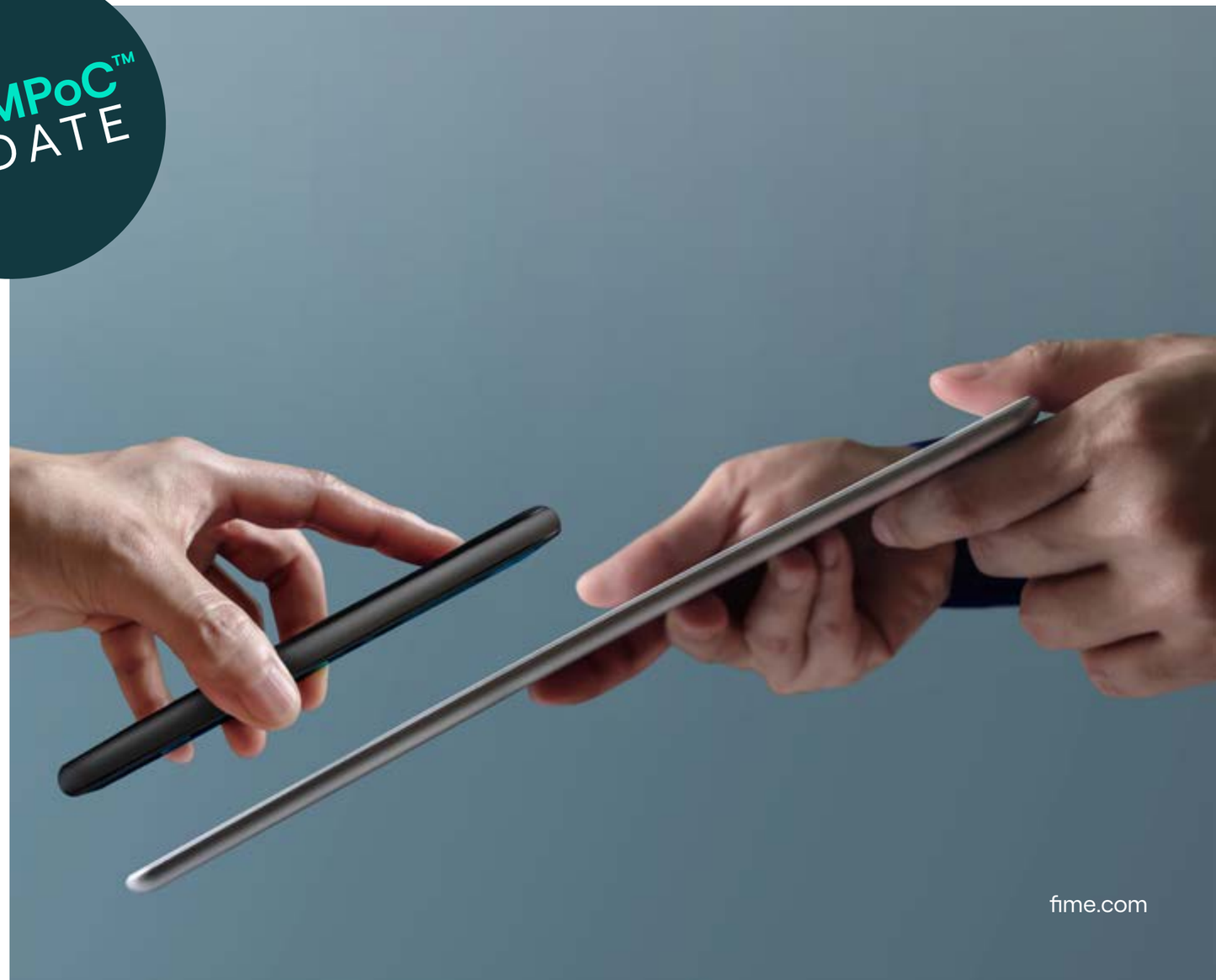
fime

eBook

PCI MPoC™ UPDATE

SoftPOS made simple.

Key considerations for developing and deploying SoftPOS payment technology.



Aug 2024

fime.com

Contents

back to contents

Consumers have become used to tapping their card to make payments. However, not all merchants can afford the onboarding and maintenance fees of legacy POS systems. SoftPOS allows them to use their own devices to accept payments, opening them up to new markets and customers.

