumptions are made throughout this document:
- This document is a global transit guide; regional variations will be addressed by Mastercard teams in the local markets
- The user of this document has a broad understanding of Mastercard rules for transaction processing

- The user has a reasonable business and technical understanding of:
  - Mastercard Contactless (formerly known as Mastercard PayPass)
  - EMV® Chip Specifications, which describe the requirements for global interoperability between chip-based payment applications and acceptance terminals to enable secure contact and contactless transactions. (For more information, see https://www.emvco.com/.)
- Authorization and Clearing Processes and Messages

Related Documents

All documentation listed below is available either publicly (at the Mastercard corporate website), on the Publications section of Mastercard Connect (the Mastercard business-to-business portal), or on the EMVCo website. To create a Mastercard Connect account, visit www.mastercardconnect.com.

These documents are frequently updated, so users should check back regularly to ensure they are working from the most recent versions.

Reference	Title
AUTHMAN	Authorization Manual
CBGUIDE	Chargeback Guide
CINTSPEC	Customer Interface Specification
EMVA	EMV Contactless Specifications for Payment Systems - Book A
EMVB	EMV Contactless Specifications for Payment Systems - Book B
EMVC2	EMV Contactless Specifications for Payment Systems - Book C2
EMVD	EMV Contactless Specifications for Payment Systems - Book D
IPMCLR	IPM Clearing Formats
MCASPEC	M/Chip Advance Card Application Specification (Payment & Data Storage)
MCAISSG	M/Chip Advance – Issuer Guide
MCREQS	M/Chip Requirements
MCRULES	Mastercard Rules
MTIPPG	M-TIP Process Guide
MTIPQR	M-TIP—Implementation Quick Reference Guide
MCRS	Mastercard Contactless – M/Chip Reader Specification
SRP	Security Rules and Procedures
SMSSPEC	Single Message System Specifications
TPRULES	Transaction Processing Rules

1 Introduction

The world is becoming more urban and connected – within the next generation, the number of people living in cities is expected to jump from 54 percent to close to 70 percent. As a result, cities around the world are struggling with population growth and are looking for better ways to provide their citizens with essentials such as housing, employment, banking and transportation.

Transit is the lifeblood of a city. Key to the success and vibrancy of any city is the ability to get around simply, easily, and without friction. The hundreds of different fare collection systems around the world, combined with the existence of multiple systems within individual cities, creates complexity and inefficiency for cities and passengers alike. Mastercard has a long history of working closely with cities to address these pain points. Mastercard solutions can make trains, metro systems, buses, ferries, bridges and tolls easier to use, thereby helping to reduce traffic congestion. In addition, Mastercard is developing new data-driven transit concepts and technologies that will help transit operators manage demand during peak travel times.

Based on in-depth studies of the transit environment, Mastercard has created unique solutions that help cities smoothly integrate payment, ticketing, and system access. By moving from proprietary ticketing technologies to globally standardized solutions, Mastercard is helping to break down barriers to travel, increasing convenience for passengers, and enabling significant gains in efficiency. The combination of card accounts and contactless technology can deliver operational improvements, enhance the passenger experience, and ensure fast and secure fare payments.

In 2014, Transport for London successfully pioneered a system-wide solution based on EMV contactless chip technology. There are now many transit operators in the process of implementing similar solutions — contactless payments that leverage bank-issued cards and mobile devices.

This guide addresses the challenges associated with implementing payment card-based solutions in complex transit systems in order to increase efficiency and passenger satisfaction.

1.1 Mastercard Contactless Transactions

Mastercard Contactless Chip technology enables fast, easy, secure, and globally interoperable payments. Contactless payments leverage the Mastercard EMV specification, M/Chip technology, and mobile wallet applications, and are supported by Mastercard and industry rules and operating requirements. Mastercard Contactless technology gives passengers a fast and convenient way to identify themselves that can also be leveraged for payment, ticketing, and access control.

Contactless technology may be embedded in a traditional plastic card, a mobile phone, or a range of other devices such as smart watches and other wearables. Throughout this document the term "Contactless card" should be assumed to include all Contactless-enabled devices.

Traditional contactless transactions, such as those taking place in the retail environment, may not be appropriate for the transit environment. Therefore, Mastercard has developed and optimized rules specifically for transit. These new rules enable passengers to use contactless cards to interact with contactless terminals at the point of system entry. Contactless cards and devices may grant immediate access to the system and be used to facilitate fare calculation and payment.

Contactless technology benefits all players in the transit value chain as described below.

Passengers:

- Fast progress through the transit system
- Secure and verifiable payment
- Simple transaction record
- Reduced need to wait in ticket queues
- Choice of payment options (credit, debit, prepaid, etc.)
- Range of convenient form factors including mobiles and wearables
- No need for additional closed-loop payment cards
- Globally interoperable and familiar solutions

Transit Operators:

- Improved customer experience: automated fare collection and fast system access using existing payment cards
- Smoother passenger flow through entry points
- Resource shift from payment functions to core transit operations
- Reduced operational expenses (via process simplification)
- No need for long-term commitment to proprietary technology
- Potential for increased ridership

Acquirers:

- Access to high-volume transit merchants
- Opportunity to add value beyond transaction processing
- Opportunity to meet specific customer (transit operator) requirements using standard Mastercard Contactless technology

Issuers:

- Greater customer (cardholder) convenience
- Potential to create customer loyalty and increase/habituate usage
- Incremental revenue generation

1.2 Overview of this Guide

This document sets forth Mastercard rules, requirements, and recommended best practices for entities implementing Contactless card-based transit programs for payment and/or system access. It describes the transaction flow, authorization and clearing messages, payment liability, risk mitigation, and potential impacts on acquirer and issuer systems. It also points users to detailed specifications and other supporting material.

The guide is structured as follows:

1. Introduction	Introduces the challenges and opportunities associated with implementing contactless card-based solutions into complex transit systems.
2. Mastercard Rules and Requirements	Serves as a quick summary of Mastercard rules and other regulations pertaining to transit transactions.
3. Transaction Flows	This chapter describes the different messages and data involved in completing transit transactions.
4. Issuer	Addresses transit-related challenges that are important to issuers.
5. Acquirer	Addresses transit-related challenges that are important to acquirers.
6. Transit Operator	Explains the role and responsibilities of the transit operator, which acts as merchant for the payment transaction but also performs many other customer-facing functions.
7. Systems Integrator	Describes the role of the systems integrator, which brings together features of different systems to create an integrated transit payment solution.
8. Transit Terminal and Reader Requirements	Provides an overview of the acceptance side of a Contactless transaction and details unique characteristics related to transit.
9. PCI	Provides an overview of industry-wide data security requirements.
10. Certification and Testing	Describes the different types of testing required to implement the transit payment eco-system, the steps involved, and the parties responsible.

1.3 Transit Ecosystem

The demands of the transit environment make it different from the traditional retail payment environment. Specifically, the transit environment requires:

- Fast and secure payments
- Control of access to the transit system (generally referred to as "permission to travel")
- Ticketing – beyond simple system access, ticket inspection establishes that the individual is authorized to take a specific trip
- A flexible relationship between access and payment, as final transaction amount is often not known until the journey is complete
- Mastercard delivers on all of these requirements through a range of transit models and related business rules that support acceptance of a broad range of contactless cards.

1.3.1 Roles and Responsibilities in the Transit Environment

Passenger

A passenger is a person holding a contactless-enabled card, mobile device, or wearable device that accesses a debit, prepaid, credit, or charge account issued by a financial institution. A passenger uses their contactless card or device in the transit network by tapping it on the contactless card reader to gain access to the system (also called "tapping in"). In some cases, a passenger will also have to "tap out" so the system can calculate the correct payment for a completed trip.

Transit Operator

The transit operator acts as the merchant, and is often supported by other solution providers and integrators. The transit operator sells trips to passengers.

The transit operator will contract with an acquirer for authorization and clearing of transactions. In addition to the transit operator and the acquirer, there may be other entities involved in transaction processing – e.g., systems integrators providing services such as gateways and switches.

Issuer

An issuer is a financial institution that provides payment card accounts to passengers.

Issuers have responsibility for transactions made using card accounts they have issued, and are responsible for debiting funds from passenger (cardholder) accounts.

Acquirer

An acquirer is a financial institution that supports the transit operator. The acquirer is responsible for authorizing and settling payments on behalf of the transit operator.

Mastercard

Mastercard manages and controls the operation of card payment transactions and supports payment settlement between all parties. Mastercard has established rules for the transit environment to address its specific needs.

Mastercard enables rapid authorization of transit transactions. Final transaction details are sent to the issuer at the end of the day, and Mastercard manage transaction settlement (moving funds from the issuer to the acquirer so the acquirer can, in turn, pay the transit operator).

Mastercard rules govern the terms and conditions under which transactions are performed. These rules ensure that all parties involved know exactly what is expected of them. These rules and other important documents can be downloaded from the Mastercard.com website (see Related Documents).

Mastercard also preserves the integrity of the payment system, working proactively and collaboratively with all stakeholders to minimize risk. The following modules, also available on the Mastercard website, explain Mastercard's Global Compliance Programs and how they help to manage risk:

- Business Risk Assessment and Mitigation (BRAM)
- Excessive Chargeback Program (ECP)
- Global Merchant Audit Program (GMAP)
- Member Alert to Control High-Risk Merchants (MATCH)
- System to Avoid Fraud Effectively (SAFE) Compliance

1.3.2 Why is Transit Different?

Transit environments utilize a wide range of payment types, and each transit system has different needs. Therefore, there is no single definition for "transit transaction". Transactions may be originated via online purchases (requiring no interaction between a card and a reader), in-app purchases (where device-generated one-time passwords may be involved), at attended or unattended ticket offices (where more typical payment transactions are performed), and/or at devices that control access to the system (e.g, a metro gate). Transactions may require online, real-time connectivity to the payment system, or may be conducted using a combination of offline and online interaction – e.g. offline chip authentication to ensure a device is genuine and subsequent online authorization to ensure funds are available.

A key requirement in many transit use cases is the need for speed. This requirement is typically addressed through a combination of:

- Contactless technology
- Parameters that reduce or eliminate the need for passenger (cardholder) verification (e.g. PIN entry)

Differing requirements for Cardholder Verification Method (CVM) across use cases have, in turn, created a need for different configurations of readers and other acceptance components. The CVM limit is the amount below which cardholder verification is not required. The limit, which varies by market, pertains to the total value of the transaction even when several fares are aggregated into one payment.

1.4 Mastercard Transit Solutions

Mastercard supports transit operators around the world with solutions that support the specific needs of their operational environment. All Mastercard transit solutions are designed to:

- Deliver a fast, intuitive, and simple passenger experience
- Provide security for transit operator revenue collection
- Enable several trips to be aggregated into a single payment

- Support varied fare structures and regimes
- Manage risk effectively given operational demands
- Address demands beyond payment (e.g., permission to travel)

In most proprietary transit models, ticket/fare information is stored on the card issued by the transit operator and used by the passenger for travel. The open-loop Mastercard solution supports account-based ticketing, meaning that ticket/fare details are stored in the transit operator's back office systems rather than on the transit or payment card.

1.4.1 Types of Transit Transactions

Based on considerable experience in the field, Mastercard has broadly defined four transit payment models:

1.4.1.1 Retail-Like Acceptance

Retail-like acceptance allows a transit operator to install Mastercard contactless terminals in their transit system – either at ticketing machines or at the point of entry. When a Mastercard contactless card interacts with a reader, a standard Mastercard retail transaction takes place. For low-value contactless transactions, transit operators may decide to support both offline and online authorization; this decision is dependent on the availability of telecommunications, passenger throughput constraints, and the operator's risk appetite. The retail-like solution works well when the full fare is known at the point of entry or purchase (e.g. fixed train fares, ride shares, ticket vending machines, etc.) and is used most often on buses and trams.

Because communications may not be reliably available in certain systems, two different authorization models may be implemented:

- Real-time authorized – authorization is conducted before the journey commences, ensuring funds are available and the card is in good standing. With real-time authorization, there is inevitably a short delay while the authorization takes place; therefore, this model is best suited to payment transactions that are not linked to the point of entry.
- Deferred authorization –authorization is not conducted until the passenger has begun their trip. This enables fast access to the transit system, but introduces risks that need to be mitigated – e.g., by checking against local Deny Lists (see Section 6.2) and enabling debt recovery transactions if the payment transaction is declined after travel has started. Deferred authorization always takes place in an online environment.

When retail-like acceptance is used with real-time authorization, transactions flow as they do in other environments; therefore, these types of transactions are not covered further in this document. When retail-like acceptance is used with deferred authorization, special attention should be paid to the content of authorization messages, debt recovery transactions, and other requirements described in this manual. (Note: there

are specific rules and restrictions in the U.K. with respect to the use of debt recovery for retail-like transactions, and other markets may introduce similar rules in the future.)

1.4.1.2 Card as Credential to Travel

Card as Credential is a pre-purchase model, whereby a Contactless card or device is associated with a passenger's fare media or concessionary entitlement. This option permits the passenger to travel by using the card at a reader as specified by the transit operator. The card is then recognized as a credential to travel throughout the passenger's trip, and presented for inspection upon request.

In the Card as Credential model, the passenger experience might work as follows:

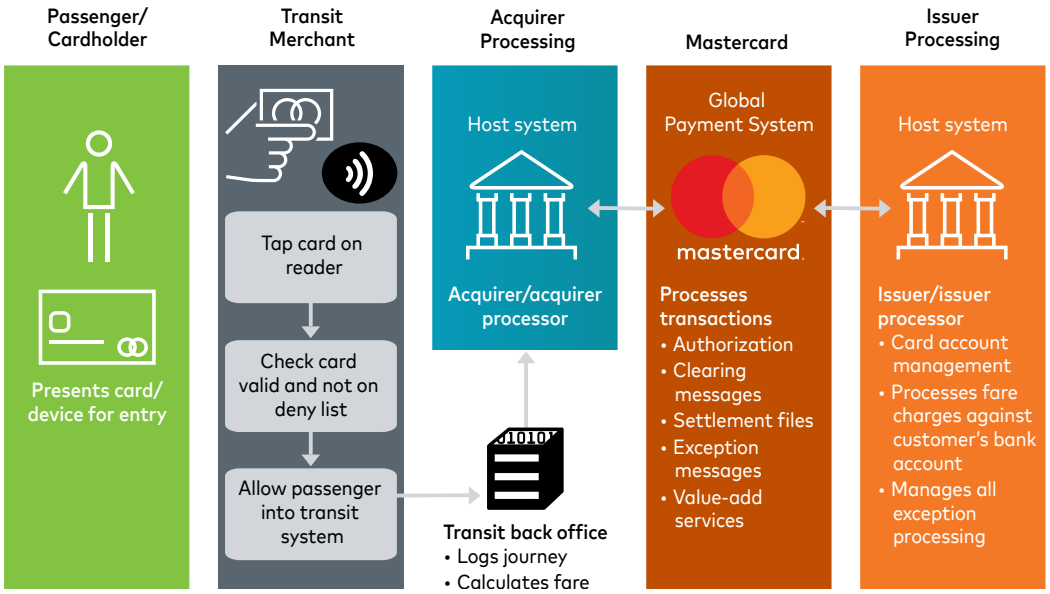
- Passenger buys bus travel online and chooses to use a Contactless card as their 'ticket' or 'authority/credential' to travel.
- Customer accesses bus by using the Contactless card at a reader at the station or on the bus
- Passenger see all completed trips on the transit operator's website
- Passenger can view transit payment details on their card statement

1.4.1.3 Pay As You Go (PAYG) Travel

Pay As You Go (PAYG), also known as Aggregation, typically involves multiple uses of a card which are aggregated into a single payment. By separating the trip from the payment, a transit operator can:

- Manage more complex pricing structures, such as weekly or monthly fare caps
- Review all completed travel at the end of a time period and calculate the best rate
- Support off-peak and concessionary fares
- Collect payment even when the final destination is not known at the start of the trip
- Support itineraries that include various transit modes (e.g. bus to train to metro)
- In this model, a single payment transaction combines one or more "taps" of the card (see Diagram 1).

Diagram 1: Stakeholder functions during PAYG



Each "tap" equates to one use of the contactless card at the transit system's contactless reader.

At the passenger's request, the transit operator must be able to provide a list of the trips (date and fare for each trip taken) that were combined into the single transaction that appears on the card statement. This information may be made available via the transit operator's app, website, and/or call-center.

In the PAYG/Aggregation model, the Contactless card is used both as the credential for travel and as the means of payment: contactless taps are recorded, trips are tracked, and the appropriate fare is calculated. Fare calculation does not necessarily happen while the passenger is traveling. Fares are aggregated into a single payment transaction at the end of a day or some other time period.

For security and credit control purposes, periodic authorizations must occur when a predetermined amount is reached or a predetermined time period has expired.

This solution works well for large multi-modal transit systems especially those with complex fare structures.

Note: for the purposes of this document, the term Pay As You Go (PAYG) has the same meaning as Aggregation.

1.4.1.4 Mobile Ticketing

Through partnerships, Mastercard offers mobile ticketing solutions that are available on any mobile device with a built-in screen. The ability to purchase and display tickets on mobile devices gives passengers a more convenient way to travel. In addition to providing a better passenger experience, this model provides transit operators with a customizable platform that reduces the customer service burden and significantly reduces operational costs.

