

Tap on Phone Implementation Guide

May 2024

Contents

1: Overview 3

1.1 What is Tap on Phone? 3

1.2 Who is this guide for? 3

1.3 What is this guide intended for? 3

2: Process 4

2.1 PCI timeline 4

2.2 Suggested market criteria 4

2.3 Solution options 4

2.4 Certification step details 5

3: FAQs 9

3.1 General 9

3.2 Certification and development 9

3.3 Merchant-focused 12

3.4 Pilots 12

4: Glossary 14

5: Resources 15

© 2024 Mastercard. Proprietary and Confidential.



1: Overview

1.1 What is Tap on Phone?

Tap on Phone (ToP) is a contactless acceptance solution that is low cost, low maintenance, and peripheral-free for merchants. Tap on Phone can allow eligible NFC-enabled mobile devices[1] to function as point-of-sale devices that accept contactless electronic payments (i.e., contactless cards, mobile wallets, wearables).

- Tap on Phone can be deployed on eligible devices with an embedded NFC antenna.
- Merchants can download a dedicated Tap on Phone app. After initializing the app and completing account set up, merchants can complete test transactions to confirm readiness for accepting contactless payments.
- At the time of purchase, the merchant will open the Tap on Phone app and enters the purchase amount. The customer will then tap their contactless card or device against the NFC antenna on the merchant's mobile device. Once the purchase is complete, the merchant can send an SMS or email receipt to the customer or print the receipt using an external printer.
- Tap on Phone transactions are protected using the same security and encryption technology offered with EMV® chip cards throughout the world, and they use the same switching process as traditional POS transactions.

See the Tap on Phone Merchant Guide in the Resources section of this document to learn more about Tap on Phone use cases, benefits and overall functionality.

1.2 Who is this guide for?

This guide is for any entity that develops, deploys or uses Tap on Phone solutions, including:

- Acquirers, payment facilitators, and solution providers.
- NFC-enabled mobile device manufacturers and OS developers that will host Tap on Phone apps.
- Merchants who use or are interested in using Tap on Phone solutions, including those who have a direct relationship with a Mastercard acquirer.
- Sub-merchants who use the services of a payment facilitator.
- Issuers and others in the payment industry interested in Tap on Phone.

1.3 What is this guide intended for?

This guide is intended to define the components of a Tap on Phone solution and provide guidance on how to enable and begin distributing a secure solution.

- Tap on Phone solutions are built around three solution elements: the merchant's existing NFC-enabled mobile device (COTS device[1]), a Tap on Phone payment application (PCI CPoC™ or MPoC™ application), and a back-end environment that engages in attestation, monitoring, and payment processing as part of the solution.
- The integrity of both the Tap on Phone payment application on the mobile device and on the host system are critically important to maintaining the security of transaction data and to helping prevent data compromise incidents.
- All Tap on Phone solutions must comply with PCI CPoC and MPoC standards and relevant EMVCo and Mastercard testing requirements. For Tap on Phone with PIN, the PCI standards have not yet been published. A Security Principles Review must still be undertaken to launch a Pilot.

1. Mobile device is referred to as commercial off-the-shelf (COTS) in PCI standards for Tap on Phone. Please refer to the glossary for COTS definition.