There are still challenges to overcome before the technology can be adopted ubiquitously. Successful solutions require careful planning and execution to ensure a positive user experience with high levels of security.

Christian Damour, Pre-sales Manager – Security at Fime

1. Untapped potential.

The pandemic has contributed significantly to the reduction of cash transactions and has accelerated a shift towards cashless solutions. Hygiene, user experience and safety have become fundamental causes for concern in the global payments market.

In June 2024, Juniper Research predicts contactless payments to surge by 113% in five years[1]. This growth is attributed to the increased availability of contactless payment for smaller businesses through Soft Point-of-Sale (POS) systems.

40%

Increase in the number of contactless payment transactions.

54%

Of consumers would consider switching retailers if they do not accept contactless payments.

Fewer than 10%

Of small merchants in emerging markets have the facilities to accept digital payments.

1 Contactless payments to surge by 113% in five years, predicts Juniper Research

So how does SoftPOS fit in?

The software-based nature of SoftPOS solutions[2] allow merchants to bypass some of the costs that come with traditional POS systems. They utilize the Near-Field Communication (NFC) capabilities of Commercial Off-The-Shelf (COTS) devices, such as smartphones and tablets.

Users can accept payments by downloading an app and registering with an acquiring bank.

2 Software Point-of-Sale (SoftPOS) is a technology that allows merchants to take contactless payments using their own device without the need for any other hardware.

This eBook will explore some of the key considerations for solution vendors, fintechs, merchants, Payment Service Providers (PSP) and banks.

2. Hardware: the right device.

Using a COTS device[3], that merchants are likely to be familiar with, brings certain benefits:

- **Devices are easy to carry**, usually fitting in an individual's pocket.
- **Little to no training is required** to get staff adept at using it, allowing for quick roll outs.
- **As the merchant is the device owner, they can change it easily.** However, they are responsible if any transaction cannot be made or if the requisite security provisions are not in place. This contrasts with traditional POS systems where the responsibility lies with the acquiring bank or the terminal supplier.

3 Read our blog > SoftPOS: Everything key players need to know about devices.

Using all the features of NFC.

SoftPOS solutions are currently mainly available on COTS devices, but Apple[4/5] has started to deploy Tap to Pay on iPhone. Nearly all COTS smart devices have NFC compatibility. It enables them to accept contactless payments provided they have the necessary software.