In this model, fares are purchased and displayed using the transit operator's mobile application. Tickets are displayed on the device screen as readable images, QR codes, or Bluetooth credentials. The app may be linked to several underlying payment methods or wallets. Mastercard's digital wallet, called Masterpass, is used in mobile ticketing for fare purchase. Tickets are visually checked or scanned by inspectors, or are scanned at a device at the point of entry.

The mobile ticketing model is not covered further in this document; for more information, please contact your local Mastercard representative.

1.5 Engagement with Mastercard on a Transit Program

Mastercard has many tools and resources all over the world that support transit programs, from conceptualization through delivery. The Mastercard Customer Delivery team acts as the key contact between transit operators or systems integrators and other Mastercard business units to ensure successful implementation.

The key components to a transit implementation project plan are:

- Selection of a transit payment model
- Supplier identification and management
- Development of risk management parameters and processes
- Preparation for transaction processing, including incorporation of transit-specific data in messages
- Creation of passenger interfaces
- Testing
- Reporting
- Marketing
- Identification of project milestones

1.5.1 Mastercard Business Partner Program for Vendors and Suppliers

The Mastercard Business Partner Program (MBPP) is a global program designed to facilitate information flow and enhance the business relationship between Mastercard and the companies that supply solutions to Mastercard customers around the world.

Three levels of participation are available: Gold, Silver and Bronze. A package of standard services is provided at all levels, with advanced services available based on the vendor's participation level.

Transit operators should expect each of their suppliers to participate in this program by contacting Mastercard Business Partner Relations at business.partners@mastercard.com.

2 Mastercard Rules and Requirements

This chapter serves as a quick reference to the Mastercard rules and other regulations relevant to transit transactions. It also includes an overview of the type of information to be found in different publications which may also pertain to the processing of transit transactions.

The chapter does not attempt to fully describe the rules relating to transit transactions, but highlights where transit environment rules diverge from those of general card acceptance environments. In several cases, the relevant rule is excerpted from the guide in question and presented in a shaded text box.

2.1 Summary of Rules and Regulations Documentation

Mastercard Rules [MCRULES] contain the fundamental rules relating to Mastercard membership, the rights and obligations of members, and the fundamental roles of different parties.

Transaction Processing Rules [TPRULES] relate specifically to the transaction, describing the requirements, expectations, and obligations of different parties in the processing of a payment.

Chargeback Guide [CBGUIDE] details specific exception cases. "Chargeback" is the term used to describe a transaction that is rejected by the issuer because some aspect of the Transaction Processing Rules has not been followed. This Guide codifies common disputes and details the requirements to initiate chargebacks.

Authorization Manual [AUTHMAN] describes the function and requirements of authorization. Detailed message specifications are contained in [CINTSPEC] and [SMSSPEC].

Security Rules and Procedures [SRP] discusses the factors that impact the security of payments and identifies which parties are responsible for each. It references specific Mastercard security-related programs as well as industry-level initiatives such as PCI.

M/Chip Requirements [MCREQS] identifies Mastercard requirements for implementing chip technology, including contactless chip on cards and terminals.

IPM Clearing Format [IPMCLR] details the technical requirements for clearing messages, detailing requirements for each data element and indicating when each element should be used.

Customer Interface Specification [CINTSPEC] details the technical requirements for authorization and authorization response messages in a dual message environment.

Single Message System Specifications [SMSSPEC] details the technical requirements for financial request and financial response messages in a single message environment. These specifications are used for various transaction types and in various regions; the exception is Maestro transactions inside the Europe Region – these are always dual message transactions.

All of these documents are updated periodically; updates are announced in Mastercard Operations announcements.

The requirements detailed in the IPM Clearing Format, Customer Interface Specification and Single Message System Specifications are also covered in the discussion of transaction flows in Chapter 3 of this Guide.

All documentation is available on Mastercard Connect.

It should be noted that regional or country specific rules exist. All parties should refer to the appropriate local documentation and ascertain whether any local rules apply in their situation.

2.2 Mastercard Rules

2.2.1 Brand Value Transaction (BVT)

The Brand Value Transaction rules relate to the use of a Mastercard card as the key to access other proprietary systems. Rule 6.6.2 specifically allows a BVT for the purpose of "Proprietary System Payments". Example: a passenger decides to pre-purchase fare value or a time-based pass product (such as a daily, weekly, monthly, or annual transit pass) with a Mastercard payment device at a fare vending machine, staffed ticket office, transit agency website, or through a mobile application. The contactless card associated with that same Mastercard account is then used at the point of entry, which is considered a BVT.

The purchased fare value is decremented by the back office of the transit agency, or the purchased time-based pass product is verified as valid or expired as per transit agency fare rules.

2.3 Transaction Processing Rules

2.3.1 Contactless Transit Aggregated Transactions

The rules relating to the use of aggregation for transit are described in this guide. Aggregated transactions occur when the transit operator combines multiple contactless taps, representing multiple trips by a passenger in the system, into a single transaction amount.

Note that use of aggregation requires an up-front authorization which is limited by amount (defined by market) or by time (maximum 14 days).

Contactless Transit Aggregated Transactions
A Contactless transit aggregated Transaction must not exceed the applicable Contactless transit aggregated Transaction limit, as defined in Appendix E.

MasterCard Contactless Transit Aggregated Transactions
MasterCard Contactless transit Transactions are permitted only in connection with specific MCCs and can be pre-funded, real-time authorized, aggregated, or for debt recovery.

A MasterCard Contactless transit aggregated Transaction occurs when the transit Merchant's Acquirer generates a First Presentment/1240 message combining one or more contactless taps performed with one MasterCard Account at one transit Merchant. A "tap" means the Cardholder's tap of the Card or Contactless Payment Device on the contactless reader of the POS Terminal with each ride taken. In order for the transit Merchant to receive chargeback protection, all of the following must occur:

1. The Merchant must send a properly identified Authorization Request/0100 message (which can be for any amount).
2. The Issuer must approve the Transaction.
3. The combined amount of the taps must be equal to or less than the applicable chargeback protection amount.
4. The maximum time period from the first tap until the First Presentment/1240 message is generated must be 14 calendar days or less.

Upon the Cardholder's request, the Merchant must provide a list of the taps (the date and fare for each ride taken) that were combined into a First Presentment/1240 message.

For MasterCard Contactless transit aggregated Transaction identification requirements, see Appendix C.

Extract from Transaction Processing Rules

2.3.2 Maestro Contactless Transit Aggregated Transactions

The rules for Maestro differ from those for Mastercard because Maestro transactions are completed as single message (combined authorization and clearing) outside of Europe. This means that at the time of the initial authorization a "hold" is put on funds for a limited timeframe (max 3 days), and at the end of the period any unused amount must be reversed. The passenger must be informed of the amount that will be held and the timeframe of the hold.

Maestro Contactless Transit Aggregated Transactions
A Maestro Contactless transit aggregated Transaction occurs when the Acquirer generates a Financial Transaction Request/0200 message for an estimated or maximum amount in connection with the use of one Maestro Account at one transit Merchant. A Maestro Contactless transit aggregated Transaction must be processed as follows:

1. The Merchant sends a Financial Transaction Request/0200 message with a value of 06 in DE 48, sub element 64, subfield 1 (Transit Transaction Type Indicator) for an estimated or maximum amount not to exceed the applicable Contactless transit aggregated Transaction ceiling limit amount.
2. The Issuer must approve the Transaction.
3. The Cardholder may make subsequent taps for additional rides; these taps will not be sent to the Issuer for authorization. The combined amount of the taps must be equal to or less than the applicable Contactless transit aggregated Transaction ceiling limit amount.
4. When the limit is reached or within three calendar days, the Merchant totals the value of all taps and generates an Acquirer Reversal Advice/0420 to reverse any unused funds. The Merchant must inform the Cardholder that the amount held from the available funds in the Account may be greater than the cost of a single fare, and the Merchant must inform the Cardholder of the amount of time that the Merchant requires to reverse all unused funds. This information may be provided on the Merchant's Website, included in call center scripts, and/or displayed within the transit Merchant's system. The Merchant must also provide specific tap information to the Cardholder upon request..

For Maestro Contactless transit aggregated Transaction identification requirements, refer to Appendix C.

Extract from Transaction Processing Rules

2.3.3 Transit Transactions Performed for Debt Recovery

This rule specifically enables the use of debt recovery transactions for Mastercard and Maestro when the card is not present and no PIN is entered. Debt recovery can also be used in conjunction with aggregation and retail-like transactions in transit. (Note: there are specific rules and restrictions in the U.K. with respect to the use of debt recovery for retail-like transactions, and other markets may introduce similar rules in the future.)

Transit Transactions Performed for Debt Recovery
An Issuer of Maestro Cards that allows its Cardholders to perform Maestro Contactless transit aggregated Transactions must be able to accept and must make an individual authorization decision for each transit debt recovery Transaction identified as a Card-not-present Transaction (for example: as a PAN key-entered, e-commerce, or mail order or telephone order (MO/TO) Transaction) when the Authorization Request/0100 or Financial Transaction Request/0200 message is properly identified with:

- A value of 07 (Debt Recovery) in DE 48 (Additional Data), sub element 64 (Transit Program), subfield 1 (Transit Transaction Type Indicator); and
- An amount in DE 4 (Amount, Transaction) that is less than or equal to the applicable Maestro Contactless transit aggregated Transaction ceiling limit.

Extract from Transaction Processing Rules

2.3.4 Contactless-Only Acceptance

Contactless-only acceptance is permitted in transit environments.

Contactless-only Acceptance
Where approved by MasterCard (either on a country-by-country or case-by-case basis), an Acquirer may sponsor Merchants that deploy POS Terminals or MPOS Terminals that utilize only contactless payment functionality.

1. Merchants that deploy single-vehicle parking meters (MCC 7523)
2. Merchants that deploy single-ride bus fare collection devices (MCC 4131)
3. Merchants that use the following MCCs:
   a. MCC 4111—Transportation—Suburban and Local Commuter Passenger, including Ferries
   b. MCC 4112—Passenger Railways
   c. MCC 4789—Transportation Services—not elsewhere classified

Extract from Transaction Processing Rules

2.3.5 Transaction Receipts

Transaction receipts need not be generated/made available at the time of the transaction.

Contactless-only Acceptance
POS Terminals that utilize only contactless payment functionality at Merchants identified with the following MCCs are not required to provide a Transaction receipt at the time the Transaction is conducted; however, the Merchant must have a means by which to provide a receipt to the Cardholder upon request. If such means involves the storage, transmission, or processing of Card data, then it must comply with the Payment Card Industry Data Security Standard (PCI DSS). The manner in which to request a receipt must be clearly displayed at the Merchant location.

- MCC 4111—Transportation—Suburban and Local Commuter, Passenger, including Ferries
- MCC 4112—Passenger Railways
- MCC 4131—Bus Lines
- MCC 4789—Transportation Services—not elsewhere classified
- MCC 7523—Automobile Parking Lots and Garages

Extract from Transaction Processing Rules

2.4 Chargeback Guide

Chargebacks are used to dispute liability for transactions when a loss has occurred and the acquirer or merchant has not properly processed the transaction according to Mastercard rules. In the case of transit transactions, disputes are extremely uncommon.

The Chargeback Guide exempts contactless transit aggregated transactions from authorization-related chargebacks when the authorization is properly identified as transit, is submitted in the appropriate time window, and does not exceed the published limit. This allows the authorization to be for a nominal amount rather than the full value of the transaction (which is not known at the time of the authorization). There are other specific exemptions from chargebacks for contactless transit aggregated transactions relating to the use of a nominal amount and the time allowed between authorization and clearing.

If a transaction amount exceeds the contactless transit aggregated transaction limit, the issuer may only dispute the amount in excess of the limit and not the full amount, provided all requirements have been complied with.

The specific requirements to properly identify a contactless transit aggregated transaction in the clearing record are shown in Appendix F of the Chargeback Guide.

2.5 Authorization Manual

2.5.1 MCCs for Transit

The requirements to obtain chargeback protection for post-authorized aggregated contactless transit transactions are described in Section 3 of this guide. The MCC codes under which contactless transit aggregated transactions may be processed are:

- 4111 (Transportation-Suburban and Local Commuter Passenger including Ferries)
- 4131 (Bus Lines)
- 4784 (Bridge and Road Fees, Tolls)

Post-authorized Aggregated Contactless Transit Transactions
A post-authorized aggregated contactless transit transaction occurs when the transit merchant generates a First Presentment/1240 message combining one or more contactless taps performed with one contactless account number and occurring with one transit merchant.

For the contactless transit merchant to receive chargeback protection all of the following must occur:

- The transit merchant must send a properly identified Authorization Request/0100 message, which can be for any amount not exceeding the cardholder verification method (CVM) limit amount, as published in Chargeback Guide on the day of the transaction.
- The issuer must have approved the transaction.
- The combined amount of the contactless taps must be equal to, or less than, the cardholder verification method (CVM) limit amount, as published in the Chargeback Guide.
- The maximum time period from the first contactless tap until the First Presentment/1240 message is generated must be 14 calendar days or less.

Note: These transit transactions are limited to MCCs 4111, 4131, and 4784.

Upon the cardholder's request, the transit merchant must provide a list of the contactless taps that were combined into a First Presentment/1240 message.

Extract from Authorization Manual

2.5.2 PAN-Association Requirements for Transit

The Authorization Manual describes the requirement for issuers to supply the Primary Account Number (PAN) to the transit operator in the authorization response message when the contactless device being used supports a tokenized PAN.

Issuers that issue alternate account numbers for contactless products and respond to Authorization Request/0100 messages from MCCs 4111, 4131, 4784, and 7523 must provide the following values in DE 48 (Additional Data—Private Use), sub element 33 (PAN Mapping File Information) when sending the Authorization Response/0110 message.

- Subfield 1 (Account Number Indicator), value E (Embossed Account Number Provided by Issuer)
- Subfield 2 (Account Number), embossed PAN
- Subfield 3 (Expiration Date), expiration date of the embossed PAN

For issuers participating in the MDES, these values will be automatically populated on their behalf in the authorization response messages.

This helps ensure that the pre-purchased fares by cardholders using the embossed PAN are properly associated with their turnstile requests. This will also help ensure proper customer service.

Acquirers processing for merchants belonging to MCC 4111, 4131, 4784, and 7523 must provide the DE 48, sub element 33 details when present in the authorization response message back to the merchants belonging to these MCCs upon their request.

Extract from Authorization Manual

2.6 Security Rules and Procedures

The Security Rules and Procedures Manual describes the security requirements for different parties to the transaction; nothing in the Manual is transit specific. However, transit operators and systems integrators need to consider the different aspects of their program – e.g., if the card number is used for fare calculation as well as payment – and determine how the data should be protected. The PCI requirements particularly apply to:

- Systems where payment data is stored
- Devices that access or read payment data

Mastercard Site Data Protection (SDP) Program
Note: This section applies to Mastercard and Maestro Transactions.

The Mastercard Site Data Protection (SDP) Program is designed to encourage Customers, Merchants, Third Party Processors (TPPs), and Data Storage Entities (DSEs) to protect against Account data compromises. The SDP Program facilitates the identification and correction of vulnerabilities in security processes, procedures, and website configurations. For the purposes of the SDP Program, TPPs and DSEs are collectively referred to as "Service Providers" in this chapter.

Extract from Security Rules and Procedure

2.7 M/Chip Requirements

The M/Chip Requirements document describes Mastercard requirements for implementing chip technology, including contactless chip on cards and terminals. The document contains a number of specific references to transit, in particular:

2.7.1 Application Transaction Monitoring

See 4.5.3 below.

2.7.2 Transaction Certificate Received in Online Request

The Transaction Certificate (TC) is a cryptogram generated by the contactless card when a transaction is approved. Normally, no authorization is required if a TC is generated during a contactless transaction.

In certain acceptance environments, a TC may be received from the card and used in a subsequent online request. This may occur in certain transit implementations. Issuers may not decline an authorization for the sole reason that the cryptogram received in an online request is a TC. (RI050.11)

2.7.3 Application Transaction Counter Update Requests

The Application Transaction Counter (ATC) is a sequential counter managed by the contactless card to ensure all cryptograms produced are unique.

ATC update requests notify the issuer that multiple "taps" have occurred and incremented the ATC; however, these requests do not generate an authorization request or clearing record.

In different transit implementations a contactless transaction may be used to enable entrance or exit from the transit system or for checking authority to travel. These transactions will only be sent online periodically to be authorized by the issuer.

To avoid that issuers are unaware that multiple transactions have been completed by the card or device, and thus the ATC has been incremented more than may be usual (which may in turn create unexpected declines), transit merchants that operate in this way must periodically send either a new authorization or an ATC Update to the issuer.

Transit merchants must, therefore, send an ATC update message at least once every 20 times a card is used since the last approved transaction from the issuer.

There is no requirement that the authorization/update message be completed in real-time before the cardholder is granted access to the system. The message must contain the DE 55 information from the most recent card tap.