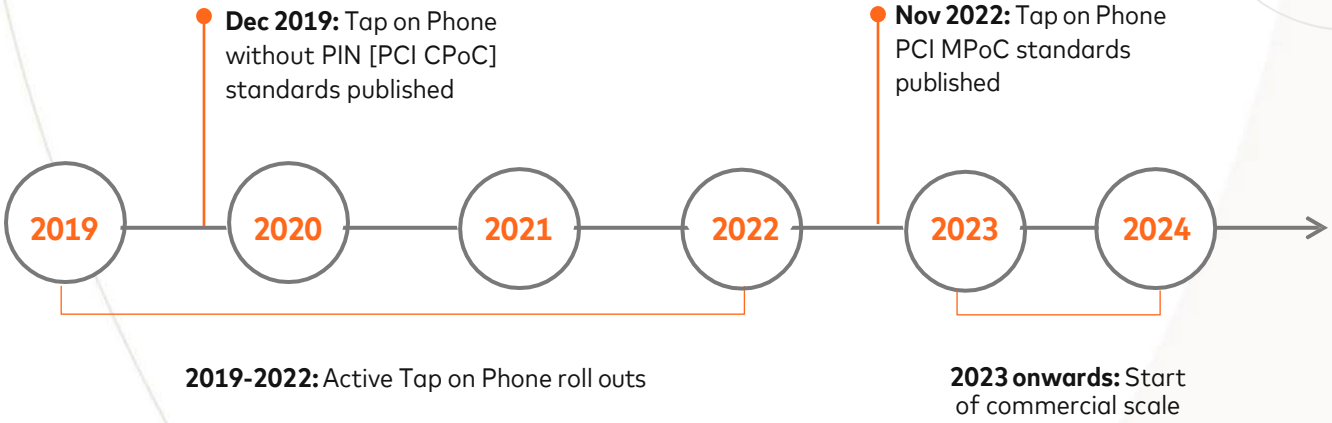
© 2024 Mastercard. Proprietary and Confidential.



2: Process

2.1 PCI timeline

Expected Tap on Phone PCI standards roadmap:



Timeline Considerations

- ✓ Mastercard Commercialization of PCI CPoC and MPoC:
  - Following the publication and after a preparation period, PCI recognized CPoC and MPoC laboratories will start evaluating solutions under the respective standards. Any solution that successfully meets these standards will be listed as an approved PCI CPoC or MPoC Solution by the PCI Council, listed on the PCI Council website and enabled for full commercialization. Mastercard will continue supporting providers and innovators around the world with guidance and best practices.
- ✓ For Tap on Phone with PIN pilot considerations, **click here.**
  - Tap on Phone with PIN Pilots are permitted dependent on developers MPoC plans and progression. Please contact mposprogram@mastercard.com for further details.

2.2 Suggested market criteria

When considering which markets to deploy Tap on Phone to, the following assessment criteria and rationale may be helpful:

High smartphone penetration	NFC-enabled mobile device is required as acceptance device for Tap on Phone transactions
High contactless card and device penetration	Contactless cards and devices are required to make Tap on Phone payments.

2.3 Solution options

Below are options for entities looking to develop or deploy a Tap on Phone solution:

1. **Tap on Phone without PIN (PCI CPoC):**
   i. PCI-Compliant Commercial Solution: Develop and certify proprietary solution against published PCI CPoC standard
   ii. Engage with Approved Vendor: Commercial agreement with vendor that offers an approved PCI CPoC solution

© 2024 Mastercard. Proprietary and Confidential.

2: Process

2. **Tap on Phone with PIN Pilots:**
    i. Develop Solution: Develop and approve solution against Mastercard Security Principles for online PIN support
    ii. Engage with Approved Vendor: Commercial agreement with vendor that offers a Mastercard Security approved solution
3. **Tap on Phone with PIN (MPoC):**
    i. PCI MPoC provides a modular, objective-based, security standard that supports various types of payment acceptance channels and consumer verification methods on COTS devices, including entry of both PIN and contactless cardholder data on the same COTS device
    ii. PCI-Compliant Commercial Solution: Develop and certify proprietary solution against published PCI MPoC standard
    iii. Engage with Approved Vendor: Commercial agreement with vendor that offers an approved PCI MPoC solution

