

# Mastercard Gateway Card Present Implementation Guide

4<sup>th</sup> February 2025



crdprsnt\_en-us

# Contents

Summary of changes, 4 <sup>th</sup> Feb 2025 .....	4
Chapter 1: Introduction .....	5
About this guide .....	6
Intended audience .....	6
Prerequisites .....	6
Where to get help .....	6
Chapter 2: Product overview .....	7
Chapter 3: Implementation .....	8
Implementation plan .....	9
Mastercard Gateway integration .....	11
Chapter 4: Integration testing .....	21
How to execute integration testing .....	22
Chapter 5: Scheme certifications .....	28
Mastercard Terminal Integration Process (M-TIP) certification .....	29
Visa Acquirer Device Validation Toolkit (ADVT) or Contactless Device Evaluation Toolkit (CDET) certification .....	29
American Express ExpressPay Certification .....	30
Mastercard Sonic branding .....	30
Chapter 6: Clearing .....	31
Overview .....	32
Tap on Phone .....	33
Transit .....	33
Chapter 7: Frequently asked questions .....	34
General card present questions .....	35
Mobile Point-of-Sale Solutions (MPOS) questions .....	35

Appendix A: Common terms..... 37

Notices ..... 38

## Summary of changes, 4<sup>th</sup> February 2025

This is a summary of changes that have occurred since the previous publication of the manual.

<b>Description of Change</b>	<b>Where to Look</b>
Revised document structure	Throughout the document

# Chapter 1 Introduction

---

About this guide .....	6
Intended audience .....	6
Prerequisites .....	6
Where to get help.....	6

## About this guide

This guide provides the necessary steps to integrate card present solutions to the Mastercard Gateway, test, and certify your solution in the Member Test Facility (MTF) test environment and process production transactions.

## Intended audience

This guide is for the following audience interested in deploying instore or card present solutions through the Mastercard Gateway:

- Acquirers, payment facilitators and solution providers
- Direct merchants

## Prerequisites

Before a project starts, customers must ensure the following:

- A contract is signed with Mastercard Gateway covering card present.
- Enrolment form is completed and signed.
- Acceptance Pilot agreement is required when Mobile Point of Sale (MPOS), that is Software Point of Sale (SoftPOS) with Personal Identification Number (PIN), is in scope.

## Where to get help

For further support contact your Mastercard Gateway account representative or the Mastercard Customer Support team through [gateway\\_support@mastercard.com](mailto:gateway_support@mastercard.com).

## Chapter 2 Product overview

Mastercard Gateway global support for card present provides customers with the ability to deploy support for a range of in person payment deployments such as generic Point of Sale (POS), Tap on Phone and Tap with PIN through a single platform. Combined with overall support for ecommerce, fraud screening, alternative payment methods and tokenization, customers have the flexibility to join different payment channels to form omni-channel payment experiences such as click and collect, buy online and return in store amongst others.

## Chapter 3 Implementation

---

Implementation plan.....	9
Mastercard Gateway integration .....	11

## Implementation plan

If PIN support is required, the customers and technology vendors must follow five steps, as described in the following table and throughout this document to implement a Mastercard Gateway Card Present solution.

The following table describes the steps required for implementation and the teams responsible.

Action	Description	Responsible team
Project Kickoff	<p>Before a project starts, customers must ensure the following occur:-</p> <ul style="list-style-type: none"> <li>• A contract is signed with Mastercard Gateway covering card present.</li> <li>• Enrolment form is completed and signed.</li> <li>• Acceptance Pilot agreement is required when MPOS, that is SoftPOS with PIN, is in scope.</li> <li>• Pilot merchant is nominated for testing in production prior to mass rollout.</li> <li>• Customers and their chosen technology vendor must complete the Mastercard Gateway integration.</li> <li>• Customer or their processor have completed card present changes for DCF 4.3.6 or later.</li> <li>• The customer or vendor or both has the necessary scheme or Payment Card Industry (PCI) certification in place.</li> <li>• Mastercard Terminal Integration Process (MTIP) certification tools and test data have been obtained from a certification lab.</li> <li>• Project request form is raised through Technical Account Manager.</li> </ul>	Customer and Mastercard Gateway Technical Account Manager