Extract from M/Chip Requirements

3 Transaction Flows

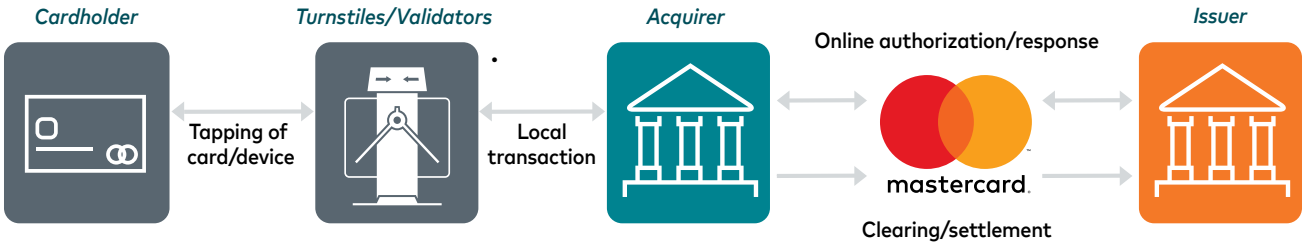
This chapter describes the messages and data involved in processing transit transactions. Detail is provided on the special data values required to identify transit transactions.

3.1 General processing flows

Transit transactions follow the same general Contactless transaction flow associated with retail transactions.

- Contactless chip protocols are used to establish the authenticity of the card during the interaction with the card reader (terminal). The interaction with the chip may also evaluate the credit risk of the transaction and/or verify the cardholder.
- An online authorization message establishes the availability of funds and checks to make sure that the card is valid for use (e.g. has not been reported as stolen).
- A clearing message subsequently confirms the full details of the completed transaction and includes the final fare amount.
- Settlement occurs when bulk amounts are exchanged (amounts including the transaction described above as well as others).

Diagram 2: Transit Transaction Flow



Single-message systems, used by Maestro in all regions except the Europe Region, combine the authorization and clearing messages into a single online message.

In the context of transit environments, the precise way in which the various processing steps occur may vary. When deferred authorizations are conducted after a card has been used as a credential to access the system, only the card-reader interaction (and not authorization) may occur at the outset of the transaction – establishing that the card is an authentic credential and not a counterfeit or fake device. Transit operators may also, at this stage, check to ensure that the card is not a known credit risk or flagged as 'blocked'.

The deferred authorization message, while typically processed in retail environments before goods are released, may occur in the transit environment after a trip has commenced. This is to ensure that entry to the system is not delayed while awaiting online confirmation. At the time of the deferred authorization message, the final transaction amount may not be known. In PAYG/Aggregation implementations, deferred

authorizations may be used at different stages of the travel/payment process to perform different functions.

Clearing messages are requests for payment of a specific sum. The amount and transaction details are what the passenger (cardholder) will see as on their account statement. In PAYG implementations, the final transaction amount is unlikely to be the same as the authorization amount. The precise liability of the different parties depends on the nature of the implementation and is also market-specific.

Settlement is a function between issuer and acquirer banks through the Mastercard system. Transit operators and passengers are not directly involved in settlement, but as a result of the process the passenger's account is debited and the transit operator receives payment for the trips undertaken.

3.1.1 Types of Contactless Payments

Contactless payments to support Mastercard product transactions follow the EMV Book C2 specification. This document assumes that transactions are completed using "EMV Mode".

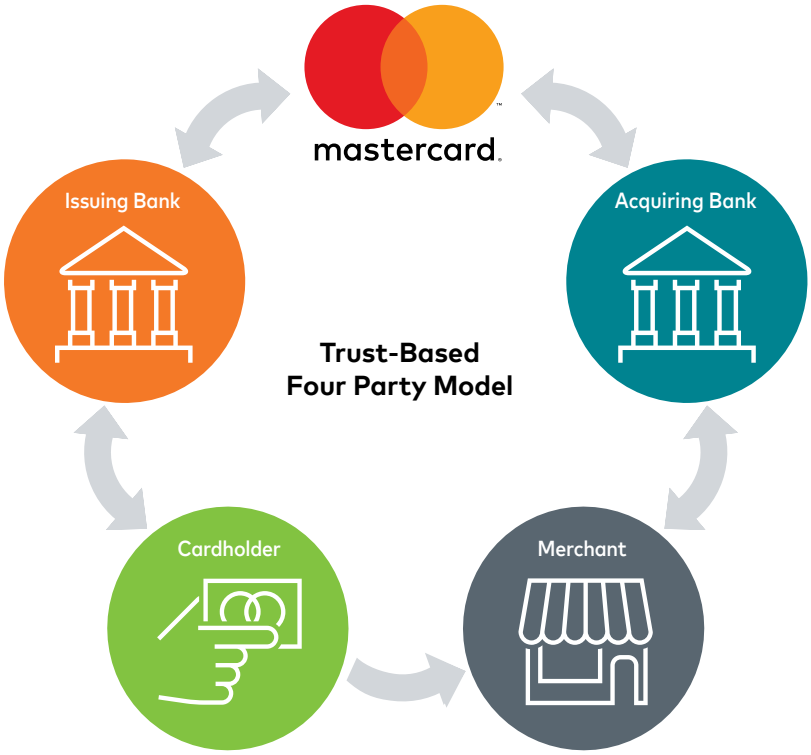
In markets that have not implemented EMV, an alternative method known as "Mag Stripe mode" is used. With Mag Stripe mode the authenticity of the card can only be established online by the issuer; for this reason, it cannot be used for the offline authentication typically required for fast entry to a transit system. In the US, EMV migration has been occurring over the past few years. While some contactless Mag Stripe mode transactions and/or devices still exist, their prevalence is diminishing.

Technologies that read a card without it being dipped / swiped, but that do not use NFC technology or follow EMV specifications, are not considered "contactless payments" by Mastercard and are not covered in this document.

3.2 Four Party Model

The payment process described above is often referred to as the "four party model," with two banks (the issuer and acquirer) responsible for supporting the passenger and the transit operator (the cardholder and the merchant) throughout the payment process.

Diagram 3: Four Party Payment Model



3.2.1 Roles and Responsibilities in Four Party Model

The players in the four-party model were introduced in Chapter 1. With respect to payment, their roles are as follows:

Passenger

A passenger is an individual holding a debit, prepaid, credit or charge card issued by a financial institution. A passenger is a customer of that financial institution, and as a customer of the transit operator is required to make payment for trips taken.

Transit Operator

The transit operator sells trips to the passenger (its customer).

The transit operator contracts with an acquirer for the authorization and clearing of transactions. In addition to the merchant and the acquirer, there may be other entities involved in transaction processing – e.g., providing services such as gateways and switches.

Issuer

The issuer is the passenger's bank or financial institution. The issuer authorizes payment transactions, manages the card account, and handles other issues on behalf of the passenger (their cardholder).

The issuer has responsibility for transactions made on cards they have issued and are responsible for debiting funds from the passenger's account.

Acquirer

The acquirer is the bank that supports the transit operator. The acquirer manages the interface between the transit operator and the payment

network and ultimately ensures the transit operator is paid for the trips taken on their system.

Mastercard Global Processing Network

Mastercard provides the technology that enables transit payments, handles payment settlement, and sets rules and policies for payments in the transit environment.

3.3 Transaction Flows in Different Transit Implementations

3.3.1 Retail-Like Acceptance

Payment transactions within the Retail-Like environment operate the same way as regular POS transactions.

In many cases, the final amount of the transaction is known at the time of transaction authorization, meaning the value used in authorization and the final transaction amount will be the same. When the final amount is not known in advance, an authorization may be performed for an estimated or maximum amount (maximum amounts vary by market and by mode of transportation); the authorization must be adjusted when the final transaction amount becomes known. Note: prompt adjustment is particularly important in the case of prepaid and debit cards, in order to avoid withholding balances from cardholders for protracted amounts of time.

Authorizations may be performed in real-time or on a deferred basis if a card is used as the key for entry into the transit system. When authorizations are deferred, the transit operator is taking a certain amount of risk until authorization has been approved. It is therefore essential that other risk control systems (e.g., authenticating the card to ensure it is genuine, or barring entry to cards which have an outstanding indebtedness to the system) are implemented before entrance to the system is allowed. Deferred authorizations should be handled as described in the PAYG section below.

3.3.2 Card as Credential to Travel

In the Card as Credential model, the underlying transit transaction is either a retail-like payment or, more often, an e-commerce transaction. There are no special requirements relating to the transaction.

The way in which the card is then used as a travel credential can vary; it may leverage the transit operator's fare database or the data storage capability of the chip card, but it is distinct from payment processing. If card data is used as part of the travel credential, Payment Card Industry (PCI) security requirements must be observed (see Chapter 9).

3.3.3 Pay As You Go (PAYG) – a.k.a. Aggregation

The remainder of this chapter describes deferred authorization and PAYG impacts on retail-like acceptance.

3.4 Deferred Authorization Transaction Flows

3.4.1 Contactless Chip Transaction

Under the deferred authorization and PAYG models, at the point of entry a contactless chip transaction is performed for a zero value. A zero value is used so as not to impact the card risk-based counters (typically ATCs). The terminal may be configured as "online only" or as "offline capable". "Online only" means that the terminal need only check for reasons to decline the transaction, as identified by events indicated in the Terminal Verification Results (TVR) matching bits in either the Terminal Action Code (TAC) or Issuer Action Code (IAC) decline. "Offline capable" means that the terminal action analysis stage checks for reasons to decline the transaction and checks to see whether online authorization is required; both reasons to decline and online authorization requirements are identified by events indicated in the TVR matching with bits set in either the TAC or IAC online. Whether the result is to request online authorization (using an Authorization Request Cryptogram, or ARQC) or offline approval (using a TC), a deferred authorization will still be requested.

Terminals will be configured by the acquirer or system integrator as "No CVM," meaning that no cardholder verification will be required for the transaction. Some mobile implementations require a cardholder Device CVM (CDCVM) in order to activate the device's payment application; any such CDCVM is unrelated to any subsequent chip-based payment transaction associated with that device.

Regardless of configuration, the terminal will request an ARQC at the first GENERATE AC command stage. If the transaction is declined for any reason at this stage, the transaction has failed and access to the transit system should not be allowed. Implicit in this is the successful completion of offline data authentication, also known as Combined Data Authentication (CDA), meaning that the card being used is authentic. If an ARQC is produced by the card, an authorization is not performed at this stage. If a TC is produced by the card, a deferred authorization will still be required. The TC cryptogram and associated data must be retained and will be used in subsequent authorization request(s).

3.4.2 Authorizations

3.4.2.1 Types of Authorization

Authorizations are handled in many different ways in PAYG implementations. This section describes the types of authorization messages that can be generated. The detailed values required in the authorization request (0100) or financial request (0200) message under each scenario are shown in the table that appears later in this section.

Nominal Authorizations (also known as Pre-Authorizations)

Nominal Authorizations (known as Pre-Authorizations in some markets) typically occur soon after a passenger taps in, and are either for a nominal amount or for the maximum possible amount. Local rules might establish a maximum liability for nominal amount authorizations.

Nominal Authorizations may occur in the following cases:

- Upon the first tap of a contactless card that the transit operator has not previously encountered
- Upon the first tap of a contactless card that has not been used at the transit operator for over 14 days (i.e. there has been no successful authorization using that card for over 14 days – suggesting an infrequent traveler)
- Upon the first tap of any card that was previously on the Deny List, but for which any issues have since been resolved (e.g., debt having been cleared). Only the first authorization after removal from the Deny List is required to be of the Nominal Authorization type.

A Nominal Authorization need not occur for every trip, nor on every day. An existing Nominal Authorization, covering the current aggregation period and volume, may still be available, even though some part of that Nominal amount may already have been used for earlier travel.

Note: Nominal Authorization requirements may vary for different product types (e.g., Maestro vs. Mastercard) and in other markets (e.g., local v international cards) where liabilities and protections may vary. In some markets, international cards may require authorization on every travel day.

Note: that the value of the authorization will be different from the zero value used to generate a chip cryptogram.

End of Day Authorizations

End of day authorizations occur during end of travel day processing. These authorizations must be identified in the system as Nominal Authorizations, because while that day's clearing amount may be covered by a previous Nominal Authorization, the end of day authorization covers multiple trips of varying amounts to occur over the next 14 days. Regular travelers will trigger a sequence of these authorizations as amounts are regularly cleared and a new aggregation begins.

End of day authorizations are typically for the final fare amount, to be set at the discretion of the transit operator.

Note: the "end of travel day" may not be at midnight, as the processing cut-off for a travel day may happen at a more logical point in time for the location (e.g., in the early hours of the morning after a transit system has stopped operating).

Debt Recovery Authorizations

Debt recovery authorizations occur when a passenger has been placed on the Deny List and needs to be removed from the List in order to travel. (For more information on the Deny List, see Section 6.2.) Debt recovery authorizations may occur under the following circumstances:

- Automatically, after set periods of time - possibly daily – to obtain authorization for the amount owed by the passenger
- Automatically after a tap from a card that is on the Deny List - usually at an attended or unattended terminal
- At a passenger's request without a card being tapped – such as via a call center or web page

The value of the authorization will be the amount that is being recovered – unless the passenger was denied access for a violation of transit operator policy (e.g. an invalid tap), in which case a system-generated or zero-value authorization may be required to remove the passenger from the Deny List.

Where a different card account (other than the account used for the original, declined transaction) is used to settle an outstanding amount, the transaction will be a retail-like transaction.

(*Note:* there are specific rules and restrictions in the U.K. with respect to the use of debt recovery for retail-like transactions, and other markets may introduce similar rules in the future.)

Penalty Fare Authorization

Depending on the model adopted by the transit operator, the contactless card may be checked by a revenue inspector on a hand-held device and the tap sent to the transit back-office for validation. In some cases, the transit operator may subsequently determine that a penalty fare must be paid because the current travel was not properly authorized by the transit operator (i.e., the tap was not valid). The collection of the penalty fare will require a separate authorization.

Error Handling Authorizations

Error handling authorization typically occur when, due to a technical issue, some tap data has arrived after end-of-day processing has begun. This is known as 'late tap data'. This might occur, for example, if a bus travels through communications blackspots and full tap details can only be collected when the trip has been completed.

Late tap data may increase the amount owed (e.g. a by adding a previously missed bus trip) or decrease the amount owed (e.g. by reversing a maximum fare that was previously charged but, based on the new tap data, should not have been charged).

- If late tap data changes that day's total spend for a given passenger, and an earlier amount was already authorized but not yet cleared, the following steps might take place:
  - A reversal of the original transaction
  - A new authorization for the corrected amount
- If late tap data arrives at the transit operator for a previous day's travel and the previous day's transaction volume has already been cleared, the late tap amount is carried over to the passenger's next travel day in the form of a credit or debit. The late tap amount will be taken into consideration on the next end of day processing. If there has been no activity on the card for a given period of time, the transit operator should refund any money owed or debit any money due. Credit balances should not be retained indefinitely

Please note the following:

- Date fields in any second authorization should match those in the original authorization.

- Chip data in any second authorization should be taken from the late tap to ensure that the transaction is unique; however, issuers should pay special attention to ATC checking in these scenarios (please refer to section 4.5.3 for more details on ATC validation).

Passenger Card Registration – Account Status Inquiries

Some transit operators may offer passengers the option to register their cards. Registration may enable passengers to take advantage of additional benefits such as:

- Email or SMS alerts if there are any issues with their card (e.g., declined authorization, card expiration, etc.)
- Richer and more detailed journey history (due to data protection laws, it may not be possible to show all trip history to non-registered passengers)
- Travel alerts
- Special offers
- Easier ways to interact with the transit operator
- Ability to 'add in' missed taps (e.g., if a passenger failed to tap out because of long lines or a faulty terminal, they could be offered a limited ability to 'self-correct' the missed taps via a tool on the transit operator's website)

Issuers are not expected to provide any information to a transit operator on a registered card account other than a response to an account status inquiry, which may include CVC2 and Address Verification Service (AVS) checks.

Passengers who are not registered with the transit operator will still be able to use their card accounts as described throughout this document; they will simply not have access to any benefits associated with registration.

Transit operators and issuers may want to encourage passengers to register, as it provides the only mechanism by which a transit operator can communicate directly with a passenger. Without registration, it may be difficult for a transit operator to, among other things, inform passengers if there are issues with their payments that may affect their ability to travel.

Transit operators may choose to support various channels for registration, such as:

- A website, using the embossed or funding PAN
- A self-service contactless kiosk which the passenger taps
- A mobile application

Acquirer Reversals

In the case of Maestro transactions (which are processed) in a single message environment, transit operators must reverse unused funds. The original financial message request (0200) will have been for an estimated or maximum amount, not a nominal amount. When the limit is reached or within three calendar days (whichever comes first), the transit operator totals the value of all taps and generates an acquirer Reversal Advice/0420 to reverse any unused funds. No clearing transactions are submitted in a single message system.

3.4.2.2 Transit Authorization Data Values

Authorizations should use the values shown in the table below; these values allow issuers to identify incoming messages as transit-related. The table does not include all data elements required – only those designated for or affected by use in transit. For full details of the contents of authorization messages, please refer to the Customer Interface Specification manual.