4 Apple brings Tap to Pay on iPhone to Germany.
5 Apple expands Tap to Pay on iPhone to France.

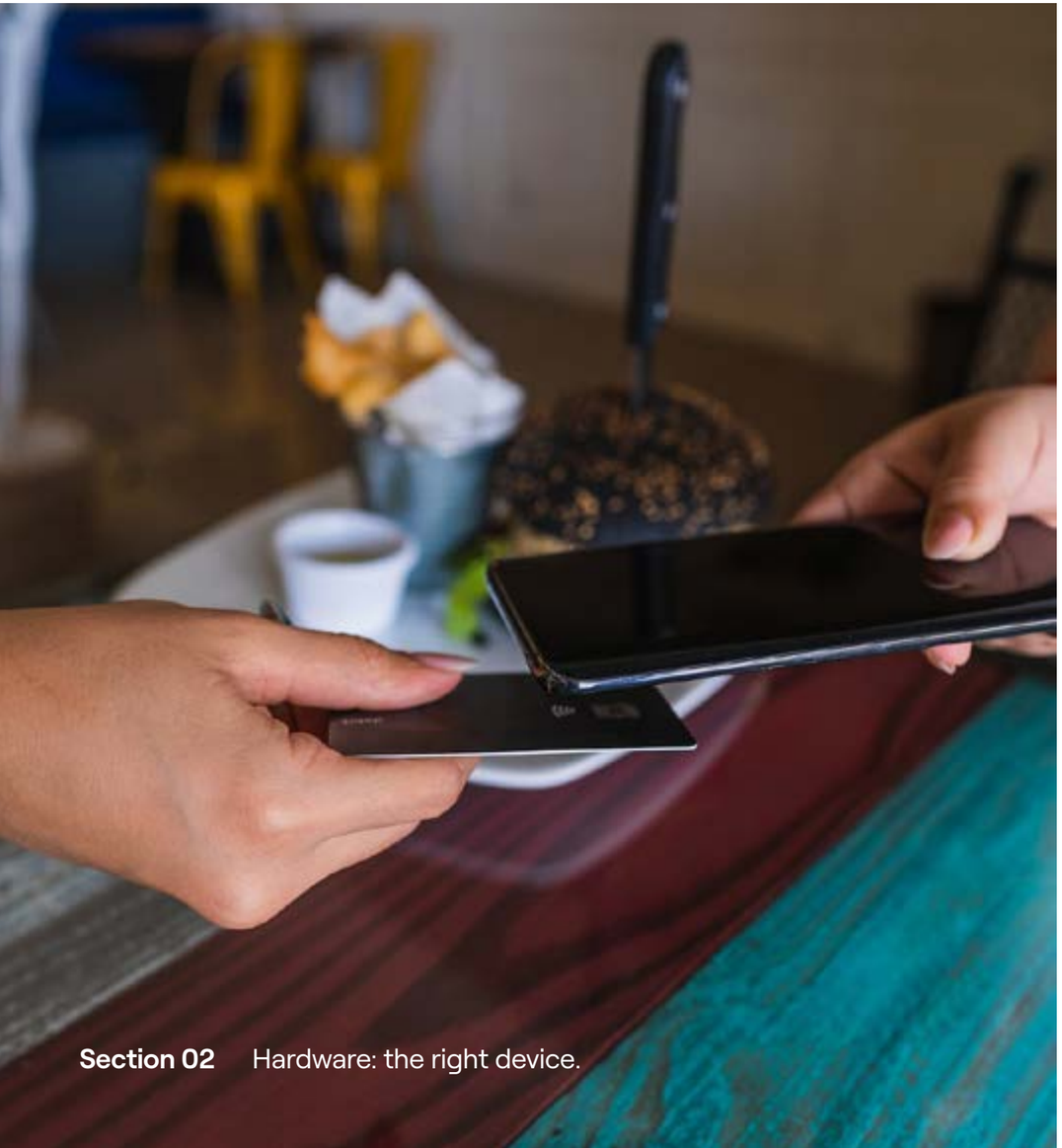
back to contents

NFC devices have the following functionalities:

- **Contactless reader mode** allows the device to accept and process SoftPOS payments.
- **Contactless card emulation mode** enables the device to act as a user's bank card to make a payment.
- **Contactless peer-to-peer mode** lets the device communicate with other NFC capable devices.

Getting the right read.

Another important factor to consider when developing a device for SoftPOS payments is the actual use case. The customer must put their card, phone or other payment device within range of the antenna of the payment acceptance device.



For developers of SoftPOS, this presents three issues:

- The position of the antenna is not currently standardized: **customers may not know where to tap.**
- The position of the antenna is usually **optimized for card emulation mode not for reader mode.**
- The read range for SoftPOS devices can be up to half of that of traditional POS devices: **customers may hold their payment device too far away.**

These concerns may mean that a customer's payment is not accepted first time. If the payment cannot be made and authorized quickly, the benefits of contactless are lost. Therefore, the product will not meet merchant or customer expectations.

To overcome this, OEMs must design their devices with this in mind.

Compliance complexity.

In lieu of the standards that govern traditional POS systems (EMV® Proximity Coupling Device (PCD) Level 1 requirements), COTS devices can seek approval with EMVCo's Tap to Mobile Program.