	Solution Options			
	PCI-Compliant Tap on Phone Commercial Solutions *(PCI CPoC and MPoC)*		**Tap on Phone with PIN Pilots**	
	i. PCI Approved CPoC and MPoC Commercial Solutions	**ii. Engage with Approved Vendor**	**i. Pre-PCI non-Commercial Solution**	**ii. Engage with Approved Vendor**
Step 1: Contactless License	✓	N/A	✓	N/A
Step 2: L1 EMVCo	EMVCo is working on defining an evaluation process for MPOS. See Step 2 of the certification details for more information			
Step 3: L2 Mastercard	✓	*	✓	*
Step 4: Security Evaluation (PCI CPoC, PCI MPoC or Mastercard Security Principles)	✓	*	✓**	*
Step 5: Pilot Enrollment Form	N/A	N/A	✓	✓
Step 6: M-TIP	✓	✓	✓	✓

*Engage with your chosen approved vendor/Mastercard MPOS team to determine whether additional certification reviews apply.

**Pilots for Tap on Phone with PIN requires security evaluation against Tap +PIN security principles by Mastercard accredited labs.

© 2024 Mastercard. Proprietary and Confidential.

2.4 Certification step details

Step 1: Contactless Development License

Contactless Development License: A vendor or solution provider that is interested in undertaking a contactless project like Tap on Phone with Mastercard must first obtain a Contactless Development License (or have an existing license that covers the proposed activity). Vendors are required to enter into a license agreement with Mastercard before developing and selling contactless-enabled equipment. All cards, devices, and readers used for performing contactless transactions must be approved and licensed by Mastercard prior to their use. Please reach out to contactless@mastercard.com to start the process and receive the Company Onboarding form.

	**Solution Provider Submits:**	1. Company Onboarding form -> to be sent to contactless@mastercard.com 2. Contactless Development License agreement (once step 1 is complete)
	**Solution Provider Receives:**	Contactless Development License

Step 2: Level 1 Testing (EMVCo)

EMVCo is currently discussing the future criteria for Tap on Phone solutions and working on defining an evaluation process for MPOS.

Notes:

- All solutions must meet EMVCo contactless standards. Please reference the architecture and general requirements document on the EMVCo website.
- Contactless Level 1 testing is a requirement for NFC-enabled solutions. However, Tap on Phone solutions on COTS devices are currently exempt from this requirement.
- Enterprise Devices are not considered COTS devices by EMVCo and are required to go through Level 1 Testing.

© 2024 Mastercard. Proprietary and Confidential.

Step 3: Level 2 Testing (Mastercard accredited functional laboratories)

*Solution providers are advised that **Step 3** and **Step 4** below can and, when possible, should be done concurrently.*

Below is a breakdown of the Level 2 contactless kernel approval process:

1. Contact the Mastercard Approvals Chip Certification Acceptance Devices team by sending an email to chip_certification_ad@mastercard.com. The provider will receive a Tap on Phone Registration form called ICS (Implementation Conformity Statement) and related Level 2 functional approval documentations.
2. The provider will send back the Tap on Phone Registration form and the Mastercard Approvals team will assign a registration number and send a related test plan called TEPS (Terminal Evaluation Plan Summary).
3. Vendor sends TEPS to their chosen accredited lab for L2 testing. Once complete, the lab issues a test report to Mastercard and the vendor/solution provider.
4. Mastercard reviews and assesses results.

	**Solution Provider Submits:**	The Registration Form, Test Plan and a Tap on Phone solution to be tested by chosen lab. Registration form to be sent to chip_certification_ad@mastercard.com
	**Solution Provider Receives:**	Functional Test Assessment Summary (TAS)

For a list of all EMVCO labs please visit the EMVCo's approved service provider list located on the EMVCo website. For a list of labs that are currently accredited by Mastercard for L2 testing of Tap on Phone solutions contact chip_certification_ad@mastercard.com.

Notes:

- All solutions must comply with the latest Mastercard contactless reader specifications, all test environment requirements and all applicable performance and implementation requirements (response times, visual and audio indications etc.). This can be found on Mastercard Connect® > Technical Resources Center -> References -> Chip and Contactless, or by contacting chip_certification_ad@mastercard.com.
- Solutions going through Level 2 functional testing must be identical to the solutions submitted to the PCI CPoC Security Evaluation.
- Any functional changes to the Tap on Phone solution that are done after functional approval shall be assessed by chip_certification_ad@mastercard.com.