DE	Sub element	Subfield	Value and Description
2			**Primary Account Number** Where the authorization is initiated by a tap, this will be the PAN read from the contactless card, which might be a tokenized PAN. For Debt Recovery authorizations, which are often card not present transactions, the embossed PAN or FPAN should be used. If the Debt Recovery authorization is initiated by a dedicated tap, then the device PAN will be used.
4			**Transaction Amount** The amount of the authorization. For pre-authorizations this may be a nominal value or the maximum liability amount. For End of Day authorizations this will normally be for the aggregate amount spent this travel period. For Debt Recovery authorizations this will be for the amount to be recovered or a nominal amount if no money owed to the transit operator, but the card is on the Deny List.
7			**Transaction Date and Time** The date and time that the transaction is sent to the Mastercard network
11			**System Trace Audit Number (STAN)** Some transit operators may use the date or time within this field, for those that do, the date/time used should be the same as those in Data Elements 12 and 13. DE 11 and DE 7 must uniquely identify the transaction.
12			**Time Local Transaction** For pre-authorizations the time will be set to the time that the cardholder tapped their card which will be earlier than the value of the time in DE7 (Transmission Date/Time). For End of Day authorizations the time will typically be set to 23:59:59 (or 235959 in hhmmss format). For Debt Recovery authorizations this will be the time the authorization is presented.
13			**Date Local Transaction** For pre-authorizations the date the cardholder tapped their card to trigger the nominal authorization. If a tap occurs during a travel day but after midnight on the calendar day, then the transit operator may set this value to the preceding day. For End of Day authorizations, the date will be the travel date – which is usually the preceding day. For Debt Recovery authorizations, the date will be set to the date the transaction was initiated.
18			**Merchant Type** The valid values are: • 4111 (Transportation – Suburban and Local Commuter Passenger, including Ferries) • 4131 (Bus Lines) • 4784 (Bridge and Road Fees, Tolls)

DE	Sub element	Subfield	Value and Description
22	1		**POS Entry Mode** For pre-authorization and End of Day authorizations: 07 (PAN Auto Entry via contactless M/Chip) for EMV Mode transactions OR 91 (PAN auto-entry via contactless magnetic stripe) for Mag Stripe Mode transactions For Debt Recovery authorizations: 01 (PAN Manual Entry) for automatic debt recovery or via a call center 81 (PAN entry via electronic commerce, including chip) for debt recovery via a website For debt recovery via a tap on a reader: 01 (PAN Manual Entry) if debt recovery is considered a CNP transaction or otherwise 07 (PAN Auto Entry via contactless M/Chip) for EMV Mode transactions OR 91 (PAN auto-entry via contactless magnetic stripe) For TVM, Kiosk or Ticket Office (when the card is read): as per standard retail transaction
22	2		**POS Terminal PIN Entry Mode** This must be set to '2' (Terminal does not have PIN entry capability) unless a retail-like transaction when '1' might apply.
37			**Retrieval Reference Number** This field must be populated by the acquirer and subsequently correctly stored by the issuer for use in any chargeback/1422 message.
41			**Card Acceptor Terminal ID** This field may represent: • The terminal where the cardholder made their tap • A generic 'terminal' used for all nominal value authorizations For Debt Recovery authorizations this field may be set to a different value may be used depending on the method of debt recovery.
42			**Card Acceptor ID Code (Merchant ID)** The transit operator may have a distinct merchant ID for different authorization types (for example: a different merchant ID for standard ticket sales, pre-authorization, end of day or debt recovery transactions).
48	1	N/A	**Transaction Category Code** Set to 'X' (Airline and other transportation services).
48	23	1	**Device Type** This is data read from the card or device. It is mandated that acquirers include this value in the authorization in some regions.
48	42	1	**Security Protocol** (positions 1) and **Cardholder Authentication** (position 2) For debt recovery via a website this must be set to 21 if SecureCode is supported or 91 if it is not. This field is not mandatory for other forms of debt recovery or other types of authorization.
48	61	5	**Final Authorization Indicator** For Debt Recovery authorizations this must contain a value of '1' unless the transaction is recovering a zero-value debt in which case this field may not be present or must be set to a value other than '1'
48	64	1	**Transit Transaction Type Identifier** This value identifies the type of transit authorization message being performed.
48	64	2	**Transportation Mode Indicator** A transit operator that uses a multi-modal transit system (for example: buses, trains and underground) will have this value set to '00' (Unknown), alternatively if only one mode is used then the value should be set to that specified in [CINTSPEC]. It is recommended that issuers do not use the information in this field to routinely decline transactions.

DE	Sub element	Subfield	Value and Description
48	92		**CVC2** This field should be populated for Debt Recovery authorizations initiated via a web site or call center. *Note:* Issuers should not routinely decline debt recovery transactions solely due to the lack of CVC 2 data.
55	All values in Data Element 55 are populated from the tap that generated the nominal value authorization (for pre-authorizations and End of Day authorizations) or the specific tap used for a card initiated Debt Recovery authorization. The content below only shows key fields that issuers may want to pay special attention to. The data presented in DE55 must be the data used in the reader / device exchange and not modified in any way – even if the underlying data subsequently changed – as the data will have been signed in the application cryptogram. Chip data will not always be present for a Debt Recovery authorization.		
55	9A		**Transaction Date** The date of the tap that generated the nominal value authorization
55	9F27		**Cryptogram Information Data** This must be set to one of the following two values • '4x' (Transaction Cryptogram (TC)) • '8x' (Authorization Request Cryptogram (ARQC)) *Note:* Issuers must ensure that their systems accept the presence of TCs in incoming authorization/0100 messages for transit transactions. The reason that this may be present is the latest tap data is always sent to the issuer in authorization request messages. As the tap is always for a zero amount (locally at the reader) a TC may be generated.
55	9F02		**Amount Authorized** This For pre-authorizations and End of Day authorizations this will have the value of 0. For card read Debt Recovery authorizations this will be the value of the transaction. *Note:* Issuers must ensure that their systems accept transit transactions where the amount in DE55-9F02 is different from the amount in DE4 (Transaction Amount). Issuers must not routinely decline transactions solely because these amounts differ
55	82		**Application Interchange Profile** The precise value of the AIP varies depending on the card application used
61	1		**POS Terminal Attendance** For pre-authorizations and End of Day authorizations this must be set to '1' (unattended terminal). Even though on a bus (for example) the terminal may have a driver sitting next to it, the reader is activated by the cardholder tapping on it, so is generally considered an unattended terminal. For Debt Recovery authorizations: • For automatic debt recovery: '2' (No terminal used) • For debt recovery via a website: '1' (unattended terminal) • For debt recovery via a call center: '2' (No terminal used) • For debt recovery via a tap on a reader (presented as CNP): '2' (No terminal used) • For debt recovery via a tap on a reader (vending machine): '1' (unattended terminal) • For debt recovery via a tap on a reader (ticket office): '0' (attended terminal) If the tap that generated the authorization was initiated from a Revenue Inspection Device that this may be optionally set to '0' (attended terminal)

DE	Sub element	Subfield	Value and Description
61	3		**POS Terminal Location** For pre-authorization and End of Day authorization this must be set to '0' (On premises). For Debt Recovery: • For automatic debt recovery: 3 (No terminal used (voice/ARU authorization) • For debt recovery via a website: 2 (Off premises (cardholder terminal including home PC, mobile phone, PDA)) • For debt recovery via a call center: 3 (No terminal used (voice/ARU authorization)) • For debt recovery via a tap on a reader (if implementing a CNP solution): this should be set to 3 (No terminal used (voice/ARU authorization) • For debt recovery via a tap on a reader (vending machine, TVM, Kiosk or Ticket Office): 0 (On premises)
61	4		**Cardholder Presence** For pre-authorization and End of Day authorization this must be set to '0' (Cardholder present). For Debt Recovery: • For automatic debt recovery: 1 (Cardholder not present, unspecified) • For debt recovery via a website: 5 (Cardholder not present, Electronic Order (home PC, Internet, mobile phone, PDA)) • For debt recovery via a call center: 3 (Phone/ARU order) • For debt recovery via a tap on a reader (if implementing a CNP solution): 1 (Cardholder not present, unspecified) • For debt recovery via a tap on a reader (vending machine, TVM, Kiosk or Ticket Office): 0 (Cardholder present)
61	5		**Card Presence** For pre-authorization and End of Day authorization this must be set to '0' (card present). For Debt Recovery: • For automatic debt recovery: 1 (Card not present) • For debt recovery via a website: 1 (Card not present) • For debt recovery via a call center: 1 (Card not present) • For debt recovery via a tap on a reader (if implementing a CNP solution): 1 (Card not present) • For debt recovery via a tap on a reader (vending machine, TVM, Kiosk or Ticket Office): 0 (Card Present)
61	6		**Card capture capability** This must be set to '0' (no card capture capability)
61	7		**POS Transaction status** For pre-authorization and End of Day authorization this must be set to '04' (preauthorized request). This must be set to '00' for certain products if the initial authorization is not treated as a pre-authorization. For Debt Recovery authorizations:: • That are for a non-zero-value: '0' (normal request) • That are zero value: '4' (preauthorized request) *Note:* Please refer to [PREAUTH] for full details. This requirement is dependent upon the merchant's location and is independent of the acquirer's location. If the transit merchant is located in the Europe region, this value must be set to '4'. If the transit merchant is located outside of the Europe region, this value may be set to '0' (normal request).

DE	Sub element	Subfield	Value and Description
61	10		**Cardholder Activated Terminal Level** For pre-authorization and End of Day authorization this must be set to '0' (Not a CAT transaction) For Debt Recovery: • For automatic debt recovery: 0 (not a CAT transaction) • For debt recovery via a website: 6 (Electronic Commerce) • For debt recovery via a call center: 0 (not a CAT transaction) • For debt recovery via a tap on a reader (if implementing a CNP solution): 0 (not a CAT transaction) • For debt recovery via a tap on a reader (vending machine, TVM, Kiosk or Ticket Office): as per standard POS
61	11		**POS Card Data Terminal Input Capability** For pre-authorization and End of Day authorization this must be set to '3' (contactless M/Chip) For Debt Recovery: • For automatic debt recovery: 6 (Key entry only) • For debt recovery via a website: 6 (Key entry only) • For debt recovery via a call center: Either 0 (Unspecified), 1 (No terminal used (voice/ARU authorization), or 6 (Key entry only) • For debt recovery via a tap on a reader (if implementing a CNP solution): 6 (Key entry only) • For debt recovery via a tap on a reader (vending machine, TVM, Kiosk or Ticket Office): as per standard POS

Distinguishing Transit Retail Payments from Aggregated Transactions

There may be situations in which a transit operator submits an authorization that looks very similar to those described in this section (3.4) but is in fact for a simple retail transaction. These retail transactions will not include Transit Transaction Identifiers. Examples of these include:

- Purchase of a single journey ticket (transaction could be for a similar amount to an end-of-day authorization and could also be contactless).
- Topping up an existing proprietary card (e.g., there may be a period during which a transit operator maintains an existing proprietary system in parallel with accepting open payments, in which case the transaction could be for a similar amount to an end-of-day authorization and could also be contactless).
- Purchase of souvenirs (some transit operators sell memorabilia; such a purchase could be for a similar amount to an end-of-day authorization and could also be contactless).

These transactions would not be exactly like the transactions defined in this section (3.4) – specifically, DE 48/sub-element 64 would not be present.

3.4.3 Authorization Responses

Issuers should take note of the following:

3.4.3.1 Nominal Authorization and End of Day Authorization

Approval of a Nominal Authorization or end of day authorization will start the aggregation of transit spend up to the aggregated amount limit. These authorizations may be for nominal values, depending on

local rules. If the aggregated amount limit is not reached over a 14-day period, the transit operator may clear multiple transactions without seeking a new authorization. The issuer has liability for all spend on the card at the transit operator provided the transit operator follows all the rules correctly.

If the aggregated spend exceeds the aggregated amount limit, the issuer has the right to charge back the amount that exceeded the limit.

Declining a properly formatted Nominal Authorization or end-of-day authorization means that:

- The cardholder (passenger) will most likely be added to the transit operator's Deny List and prevented from any further travel until the issue is resolved. This restriction on travel may prompt the cardholder to contact the issuer for resolution.
- In some markets, local rules may hold domestic issuers liable for the cost of the first trip taken even if the authorization was declined.

Deny List Responses

- Approval of a debt recovery transaction will remove the passenger from the Deny List; however, the transit operator will not be allowed to start a new aggregation cycle until the passenger has performed a new tap – i.e., approval of the debt recovery authorization does not trigger a new aggregation period/amount.
- Decline of any debt recovery transaction will cause the passenger to remain on the Deny List.

3.4.3.2 Additional Information in Authorization Response Messages

Cards that contain an alternate PAN (also referred to a pseudo, digital, or tokenized PAN) must return the embossed PAN in the authorization response so that the transit operator can deal with any customer service inquiries. The passenger is usually unaware of the alternate PAN and will not use it for making inquiries.

As the transit operator will not know the embossed PAN, the issuer must populate the following data element and subfields in the authorization response:

- Data Element 48 (Additional Data) Sub-element 33 (PAN Mapping File Information)
  - Subfield 1 (Account Number Identifier) – must have the value 'E'
  - Subfield 2 (Account Number) – must contain the embossed PAN
  - Subfield 3 (Expiry Date) – must contain the expiration date of the embossed PAN
  - Subfield 4 (Product Code – e.g., debit, credit) – is optional in most markets and mandated in Europe.

This data is generated automatically if the Mastercard Digital Enablement Service (MDES) is used by the issuer for account tokenization (i.e. creating contactless PANs that map to FPANs).

Issuers that do not use alternate PANs (i.e. the PAN embossed on the card is the same as the contactless PAN) do not need to include the mapping information in authorization response messages.

3.4.3.3 Application Response Cryptogram (ARPC)

Issuers should not generate an ARPC, ARPC response data, or script messages in the transit environment – this data will not be sent to the card for the following reasons:

- SECOND GENERATE AC is not supported over the contactless interface, and
- The card is no longer present at the reader

3.4.3.4 Refer to Issuer Response

The issuer must not generate a "Refer to Issuer" response. If a transaction is referred to issuer (i.e., DE 39 of the 0110 Authorization Response has a value of '01' or '70'), the transit operator and/or their acquirer may treat it as a decline.

3.4.3.5 Impact of Stand-In on Authorization Responses

When authorization responses are generated by Stand-In Processing (STIP), issuers must be aware that:

- A response sent during STIP carries the same liability and implications as an issuer response.
- Issuers can configure some STIP instructions to identify and act on transit transactions based on transaction characteristics (e.g., Card not Present, contactless, transaction amount, MCC, etc.).
- An issuer should look at their STIP parameters to ensure that:
  - Deny List authorization requests are not routinely incorrectly declined (as this will prevent passengers from automatically being removed from the Deny List) or routinely incorrectly approved (as this may remove passengers from the Deny List when they are still overdrawn).
  - End of day and Nominal Authorization requests are not routinely declined, as this will add the passengers to the Deny List.

3.4.3.6 Payment Account Reference

The Payment Account Reference (PAR) is a unique customer reference that links multiple tokenized PANs to the underlying cardholder (passenger). It enables transit operator and acquirer fraud controls or customer service systems to recognize the individual customer irrespective of which tokenized device they are using.

Once PAR is implemented, Acquirers can expect to receive the PAR value in authorization response messages. The PAR will be present in DE 56.

3.4.4 Clearing Messages

3.4.4.1 Types of Clearing

Contactless Transit Aggregated Transaction Clearing

Contactless Transit Aggregated Transaction (CTATC) occurs when one or more trips are aggregated and cleared as a single amount. This type of clearing may be performed every day, once the maximum aggregate value is reached, or once the maximum time threshold is reached.

Note that a single authorization may, in some markets, result in multiple (typically daily) clearing transactions. An example of this is the Authorized Aggregated Split-Clearing transaction, which was implemented in the UK.

Debt Recovery Clearing

Debt Recovery Clearing (DRC) transactions occur when fares are incurred after entry to the system but before the associated authorization request is declined by the issuer. The transit operator will perform debt recovery authorizations to ensure funds are available before presenting transactions for clearing.

Revenue Inspection Clearing

Revenue inspection clearing occurs when a revenue inspection event reveals that the passenger did not obtain proper permission to travel (e.g., the cardholder did not tap in to enter the system).

The process for revenue inspection varies from transit operator to transit operator. Some transit operators may simply block a card from use in the system until the passenger contacts them to resolve the issue; others may charge a penalty fare; still others might use a combination of these measures.

If a penalty fare is charged, a separate retail payment transaction may be generated or the revenue inspection amount may be included within the aggregated clearing transaction.

3.4.4.2 Transit Clearing Data Values

This section describes some of the specific values that will be present in incoming Integrated Product Message (IPM) files received by issuers; these values will help issuers identify transit transactions.

DE/PDS	Sub element	Subfield	Value and Description
DE2			**Primary Account Number** For Contactless Transit Aggregated Transaction Clearing (CTATC) this will be the contactless PAN For Debt Recovery Clearing (DRC) this will be the embossed PAN
DE4			**Transaction Amount** For CTATC this will be the amount of the aggregated spend. This may be more than the Chargeback Protection Amount if, for example: the cardholder has been charged multiple 'maximum fares' as a result of failing to tap-in or tap-out, or if the cardholder's travel exceeds the Chargeback Protection Amount. For DRC this will be the debt amount. If a cardholder had a 'zero value debt' and the debt recovery authorization was approved there will be no clearing record.