Action	Description	Responsible team
Integrate and Test	<ul style="list-style-type: none"> <li>A new card present Merchant Services Organizations (MSO) will be created, mirroring their existing MSO.</li> <li>Once MSO is ready, customers should conduct some basic tests through MTF prior to moving on to certify their solution. For more information, see <a href="#">Integration testing</a>.</li> </ul>	Customer
Exchange PIN Keys, if required	<ul style="list-style-type: none"> <li>As part of the project implementation, three Zone Master Key (ZMK) clear components will be couriered to nominated key custodians. Once the custodians confirm receipt and correctness of the combined KCV, an encrypted Base Derivation Key (BDK) cryptogram will be couriered.</li> </ul> <p><b>NOTE: Separate keys are necessary for test and production and for different Point of Sale (POS) or Tap on Phone platforms.</b></p>	Mastercard Gateway
Certify Solution	<ul style="list-style-type: none"> <li>After conducting your own internal tests, you are now ready to complete scheme certification. For more information, see <a href="#">Scheme certifications</a>.</li> <li>In coordination with your project manager, you should now complete Level 3 certifications for Mastercard Terminal Integration Program (M-TIP) and Visa Contactless Device Evaluation Toolkit (CDET).</li> <li>Mastercard branding approval must be obtained, as mentioned in <a href="#">Mastercard Sonic branding</a>.</li> </ul>	Customer

Action	Description	Responsible team
Go Live	<ul style="list-style-type: none"> <li>Once successfully certified, your project manager will arrange to move your implementation setup over to Production.</li> <li>Post Production validation is mandatory and project support will remain available for 30 days after go live.</li> </ul>	Mastercard Gateway Project Manager

## Mastercard Gateway integration

### Overview

Mastercard Gateway integration for card present is in two distinct parts:

- Application Programming Interface (API) integration – Required for transaction processing and authorization. This will be performed by specialist solution providers, such as Tap on Phone or traditional PoS providers, wishing to use the Mastercard Gateway to process contactless transactions.
- DCF clearing – For acquirers and payment facilitators who provide clearing and settlement services, using the DCF.

### API version

Mastercard Gateway Card Present transactions are supported through the Direct API interface using API version 77 or later.

Existing integrations using earlier API versions and performing PIN verification need to update their integrations to use API version 77 and Single Tap with PIN before the end of 2024 as per Mastercard announcement AN6563.

### Authentication to the Mastercard Gateway

Authentication to the Mastercard Gateway can be developed through either passwords or SSL certificate. The acquirer must determine the appropriate method to be used for the implementation. For more information, see: [Secure Your Integration with Passwords or Certificates](#).

### Supported operations

Card present processing is supported through the following transaction operations:

- AUTHORIZE or CAPTURE
- PAY

- REFUND
- VOID
- VERIFY

**NOTE: Pay operation is not suitable for Transit integrations.**

Authorize, Pay and Verify are the main transaction operations that must contain the Europay, Mastercard, VISA (EMV) data within the API request. EMV data is not required as part of Capture, Void and Refund requests. For more information about EMV transactions, see [Process an EMV Transaction](#).

The following section provides a summary of the information required for integration, detailing the transactions operations supported, required API fields and corresponding EMV tags necessary to process card present transactions.

For Transit integrations, see the Transit Implementation Guide.

### Single tap with PIN

This section is for terminals, supporting Online PIN cardholder verification.

Terminals must send "posTerminal.singleTapIndicator": "true" to flag they are capable of processing single tap transactions. If the Issuer response indicates additional cardholder verification is required, the Mastercard Gateway response will include: "gatewayCode": "DECLINED\_PIN\_REQUIRED"

The terminal must then send a second request for the same transaction, this time with the PIN data:

- `sourceOfFunds.provided.emv.card.pin.keySerialNumber`
- `sourceOfFunds.provided.emv.card.pin.payload`
- `targetTransactionId` using the same ID from the first request.

### Web Services Application Programming Interface (WS API) fields

The following fields are required to process Authorize and Pay requests:

WS-API field	Expected input
order.amount	The total amount for the order.
order.currency	ISO 4217, alpha code. For example, USD, GBP
transaction.source	CARD_PRESENT
transaction.transit.knownFare.type Transit:	FARE_REAL_TIME_AUTHORIZATION
posTerminal.cardPresenceCapability	CARD_PRESENT
posTerminal.attended	ATTENDED