© 2024 Mastercard. Proprietary and Confidential.

Step 4: Security Evaluation: PCI CPoC / PCI MPoC / Mastercard Security Principles

1. **Tap on Phone [PCI CPoC] solutions ONLY: PCI CPoC**
   Following publication of the PCI CPoC standard by the PCI Council in December 2019, all solution providers of Tap on Phone [PCI CPoC] Solutions are required to submit their solutions to a PCI recognized CPoC security laboratory for evaluation per the PCI CPoC standard. A list of PCI recognized security laboratories is available on the PCI website.
2. **Tap on Phone with PIN [Tap +PIN] solutions ONLY: Mastercard Security Principles**
   We are supporting ToP with PIN pilots and Mastercard-approved laboratories will continue evaluating any ToP with PIN solution under the Mastercard Security Principles document ("Embedded Contactless Reading with PIN for MPOS Pilots"). Baseline CPoC compliance for Tap +PIN pilots is not expected but is recommended as it might enable solution providers to go to market faster once PCI standards for Tap +PIN are in place.
3. **Tap on Phone [PCI MPoC] solutions ONLY: PCI MPoC**
   Following publication of the PCI MPoC standard by the PCI Council in November 2022, all solution providers of Tap on Phone [PCI MPoC] Solutions are required to submit their solutions to a PCI recognized MPoC security laboratory for evaluation per the PCI MPoC standard.

In order to facilitate the evaluation process prior to the actual testing of the solution, security laboratories may offer the following services to solution vendors and providers:

1. Guidance on designing POIs that meet PCI CPoC and MPoC security requirements
2. Review of the vendors POI design, responses to questions via email or phone, participation in conference calls to clarify requirements, and performance of a preliminary physical security assessment on a vendor's hardware.
3. Guidance on bringing a vendor's POI into compliance with the PCI CPoC and MPoC standards, if areas of non-compliance are identified during the evaluation.

Solution Provider Submits:	**CPoC or MPoC**: Solution as per PCI requirements **Tap on Phone with PIN Pilots**: Solution as per Mastercard Security Principles
Solution Provider Receives:	**CPoC or MPoC:** Security report from labs → Review by PCI Council → if approved, published to PCI website **Pilots:** Provider receives Security report and attestation from lab + MA review and risk assessment

Notes:

- If any changes are made to the solution after the security review, the solution will need to be re-reviewed by a lab.
- For SDK integrated solutions, either a full security review or an integration review may be required. For more information, please visit the SDK Integration security review section of the FAQ.

© 2024 Mastercard. Proprietary and Confidential.

Step 5: Pilot Enrollment Form (Tap +PIN only)

After the solution vendor has successfully completed the L2 testing and security evaluation, the acquirer who will pilot the solution, will sign Mastercard's enrollment form. For more details, reach out to mposprogram@mastercard.com.

	Acquirer Submits:	Pilot Plans/Terms
	Acquirer Receives:	Signed enrollment form

Notes:

- This step is only applicable for Tap +PIN solutions.

Step 6: M-TIP Testing (Level 3)

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 CPoC or MPoC solution to generate the applicable test plan.
3. The acquirer executes the test plan, using their M-TIP test tool, and records the related test results and transaction logs with TSE or their M-TIP test tool.
4. The acquirer sends the test results (TSE file) to their M-TIP Service Provider for validation.
5. An M-TIP Letter of Approval (LoA) is delivered upon successful execution of M-TIP.