DE/PDS	Sub element	Subfield	Value and Description
DE12		1	**Date Local Transaction** For CTATC this will either be the 'Travel Day' date. (A 'Travel Day' may span two calendar days) or the date the transaction was initiated. For DRC the date will be set to the date the transaction was initiated. The format is YYMMDD.
DE22		1	**Terminal Data: Card Data Input Capability** For CTATC this will be set to 'M' (PAN Auto Entry via Contactless M/Chip) For DRC this value should map to the correct value in the authorization message depending on the type of debt recovery performed. Please refer to [IPMCLR] for the correct mapping
DE22		2	**Terminal Data: Cardholder Authentication Capability** This will be set to '0' (No electronic authentication capability)
DE22		3	**Terminal Data: Card Capture Capability** This will be set to '0' (No capture capability)
DE22		4	**Terminal Operating Environment** For CTATC this will be set to '2' (On acceptor premises, unattended) For DRC this value should map to the correct value in the authorization message depending on the type of debt recovery performed. Please refer to [IPMCLR] for the correct mapping
DE22		5	**Cardholder Present Data** For CTATC this will be set to '0' (Cardholder present). For DRC this value should map to the correct value in the authorization message depending on the type of debt recovery performed. Please refer to [IPMCLR] for the correct mapping
DE22		6	**Card Present Data** For CTATC this will be set to '1' (Card present) For DRC this value should map to the correct value in the authorization message depending on the type of debt recovery performed. Please refer to [IPMCLR] for the correct mapping
DE22		7	**Card Data: Input Mode** For CTATC this will be set to 'M' (PAN Auto Entry via Contactless M/Chip) For DRC this value should map to the correct value in the authorization message depending on the type of debt recovery performed. Please refer to [IPMCLR] for the correct mapping
DE22		8	**Cardholder Authentication Method** This will be set to '0' (Not Authenticated)
DE22		9	**Cardholder Authentication Entity** This will be set to '0' (Not Authenticated)
DE26			**Merchant Type** The valid values are • 4111 (Transportation – Suburban and Local Commuter Passenger, including Ferries) • 4131 (Bus Lines) • 4784 (Bridge and Road Fees, Tolls)
DE37			**Retrieval Reference Number** This field must be populated and subsequently correctly stored by the issuer.
DE38			**Approval Code** This will be the issuer generated authorization code that was sent in the authorization response. *Note:* that in some implementations, the same authorization is used for multiple clearing items and thus the same value may be received in more than one clearing record.

DE/PDS	Sub element	Subfield	Value and Description
DE41			**Card Acceptor Terminal ID** This field may represent: • The terminal where the cardholder made their tap • A generic terminal used for all aggregation transactions. This field may either represent the terminal where the cardholder made their tap or may represent a generic terminal used for debt recovery transactions.
DE42			**Card Acceptor ID Code (Merchant ID)** The transit operator may have a distinct merchant ID for CTATC and DRC as opposed to the merchant ID for standard ticket sales.
55	Values in Data Element 55 are populated from one tap relating to the aggregated travel period. The content below only shows key fields that issuers may want to pay special attention to. The data presented in DE55 must be the data used in the reader / device exchange and not modified in any way – even if the underlying data subsequently changed – as the data will have been signed in the application cryptogram. Data Element 55 will only be present on DRC messages if the debt recovery was performed as a card present transaction (for example: at a kiosk or ticket office).		
55	9F27	N/A	**Cryptogram Information Data** This must be set to one of the following two values • '4x' (Transaction Cryptogram (TC)) • '8x' (Authorization Request Cryptogram (ARQC))
55	9F02	N/A	**Amount Authorized** This will have the value used at the time of the interaction with the contactless card and will not be the final transaction amount. *Note:* Issuers must ensure that their systems accept transit transactions where the amount in DE55-9F02 is different from the amount in DE4 (Transaction Amount).
55	82	N/A	**Application Interchange Profile** The precise value of the AIP varies depending on the card application used
DE63			**Transaction Lifecycle ID (Trace ID)** This shall contain the value of the most recent Trace ID. For example: a transaction that was authorized today and is being cleared today will have the value of today's authorization.
PDS0023	N/A	N/A	**Terminal Type** This will be set to N/A[1]
PDS0210	N/A	1	**Transit Transaction Type Identifier** This must be present and set to the appropriate value specified in [IPMCLR].
PDS0210	N/A	2	**Transportation Mode Indicator** A transit operator that uses a multi-modal transit system (for example: buses, trains and underground) will have this value set to '00' (Unknown), alternatively if only one mode is used then the value should be set to that specified in [IPMCLR].

[1] This is correct at the time of publication; however, it should be noted that the value of the CAT indicator is currently under review

3.4.4.3 Refunds and Reversals

PAYG transactions are unlikely to result in refund transactions; but if refunds are generated, no special requirements apply.

For Maestro single message transactions, see 3.4.2.1 Acquirer Reversals.

See also Goodwill Payments in section 3.5.

Technical reversals may be required at times in order to correct errors.

3.4.4.4 Disputes and Chargebacks

See section 2.4 for requirements related to the handling of disputed transactions.

3.4.4.5 Handling Maximum Fares

A maximum fare may be applied when a cardholder taps in at the start of a trip but fails to tap out at the end of that trip (where tapping out is required). In such a case, the specific fare cannot be calculated. Maximum fares may or may not be aggregated and may be cleared individually.

3.5 Processing Goodwill Payments

In some instances, a transit operator may wish to make goodwill payments to passengers. Examples include:

- When there has been major service disruption, a transit operator may wish to pay compensation to passengers; the compensation might exceed the fare paid.
- When the transit operator feels that a customer has been unfairly treated (e.g. given incorrect information by a staff member).

In these instances, the transit operator may, at its discretion, establish a method for compensating the passenger.

4 Issuer

This chapter highlights transit-related concerns that are important to issuers.

4.1 Card Products

4.1.1 Debit, Credit and Prepaid Programs

All contactless card types should be usable in any transit environment that accepts financial institution-issued contactless cards for payment or access to the transit system. Issuers of debit, credit or prepaid contactless cards must be familiar with the particular requirements of the transit environment:

- Cards must support offline card authentication, also known as Combined Data Authentication (CDA); this is especially important in situations where offline transactions are used to enable rapid access to the system.
- Managing the Application Transaction Counter (ATC) - which ensures the cryptogram generated by the card is unique – can be more complex, as ATCs may be presented out of sequence (due to offline transactions and deferred authorizations) and a wider range of possible ATCs is required as frequent offline transactions which are never presented to the issuer may occur (see section 4.5.3)
- Issuers must recognize and take action based on certain Data Elements that are unique to transit transactions (see section 3.4.4.2)
- Issuers should ensure that each card is unique with respect to PAN, Expiration Date, and PAN Sequence Number, so multiple instances of the same "card" cannot occur within the transit system at the same time.
- Advise cardholders (passengers) to use the same card/device to "tap in" and "tap out" for any given trip in order to properly calculate the fare. The cardholder should not, for example, use a card to tap in and a mobile device to tap out.

If cards are not configured in a way that enables acceptance in local transit operations, cardholders (passengers) are likely to form a negative perception of the issuer, as their ability to use the transit system may be impeded.

4.1.1.1 Deferred Authorization

A significant transit-related variation on the normal transaction process is the use of deferred authorization.

To enable fast access to the system, an offline transaction can be performed at the point of entry whereby the card is authenticated using the chip's offline authentication (CDA) capability. At the same time, the card is checked against the transit operator's Deny List. The Deny List records card accounts with outstanding (unpaid) funds or which are not

permitted to access the system for some other reason. If authentication is completed and the card is not on the Deny List, access to the system is allowed.

At some later stage, likely while the passenger is in transit, the transit operator will initiate a deferred authorization for a nominal amount (as at this stage the actual trip cost may not be known). In cases when a deferred authorization is required, the authorization is sent to the issuer as soon as possible, depending on the connectivity of the terminal's telecommunications functionality.

If the deferred authorization is declined, the passenger will not be prevented from exiting the system. However, it is unlikely the passenger will be permitted to re-enter the system until any outstanding fares have been paid (i.e., the card will be added to the Deny List).

For more detailed explanations of these transit-related requirements, refer to Chapter 3.

4.1.1.2 M/Chip Advance

Mastercard provides a chip card specification known as M/Chip Advance that was designed for use in transit. M/Chip Advance products are available from a wide number of card suppliers. The application supports both contact and contactless payments and is able to support a wide variety of different products, markets, and individual implementations. M/Chip Advance utilizes data storage on the chip to emulate closed loop transit in order to support monetary balances and time based fares.

For details on M/Chip Advance, see [MCASPEC] and [MCAISSG].

4.1.2 Prepaid for Transit

Prepaid contactless cards may be issued as open-loop (for general use including transit) or closed-loop (for use only in a transit environment). Both models are powered by Mastercard contactless technology. Closed-loop prepaid can serve as a stepping stone to open-loop prepaid.

Mastercard Prepaid for Transit solutions address the needs of visitors to a region or city, individuals who do not qualify for a financial institution-issued debit or credit card, and passengers who prefer not to use financial institution-issued cards for transit.

It is important to note that prepaid cards are configured as "online only". Some level of credit risk may exist because transit agencies will generally send a deferred authorization rather than real-time. (See Deferred Authorizations in Section 3.4.)

Mastercard Prepaid payments are authorized online against available prepaid funds, which the cardholder (passenger) can reload as needed. All entities involved need to determine how to manage any risk associated with the need for rapid system access vs. the timing of funds transmission throughout the transaction flow.

4.1.2.1 Open-loop

An open-loop Mastercard Prepaid for Transit program allows passengers to use a financial institution-issued Mastercard Prepaid card to access the transit system. This solution has minimal impact on the issuer and the transit operator, and no impact on acquirers (which see and treat Mastercard Prepaid transactions the same way as other Mastercard transactions).

Open-loop Mastercard Prepaid cards operate in the same way as all other Mastercard Credit and Debit cards. Rather than granting credit or posting transactions to a cardholder bank account, however, the issuer only approves transactions that have been pre-funded by the cardholder (passenger). The method of pre-funding is at the discretion of the issuer. Open-loop prepaid cards are particularly appropriate for individuals who choose not to use or are unable to obtain credit or debit cards.

Open-loop prepaid cards give cardholders the ability to set spending limits for themselves and/or dependents, and do not require a banking relationship with the card issuer. Individuals can purchase prepaid cards through various channels, including the Internet, issuer bank branches, and retail stores. Individuals may purchase multiple prepaid cards (e.g. for family members or visitors).

Role of Prepaid Issuer

The Prepaid issuer is ultimately responsible for customer service, operations and risk management, transaction settlement and reporting, and compliance with the Mastercard Rules.

There are three types of open-loop prepaid accounts:

- Personalized
- Non-personalized
- Anonymous

On a personalized prepaid card, the cardholder name is printed/embossed on the card and encoded in the chip data.

In the case of non-personalized cards, personal cardholder information is associated with the account but is not embossed, printed, or encoded on the card; instead, a generic program name (e.g. the name of the transit operator or the transit operator's program) must be embossed or printed on the plastic and encoded in the name field of the magnetic stripe. Non-personalized cards are generally used in instant issuance situations – e.g. when a Mastercard partner, such as a transit operator or retailer, holds a stock of cards that can be issued as needed without the delay associated with a centralized card personalization system.

Anonymous cards carry no personal cardholder information and are limited to single-load (disposable), instant-issue prepaid cards. These cards pose higher levels of risk.

Loading is the process of adding value to a prepaid account. Funds can be loaded via account transfers, payments from other card accounts, Internet value transfers, or cash deposits at convenient stores or other locations.

Prepaid issuers may only use contactless cards that are certified to properly support Mastercard products and contactless payments. The contactless cards must support CDA to enable offline authentication at the transit point of entry.

Role of Program Manager

Many open-loop prepaid card programs are managed by a Program Manager. The Program Manager must carefully monitor and execute tasks associated with ongoing prepaid program operations. The responsibility of a Program Manager will vary depending on the transit operator's requirements to support open payments at the point of entry.

4.1.2.2 Closed Loop (Private Label)

The Prepaid for Transit closed-loop (Private Label) solution adds Mastercard Contactless to a pre-funded card that can only be used in the transit environment. This product leverages Mastercard-issued BINs, chip application identifiers, and payment infrastructure, making it a robust solution for transit operators.

Private Label programs leverage the same technology assets as those used for open-loop Mastercard payment solutions. This includes M/Chip card and Mastercard digital technology, which support a range of mobile solutions and digital wallets. Private Label cards do not, however, carry the Mastercard brand and are only usable in the transit environment.

4.2 Multi-Application Programs

Multi-application programs are hybrid solutions that involve adding the transit operator's proprietary payment application to a Mastercard Chip card. Typically, transit applications use contactless technology for proprietary (closed-loop) payments.

The hybrid solution has minimal impact on issuer or transit operator systems, as existing processes continue – just using a combined form factor. For this reason, the hybrid solution has quite low operational and implementation risks. The solution does, however, have an impact on card procurement and personalization as both applications must be coded onto the chip.

Issuers can benefit from the hybrid solution because the transit feature increases card usage and can create preference for usage outside the transit system (a top of wallet effect). The transit operator can enjoy potentially reduced costs, as the card platform is shared and the need for dedicated cardholder operational support may be reduced. Obviously, there will be a continued need to support the dedicated transit application throughout the transit network, and both issuer and transit operator will have to make changes to accommodate the new card issuance process. The hybrid card solution creates minimal integration requirements for a transit operator or issuer, as the basic acceptance process for both applications remains unchanged.

The multi-application solution has no systems impact on acquirers.

The hybrid solution may serve as a stepping stone to a full open-loop system, as hybrid cards may continue to be used in open-loop fashion as a program evolves.

In a hybrid solution, the issuer is responsible for the open-loop payment application and the transit operator is responsible for the transit payment application. However, there will be a need to define other responsibilities – e.g., how costs will be shared if a card needs to be re-issued due to the malfunctioning of one application.

Passenger Impacts

Passengers (cardholders) benefit from being able to use a single card for transit and other payments. Consideration must be given to how the bank and transit agency will support cardholders.

While the payment and transit applications may be technically distinct, cardholders will likely expect a single point of contact for their inquiries. This might be achieved with a single customer service number and an interactive voice system directing the inquiry to the appropriate party.

4.3 Mobile

Payments can be made using a mobile phone in exactly the same way as a contactless card is used. The mobile phone must be NFC-enabled and loaded with the account details, usually stored in a digital wallet on the phone. The passenger selects which card account to use for payment before the phone is tapped. The interaction between the contactless reader and the mobile phone is exactly the same as when a contactless card is used – indeed, the reader may not be able to detect what type of device is being tapped.

Major digital brands offer their own versions of digital wallets on their mobile devices and brand the associated payments accordingly. The payment technology for any given card brand is based on the same exchange of information and credentials regardless of which wallet brand is being used.

There are different technical approaches to securing mobile payment data . The choice of approach depends upon the partners involved and their ability to access different areas within the architecture of the device. Data may be stored in a secure area on the mobile device (usually referred to as the Secure Element (SE)) or in the cloud (known as Host Card Emulation (HCE)).

Card accounts that have been loaded into a digital wallet may also be used for secure mobile commerce transactions through the internet interface (i.e. not using contactless technology). These transactions are secured using strong EMV-style cryptography, in the same way as in-person payments. Mobile commerce payments may be relevant to transit operators when using "card as credential to travel" solutions where the actual payment precedes the travel. Mastercard refers to these secure internet transactions as Digitally Secure Remote Payments (DSRPs).

4.3.1 Secure Element-Based Solutions

In Secure Element-based solutions, critical account data is stored within the Secure Element on the device, which manages access to and use of the data. Critical data typically includes the secret or private keys used to generate cryptograms. The Secure Element is normally managed either by the equipment manufacturer (if the SE is part of the device) or network operator (if the SE is on the SIM card); the transit operator should make arrangements with these parties to gain access to and use the appropriate SE.

4.3.2 Mastercard Cloud Based Payments (MCBP)

Host Card Emulation (HCE) technology offers an alternative to the Secure Element. Mastercard Cloud-Based Payments (MCBP) is a Mastercard solution that leverages HCE technology. With MCBP, secure payments can be made without the need for a business arrangement between the transit operator and the controller of the SE.

For details on Mastercard Mobile Solutions, visit the Mastercard Connect website.

4.3.3 Tokenization

Token accounts are used in the provisioning of many mobile wallets to further secure account information. Token accounts limit the exposure of the originating funding PAN (referred to as the FPAN) when a card account is added to and used by a mobile wallet. A token account number serves as an alias or proxy to allow the passenger's mobile device to initiate an immediate or future payment transaction – e.g. via a contactless tap, from within a mobile application, or using a mobile browser (DSRP).

The transit operator must be able to ascertain whether the device's token account correlates to a funding account that was used for a pre-purchased fare. Therefore, the transit operator requires the return of the underlying funding PAN in authorization responses for reconciliation of a device with the account associated with the pre-purchased fare.

4.3.4 Payment Account Reference (PAR)

EMV Payment Tokenization was developed for use in various digital payment solutions. Payment Tokenization enhances the underlying security of digital payments by limiting the risks associated with unauthorized or fraudulent use of PANs. Payment Tokenization achieves this additional level of security by replacing PANs with Payment Tokens that cardholders can choose to suspend or deactivate in order to control or restrict usage.

A long-term, industry-wide solution called Payment Account Reference (PAR) was introduced by EMVCo in order to transition acquirers and transit operators away from dependence on Funding PAN for historical analysis of transactions initiated by both PAN and affiliated Payment Tokens. PAR enables merchants and acquirers to forgo use of the PAN for fraud, loyalty and reporting programs. PAR values cannot be used to make financial transactions.

PAR links tokenized and PAN-based transactions so the PAN does not have to be used as the linkage mechanism. A 1:1 relationship exists between PAR and the funding PAN. The PAR can also link all associated cards and devices with trips taken for the purposes of audit or fare calculation (e.g., tapping in with a mobile device and tapping out with the corresponding contactless card due to low battery issues).