<b>WS-API field</b>	<b>Expected input</b>
posTerminal.cardholderActivated	MPOS_ACCEPTANCE_DEVICE
Tap on Phone:	NOT_CARDHOLDER
Standard POS:	ACTIVATED
posTerminal.mobile.cardInput.Device (Mastercard only)	BUILT_IN
Tap on Phone: (Not required for Visa)	
posTerminal.location	MERCHANT_TERMINAL_ON_PREMISES
posTerminal.lane	Use a unique Terminal ID for the device. Do not use a fixed Terminal ID value across the estate.
posTerminal.inputCapability	CONTACTLESS_CHIP
posTerminal.pinEntry capability	SOFTWARE_ONLINE_PIN_ONLY
Tap on Phone (MPoC / SPoC) - Mastercard:	PIN_SUPPORTED
Tap on Phone (MPoC /SPoC) - Visa:	PIN_NOT_SUPPORTED
Tap on Phone (CPoC): Standard POS:	PIN_SUPPORTED
posTerminal.pinLengthCapability	Numeric 4-12 Required for terminals with PIN Entry capability.
pos.Terminal.singleTapIndicator	TRUE Required for terminals supporting Single Tap with PIN.
transaction.targetTransactionID	Required for terminals supporting Single Tap with PIN when submitting the second transaction following a 'DECLINED_WITH_PIN_REQUIRED' response.
posTerminal.panEntryModeTap on Phone: Standard PoS:	CONTACTLESS or CHIP or SWIPE-WITH-SIGNATURE or SWIPE or KEYED
posTerminal.onlineReasonCode	CHIP_APPLICATION_DATA_FILE or CHIP_COMMON_DATA_FILE_ERROR or FORCED_BY_CHIP or FORCED_BY_ISSUER or FORCED_BY_MERCHANT or FORCED_BY_TERMINAL or MERCHANT_SUSPICIOUS or OVER_FLOOR_LIMIT or RANDOM_SELECTION_BY_TERMINAL orUNABLE_TO_PROCESS_CHIP
sourceOfFunds.type	CARD
sourceOfFunds.provided.emvRequest	EMV Tags as per the table on the following page.
SourceOfFunds.provided.track2	Track2

WS-API field	Expected input
sourceOfFunds.provided.card.expiry.month	Expiry Month, length 2, Digits 1-12
sourceOfFunds.provided.card.expiry.year	Expiry Year, length 2, Digits 00-99
sourceOfFunds.provided.card.sequenceNumber	Application PAN Sequence Number (APSN)
sourceOfFunds.provided.emv.card.pin.encryptedPayload	"VALID" or "INVALID" (Optional field, default is "VALID") Only required for terminals with PIN Entry capability
sourceOfFunds.provided.emv.card.pin.keySerialNumber	The DUKPT key serial number supplied by the terminal Only required for terminals with PIN Entry capability.
sourceOfFunds.provided.emv.card.pin.payload	The DUKPT encrypted payload supplied by the terminal Only required for terminals with PIN Entry capability.
partnerSolutionId – max 40 characters	A field to uniquely identify the solution and integrator separated by underscore:
Tap on Phone	MPOS_<integrator name>
Cloud Commerce	MPOSCC_<integrator name>
POS – retail	POSRETAIL<integrator name>
POS – food & beverage	POSF&B<integrator name>
POS - hotel	POSHOTEL<integrator name>
Mobility – transit aggregation	TRANSITAGG_<integrator name>
Mobility – transit known fare	TRANSITKFT_<integrator name>
Mobility – in car commerce	INCARCOM_<integrator name>
Mobility – parking	PARKING_<integrator name>
Mobility – electric vehicle charging	EVCHARGE_<integrator name>
Mobility – fuel	FUEL_<integrator name>
Mobility – tolls	TOLLS_<integrator name>
Mobility – micro mobility	MICROMOB_<integrator name>
Onboard – airlines	ONBOARDAIR_<integrator name>
Onboard - cruise	ONBOARDCRS_<integrator name>

### EMV tags

The following EMV tags are required to be included in sourceofFunds.provided.card.emvRequest to implement card present in the Mastercard Gateway. The complete list of supported EMV tags is provided in the online WS API documentation.

<b>EMV Tag</b>	<b>Description</b>	<b>Format</b>	<b>Length</b>	<b>Mandatory</b>
5F2A	Transaction Currency Code	n3	2	Yes
5F34	Application PAN Sequence Number	n2	1	No
82	Application Interchange Profile (AIP)	b	2	Yes
84	Dedicated File Name	b	5-16	Yes
95	Terminal Verification Results (TVR)	b	5	Yes
9A	Transaction Date	n6	3	Yes
9B	Transaction Status Info. (TSI)	b	2	No
9C	Transaction Type	n2	1	Yes
9F02	Amount Authorized	n12	6	Yes
9F03	Amount Other	n12	6	If >0.00
9F06	Application Identifier	b	5-16	No
9F07	Application Usage Control	b	2	No
9F09	Terminal Application Version Number	b	2	No
9F10	Issuer Application Data (IAD)	b	var up to 32	Yes
9F1A	Terminal Country Code	n3	2	Yes
9F1E	Interface Device (IFD) Serial Num			No
9F26	Application Cryptogram (AC)	b	8	Yes
9F27	Cryptogram Information Data (CID)	b	1	Yes

