Tap on Phone Implementation Guide

September 2025

Table of contents

1: Overview

1.1 What is Tap on Phone?

Tap on Phone (ToP) is a contactless merchant acceptance solution that is low cost, low maintenance, and peripheral-free. 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 that have an embedded NFC antenna.
- Merchants download a dedicated Tap on Phone app and after initializing the app and completing account set up, they 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 enter 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.

Tap on Phone can support merchants of all sizes and categories to drive incremental growth including cash only merchants, mobile and online merchants, retail, transit, and more. For more information, visit our website.

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 (also known as Vendors or SDK Vendors).
- 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 defines the components and requirements of Tap on Phone solutions and implementations and provides 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 MPoC™ Solution (i.e., 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 / implementations must comply with Mastercard Rules, PCI MPoC standard and relevant EMVCo and Mastercard testing requirements.

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.

2: Requirements & Process

2.1 Mobile devices & Level 1 Testing (EMVCo)

Tap on Phone solutions enable contactless payment acceptance using general and multipurpose mobile devices, such as smartphones and tablets, that are not designed for payment processing.

An increasing number of merchants value the flexibility and cost-effectiveness of using their personal mobile phones to accept contactless payments. Similarly, merchants that rely on fleets of mobile devices, including delivery, transportation, inventory management, and restaurants, are also recognizing the benefit of enabling contactless payments on those devices.

However, not all devices perform equally and until recently there was no required standard to test against. EMVCo has now introduced Level 1 requirements for Devices used in Tap on Phone solutions, establishing a benchmark for performance and reliability.

Mastercard guidelines are as follows:

- Multipurpose mobile devices, such as smartphones and tablets, that are not designed for payment processing are recommended to have undergone EMVCo L1 Reduced Read Range testing, where possible.
- Contactless acceptance devices designed for payments as a main use case are required to hold an EMVCo Full Range Letter of Approval (LoA).

The EMVCo Level 1 Reduced Range evaluation process is available to all NFC device manufacturers (e.g., phone and tablet manufacturers) to test the NFC part of their devices for payment in reader mode, for use cases where payment is not the primary function. Additional detail can be found below.

Type of deployment	Mastercard Read Range Requirement
Personal Devices (Merchant using their own/personal mobile (COTS) device)	EMVCo Reduced Range LoA recommended
Fleet Deployments (Merchant deploying specific mobile device(s))	Until end 2026[1] EMVCo RR L1 tests required From 1 Jan 2027[2], Minimum EMVCo RR 1cm LoA required

Note: These requirements may evolve over time.

[1] Until end 2026, in cases where due to test results, EMVCo cannot issue a Reduced Range LoA, please contact Mastercard to assess the results. More information on the EMVCo Reduced Range approval process can be found at: https://www.emvco.com/processes/reduced-range-pcd-level-1-approval-process/

[2] From Jan 2027, devices used for fleet deployments must have an EMVCo Reduced Range 1cm LoA minimum. Contacts: chip_certification_ad@mastercard.com / mposprogram@mastercard.com

2.2 Solution details

Below is an overview for entities looking to develop or deploy a **PCI Mobile Payments on COTS (MPoC)** Tap on Phone solution.

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.

Partners looking to deploy their own Tap on Phone solution can either develop and certify their own proprietary solution against the published PCI MPoC standard by following the *Solution components* steps below or they can engage with a solution provider that offers an approved PCI MPoC solution.

2.3 Certification step details

Step 1: Contactless Development License

Contactless Development License: A 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 this activity). Solution providers 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

Once your Contactless License is received, you can request access to Mastercard's Contactless Reader SDK. The SDK includes a selection module and kernel compliant with Mastercard contactless specifications and can be used to read contactless Mastercard cards. It is offered free of charge.

Mastercard's Contactless Reader SDK information and request form can be found on Mastercard Developers.

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

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 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. Solution provider sends TEPS to their chosen accredited lab for L2 testing. Once complete, the lab issues a test report to Mastercard and the solution provider.

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 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 MPoC 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.

1 Contactless License → 2 L2 Mastercard → 3 PCI MPOC Solution Listing → 4 M-TIP

Step 3: Security Evaluation: PCI MPoC Listings

Providers of complete Tap on Phone Solutions or components (such as Merchant Apps, SDKs or Security Services) are required to submit their solutions or components 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 or component, security laboratories may offer the following services to solution providers:

1. Guidance on Solutions with Components that meet MPoC security requirements
2. Review of the solution providers POI design, responses to questions via email or phone, participation in conference calls to clarify requirements, and performance of a preliminary security assessment on on the solution provider's offer

3. Guidance on bringing a solution or components into compliance with the PCI MPoC standard, if areas of non-compliance are identified during the evaluation.