Devices that are provisioned using MDES will automatically be assigned a PAR. Once a PAN has been linked to a PAR, the PAR will be provided to the acquirer in each authorization response related to that PAN.

4.3.5 Cardholder Device CVM

Cardholder Device Cardholder Verification Method (CDCVM) is used to verify cardholders using mobile devices for payment transactions. While many transit transactions are low-value and do not require cardholder verification, some transit transactions are of higher value, especially those occurring in retail-like acceptance environments. CDCVM requires an interaction between the user and the mobile device; the mobile device then informs the reader that cardholder verification has been successfully performed.

The actual method of CDCVM depends upon the capability of the mobile device and the wallet application being used. The CDCVM might include a secret known only to the cardholder (e.g., PIN number or password) or a physical feature (e.g., fingerprint or image). Many mobile implementations always require CDCVM to unlock the payment wallet. The CDCVM is typically activated by the cardholder a short time before the mobile is used, rather than requiring action at the precise moment the interaction with the reader is occurring.

4.3.6 Wearables

Wearables offer functionality in different form factors; these form factors are usually linked to a mobile phone. Smart watches, for example, can display communications such as texts or emails, information such as transit schedules, and web content. Payment functions can be added to wearable devices for use in transit.

A wearable is usually controlled by a mobile phone. The wearable manufacturer typically limits its functionality and capabilities; precise implementations vary considerably based on the purpose of the wearable and the parties involved.

Transit payment wearable implementations are governed by the same requirements as mobile devices and cards, especially the need to support offline card authentication to enable fast access. Issuers should note:

- The requirement to provide the FPAN in the authorization response when a tokenized device is used to initiate the authorization (this will automatically be provided by MDES when MDES performs the tokenization/detokenization)
- When "tap in" and "tap out" are both required for a particular system, the requirement that the cardholder use the same device to tap at each end of the trip to avoid problems with fare calculation.

4.4 Card Authentication

In deferred authorization and PAYG systems, where entry is permitted after checking the authenticity of a contactless card, the ability of the contactless card to support offline card authentication (CAM) is essential.

Mastercard rules permit issuers in some regions to issue "always online" Contactless cards that do not support offline card authentication. These contactless cards are not suitable for use in deferred authorization or PAYG models. Issuers of cards for use in deferred authorization or PAYG situations should support offline CAM using CDA, as some transit operators might choose to restrict the use of cards/devices at the point of entry (i.e. turnstiles, validators) if those cards/devices do not support CDA.

Offline CAM also enhances security by preventing fraudulent alteration of data as it is exchanged between the card and the reader.

4.5 Authorization Processing

4.5.1 Data Consistency

Although the information in DE 55 (chip data) is usually consistent with other data elements in the authorization or clearing message, there may be some differences for certain data elements. In some cases, transaction details may result in a mismatch between transaction amounts in the authorization message (i.e., between DE 4 and tag 9F02 in DE 55). Issuers are already advised not to cross-check these fields and not to decline for the sole reason that the values are different. The following data elements are typically consistent with DE 55:

- DE 3 (Processing Code) and tag '9C' Transaction Type
- DE 4 (Transaction Amount) and tag '9F02' Amount Authorized
- DE 13 (Transaction Date) and tag '9A' Transaction Date
- DE 43 (Card Acceptor Name and Location) and tag '9F1A' Terminal Country Code
- DE 49 (Transaction Currency Code) and tag '5F2A' Transaction Currency Code
- DE 54 (Additional Amounts) and tag '9F03' Amount, Other

If the application cryptogram is correct (based on the data in DE 55), the decision to approve or decline the transaction should use the information in the above data elements rather than the corresponding information in DE 55 if present. This is particularly important in transit implementations, where a zero-value debt recovery authorization may be used to enable entry to the transit system (to calculate the ARQC) but an online authorization for the transit fare (shown in DE 04) may be processed after entry is granted.

4.5.2 Transit Transaction Indicator

Issuers should consider the presence of the Transit Transaction Indicator (TTI) in DE 48 (Additional Data), sub element 64 (Transit Program) in the authorization decision process. The presence of the TTI might indicate a new aggregation period, in which case issuer liability would be greater than the Transaction Amount in DE 4.

4.5.3 Application Transaction Counter Monitoring

The Application Transaction Counter (ATC) ensures that every cryptogram produced by a genuine card is unique.

The ATC is incremented by the card during each transaction. Though ATC values are generated sequentially, they may not be presented to the issuer in this way. Transit transactions might be completed offline, completed with deferred authorization, or not completed at all due to technical problems. Because of this, ATCs could be missing in the sequence received by the issuer, or ATCs could be received out of sequence.

For transactions where the application cryptogram has been successfully validated, issuers should keep a record of the most recent ATC received (the "highest received ATC"). Issuers should set an ATC range outside of which a value will be considered suspicious. An out-of-range value may be due to fraud, or indicate that a cardholder is having problems using their card. For transactions with out-of-range ATC values, issuers should raise a post-event alert and conduct further investigation, but should not decline the transaction for this reason only. A suitable value for this range will depend on the market environment where the card is used. For example, if offline transactions are frequently performed (e.g. on buses), a wider range will be required. ATC ranges can vary by issuer.

Issuers should not routinely decline transactions if the ATC is out of the range they have set or if ATCs arrive out of sequence.

To detect duplicate ATCs, issuers may also consider keeping a record of previous ATCs received (in a practical time frame or ATC range) where the application cryptogram has been successfully validated, or of all ATCs missing from the sequence up to the highest received ATC. If the same ATC is received twice with valid but different application cryptogram values, the secret keys of the card may have been compromised. If the same ATC is received twice with valid but identical application cryptogram values, attempted replay fraud may have occurred. In both cases, the issuer should decline the transaction and investigate further.

For further information on the role of ATC for MCBP transactions, issuers may refer to the Mastercard Cloud-Based Payments-Issuer Security Guidelines manual, available on Mastercard Connect.

4.5.4 ATC Update Request

Authorization Request/0100 messages containing DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status), value 6 (ATC Update) are used to notify the issuer of the most recent ATC (Application Transaction Counter) value for the contactless card or device that was used to tap. This enables the issuer to take account of multiple "taps" that have incremented the ATC but that have not yet led to an authorization request or clearing record.

All ATC Update authorization requests will have a zero value for the transaction amount. ATC update transactions may be sent on a regular basis, and issuers must ensure that these transactions do not affect the issuer's velocity checks. Issuers should use the following DE 39 (Response Code) values:

- To approve transactions (when the ATC value does not indicate fraudulent activity): use 00 (approved or completed successfully) or 85 (not declined)
- To decline transactions (when the ATC is outside of the issuer's ATC tolerance): use 05 (do not honor)

Acquirers supporting merchants that implement the MasterCard Contactless aggregated models may support zero amount Application Transaction Counter (ATC) update Authorization Request/0100 messages to notify issuers of the most recent ATC values for offline cardholder aggregation activity.

4.6 Lost, Stolen, or Expired MasterCard Payment Device

When pre-funded travel is purchased, a balance or a time-based pass product may exist for an extended period of time. During that time, the card or device used to purchase that pre-funded travel could be lost or stolen or expire. If that were to occur, the following actions would be taken:

- If the payment device was originally issued as a plastic card or mobile sticker/tag, a new MasterCard payment device would be re-issued to the cardholder in the same form factor.
- If the payment was made using a digital device, the MasterCard account associated with the pre-funded travel would be re-provisioned to a new digital device.

When cards are renewed in the normal replacement cycle, the same PAN is typically used and no action is required to transfer travel privileges (e.g., time-based products). When a card has been lost or stolen, a new PAN is typically assigned; therefore, the new PAN will have to be linked to the existing privileges.

Transit operators should encourage passengers to contact their customer service operation in order to transfer any privileges associated with the old PAN to the new PAN.

5 Acquirer

This chapter highlights transit-related issues that are important to acquirers. More detailed information appears in chapters dedicated to specific topics.

5.1 Payment Processing

An acquirer contracts with a transit operator and other parties (e.g. a system integrator) to implement contactless acceptance in transit environments.

The acquirer is responsible for connecting all points of interaction to the payments infrastructure and conducting all required testing and certification.

Although an acquirer may already have implemented contactless payments for other retail merchants, a new project must be opened with the Mastercard Customer Delivery team for transit implementations in order to ensure the specific requirements of transit are met. This will include formal approval of contactless transit readers and all the associated integrity testing Mastercard requires. More details on Testing is provided in Chapter 9.

Transit models fall into four broad categories (see Section 1.4).

When the fare is known at the time of tap, a regular contactless transaction takes place as in any other environment. For PAYG and pre-purchased access, card interaction with the contactless reader is the same as card interaction in other contactless transactions, except for certain transit-specific characteristics (e.g., no CVM requirement at the point of entry).

5.1.1 Refunds

Acquirers must be able to refund a fare payment transaction using the same Mastercard Contactless card that was used to make the fare purchase.

5.1.2 ATC Update Request

Acquirers supporting merchants that implement the MasterCard Contactless aggregated models may support zero amount Application Transaction Counter (ATC) update Authorization Request/0100 messages to notify issuers of the most recent ATC values for offline cardholder aggregation activity. (See section 2.7.3.)

6 Transit Operator

This chapter explains the role and responsibilities of the transit operator. The transit operator acts as the merchant for transit payment transactions, but also performs many other customer-facing functions.

6.1 Customer Experience

Transit operators and financial institutions both want the best experience for their passengers/cardholders, and typically the needs of the parties are aligned:

- Passengers and transit operators want easy, smooth passage through the transit system without undue delays or interruptions.
- Financial institutions and transit operators want the payment to be collected quickly, but without undue risk or costly exception processing.
- All parties want efficient implementation, ensuring solution integrity while minimizing systems or operational problems.

A good passenger experience makes for a successful, cost-effective solution.

6.1.1 Entry to the Transit System

Passengers must know where they can use their card and what is expected of them. This includes:

- Clearly identifying the readers onto which contactless cards must be tapped. The more consistent the implementation, the easier and faster it will be for passengers (e.g., all entry gates should have the same design).
- Ensuring requirements are effectively communicated – e.g., the need to "tap in" and "tap out" in order to calculate the appropriate fare for a trip. This is especially important where there is no physical barrier controlling entry or exit to the system.

6.1.2 Fare Capping

Historically, transit operators have offered time-based fares in the form of daily, monthly, or annual transit passes (a.k.a. tickets). With open-loop payment solutions, this capability can be implemented dynamically, so passengers can be converted to time-based status using data from their travel patterns. In other words, passengers do not have to purchase time-based tickets in advance in order to benefit from time-based fare concessions.

Fare capping is the practice of identifying a time-based passenger by automatically aggregating their fares up to a time-based threshold (e.g.. daily or weekly). Once a passenger meets a time-based maximum fare, they will no longer be charged further single fares until they reach the end of that time threshold or qualify for an even longer time threshold/ more advantageous maximum fare.

Fare capping policy is implemented within the core fare system and does not impact the entry/exit process in any way. Removing the need to issue and manage time-based tickets can create major cost savings for the transit operator and convenience for passengers.

Contactless transactions without cardholder verification are restricted to a limit which varies by market. Transaction amounts above the cardholder verification limit will require an appropriate form of verification.

6.1.3 Trip History

When several trips are aggregated into a single payment on a passenger's billing statement, the passenger may want to know which trips contributed to the total – especially if the amount is greater than they expected. For aggregated solutions, therefore, passengers must have access to their trip history and a way to inquire about any discrepancies.

Access to trip information may be provided via a call center, but is more simply provided via a website or mobile app. For a web or app-based solution, passengers will need to have a way to log in to the system and link their card(s) to their transit records.

The statement description may contain a unique identifier to enable easy transaction look-up.

6.1.4 Revenue Inspection

Transit operators should carry out revenue inspection regardless of how the customer has paid or is expecting to pay for travel; as such, revenue inspection policies and processes will apply to the use of contactless cards. Traditional revenue inspection relies on reading information from a ticket or closed-loop contactless card to determine if a passenger has purchased a ticket, or (if PAYG/deferred authorization) has been validated at the start of their trip. This allows a Revenue Inspector to issue a penalty on the spot for any infraction.

When using an account-based back office with EMV, as in the PAYG model, no transit specific information (e.g. fare product purchased) is written to the card itself. In this case, a new model for revenue inspection is necessary. This is likely to involve reading data from the contactless card to ensure that the card has been used to make a valid tap. This can be achieved by performing a zero-value transaction with the card. The tap data is then used to reference the travel history in the back office system.

Care must be taken to comply with PCI requirements whenever payment card data is read, transmitted or stored. (See Chapter 9.)

If revenue inspection results in the payment of a penalty, any transaction to collect that fare must be performed in accordance with the requirements in this guide.

6.1.5 Mobile Application

Transit operators might use a mobile app to provide general customer information (e.g., route maps, timetables, travel conditions, planned maintenance, etc.). Contactless payments cannot be integrated directly into this app, as contactless payments have specific security and operational requirements. However, when the app enables transit purchases to be made, payment functionality can be integrated to enable fast in-app payments using cards stored in a mobile wallet.

6.1.6 Payment Account Statement

The passenger statement should enable easy recognition of transactions as transit related. System reference numbers should not be used in isolation, as these will mean little to passengers. Where an amount is aggregated, the statement description should display the time period during which individual trips occurred.

6.2 Deny List

The Deny List is used to limit transit operator risk and support rapid access to the transit system when real-time authorization of a card is not possible. As an authorization has not been completed prior to system entry, the transit operator assumes some risk: financial responsibility for the fare will only be fully assumed by the issuer once an authorization request has been approved.

In this scenario, two checks are performed rapidly offline:

- Authenticity of the contactless card is checked by completing an offline chip transaction using Combined Data Authentication (CDA). This ensures that the card is genuine and certain critical account data is not changed during the interaction between the card and reader.
- The card is checked against the "Deny List". This list might include known stolen contactless cards or cards that owe payment to the transit operator.

These two checks provide essential protection to the transit operator and ensure the integrity of the system for all users.

Transit operators should add cards to the Deny List whenever the card has been used for access but a subsequent authorization has been denied – meaning that funds are owing to the operator. Cards might also be added based on information available locally (e.g., lost and stolen hot lists). transit operators may also want to consider denying cards with a persistent pattern of fare avoidance (e.g., multiple failed revenue inspections or penalties). It is important for the transit operator to distinguish between declines for technical reasons (which are beyond the control of the passenger) and those due to lack of passenger funds.

Card issuers may decline authorization requests for a number of reasons; the principal reasons are:

- The cardholder (passenger) has insufficient funds for the transaction
- The transaction has a high probability of being fraudulent

Decline rates may vary across card issuers based on their fraud risk appetite.

Transit operators should add any card that has a declined transaction for any value to the Deny List upon tapping at the reader or the point of entry. This should be done as soon as possible but at the latest within 24 hours. Passengers on the Deny List will not be allowed to travel again until a successful authorization has taken place.

To provide good customer service, the Deny List should be managed in a careful and timely manner. Once amounts in arrears have been paid, passengers should be promptly removed from the Deny List and allowed access to the system again.

Passengers should have the ability to ascertain whether their card is on the Deny List, and should be able to contest inclusion on the list if they believe they are up to date on payments.

6.3 Revenue Inspection

Revenue inspection occurs during a trip when passengers are asked to prove they have authority to travel.

Traditional revenue inspection relies on reading information from a ticket or that held on a closed-loop contactless card in order to determine whether a passenger has purchased a ticket or (if deferred authorization/ PAYG) has been validated at the start of their trip.

When using an EMV payment card with an back office system (as in the PAYG model), no transit specific information is written to the card itself. The Revenue Inspector reads the card data using an approved device, which then sends information (in real-time or at a later stage) to the back office where the credential to travel is checked and any penalty is assessed.

Other implementations may make use of other revenue inspection solutions, e.g. checking that the card has been validly tapped at a point of entry or leveraging chip card capabilities like data storage.

6.3.1.1 Permissible Use of a MasterCard Contactless Device as a Transit Credential

If a MasterCard Contactless card is used for access to a transit environment, the account associated with that card must also be used for payment of the transit fare. Mastercard Contactless cards may not be used for access only.

6.4 Lost, Stolen or Expired Cards

When cards are replaced in the normal renewal cycle the same PAN number is typically used and the expiration date and PAN Sequence Number are updated. Transit operators must ensure that privileges earned on the old card (e.g., prepaid or time-based) are transferred to the new card.

When cards are lost or stolen, cardholders are typically issued a new PAN. Transit operators must provide a method for passengers to associate the new PANs with their existing privileges.

7

Systems Integrator

This chapter describes the role of the Systems Integrator, which brings together many different systems to create an integrated transit payment solution.

Transit implementations can be complex, as they can involve:

- Multiple modes of transportation, with different operational environments, features, and constraints
- Multiple transit operators
- A variety of IT systems handling the different elements of the payment eco-system
- Complex fares – time-based fares (e.g. daily, weekly), time-of-day fares (e,g. off peak), zone-defined fares, different classes of travel, or concessions (e.g. for students, seniors, welfare recipients).
- A variety of legacy operating infrastructures
- A variety of points of passenger interaction (e.g. transit gates, on-platform validators, inside vehicles, ticket offices, passenger-operated machines, TVMs, agents, call centers, mobile apps, and the web)
- Different transit payment models (e.g. retail-like acceptance at contactless readers, ticket machines, prepaid solutions, and PAYG)
- Split between different payment methods (e.g. contactless reader, local devices, centralized billing)

Due to this complexity, acquirers and transit operators will often seek support from a Systems Integrator to bring together the many different aspects of an implementation.