EMV Tag	Description	Format	Length	Mandatory
9F33	Terminal Capabilities	b	1	U.S. only
9F34	Cardholder Verification Results (CVMR)	b	3	Yes
9F35	Terminal Type	n2	1	No
9F36	Application Transaction Counter (ATC)	b	2	Yes
9F37	Unpredictable Number	b	4	Yes
9F41	Transaction Sequence counter	n4-8	2-4	No
9F53	TCC	an	1	No
9F6E	Device Type or Form Factor Visa only requirement for 9F6E Form Factor byte 4 bit 8: <ul style="list-style-type: none"> <li>• 0 =The transaction did not originate from a tap-to-phone acceptance device.</li> <li>• 1 =The transaction originated from a tap- to-phone acceptance device.</li> </ul>	B	2-26	Yes

### Format definitions

The following table provides definitions for the entries in the Format column on the previous page.

Format	Definition
b	<p>These data elements consist of either unsigned binary numbers or bit combinations that are defined in the EMV specification.</p> <p>Binary example: The Application Transaction Counter (ATC) is defined as "b" with a length of 2 bytes. An ATC value of 19 is stored as Hex '00 13'</p> <p>When passing binary data in the sourceOfFunds.provided.card.emvRequest field they must be represented as a HEX-encoded string.</p>
n	<p>Numeric elements consist of two numeric digits, having values in the range Hex 0 - 9, per byte. These digits are right justified and padded with leading hexadecimal zeroes.</p> <p>Other specifications sometimes refer to this data as Binary Code Decimal (BCD) or unsigned packed.</p>
an	<p>Alphanumeric data elements contain a single character per byte. The permitted characters are alphabetic, a to z lower case and A to Z upper case, and numeric ranging from 0 to 9.</p>

### Sample API request and response message

#### API Request for Tap with PIN – Pay Operation

```
{
  "apiOperation": "PAY",
  "order": {
    "amount": "123",
    "currency": "AUD"
  },
  "posTerminal": {
    "address": {
      "country": "AUS",
      "postcodeZip": "4000"
    },
    "attended": "ATTENDED",
    "cardPresenceCapability": "CARD_PRESENT",
    "cardholderActivated": "MPOS_ACCEPTANCE_DEVICE",
    "inputCapability": "CONTACTLESS_CHIP",
    "lane": "teapost",
    "location": "MERCHANT_TERMINAL_ON_PREMISES",
    "panEntryMode": "CONTACTLESS",
    "pinEntryCapability": "PIN_SUPPORTED",
    "pinLengthCapability": "6",
    "singleTapIndicator": "true",
    "mobile": {
      "cardInputDevice": "BUILT_IN"
    }
  }
},
```

```

"sourceOfFunds": {
  "provided": {
    "card": {
      "emvRequest": {
        "5F2A": "036",
        "5F34": "00",
        "82": "5C00",
        "84": "A0000000031010034761739000000000",
        "95": "0000262144",
        "9A": "210209",
        "9C": "00",
        "9F02": "000000003100",
        "9F03": "000000000000",
        "9F10": "06020103A02000",
        "9F1A": "036",
        "9F1E": "2BC7A55C",
        "9F26": "51B579DE8D55E180",
        "9F27": "80",
        "9F33": "60F0C8",
        "9F34": "000000",
        "9F36": "0201",
        "9F37": "6388675D",
        "9F6E": "00560000313400"
      },
      "expiry": {
        "month": "12",
        "year": "24"
      },
      "pin": {},
      "track2": "512345xxxxxx2346=17051019681143384001"
    },
    "type": "CARD"
  },
  "transaction": {
    "source": "CARD_PRESENT"
  }
}

```

#### API Response for Tap with PIN – Pay Operation

```

{
  "authorizationResponse": {
    "commercialCard": "123",
    "commercialCardIndicator": "1",
    "date": "0201",
    "financialNetworkCode": "MCC",
    "posData": "0000000009300",
    "posEntryMode": "071",
    "processingCode": "003000",
    "responseCode": "00",
    "stan": "79533",
    "time": "102734",
    "transactionIdentifier": "677980519",
    "transactionIntegrityClass": "A1"
  },
  "gatewayEntryPoint": "WEB_SERVICES_API",
  "merchant": "CYG_S2I_MER1",
  "order": {
    "amount": 123,
    "authenticationStatus": "AUTHENTICATION_NOT_IN_EFFECT",
    "chargeback": {
      "amount": 0,