PCI MPoC is a modular standard with several potential listings in addition to a complete Solution: Software, A&M Services, Applications and SDKs. The content of PCI MPoC Solution listings are a resource primarily intended for Merchants, Acquirers and other organizations needing to verify the Applications used by those merchants. Application developers and solution providers should consume the contents of PCI MPOC Software and MPOC Service listings.

The evaluation of Solutions, its subcomponents and integration of components is normally performed by PCI recognized laboratories. To facilitate the scalable development of MPoC Apps integrating MPOC SDKs, developers of isolating SDKs may themselves verify the integration of their SDKs by their customers' applications.

Prior to step 5 (M-TIP) all MPOC applications must be listed in a MPOC Solution. Calling Apps (Merchant Apps that call MPoC Apps) must be listed in a MPOC Solution. The below table lists the various components of PCI MPoC, their variants and the Acquirers' requirements in order to deploy a listed solution.

M-TIP Eligibility Criteria related to the PCI MPoC standard, MPoC Product or sub-element	Variants	Application Integration[1] Security Requirements	MPoC App Integration Applicability	Acquirer Responsibility[2]
MPoC Software	MPoC Software without MPoC sdk monolithic) or MPoC Software co-listing MPoC SDKs (Isolating or non-isolating SDKs)	NA	NA[3]	NA An MPOC Solution always references the necessary MPOC Products and sub-elements
MPoC Solution	Monolithic or Non-monolithic (composite)	NA	NA	Identify[4] the MPoC Solution that co-lists the Apps (and optional external readers) used by their sponsored merchants[5]
MPoC Applications	MPoC Application (A MPoC App not integrating an MPoC SDK)	NA	NA	Validate that MPoC Apps used by merchants are listed in the MPoC Solution
	Composite MPoC Application (An MPoC App using up to two MPoC SDKs)	MPoC Module 2A: MPoC SDK Integration	Yes (After review by laboratory (or MPoC SDK vendor in case Vendor Verification is permitted)	Validate that MPOC Apps used by merchants are listed in the MPoC Solution
	Calling App[6] (not listed at this stage at PCI)	NA	NA	N/A

[1] Listed MPoC Apps may integrate up to two listed MPoC SDKs
[2] Acquirers, in addition to the transaction processing role, may also play roles in the MPoC ecosystem (App/SDK vendor, Solution vendor, etc.)
[3] MPOC Apps (integrating or not SDKs) may be listed in MPoC Software and MPoC Service; however, only the MPoC Applications which are included as part of an MPoC Solution Listing have undergone validation to all of the MPoC standard requirements and are the ones that should be used by merchants (either directly or through a Calling App).
[4] All the information relevant to M-TIP is summarized in M-TIP Process Guide available on "Technical Resource Center" on Mastercard Connect.
[5] Merchants may use PCI listed MPOC Apps or "Calling Apps" (the latter using the security services offered by the MPoC Solution).
[6] Any MPoC Application may optionally support APIs that accept non-sensitive payment initiation data, such as an amount, from another "calling" application.

Notes

- These requirements are valid as of September 2025 and correspond to PCI MPoC 1.1. Please note they may evolve over time.
- In addition to security eligibility criteria (PCI MPoC) the M-TIP process also tests/checks other Mastercard requirements.

Solution Provider Submits:	**MPoC:** Solution as per PCI requirements
Solution Provider Receives:	**MPoC:** Security report from labs → Review by PCI Council → if approved, published to PCI website

Step 4: 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.
   i. The Acquirer must reference a PCI Listed Solution and Reference number during the M-TIP onboarding.
2. The acquirer initiates a M-TIP session in the M-TIP Test Tool, by selecting the latest Test Set version and uses it to enter the details of their 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
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 listed by PCI on their website. Please keep in mind that the PCI MPoC listing MUST be for a Solution not just a component listing: Software or Services.
- All software-based MPOS solutions must include the MPOS indicators in transaction data; more information in the following section.
- 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.

2.4 Transaction identification requirements

Mastercard requires certain transaction coding in authorization and clearing messages to differentiate between software- and hardware-based MPOS terminals and PIN entry support. The requirements can be summarized as follows:

- MPOS transactions must be identified in authorization messages:
  - DE 61 subfield 10 (Cardholder-Activated Terminal Level) must be set to '9' (MPOS Acceptance Device)
- MPOS transactions must be identified in clearing messages:
  - Private Data Subelement (PDS) 0023 (Terminal Type) must be set to value CT9 (MPOS Acceptance Device)
- Additional fields must be configured for software-based MPOS solutions in both authorization and clearing, as referenced in AN 7986 through the "Technical Resource Center" on Mastercard Connect.