This chapter describes factors that might create complexity during implementation.

7.1 Terminal and Network Approval and Certification

More details on this topic are given in Chapter 9 and in guides related to the specific processes and services.

7.1.1 Terminal Type Approval

Terminal Type Approval is typically completed by vendors that supply readers and terminals to transit operators.

The concept of "terminal" is somewhat complicated, because different aspects of the functionality typically associated with a terminal device are often spread over different functional elements. Consideration must be given to functions that are outside of the normal EMV-defined transaction flow but that need to occur within the context of a transit operation (e.g., checking the Deny List before granting admission to the system).

Whether new or repurposed from prior (non-EMV) use, readers must be type-approved as stand-alone devices. If the same type of reader is used for multiple purposes, care must be taken to ensure that the appropriate approvals have been obtained for each implementation. For example, the functionality required at an entrance/exit gate might be different from the functionality required at a ticket office or vending machine (e.g., chip/PIN). In other words, even if the same version of the reader is used in both locations, it may be necessary to support other functional aspects of the terminal.

Terminal Type Approval can follow either of two independent processes:

- Mastercard Contactless Reader Approval Process: tests whether the reader is compliant with the Mastercard Contactless reader specifications
- EMVCo Contactless Product Type Approval: tests whether the reader is complaint with EMV Contactless specifications.

Both processes require the EMVCo Type Approval Contactless Terminal Level 1 to be completed as a pre-requisite.

Successful completion of either Mastercard Contactless Reader Approval Process or EMVCo Contactless Terminal Type Approval is covered by a Letter of Approval.

Note: that Type Approval is only one of the processes required for proper implementation. Other approval processes may be required, e.g. Terminal Quality Management (TQM) or (if the terminal, e.g. in a ticket office, supports PIN) Payment Card Industry – PIN Transaction Security (PCI-PTS). (See sections 10.3.2 and 9.1.)

7.1.2 Mastercard Terminal Integration Process (M-TIP)

The Mastercard Terminal Integration Process (M-TIP) tests the behavior of the terminal/reader once it has been integrated with the acquirer host in a test environment. M-TIP is designed to ensure that an acquirer deployment will not cause unacceptable damage to Mastercard operations or the brand's reputation. It is an important resource for system integrators.

M-TIP focuses on requirements that directly affect acceptance, but it is not an exhaustive functional certification process. It remains the acquirer's responsibility to ensure that all terminals are compliant with Mastercard rules and requirements.

Terminals submitted for M-TIP testing must have obtained all the vendor Terminal Type Approval processes listed above, as applicable.

Please see section 10.4 for more information about M-TIP.

8 Transit Terminal and Reader Requirements

This chapter provides an overview of the acceptance side of a contactless transaction and details specific exceptions and variances related to transit.

Full details of the requirements for contactless acceptance are contained in [EMVA], [EMVB], [EMVC2] and [EMVD].

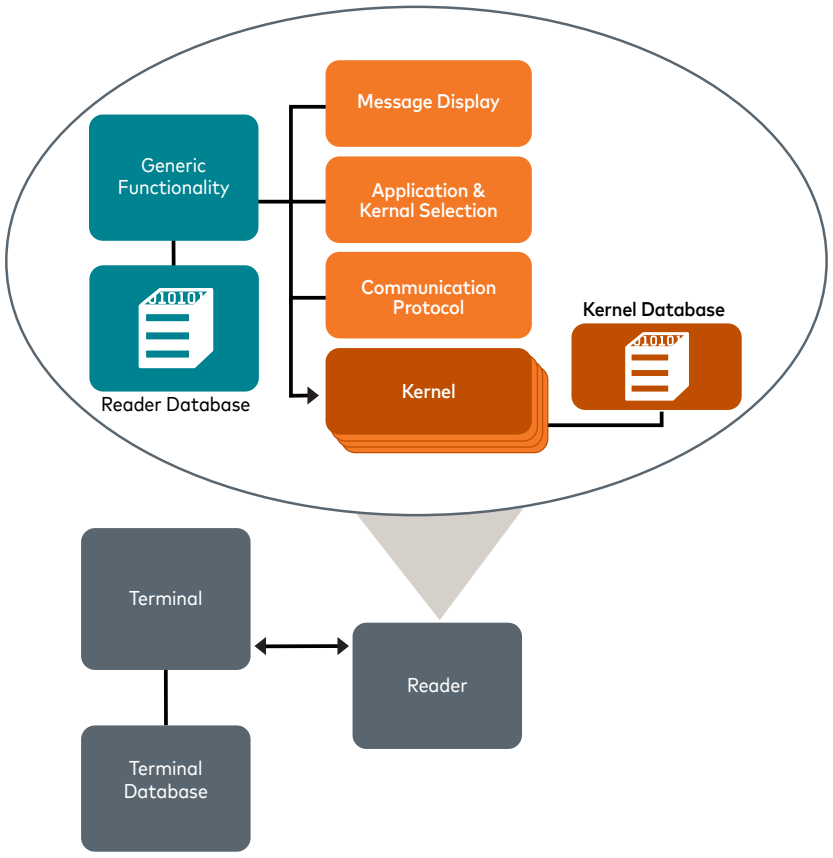
8.1 Contactless Acceptance Architecture

The term "transit devices" refers to the contactless acceptance equipment at the Point of Entry into a transit network, e.g. a train station gate or an Electronic Ticketing Machine (ETM) on a bus. This equipment may be a single integrated piece of equipment or a set of separate physical components that together form the card acceptance device.

The acceptance of a contactless card or device requires:

- A contactless reader
- A terminal

Diagram 4: General Point-of-Sale Architecture



The contactless reader is responsible for interaction with the contactless card or device. This includes managing contactless communications, application selection and selection of the appropriate kernel (explained in [EMV Book B], Entry Point specification), completion of the EMV

transaction flow, and transmission of the required data to the terminal. The contactless reader design must also include some form of visual indication -- a set of four clearly visible status indicators (e.g. LEDs), a display (e.g. LCD), or both.

The terminal is responsible for controlling the interface with the card reader, managing other devices (such as PIN pads or printers), and interfacing with the acquirer host system. Transaction detail is collected by the terminal and presented to the reader, along with any contextual information and information on the capabilities of the terminal (e.g. whether CVM options are supported). The kernel may also hold static configuration data.

There are three principal transit environments where contactless readers are deployed:

- Mass transit systems where gated systems control access
- Attended or unattended ticket machines
- Where 'ticket' validation as opposed to ticket sales or entrance control is supported, e.g. bus, tram, and gateless rail platforms. This environment is more likely to include bus Electronic Ticketing Machines (ETMs) with embedded or standalone connected contactless readers and platform validators, usually known as PVALs.

8.2 Contactless Acceptance

8.2.1 Mastercard Contactless Transaction Data Editing

Data received from the contactless card is used by the card issuer during online authorization to validate that the card is genuine. Therefore, all data retrieved from the contactless card must be presented to the acquirer or payment processor without modification.

8.2.2 Terminal or Transit System Generated Transaction Reports

To simplify any transaction queries, the method of data input needs to be recorded on all transaction logs or reports produced by the transit terminal or transit operator's back office system. Any report produced by the transit system must specifically identify Mastercard contactless transactions.

8.2.3 Design Considerations

When designing a Mastercard contactless terminal, the terminal vendor must make allowances for both left and right handed, visually impaired, aurally impaired, and otherwise disabled passengers.

Some markets may also have statutory requirements with respect to product safety, emissions, and susceptibility to environmental impacts (e.g. temperature extremes). All contactless terminal equipment must fulfill these requirements and be certified as required by statutory bodies.

Terminal vendors and transit operators should consider that a passenger-facing terminal could be subjected to vandalism. Terminals should be constructed using durable materials, and readers should be securely embedded in the terminal architecture.

8.2.4 Data Validation

Contactless transactions do not require any additional data validation beyond the processes described in the Mastercard Contactless Reader Specifications.

8.2.5 Terminal Capabilities

Transit terminals must be able to provide information to connected systems on (a) the method used for reading the contactless card, for each transaction and (b) the terminal's ability to complete the various reading methods.

8.2.6 Receipt Requirements

Receipts are not required in transit environments, but the transit operator must provide the passenger with transaction history and the individual trips that make up any aggregated payment. This will usually be provided via a website or smartphone app. (See section 2.3.5.)

8.2.7 EMV Contactless Symbol

All Mastercard Contactless terminals must identify exactly where passengers are to tap their contactless cards. This area is referred to as the "landing zone."

The EMV Contactless Symbol must always be placed in the center of the landing zone, indicating the strongest part of the radio frequency signal (referred to as the "operating volume"). All contactless terminals must permanently display the EMV Contactless Symbol in the center of the landing zone.

The EMV Contactless Symbol should be visible before and during the transaction process to ensure the passenger is aware of the contactless capability of the terminal and can see exactly where to tap the contactless card.

If space permits, Mastercard Contactless and other payment brands may also be placed on the landing zone – as long as branding rules are maintained and the contactless symbol is not obscured or relocated from the center of the zone. If space on the landing zone does not permit, any additional branding should be positioned so as not to distract the passenger from the EMV Contactless Symbol and the landing zone.

EMV Contactless Landing Zone Symbol

The size of the landing zone symbol may be changed to fit the ergonomics of the landing zone, as defined in the Mastercard Contactless Branding Standards.

The branding requirements for Mastercard Contactless terminals and readers are defined in the Mastercard Contactless Branding Guidelines. These guidelines specify artwork, colors, and minimum size requirements.

It should be noted that where the Mastercard Contactless brand identifier is displayed along with other brands on a POS terminal, the Mastercard Contactless brand must appear in a size at least equal to the largest other brand displayed.

The terminal vendor and transit operator should use materials for the Contactless Symbol that are not degraded by use. The Contactless Symbol should show no significant degradation after one million "contacted" presentations (where the contactless card physically touches the landing zone during the tap).

Contactless terminals should be designed with no physical obstruction around the landing zone and/or antenna that would prevent the acceptance of payment devices larger than a mobile phone (such as a tablet) or wearable devices (such as a watch).

8.2.8 Audio Visual Capabilities

The overall cardholder experience of using a Mastercard Contactless card should always be a consistent one. However, it is recognized that the purpose of audiovisual indication in the transit environment is different from that in the retail environment.

The primary purpose of the audiovisual indication is to advise the cardholder, and, if appropriate, transit agency staff, of an access control decision (access to the transit system either granted or denied with or without restrictions for example: 'child card').

8.2.8.1 Visual Indication

Visual indicators should consist of clearly visible visual status indicators (e.g. LEDs), a display (e.g. LCD) that supports a graphic representation of the visual indicators, or both. The visual indicators should show the status of the transaction (or, between transactions, of the reader).

The terminal or reader should be designed so that the status indicators are clearly visible to the passenger when a card has been presented and a card read is in progress. When LEDs are used, Mastercard recommends the use of a single color (green).

In the case where only a display is used, it should contain a minimum of three lines of characters to allow the display of status indicators in the

followed by two lines of sixteen 8x5 dot matrix low-resolution characters for passenger messages.

8.2.9 Branding Requirements

For the Mastercard branding requirements please see https://brand.mastercard.com/ .

8.3 Contactless Reader

The business requirements and constraints of the transit environment differ from those of other retail environments; because of this, the implementation of Mastercard Contactless readers for deferred authorization/PAYG transit use comes with unique requirements.

Where Mastercard Contactless readers are added as terminal modules, they must meet the same requirements as the base unit, including compliance with:

- Electrical regulations
- Environmental specifications
- Transportation (shock and bump, etc.) specifications
- Early life failure mode specifications
- Electromagnetic Compatibility (EMC) specifications
- Electrostatic Discharge (ESD) specifications

8.3.1 License and Specifications

The Mastercard Contactless Reader Specifications and Mastercard Contactless Branding Guidelines must be used by any vendor that has entered into a license agreement with Mastercard for the purposes of producing contactless readers.

Note: To become a Mastercard Contactless licensee and obtain the latest specifications, an email should be sent to contactless@Mastercard.com, including the company name and contact information.

The license agreement allows the licensee to submit contactless-enabled terminals to Mastercard for testing and type approval; the Mastercard testing and approval process determines terminal compliance with all requirements. Information on the testing and certification processes for Mastercard Contactless terminals can be found in Chapter 9 of this document.

The Reader Specifications should be reviewed in conjunction with the following publications from EMV Co:

- EMV Contactless Specifications for Payment Systems, Book A - Architecture and General Requirements [EMVA]
- EMV Contactless Specifications for Payment Systems, Book C-2 - Kernel 2 Specification, [EMVC2]
- EMV Contactless Specifications for Payment Systems, Book D- EMV Contactless Communication Protocol Specification [EMVD]

8.3.2 Reader Support for Non EMV-Compliant Contactless Card Types

Transit readers may need to accommodate card types that support communication technologies other than those used for EMV transactions (e.g. NFC-F or FeliCa). This might be the case, for example, if Mastercard Contactless acceptance is being introduced into an existing electronic fare collection system that uses one of these other technologies. These other technologies might not support collision resolution, ISO/IEC 14443-4, and/or variants of ISO/IEC 14443 (e.g. Calypso).

Given all the possible combinations of contactless card types, Mastercard cannot define a single polling loop and protocol activation sequence that works for all.

The relevant EMVCo requirement is that the reader detects and activates a single card that supports ISO/IEC 14443-4 and ISO 7816-4 as defined in the EMV specifications.

Mastercard requires that:

- Transit readers have a configuration setting to activate the EMV Co polling and protocol activation sequence.
- Regular EMVCo testing be performed on this configuration setting. If the reader supports Mifare and/or NFC-F (or FeliCa), Mastercard also requires that Mastercard Contactless Integrity Testing be performed.

Transit readers may have another configuration setting to activate another polling cycle(s) and protocol activation sequence they might otherwise use. Integration (regression) testing and performance (regression) testing must be performed on this configuration setting in combination with:

- A single card that only supports ISO 14443 and ISO 7816-4.
- A single card that supports ISO 14443-4 and a combination of Mifare/Desfire or NFC-F (or Felica)

8.3.3 Contactless Interface (Level 1)

All newly developed Mastercard Contactless readers should comply with the latest version of [EMV Book D] but must, at a minimum, comply with the version in the most recent version of the Mastercard EMV Device Approval—Application Note.

8.3.4 Mastercard Contactless Specifications (Level 2)

Mastercard supports multiple versions of the Mastercard Contactless Reader Specifications. All new deployments should be based on the most recent version of the Contactless Specifications.

Contactless terminals submitted for Type Approval must comply with the allowed versions of the Mastercard Contactless Reader Specifications as indicated in the latest applicable operations announcements, application notes, and specification release notes, all available on Mastercard Connect.

Contactless transit readers in the Europe Region are not required to support contactless magnetic stripe.

8.3.5 Transaction Processing Speed

To ensure an acceptable cardholder experience, the interaction between the contactless card and the contactless terminal must take place in as short a time as possible.

In the transit environment, the time taken for the transaction to be approved or declined (and hence an access control decision made) is critical to ensure the steady flow of customers through access gates or onto a bus or tram. This contrasts with general retail transactions, where the key performance requirement is the amount of time the card must be held in the reader field (i.e. the duration of the 'tap').

In the transit environment, therefore, there is more emphasis on the reader and the terminal working effectively together.

[EMVA] refers to Transaction Processing Time as the availability of the Offline Transaction Disposition under Section 10.3.1.

Due to the critical need for speed in the transit environment, transit readers should perform faster than certified retail readers. By improving the performance of the card/reader interaction, the designer of the transit reader can 'buy time' for access control processing and indication functions.

If PAN, expiration date, and/or PAN Sequence Number need to be used for additional terminal-based or back office access control processing, the tag containing them can be sent to the terminal prior to delivery of the authorization/response and clearing data.

Tags can be configured in a reader using [MCRS] or [EMVC2] in the "Tags To Read" data element (Tag: 'DF8112'). When the reader has completed the outstanding requests from the terminal, it sends the data to the terminal via the Data Exchange mechanism.

In combination with a reader that meets the performance requirements as described in "Duration of Card/Reader Interaction", the terminal receives the data elements listed above 250 to 300 milliseconds after a transaction has started.

8.3.6 Collision Detection/Resolution Testing

[EMVA] Section 5.5.2 deals with overlapping transactions.

In transit environments, it may be important for a terminal to check that a card has been physically removed, and to ensure that the next transaction is not initiated until the prior passenger has made sufficient progress through the gate.

Note: that the removal procedure for a card as defined in [EMVD], Section 9.5, could be started when the kernel indicates 'Card Read Successfully status, 1' as this is the earliest point in a transaction at which a card can be removed.

In the event that more than one card is detected in the reader field at the same time (that is, a data collision is detected), some readers are configured to resolve the collision (i.e., select one card for the transaction). EMV Co Contactless requires that if a data collision is detected, the reader must not transact but instead report an error condition. In this case, the reader will not transact until all cards have been removed from the field and a single card is re-introduced.

8.3.7 Application Version Number

Any hardware and software elements or components used to create a contactless-enabled terminal must be individually identifiable; this reduces the need to retest already approved contactless product components. In addition, the application logic component must also preserve the version number of the Mastercard Contactless Reader Specification [MCRS] with which it is compliant.