```

```

    "currency": "AUD"
  },
  "creationTime": "2024-02-01T10:27:33.954Z",
  "currency": "AUD",
  "id": "532612595",
  "lastUpdatedTime": "2024-02-01T10:27:35.736Z",
  "merchantAmount": 123,
  "merchantCategoryCode": "1234",
  "merchantCurrency": "AUD",
  "status": "CAPTURED",
  "totalAuthorizedAmount": 123,
  "totalCapturedAmount": 123,
  "totalDisbursedAmount": 0,
  "totalRefundedAmount": 0
},
"posTerminal": {
  "address": {
    "country": "AUS",
    "postcodeZip": "4000"
  },
  "attended": "ATTENDED",
  "cardPresenceCapability": "CARD_PRESENT",
  "cardholderActivated": "MPOS_ACCEPTANCE_DEVICE",
  "inputCapability": "CONTACTLESS_CHIP",
  "lane": "teapost",
  "location": "MERCHANT_TERMINAL_ON_PREMISES",
  "mobile": {
    "cardInputDevice": "BUILT_IN"
  },
  "panEntryMode": "CONTACTLESS",
  "pinEntryCapability": "PIN_SUPPORTED",
  "pinLengthCapability": 6,
  "singleTapIndicator": true
},
"response": {
  "acquirerCode": "00",
  "acquirerMessage": "Approved",
  "gatewayCode": "APPROVED",
  "gatewayRecommendation": "NO_ACTION"
},
"result": "SUCCESS",
"sourceOfFunds": {
  "provided": {
    "card": {
      "brand": "MASTERCARD",
      "emvRequest": {
        "82": "5C00",
        "84": "A0000000031010034761739000000000",
        "95": "0000262144",
        "5F2A": "036",
        "5F34": "00",
        "9A": "210209",
        "9C": "00",
        "9F02": "000000003100",
        "9F03": "000000000000",
        "9F10": "06020103A02000",
        "9F1A": "036",
        "9F1E": "2BC7A55C",
        "9F26": "51B579DE8D55E180",
        "9F27": "80",
        "9F33": "60F0C8",
        "9F34": "000000",
        "9F36": "0201",
        "9F37": "6388675D",

```

```
    "9F6E": "00560000313400"
  },
  "emvResponse": {
    "72": "9F180408041215860E04DA9F5809030691D72E6F027DC6",
    "91": "B7D5309D4B3E6CDB3030"
  },
  "expiry": {
    "month": "12",
    "year": "24"
  },
  "fundingMethod": "DEBIT",
  "number": "512345xxxxxx2346",
  "scheme": "MASTERCARD",
  "storedOnFile": "NOT_STORED",
  "trackDataProvided": true
}
},
"type": "CARD"
},
"timeOfLastUpdate": "2024-02-01T10:27:35.736Z",
"timeOfRecord": "2024-02-01T10:27:34.018Z",
"transaction": {
  "acquirer": {
    "batch": 20240201,
    "date": "0201",
    "id": "CYG_TESTACQ_S2I",
    "merchantId": "9808",
    "settlementDate": "2024-02-01",
    "timeZone": "+1000",
    "transactionId": "677980519"
  },
  "amount": 123,
  "authenticationStatus": "AUTHENTICATION_NOT_IN_EFFECT",
  "authorizationCode": "112233",
  "currency": "AUD",
  "id": "565396098",
  "receipt": "403210079533",
  "source": "CARD_PRESENT",
  "stan": "79533",
  "terminal": "0001",
  "type": "PAYMENT"
},
"version": "79"
}
```

## Chapter 4 Integration testing

---

How to execute integration testing..... 22

The integration testing guidelines documented in this section provide the necessary information and resources to test the Mastercard Gateway Card Present solution.

## How to execute integration testing

Customers are advised to run some internal card present tests utilizing the Mastercard Gateway prior to scheme certification. Complete the below tests and ensure your solution has achieved the expected results as indicated within Expected Result.

The following tests need to be performed using values below the Cardholder Verification Method (CVM) limit for the country and repeated using values above the CVM limit, so PIN entry is requested.

## Test scenarios

<b>Transaction</b>	<b>Functionality</b>	<b>Pre-condition</b>	<b>Sub-function** amount and currency can be changed as per country requirements</b>	<b>Scheme</b>	<b>Expected Result</b>
Authorization	Auth or Capture, only if scoped	Test Card is available	Perform an Authorize transaction for \$20.50.	Mastercard	Authorize request approved for \$20.50
		Auth is successful	Request Capture	Mastercard	Capture request approved
		Test Card is available	Perform an Authorize transaction for \$20.50.	Visa	Authorize request approved for \$20.50
		Auth is successful	Request Capture	Visa	Capture request approved
		Test Card with PIN capability is available	Perform an Authorize transaction over country CVM limit; therefore requiring PIN.	Mastercard	Authorize request approved for specified amount, determined by customer.
		Auth with PIN is successful.	Request Capture	Mastercard	Capture request approved
		Test Card with PIN capability is available.	Perform an Authorize transaction over country CVM limit; therefore requiring PIN.	Visa	Authorize request approved for specified amount, determined by customer.
		Auth with PIN is successful.	Request Capture	Visa	Capture request approved