	Acquirer Submits:	TSE file: Send to M-TIP Service Provider Pilots: Mastercard email approval to proceed to M-TIP → M-TIP Service Provider
	Acquirer Receives:	M-TIP Service Provider generates report for MA → MA reviews and issues LoA

Notes:

- An M-TIP test can be initiated as soon as the Tap on phone solution has been granted a Level 2 Functional TAS (Test Assessment Summary). If all the necessary security information and confirmation is shared with chip_certification_ad@mastercard.com, a CCS (Component Conformity Statement), including functional and security evaluation confirmations, could be released by Mastercard based on customer request.
- All software-based MPOS solutions must include the MPOS indicators in transaction data; more information in the FAQ section.
- Solution providers who successfully pilot or certify a Tap on Phone solution will need to repeat Steps 1 through 6 of this guide for future pilots of Tap on Phone with PIN (step 1, obtaining the contactless license, can be skipped if already obtained).
- M-TIP related online sources (M-TIP Process Guide, list of M-TIP test tools,TSE, etc.), as well as a list of M-TIP Service Providers, are available to customers through the "Technical Resource Center" on Mastercard Connect (once logged in to Mastercard Connect®, click on "Visit the TRC" under the Technical Resource Center box. Once in the Technical Resource Center, select "References", and search by keywords).
- For more information regarding M-TIP, please contact: chipservicesmanagement@mastercard.com or your M-TIP Service Provider.

© 2024 Mastercard. Proprietary and Confidential.



3: FAQs

3.1 General

What are Tap on Phone features?

Tap on Phone runs via mobile application on eligible NFC-enabled mobile devices to support acceptance from contactless-enabled cards and devices (e.g., smartphones and 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 (e.g., 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 eligible NFC-enabled mobile devices 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 an ideal payment method for customers when they just need to pay and go. As a merchant, you can transform any enabled mobile device into a payment terminal. Each Tap on Phone transaction is protected through the same technology as chipped card transactions but provides a faster and, therefore, more pleasant customer experience.

Are Tap on Phone payments secure?

Yes: Tap on Phone payments are card present contactless EMV transactions and use the same security technology offered as EMV chip cards that are deployed throughout the world.

3.2 Certification and development

Would I ever need to recertify my solution?

Yes, however it depends on the type of changes being made and the solution's architecture. Please visit the PCI Security Standards Council website for more information about security changes. Changes that could impact the functional evaluation should be communicated to chip_certification_ad@mastercard.com for assessment.

Does a solution with an embedded SDK need to undergo security reviews?

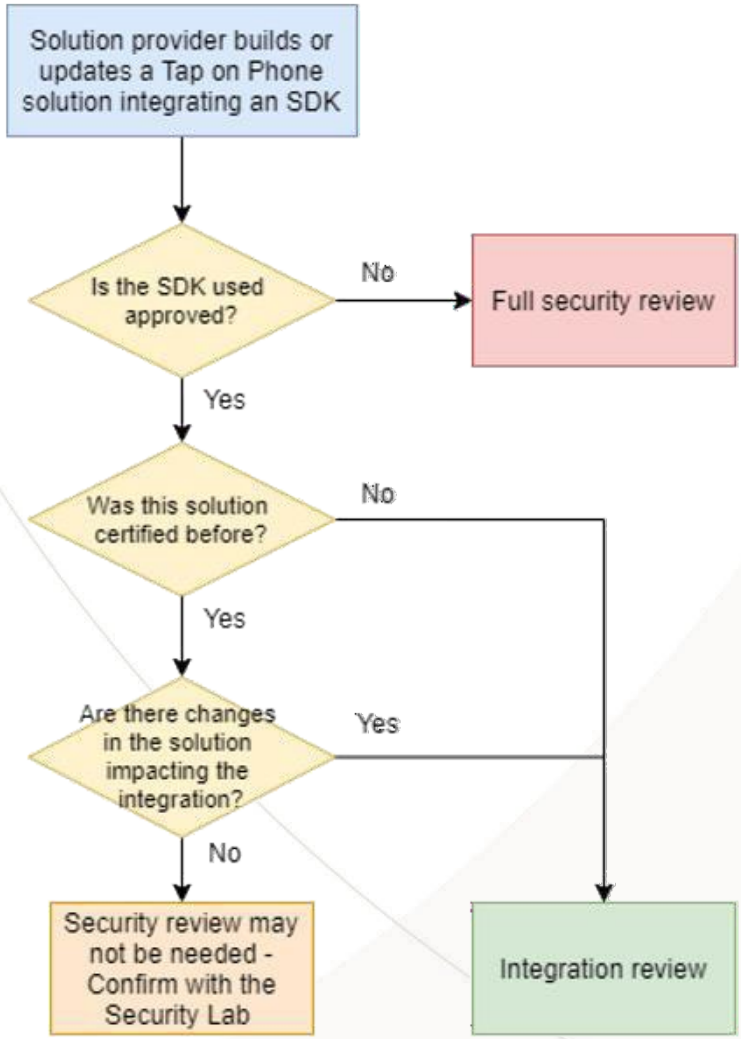
Yes. However, the security review required will depend on the approval status of the embedded SDK and the type of integration. SDK integrators will likely need to go through one of the following types of security review:

1. **Full security review**: full evaluation of a solution whose embedded SDK has not been approved or evaluated yet. Usually takes around 10 weeks.

2. **Integration review**: lightweight review of a solution integrating an SDK that has been evaluated before. The goal is to ensure that by integrating the SDK no security vulnerabilities are introduced into the final solution. Most solution providers integrating SDKs will have to perform Integration reviews.

Note: In order to reduce the certification time, it is strongly encouraged that integrators evaluate their solutions using the same security lab as their SDK providers.

The below flow chart can be used to check which type of security review will be required:



Are there any existing SDKs available for development with Tap on Phone solutions?

Yes, Mastercard has created a Contactless Reader SDK (including a selection module and kernel compliant with Mastercard contactless specifications) that can be used to read contactless Mastercard cards. This is SDK is offered free of charge. Please contact mposprogram@mastercard.com for further details.

Are solutions required to go through EMVCo PCD Level 1 Approval Process?

Tap on Phone solutions are currently not required to go through the EMVCo PCD Level 1 Approval Process. Mastercard is currently discussing the future criteria for Tap on Phone solutions with EMVCo.

Do the PCI CPoC and MPoC standards support all EMV and magstripe transactions (contact and contactless)?

No, CPoC solutions support only contactless transactions.

Do the PCI CPoC and MPoC standards support offline transactions?

No, CPoC only supports only online transactions; however, MPoC can under certain conditions. Please reference *Module 1F: Offline Payment Transactions* in the "PCI MPoC Security and Test Requirements."

Do PCI CPoC and MPoC Solutions require Mastercard approval?

All PCI approved solutions should follow the PCI CPoC or PCI MPoC certification process, which does not require any pilot approval from Mastercard.

Do PCI CPoC and PCI MPoC solutions require M-TIP approval for use with Mastercard acceptance?

Yes, all MPOS solutions accepting Mastercard require M-TIP certification.

Does the PCI MPoC standard support PIN-required transactions? What happens with transactions over the CVM limit?

Yes, the PCI MPoC standard does support online PIN. However, please note that what happens with transactions over the CVM limit is market-specific:

- If the preferred CVM in a particular country is PIN-entry, please consider developing and deploying a PCI MPoC certified solution.
- If the preferred CVM in a particular country is Signature, the collection of signature is optional for **all** Mastercard transactions regardless of terminal type (ref to AN_1712). For optimal customer experience, we recommend not to prompt the cardholder for signature.
- Any other alternatives will be regulated by the corresponding standard (e-commerce, MPOS, etc.).

Are the Mastercard-approved security laboratories the same as PCI CPoC and MPoC recognized laboratories?