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, sub-element 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	3	0	3	0
Embedded reader and no PIN entry (also known as Tap on Phone with no PIN)	2	1	0	1
Embedded reader and software PIN entry (also known as Tap on Phone with PIN)	3	1	3	1

2.5 Branding requirements

Mastercard brand requirements 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.

3: Activation & scale

3.1 Commercial success

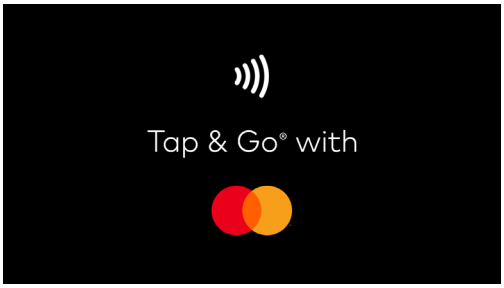
Tap on Phone deployments are the most successful when merchants and customers are excited and educated on the product.

Partners can maximize the benefits of Tap on Phone and prepare for commercial success by understanding and executing key success drivers:

1. Awareness

Amplify with Tap on Phone use cases and successes

- Merchant spotlights and testimonial videos are great ways to showcase Tap on Phone
- Events – showcase product at relevant industry events
- Webinars – showcase benefits during webinars



2. Education

Train on ease of using Tap on Phone

- Product Ambassadors – direct partner involvement with their merchants at initial deployment is key
- Consumer education – spread the word about Tap on Pone with social media campaigns
- Signage – merchants should have signage in their store and at POS

3. Enrollment

Drive merchant adoption of Tap on Phone

- Promotions and incentives can be used to drive merchant engagement including: refer-a-friend promotions, merchant competitions, discounts or incentives, loyalty rewards

Refer to our activation guide here for additional detail

3.2 Mastercard support

Mastercard offers a variety of support and resources to help partners launch and maintain successful Tap on Phone deployments

Data & Services

Professional services arm of Mastercard, focused on driving value beyond the transaction through each stage of a partner's enablement journey including:

- ✓ Consulting Services
- ✓ Data & Analytics
- ✓ Test & Learn
- ✓ Loyalty Solutions
- ✓ Marketing Services
- ✓ Labs as a Service

Branding

Mastercard offers Tap on Phone decal stickers artwork that can be downloaded on our Brand Center. A visual can help cardholders specify where to tap to reduce Tap on Phone transaction errors

*To find our decal files, please visit our Brand Center linked HERE → Contactless branding for Tap on Phone and other SoftPOS solutions → scroll all the way to the bottom of the section for the files.

Resources

Our library of resources can help boost awareness and education:

- ✓ Merchant guide
- ✓ Acquirer GTM guide
- ✓ Case studies
- ✓ Testimonial video
- ✓ Tap on Phone websites
- ✓ Sample merchant surveys

*Please visit our Tap on Phone website for resources and more!

4: Tap to More

4.1 Overview

As the physical and digital experiences continue to converge, Mastercard is focused on bringing security, simplicity, speed and choice to digital payments. We are introducing Tap to More to bring the best of contactless payments on mobile devices to a wide set of commerce use cases where people can instantly provision a card into a mobile wallet, verify a transaction or even send money to their friends and family – all with just a tap.

See below for the range of use cases that Tap to More can help bring to life:

Non-Payment Use Cases

Tap to Add
Consumer taps their card to add it to their phone's mobile wallet or store on file with a merchant or e-commerce wallet.

Tap to Verify
Consumer is requested to tap their card to confirm they are in possession of their card while using their phone's mobile wallet, bank app, or a merchant app

Tap to Activate
Consumer taps their card to activate it instead of going to an ATM or calling their bank

*All the above use cases are powered by Mastercard Digital Enablement Services (MDES) and Mastercard Checkout Solutions;

Payment Use Cases

Tap to Pay
Consumer taps their card or wearable against their mobile device to complete on e-commerce purchase

Tap to Send or Receive
Consumer taps their card or mobile phone against another person's/own phone to send/receive money or fund/payout to/from an account

***Tap to Send or Receive** is powered by Mastercard Send

4.2 Resources

Mastercard has developed a range of resources for Tap to More that help showcase the benefits of these new and emerging use cases:

- External Summary
- Program Guide
- Security Guidelines
- Use cases video

Please reach out to mposprogram@mastercard.com to gain access to the resources listed above and to learn more about Mastercard's program framework and requirements to launch Tap to More use cases.

5: 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

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

Device Preferring: deployment on specific NFC enabled mobile devices / hardware (e.g., fleet deployment of Enterprise, Business devices or any NFC enabled COTS mobile device

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

Solution Providers: Players that build and develop PCI MPoC Software (SDKs) and related Solutions and/or Services. The term *Solution Provider* may be used interchangeably with *Vendor*.