Transaction	Functionality	Pre-condition	Sub-function-- amount and currency can be changed as per country requirements	Scheme	Expected Result
	Pay or Purchase, only if scoped	Test Card is available.	Perform a Purchase or Pay transaction for \$15.25.	Mastercard	Purchase or Pay request approved
		Test Card is available.	Perform a Purchase or Pay transaction for \$15.25.	Visa	Purchase or Pay request approved
		Test Card with PIN capability is available.	Perform a Purchase or Pay transaction over country CVM limit; therefore requiring PIN.	Mastercard	Purchase or Pay request approved
		Test Card with PIN capability is available.	Perform a Purchase or Pay transaction over country CVM limit; therefore requiring PIN	Visa	Purchase or Pay request approved
Void		Test Card is available.	Perform a Void request for \$15.25.	Mastercard	Void is successful
		Test Card is available.	Perform a Void request for \$15.25.	Visa	Void is successful
Refund		Test Card is available.	Perform an Auth or Capture or Pay for \$25.75.	Mastercard	Request is approved
		Auth or Capture or Pay is Successful.	Refund previous transaction	Mastercard	Refund request approved
		Test Card is available.	Perform an Auth or Capture or Pay for \$25.75.	Visa	Request is approved

---

<b>Transaction</b>	<b>Functionality</b>	<b>Pre-condition</b>	<b>Sub-function.. amount and currency can be changed as per country requirements</b>	<b>Scheme</b>	<b>Expected Result</b>
		Auth or Capture or Pay is successful.	Refund previous transaction	Visa	Refund request approved

---

<b>Transaction</b>	<b>Functionality</b>	<b>Pre-condition</b>	<b>Sub-function.. amount and currency can be changed as per country requirements</b>	<b>Scheme</b>	<b>Expected Result</b>
Clearing	DCF Card Present records validation	Authorizations are successful	DCF validation	Mastercard	Record Types 6220, 6221,6225, 6271 and 6222 are available in DCF reflecting correct details such as amount, card - IPM is successful with Card Present data, for example:· <ul style="list-style-type: none"> <li>• PIN Capture Capability</li> <li>• Cardholder Authenticati on Method</li> <li>• Cardholder Authenticati on Entity</li> </ul>

Transaction	Functionality	Pre-condition	Sub-function.. amount and currency can be changed as per country requirements	Scheme	Expected Result
		Authorizations are successful	DCF validation	Visa	Record Types 6220, 6221,6225, 6271 and 6223 are available in DCF reflecting correct details such as amount, card - BASE    is successful with Card Present data:· <ul style="list-style-type: none"> <li>• PIN Capture Capability</li> <li>• Cardholder Authenticati on Method·</li> <li>• Cardholder Authenticati on Entity</li> </ul>

## Chapter 5 Scheme certifications

---

Mastercard Terminal Integration Process (M-TIP) certification .....	29
Visa Acquirer Device Validation Toolkit (ADVT) or Contactless Device Evaluation Toolkit (CDET) certification.....	29
American Express ExpressPay Certification.....	30
Mastercard Sonic branding.....	30

Acquirers must complete Level 3 certifications with the supported card schemes as part of the implementation process.

## Mastercard Terminal Integration Process (M-TIP) certification

M-TIP certification requires the following typical certification steps:

1. The acquirer orders an M-TIP service from a Mastercard accredited M-TIP Service Provider of their choice and procures a qualified M-TIP test tool.
2. The acquirer downloads the latest Test Selection Engine (TSE) software (and TSE configuration file) from Mastercard Connect and uses it to enter the details of their solution to generate the applicable test plan.
3. The execution of test cases is coordinated with the Customer Implementation Services Implementation Manager (CIS IM). The acquirer executes the test plan, using their M-TIP test tool, and records the related test results. The Mastercard Authorization Simulator transaction logs are provided by the CIS IM for including with TSE or their M-TIP test tool.
4. The acquirer sends the test results to their M-TIP Service Provider for validation.
5. An M-TIP Letter of Approval (LoA) is delivered upon successful execution of M-TIP.