No, some laboratories are approved by both the PCI Council for CPoC / MPoC security evaluations and Mastercard, while others are not. Please, review the list of PCI-recognized CPoC laboratories on the PCI website: https://www.pcisecuritystandards.org/assessors_and_solutions/pci_recognized_laboratories.

What is the MPOS indicators requirement?

Overview:

Mastercard is introducing new MPOS indicators in authorization and clearing messages to differentiate between software- and hardware-based MPOS terminals and PIN entry support.

Hardware-based MPOS terminals are PCI-compliant card reader accessories (dongles) with a hardware-based PIN pad paired with a merchant's mobile device. Software-based MPOS solutions take advantage of merchant's off-the-shelf mobile devices for either PIN entry or for acceptance of contactless transactions, thus reducing the cost of payment terminals and promoting card acceptance.

© 2024 Mastercard. Proprietary and Confidential.

3: FAQs

Requirements variations for MPOS:

Requirements applicable to regular POS terminals are slightly adapted for MPOS due to technology constraints, or different use cases for this type of terminals. The most important ones can be summarized as follows:

- Support of contact magstripe is made optional for MPOS in Europe Region (RA001.18 not applicable to MPOS; soon to be extended to rest of world)
- MPOS transactions must be identified in authorization messages:
  - DE 61 subfield 10 (Cardholder-Activated Terminal Level) must be set to '9' (MPOS Acceptance Device)
- Additional fields must be configured for software-based MPOS solutions in both authorization and clearing, as introduced in AN_1626.

The following table illustrates these fields.

	Authorization & Single Message System		Clearing	
For this MPOS device type:	**In DE 22, subfield 2, use a value of:**	**In DE 48, subelement 21, subfield 01, use a value of:**	**In DE 22, subfield 2, use a value of:**	**In PDS 0018, subfield, 01, use a value of:**
External reader and software PIN entry (also known as SPoC)	3	0	3	0
Embedded reader and no PIN entry (also known as CPoC with no PIN or Tap on Phone)	2	1	0	1
Embedded reader and software PIN entry (also known as Tap on Phone with PIN)	3	1	3	1

Does Mastercard have brand requirements?

Yes, Mastercard has brand requirements that must be followed when a Tap on Phone solution that accepts the Mastercard network is created. Additional detail can be found below and on Mastercard Brand Center.

Pre-Payment Acceptance Requirements

Prior to payment acceptance on the device screen, branding within Tap on Phone solutions must:

- Display the Contactless Symbol
- Display Mastercard and/or Maestro, and other network acceptance marks, in accordance with applicable network requirements

Post-Payment Acceptance Requirements

Tap on Phone solutions should enable Mastercard Sonic Branding (Sonic Checkout Sound, Animation, and haptics vibration) to indicate the approval of a Mastercard payment transaction.

Technical implementation assets are available in Mastercard Developers in the form of Android and iOS SDKs along with step by step integration instructions and Mastercard Sonic guidelines.

Device Branding Recommendations

Merchants with NFC-enabled phones, tablets, and similar devices that are enabled acceptance devices, through a Tap on Phone app, may place a decal sticker on the device near the NFC antenna location to signal where a customer may tap to pay. A visual will help cardholders specify where to tap to reduce transaction errors. Please visit Mastercard Brand Center for how to obtain Tap on Phone decal stickers artwork.

© 2024 Mastercard. Proprietary and Confidential.

3.3 Merchant-focused

How do I know if a customer can pay via Tap on Phone?

Physical Card: Look for the contactless indicator  on the card – it's usually on the front but may be on the back. If you do not see the waves, the card won't be able to tap.

Device: If the customer has a mobile wallet (e.g., a Mobile Banking issuer application with NFC capabilities: Apple Pay®, Samsung Pay®, Google Pay®), they can Tap & Go® if they have previously loaded their card into their mobile wallet. Only the customer will know if they have done this.

Where does the customer tap?