8.3.8 Traceability

Mastercard Contactless readers must implement a traceability function that allows the contact and contactless terminal application, kernel version, Level 1 hardware version, and Level 1 and 2 software versions to be retrieved from the terminal or reader. This function may be provided in printed or displayed form but must be fully documented in the reader's user manual.

Note: In cases where Level 1, Level 2, and acquirer application modules are all compiled within the same software, the firmware/build name and version number may be acceptable.

8.4 Contactless Reader to Transit Terminal Interface Requirements

The Transit terminal developer is free to select the most appropriate interface type and protocol to be used between the contactless reader and the transit terminal. Other than transferring the data correctly and being able to identify the entry method as contactless, no further requirements are currently defined for this interface.

Mastercard has no globally specified requirements for how the contactless reader on a terminal is controlled. It should be noted that in transit, the contactless reader is active at all times. So, it is recommended that the flexibility of this control be considered by terminal manufacturers during device development.

The timing of a tap should have no adverse effect on the processing of the transaction. The transit device must not buffer or store card details when a contactless card is presented in advance of a new transaction starting. This is to ensure that details from a previous transaction are not mistakenly used. Mastercard contactless card data must not be stored or buffered, and must only be accepted after the payment part of the transaction process has commenced. See also PCI (Section 9).

8.5 Contactless Terminal

8.5.1 Online and Offline Capabilities

Transactions initiated at readers that enable access to the system will not generate real-time authorization messages; however, terminals should be configured as online-capable and not as offline devices. At the point of access, cards will not be authorized based on the availability of funds – this will be checked in due course – so as to avoid Application Authentication Cryptogram (AAC) decline responses that generally do not enable CDA.

Terminals should be configured as online-capable or online-only.

8.5.2 Cardholder Verification

In PAYG implementations, there is no need to support cardholder verification as no high value transactions are ever performed. Normal EMV CVM processing is performed by the reader, but the terminal will advise the reader that only "No CVM" is supported. All contactless cards must support No CVM.

Many mobile devices support cardholder device CVM (CDCVM) such as touch ID or password solutions. These are often required to unlock wallets or cards to enable payments but are not, for the purpose of the cardholder authorizing the payment, a requirement for the tap. The reader will recognize that CDCVM has been performed but will still proceed with the transaction even if it has not.

8.5.3 Mastercard Contactless Payment Processing Requirements

A terminal will only send the purchase amount to the linked transit back office system if the fare is paid for when boarding the bus, tram or other mode of transport.

9

PCI

This chapter gives an overview of industry-wide data security requirements.

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle payment card-related data.

The PCI Standard is administered by the Payment Card Industry Security Standards Council. It was created to increase controls around cardholder data in order to reduce fraud. The PCI Data Security Standard specifies twelve requirements for compliance, organized into six distinct goals.

All entities handling card data need to respect PCI DSS. This applies both to core payment systems and any other systems that leverage card data, e.g. transit systems that record card data in order to calculate fares based on "tap in" and "tap out" information.

Validation of compliance with the Standard must be performed before systems are live and then again annually. Validation may be conducted by an external Qualified Security Assessor (QSA), by a firm specific Internal Security Assessor that creates a Report on Compliance (for organizations handling large volumes of transactions), or using a Self-Assessment Questionnaire (SAQ) (for companies handling smaller volumes).

Although the PCI DSS must be implemented by all entities that process, store, or transmit cardholder data, formal validation of PCI DSS compliance is not mandatory for all entities.

In the event of a security breach, any compromised entity which was not PCI DSS compliant at the time of the breach will be subject to additional payment brand penalties, such as fines.

Further information about the requirements for Site Data Protection can be found at www.mastercard.com/sdp.

9.1 PCI PTS

If a terminal is PIN-capable it must meet the PCI-PTS requirements.

10 Certification and Testing

This chapter identifies the different types of testing required to implement transit payment programs, including the steps involved and the parties responsible.

10.1 About Certification and Testing

Mastercard requires different aspects of transit payment systems to be tested and certified at different stages of an implementation. It is likely that different types of testing will be completed by different parties.

Network Interface Validation – this testing ensures that the acquirer correctly interfaces with the Mastercard Network for handling authorization, clearing, settlement and exception messages. It is performed by the acquirer, and will likely have already been completed independent of the transit implementation. While transit may use authorizations differently, transit implementations do not involve new message types.

Terminal Approval Process - Acquirers and transit operators must only use approved terminals.

All chip capable terminals and readers must undergo Type Approval testing to ensure they comply with EMV and Mastercard standards. Vendor Terminal Approval Processes are initiated and performed by vendors to certify their own terminals/readers.

- Terminal Type Approval—The testing in this certification can follow either of the following independent processes:
  - Mastercard Contactless Reader Approval Process: tests whether the reader is compliant with Mastercard Contactless reader specifications
  - EMVCo Contactless Product Type Approval: tests whether the reader is complaint with EMV Contactless specifications.

Both processes require the EMVCo Type Approval Contactless Terminal Level 1 to be completed as a pre-requisite. Successful completion of the Mastercard Contactless Reader Approval Process or EMVCo Contactless Product Type Approval is covered by a Letter of Approval.

- Terminal Quality Management (TQM): the Terminal Quality Management program is a Mastercard process that helps ensure the overall quality of terminal/reader production, including physical manufacturing and the vendor's quality control and customer service processes.
- Payment Card Industry – PIN Transaction Security (PCI-PTS) (if terminal is PIN capable): The Payment Card Industry - PIN Transaction Security (PCI-PTS) testing is owned by the Payment Card Industry Security Standards Council and checks whether a submitted PIN Entry Device is compliant with PCI security standards as set forth in the PIN Transaction Security (PTS) requirements.

Terminal Integration Process (M-TIP) – this suite of testing ensures that certified chip components and pre-certified networks work effectively together and that terminals/readers are in compliance with Mastercard rules. M-TIP takes place once terminals and readers have been integrated with the acquirer host. It is the responsibility of the acquirer to complete M-TIP testing, but the acquirer will rely on close co-operation with the transit operator and Systems Integrators. Terminals submitted to M-TIP testing must have obtained all the Vendor Terminal Type Approval processes listed above, as applicable.

For complex transit implementations, the functions of the "terminal" may be split across different system components. For example, the card-terminal interface functions may be performed by a card reader at the transit gate that connects to a central POS terminal. Several POS terminals may be connected in turn to the transit host system that collects transactions and that may perform parts of the EMV processing (e.g. checking warning bulletins).

Where the payment functionality is split between different devices, the overall system is considered to be the EMV terminal; in this case, the overall system must perform the functions required by EMV and be tested in the same way as any POS terminal. In other words, split systems formed from different combinations of hardware and software must have a valid EMVCo approval and pass M-TIP in the same way as stand-alone terminals.

10.2 Network Interface Validation

Network Interface Validation (NIV) testing will be performed by the acquirer to ensure their system interfaces correctly with Mastercard.

There are specific transit-related test cases specified by Mastercard; Acquirers should run these specific tests before commencing transit operations.

Six (6) test cases relate to card-present transit transactions and two (2) pertain to e-commerce transit transactions. The tests ensure the correct marking of transit transactions (e.g. DE 48, se 64 as Transit Transaction Type Identifier).

These tests are detailed in the Testing Reference Information Center on Mastercard Connect. They appear in the Test Selection Engine (TSE) section of the Information Center (Transit Program Transactions).

For more detail on NIV please go to:

1. www.mastercardconnect.com
2. Publications
3. Testing Reference Information Center
4. Customer NIV Test Case Table Search

10.3 Terminal Approval Process

The terminal approval process will normally be completed by a vendor who will obtain a Letter of Approval for terminal/reader functionality.

10.3.1 Contactless Reader Approval

Mastercard provides a range of services and technical support to assist vendors during Mastercard Contactless development and installation. The support services include product approval and a help desk for responding to technical questions regarding Mastercard Contactless specifications. The contact email address for this service is chip_certification_ad@Mastercard.com.

The Mastercard terminal approval process is based on the following principles:

- Terminals supporting Mastercard contactless acceptance need to be type approved.
- Approval tests are performed in Mastercard-accredited testing laboratories.
- Testing laboratories sign a service agreement with the vendor.
- Testing laboratories prepare a detailed test report for the vendor.
- The vendor needs to request approval from Mastercard.
- Mastercard is the approval authority and issues the approval statement.

Mastercard provides a Terminal Design Review service that evaluates the design of the terminal at the earliest possible stage against the implementation requirements outlined in this document. This service also ensures that the Type Approval testing services are appropriate for the terminal's design.

For more information please refer to the Mastercard Contactless Reader Approval Process Guide V2.0, available on Mastercard Connect™.

10.3.2 Mastercard TQM Program

The Mastercard TQM program assures quality levels for all Mastercard contactless terminals. Repeated product conformity is a crucial element of quality control that is assured through the TQM program. TQM provides transit operators and acquirers with assurances that the terminal vendor has the capability to continually produce Mastercard Contactless products consistent with the original samples for which a Mastercard Contactless Letter of Approval was granted.

For more information please refer to the Mastercard Contactless Reader Approval Process Guide V2.0, available on Mastercard Connect.

10.4 M-TIP

M-TIP ensures that the approved terminal and reader operate according to Mastercard requirements. It is an essential part of ensuring the integrity of the payment system and provides vital reassurance to acquirers and transit operators prior to going live.

M-TIP must be completed by the acquirer in close co-operation with the transit operator and the Systems Integrator.

Details on the prerequisites to initiate M-TIP are listed in the [MTIPPG] and [MTIPQR]. Please refer to the current versions of these documents, which can be found in the Chip Information Center on Mastercard Connect.

Support for transit testing has been integrated into the M-TIP Test Set, as of version 235 (available on MC Connect). M-TIP currently supports transit terminal implementations with the following characteristics:

- Acceptance restricted to cards which support CDA (online-only cards without CDA will be declined)
- Uses fixed/placeholder amount (such as zero amount)
- Approves transactions offline
- Supports Post-Authorized Aggregated transactions
- Does not support contactless mag-stripe mode
- Does not support transactions above the CVM Required Limit

Transit terminal implementations that are compliant with the above requirements must select 'Transit Open Loop Payment Acceptance - Type 1' under the "Environment of use" question in the TSE.

Glossary

Term	Definition
Access Control	The method of passenger entry into the transit system, e.g. automated ticket gates.
Acquirer	The financial institution that supports the transit operator. This bank is responsible for interfacing with Mastercard on behalf of the transit operator and receives settlement for transactions.
Aggregated Transaction	Fares for multiple trips added together and presented as one amount for payment.
Authorization	An online message sent to the issuer requesting approval for a transaction.
Authorization Response Cryptogram (ARPC)	Generated by an issuer's host system in response to an online EMV transaction. ARPC is returned to the chip card and checked by the card to verify that the response came from the issuer.
Blocked Status	A condition that prevents a card from being used for payment (e.g. if the card has been reported stolen).
Cardholder Device	A contactless card that is not a plastic card, e.g. a mobile phone or a smart watch.
Chargeback	A codified rule violation whereby the issuer attempts to reclaim money from the acquirer. Where transactions are completed according to specifications, chargebacks seldom occur.
Clearing	The financial details presented for payment.
Closed-Loop	A payment solution in which cards can only be used in a restricted range of terminals, typically linked to one merchant (transit operator) or card brand.
Contactless Card	A card that can perform transactions using NFC communication with a terminal. In this document "contactless card" is used to refer to plastic cards and any other device (e.g. mobile phones, smart watches) that can perform contactless transactions.
Credential to Travel	A ticket, electronic token, or database entry signifying that a passenger has the appropriate authority to take the current trip.
Customer / Cardholder / Passenger	The individual making the journey and paying the fare.
Debt Recovery	The collection of fares or aggregated fares outside the normal cycle after the initial attempt to obtain payment has been declined.
Deferred Authorization	An authorization that happens at a later time than the interaction between the contactless card and the reader.
Deny List	A list of cards that will not be allowed access to the system, usually due to outstanding debts.
Dual Message	A payment system where approval of the funds (authorization) and collection of the funds (clearing) happen using two discrete messages.
EMV Mode	A method of performing a contactless transaction where a broad set of data is exchanged and presented to the issuer. All contactless transactions in transit are EMV Mode.
Fare Capping	The practice of identifying a time-based customer through fares that accrue to a time-based threshold (i.e. daily or weekly maximum). Once a customer meets a daily or weekly maximum, they would no longer be charged for further individual fares during that time period.
Four Party Model	Description of payment solution involving the transit operator and passenger, each supported by financial institutions that exchange transactions through a payment brand's network. The four-party model enables open-loop solutions in which cards issued by any financial institution can be used in the system.
GENERATE AC	A chip command that will generate an Application Cryptogram (AC).

Term	Definition
Host Cloud Emulation	A means of performing transactions using a mobile device without having to store secret data on the device.
Issuer	A financial institution that provides payment cards to their customers.
Kernel	The software in the reader attached to the terminal. Different kernels perform contactless transactions in different ways. A single reader will probably support multiple kernels allowing it to perform transactions with a wide variety of cards.
Mag Stripe Mode	A method of performing a contactless transaction where a narrow set of data is exchanged and presented to the issuer. Mag Stripe Mode is not used for the solutions described in this document.
One-Time Password	A digital credential that is produced by one entity and can be validated by another (e.g. generated by the card and validated by the issuer). Dynamic data ensures that each time a password is produced it will be unique.
Online-Only	A terminal configuration that requires all transactions to be authorized online, i.e. transactions cannot be completed offline. An online-only configuration might be used with deferred authorizations.
Open-loop	Payment solution where cards can be used in a wide range of terminals. Financial institution-issued payment cards are normally open-loop.
Penalty Fare	A fee for traveling without proper credentials or failing to validate credentials at the start of a trip.
Point of Entry	The or entrance to the transit system where credentials are typically validated.
Prepaid	Payment solutions in which the user pre-funds an account.
Private Label	Cards issued in a closed-loop solution.
Reader	The part of the terminal that controls communication and message flow with a contactless card.
Real-time Authorization	An authorization performed immediately upon card/reader interaction (as opposed to deferred authorization).
Retail Like Acceptance	Acceptance models which are similar to payment for goods in a shop. Typically, the final amount is known at the time of payment. Authorizations may be real-time or deferred.
Revenue Inspection	Checking credentials to travel.
Secure Element	A piece of memory within a contactless device that enables secret data to be stored without the risk of being altered by an unauthorized entity.
Single Message	A payment system where approval of the funds and collection of the funds are performed in the same messages. Single message systems require the transaction amount to be known at the time of the message, or the message will require a later correction.
Systems Integrator	An entity that brings together many features of different systems to provide an integrated transit payment solution.
Tap	Bringing a contactless card into proximity with a reader to enable a transaction.
Tap In	A tap at the start of a trip.
Tap Out	A tap at the end of a trip.
Tokenization	An alias or proxy of the account identifier provisioned to a contactless device for use in payment transactions.
Wearables	Contactless devices which may be worn, such as smart watches.

Acronyms

Term	Definition
AAC	Application Authentication Cryptogram
AC	Application Cryptogram
AIP	Application Interchange Profile
ARPC	Application Response Cryptogram
ARQC	Application Request Cryptogram
ATC	Application Transaction Counter
AVS	Address Verification Service
BIN	Bank Identification Number
BRAM	Business Risk Assessment and Mitigation
BVT	Brand Value Transaction
CAM	Card Authentication Method
CDA	Combined Data Authentication
CDCVM	Cardholder Device Cardholder Verification Method
CNP	Card Not Present
CTATC	Contactless Transit Aggregated Transaction Clearing
CVC2	Card Verification Code 2
CVM	Cardholder Verification Method
DE	Data Element
DRC	Debt Recovery Clearing
DSRP	Digitally Secure Remote Payments
ECP	Excessive Chargeback Program
EMC	Electro Magnetic Capability
ESD	Electro Static Discharge
ETM	Electronic Ticketing Machine
EMV	Europe, Mastercard, Visa
FPAN	Funding Primary Account Number
GMAP	Global Merchant Audit Program
HCE	Host Cloud Emulation
IAC	Issuer Action Code
IEC	International Electrotechnical Commission
ISO	International Standards Organization
LCD	Liquid Crystal Display
LDA	Local Data Authentication
LED	Light Emitting Diode
M-TIP	Mastercard Terminal Integration Process
MATCH	Member Alert to Control High-Risk Merchants
MBPP	Mastercard Business Partner Program
MCBP	Mastercard Cloud Based Payments
MCC	Merchant Category Code
MO/TO	Mail Order / Telephone Order
MPOS	Mobile Point of Sale (Terminal)
NFC	Near Field Communication
NIV	Network Interface Validation
PAN	Primary Account Number
PAR	Payment Account Reference
PAYG	Pay-As-You-Go (also known as Aggregation)

Term	Definition
PCI	Payment Card Industry
PCI - DSS	Payment Card Industry – Date Security Standard
PCI - PTS	Payment Card Industry – PIN Transaction Security
PIN	Personal Identification Number
POS	Point of Sale (Terminal)
QSA	Qualified Security Assessor
RI	Requirement, Issuer
SAFE	System to Avoid Fraud Effectively
SE	Secure Element
STAN	System Trace Audit Number
STIP	Stand-In Processing
TAC	Terminal Action Code
TC	Transaction Certificate
TQM	Terminal Quality Management
TVR	Terminal Verification Results
TVM	Ticket Vending Machine