M-TIP-related online sources such as M-TIP Process Guide, list of M-TIP Service Providers, list of M-TIP test tools, TSE, and so on are available to customers through the Chip and Contactless Information Center on Mastercard Connect <https://www.mastercardconnect.com/business/public/en-us/public/signin.htm>

## Visa Acquirer Device Validation Toolkit (ADVT) or Contactless Device Evaluation Toolkit (CDET) certification

Visa CDET certification requires the following typical certification steps:

1. The acquirer is required to execute CDET and ADVT test cases and upload the results through the Chip Compliance Reporting Tool (CCRT).
2. Test execution will need to be coordinated with the CIS IM. Configuration changes will be applied to route the transactions to the Visa test system.
3. No host simulator logs are provided for Visa certification. Acquirers are expected to record the Retrieval Reference Number (RRN), provided in the receipt tag in the API response, against each test case while uploading the test cases to Visa.

Acquirers are required to liaise with Visa for any scheme documentation related to card present certifications.

## American Express ExpressPay Certification

American Express ExpressPay requires the following typical certification steps:

1. The acquirer is required to raise an ExpressPay Certification project with American Express.
2. Test execution will need to be coordinated with the CIS IM. Configuration changes will be applied to route the transactions to the AMEX test system.
3. Acquirers are required to liaise with American Express for any scheme documentation related to card present certifications

## Mastercard Sonic branding

Partners should present Mastercard Gateway Sonic Branding in environments where cardholders present their payment credentials at an acceptance device or application.

This includes:

- Stand-alone and integrated POS terminals.
- Automated retail or vending.
- Tap on Phone and mPOS.

The sonic brand triggers immediately upon a Mastercard transaction approval or completion. Both of the following technical implementation asset details are available on the [Mastercard Developer Zone](#):

- Android and iOS SDKs and static assets.
- Sonic Branding guidelines.

Before going live, all partners must submit a [Sonic Approval](#) form with Sonic asset information, a demo, and receive Mastercard approval.

## Chapter 6 Clearing

---

Overview .....	32
Tap on Phone .....	33
Transit.....	33

Clearing is the process of settling transactions and the responsibility of the acquirer.

## Overview

The Mastercard Gateway provides a Draft Capture File (DCF) containing all the authorised transactions within a trading period.

The acquirer's processing platform needs to be able to process the DCF file and convert it to the clearing format required for each scheme.

Card present transactions include additional data, such as terminal and EMV data, which must be supported.

To receive the required card present settlement information, customers must implement DCF specification v4.3.8 or later and consider the following records:

Purpose	Record type
All schemes:	Record type:
Mandatory 1	6220
Mandatory 2	6221
EMV Data record 1	6225
EMV Data record 2	6271
Mastercard only	6222
Visa only	6223

During DCF implementation, data integrity should be followed to ensure data meets scheme requirements.

For example, cardholder verification:

Cardholder Verification Method	6225 Rec, Field 17 EMV Tag 9F34 CVM Results Byte 1	IPM DE 22 SF8 Cardholder Authentication Method	IPM DE 22 SF9 Cardholder Authentication Entity
No CVM	1F or 3F	0	0
Online PIN	02 or 42	1	3
Offline PIN:	Value:	1	1
• Enciphered	• 04 or 44		
• Plaintext	• 01 or 41		
Signature	1E or 5E	5	4

## Tap on Phone

Tap on Phone solutions only must also include:

Description	DCF Record, Field / Position	Mastercard IPM / Visa Base II
Mastercard mPOS Acceptance Device Type (DE48 SE21 SF1)	6221, Field 20, Pos. 178	PDS 0018 – SF 1: <ul style="list-style-type: none"> <li>0 – Dedicated mPOS</li> <li>1 – Off the Shelf</li> </ul>
Mastercard Cardholder-activated Terminal Level Ind=9 MPOS Acceptance Device (DE61 SF10)	6220, Field 33, Pos. 178	PDS 0023 <ul style="list-style-type: none"> <li>CT9 – MPOS Device</li> </ul>
Visa Tap-to-phone-indicator Tag 9F6E Form Factor indicator	6271, Field 5, Pos. 45-108byte 4, bit 8	TC 33.A CP 02 TCR 0 EMV DATA Position 150

## Transit

Transit solutions only must also include:

Description	DCF Record, Field / Position	Mastercard IPM / Visa Base II
Mastercard Transit Transaction Type Indicator (DE48 SE64 SF1)	6222, Field 11, Pos. 64-65	PDS 0210 – SF 1: <ul style="list-style-type: none"> <li>02 - Real-time Authorized</li> <li>03 - Post-Authorized Aggregated</li> <li>07 - Debt Recovery</li> </ul>
Mastercard Transit Transportation Mode Indicator (DE48 SE64 SF2)	6222, Field 12, Pos. 66-67	PDS 0210 – SF 2
Visa Date of First Tap in the travel period	6223, Field 16, Pos. 85-90	TCR0 Pos. 58-61

## Chapter 7 Frequently asked questions

---

General card present questions .....	35
Mobile Point-of-Sale Solutions (MPOS) questions .....	35

## General card present questions

### **Which card schemes are supported through the Mastercard Gateway?**

Mastercard Gateway supports Mastercard, Visa, and American Express card present.