The customer should take out their NFC card or enabled device, identify the NFC antenna and hold it in proximity until the payment has been accepted. If available, a sticker can help indicate where the NFC antenna is located.

What if the transaction does not process?

Make sure your device has a data connection available/active, check that the mobile device cover is removed and retry tapping.

Which operating systems are supported?

Tap on Phone is available on devices and operating systems that meet the security requirements from PCI Council and Mastercard.

Do Tap on Phone solutions support all payment brands (Mastercard, Visa, etc.)?

A solution can support other payment brands if it is built with the brand's EMV kernel and is approved by the brand.

3.4 Pilots

Can I start a new Tap on Phone with PIN pilot?

Under Certain Conditions Tap on Phone with Pin pilots are possible. For information on how to launch a pilot, please refer back to section 2 (Process). In addition, Mastercard would need to review your MPoC migration plans and adjust the Pilot Enrollment Form, allowing a reasonable time frame for PCI MPoC certification without altering the continuity of the acquiring business. Please contact mposprogram@mastercard.com for additional information.

© 2024 Mastercard. Proprietary and Confidential.



4: Glossary

Contactless payments: A payment method that enables consumers to purchase products and services via debit/credit card or mobile devices that use Near Field Communication

CPoC: Contactless Payments on COTS, also known as Tap on Phone without PIN

COTS: Commercial off-the-shelf device. A mobile device (e.g., smartphone or tablet) that is designed for mass-market distribution

Electronic payments: A transaction processed by an electronic medium, as opposed to a cash transaction or payment by paper checks

EMV®: A global standard for cards that uses chip technology to authenticate (and secure) chip-card transactions, taking its name from the card schemes that developed it – Europay, Mastercard, and Visa

Level 1 Testing: Level 1 (L1) testing is an EMV specification for cards, acceptance devices and mobile phones (in card emulation mode) and is a requirement on NFC mobile device vendors. L1 certification ensures that the device meets the lower-level electromagnetic and communication requirements. It includes operating distance tests, in which reference cards are placed at a set of predefined positions in proximity to the device's antenna

Level 2 Testing: Level 2 (L2) certification validates the software, which implements the payment functionality that runs on the EMV-approved device. This software is referred to as a payment "contactless kernel" (also includes the application selection module). The supported contactless payment schemes (Mastercard/Maestro, Visa, American Express, etc.) determine which of the payment kernels will be implemented

MPoC: PCI Mobile Payments on COTS, also known as Tap on Phone with PIN

MPOS: Mobile point of sale, including mobile devices, tablets and wireless portables

M-TIP testing: M-TIP (also known as Level 3 certification) ensures that the configuration of the software on the device and the acquiring chain, including the acquirer host and the connection to Mastercard, meet the Mastercard brand requirements

Near field communication (NFC): The technology that allows two contactless enabled devices (credit card, mobile phones) and payment terminals to contact each other when they are in range, (e.g., contactless payments)

PCI DSS: The Data Security Standard published and maintained by the Payment Card Industry Security Standards Council. PCI DSS provides a baseline of technical and operational requirements designed to protect account data

Software Development Kit: A tool that allows solution providers to integrate third-party features into their own software, apps or platforms

© 2024 Mastercard. Proprietary and Confidential.



5: Resources

Mastercard Resources:

1. Tap on Phone Merchant Guide
2. Tap on Phone Pilot Case Studies
3. Tap on Phone Go-to-Market Guide
4. Contactless Reader SDK[1]

Please visit Mastercard's Mobile Point-of-Sale Website to gain access to guides and case studies.

PCI CPoC Documents

1. PCI Security and Test Requirements
2. PCI Program Guide
3. PCI Technical FAQs

PCI MPoC Documents

1. PCI Security and Test Requirements
2. PCI Program Guide

1. Mastercard's Contactless Reader SDK information and request form can be found HERE.

© 2024 Mastercard. Proprietary and Confidential.