### **Are solutions required to go through Level 3 Certification?**

Yes, customers must obtain Mastercard M-TIP, Visa CDET and Amex ExpressPay approval before their card present solution can go live within Production.

### **Why are my scheme certification tests highlighting errors after following this guide?**

On most occasions tests fail due to missing EMV tags or incorrect value based on the terminal type the scheme was expecting. Customers are advised to review terminal capabilities and ensure EMV tags are correct. Consult with your CIS representative if further information is required.

## Mobile Point-of-Sale Solutions (MPOS) questions

### **What are Tap on Phone features?**

Tap on Phone runs through mobile application on many Near Field Communication (NFC) - enabled Android devices to support acceptance from contactless-enabled cards and devices such as smartphones, smart watches, and wristbands. After consumers complete their purchases with Tap on Phone, merchants can send a paperless receipt through SMS or email, or they can print the receipt using an external printer.

Acquirers can integrate Tap on Phone with additional business solutions such as invoicing, inventory management, and analytics reporting to provide incremental value to their merchant customers.

### **How is Tap on Phone different from other POS solutions on the market?**

Current solutions require additional hardware to accept digital payments. Tap on Phone enables merchants to accept contactless payments using the Android device they already own.

### **What are some of the use cases for Tap on Phone?**

- Offer alternative to purchasing dedicated POS hardware.
- Support payment on delivery, displacing cash.
- Provide an immediate and quality customer experience with in-aisle checkout.
- Empower on-the-go vendors.
- Facilitate entertainment, sporting and philanthropic events.

### **Why Tap on Phone?**

Tap on Phone is quick, simple, and secure. It is an ideal payment method for customers when they just need to pay and go. Merchants can transform any enabled mobile device into a payment terminal. Each Tap on Phone transaction is protected through the same technology as dipped card transactions but provides a faster and, therefore, more pleasant customer experience.

### **Are Tap on Phone payments secure?**

Tap on Phone payments use the same security technology offered as EMV chip cards that are deployed throughout the world.

## Appendix A Common terms

The following common terms can be useful for reference during the implementation of Card Present.

Term	Description
CIS	Customer Implementation Services Responsible for setting up customers on an ongoing basis.
CVM	Cardholder Verification Method A method to verify that the person using the card or digital wallet is the legitimate cardholder.  <b>NOTE: It is the responsibility of the customer and solution provider to set appropriate country CVM limits relating to specific countries the solution has been deployed.</b>
COTS	Commercial off-the-shelf devices, such as tablets and smartphones.
DCF	Draft Capture File A file containing transaction information required for settlement.
IM	Implementation Manager Assigned from the CIS Team.
L3 Certification	Level 3 Certification, refers to the certification of a terminal integration. See Mastercard MTIP or Visa CDET.
MTF	Member Test Facility A testing environment that enables customers to test transactions prior to processing live transactions through Production.
PCI MpoC	Payment Card Industry standard for Mobile Payments on COTS device.
PCI CpoC	Payment Card Industry standard for Contactless Payments on COTS device.
Production	Live transaction processing environment.

# Notices

Following are policies pertaining to proprietary rights, trademarks, translations, and details about the availability of additional information online.

## Proprietary Rights

The information contained in this document is proprietary and confidential to Mastercard International Incorporated, one or more of its affiliated entities (collectively "Mastercard"), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of Mastercard.

## Trademarks

Trademark notices and symbols used in this document reflect the registration status of Mastercard trademarks in the United States. Consult with the Global Customer Service 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.

EMV® is a registered trademark of EMVCo LLC in the United States and other countries. For more information, see <http://www.emvco.com>.

## Disclaimer

Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to this document 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) or achievement of any particular result.

## Translation

A translation of any Mastercard manual, bulletin, release, or other Mastercard document into a language other than English is intended solely as a convenience to Mastercard customers. Mastercard provides any translated document to its customers "AS IS" and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall Mastercard be liable for any damages resulting from reliance on any translated document. The English version of any Mastercard document will take precedence over any translated version in any legal proceeding.

**Information Available Online**

Mastercard provides details about the standards used for this document, including times expressed, language use, and contact information, on the Technical Resource Center (TRC). Go to the Rules collection of the References section for centralized information.