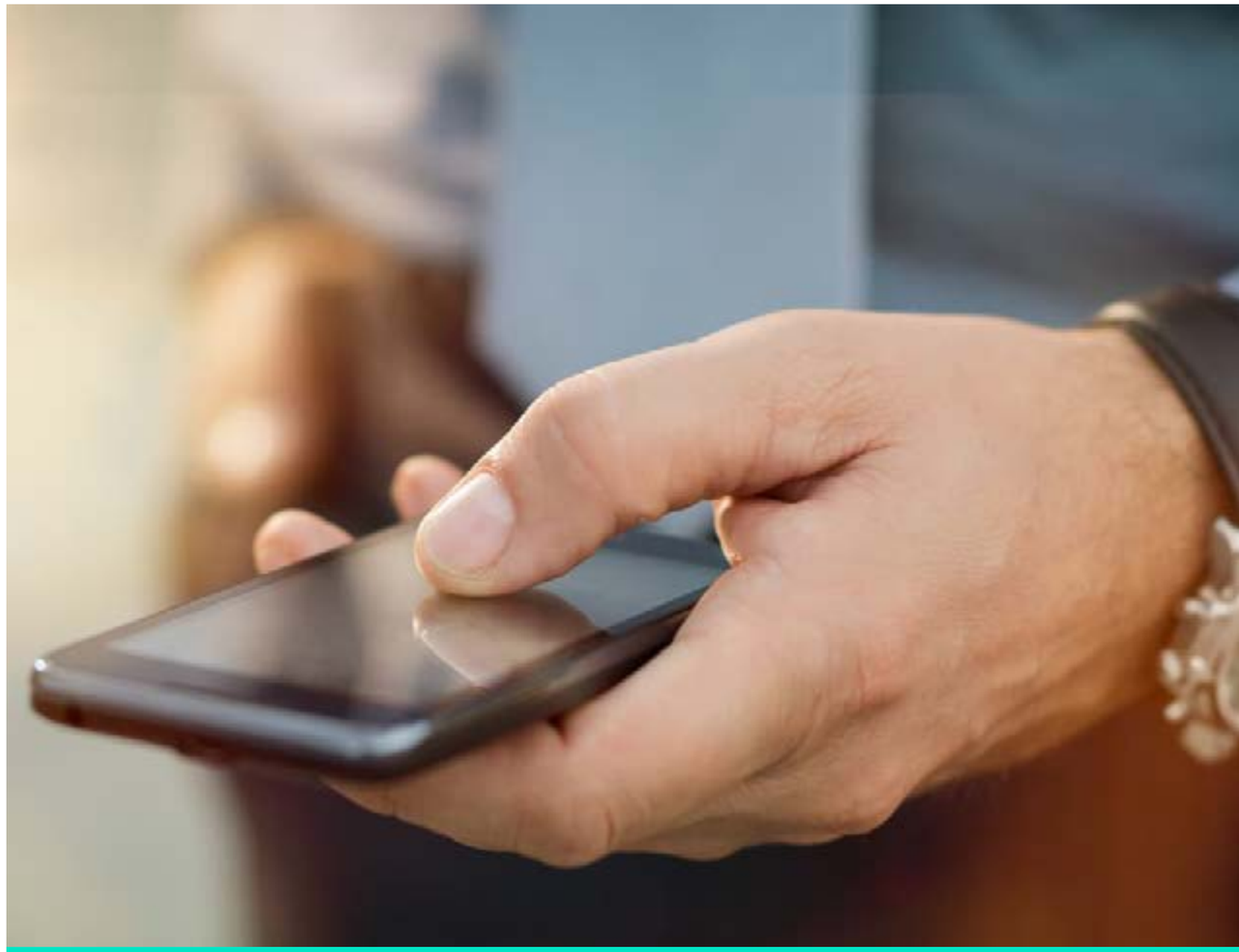
This evaluation process enables OEMs to test their device's performance, interoperability, user experience and read range.

back to contents

This program is not a requirement for deployment. But it marks the onset of a standardized certification process for SoftPOS solutions.

3. Software: creating a seamless system.

Developers must navigate the minefield of technical and practical considerations. This is to ensure their SoftPOS software[6] can provide a seamless and secure payment experience. This challenge is further heightened by each payment scheme because they have their own unique ways of accepting and processing contactless transactions. Thus, developers must make sure their apps and any embedded kernels are compliant with the requirements of multiple different schemes.



6 Read our blog > SoftPOS payments: getting the software right.

So, what must they do?

Twin systems.

To create a mobile payment acceptance solution, developers must create two different systems that work side by side to seamlessly accept and authorize transactions. These systems are:

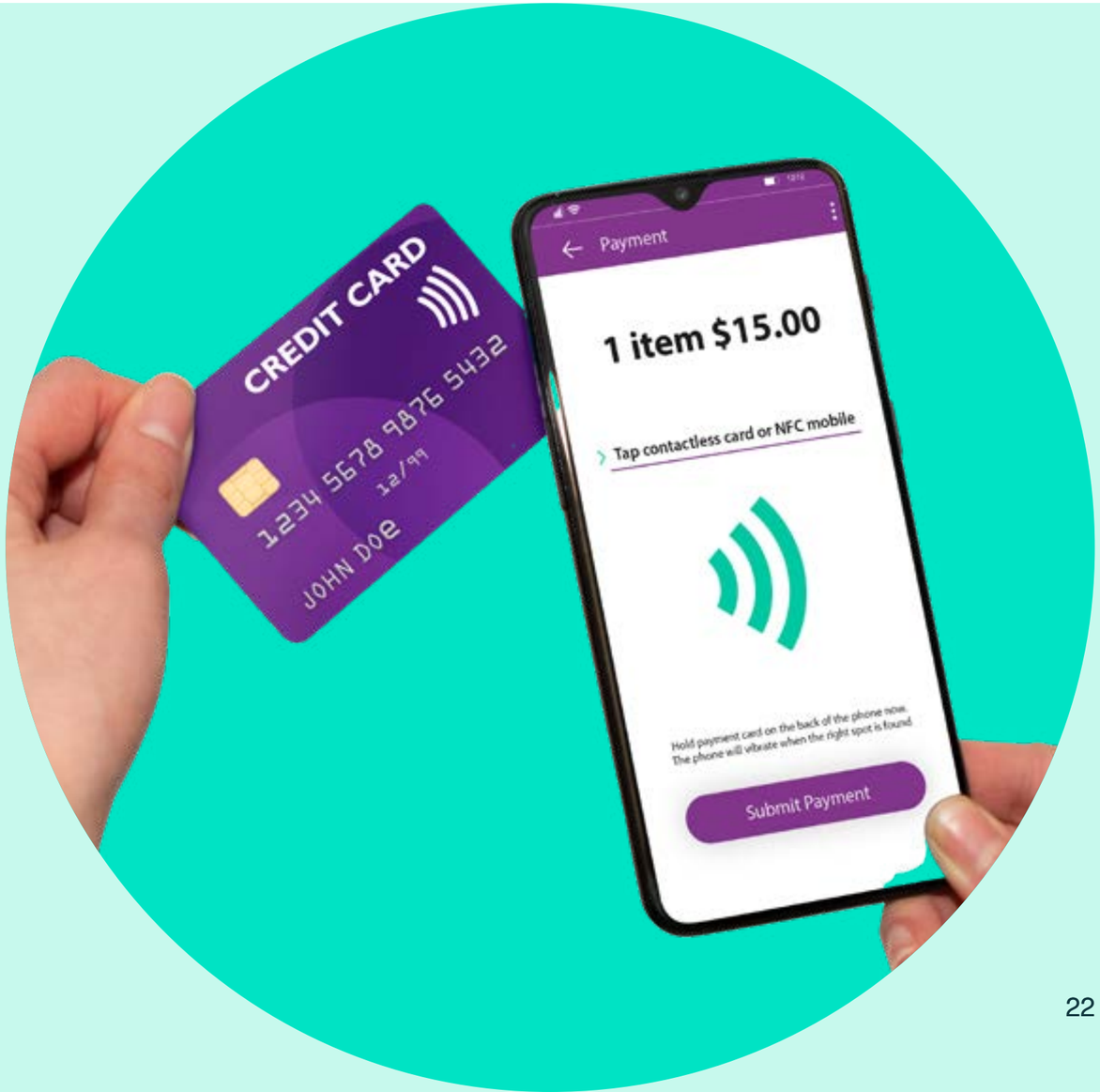
- **The local component** – the app on the user's device which contains the user interface and manages the connection to the back-end.
- **The back-end system** – which includes the Attestation and Monitoring server and the payment processing server which handles the actual payment transaction itself.

To facilitate the harmonization of these two systems, multiple different software components must also be able to work together:

- **The payment kernels** (one per payment scheme) provide all the processing logic and data required to process an NFC card payment transaction.
- **The merchant application** uses the card processing kernel's Application Programming Interface (API) and connects to the back-end system.
- **Various security modules** as well as an Attestation and Monitoring back-end must work with the other components to fulfil PCI MPoC™ requirements.

Creating these separate components and getting them to work in perfect harmony is an immense challenge.

Developers need a comprehensive understanding of all the functions of the different actors within the payments ecosystem. They must also be able to anticipate any potential problems that could interrupt or affect a transaction and mitigate them, to not undermine user confidence in the system.



Ticking the boxes.

A number of base requirements relating to both the user experience and the app's performance must be tested before payments software can be rolled out, including:

- The app's functionality.
- Its compatibility with a set of representative devices it will run on.
- The interoperability and performance of the app.
- The user interface and how it is optimized for different devices.

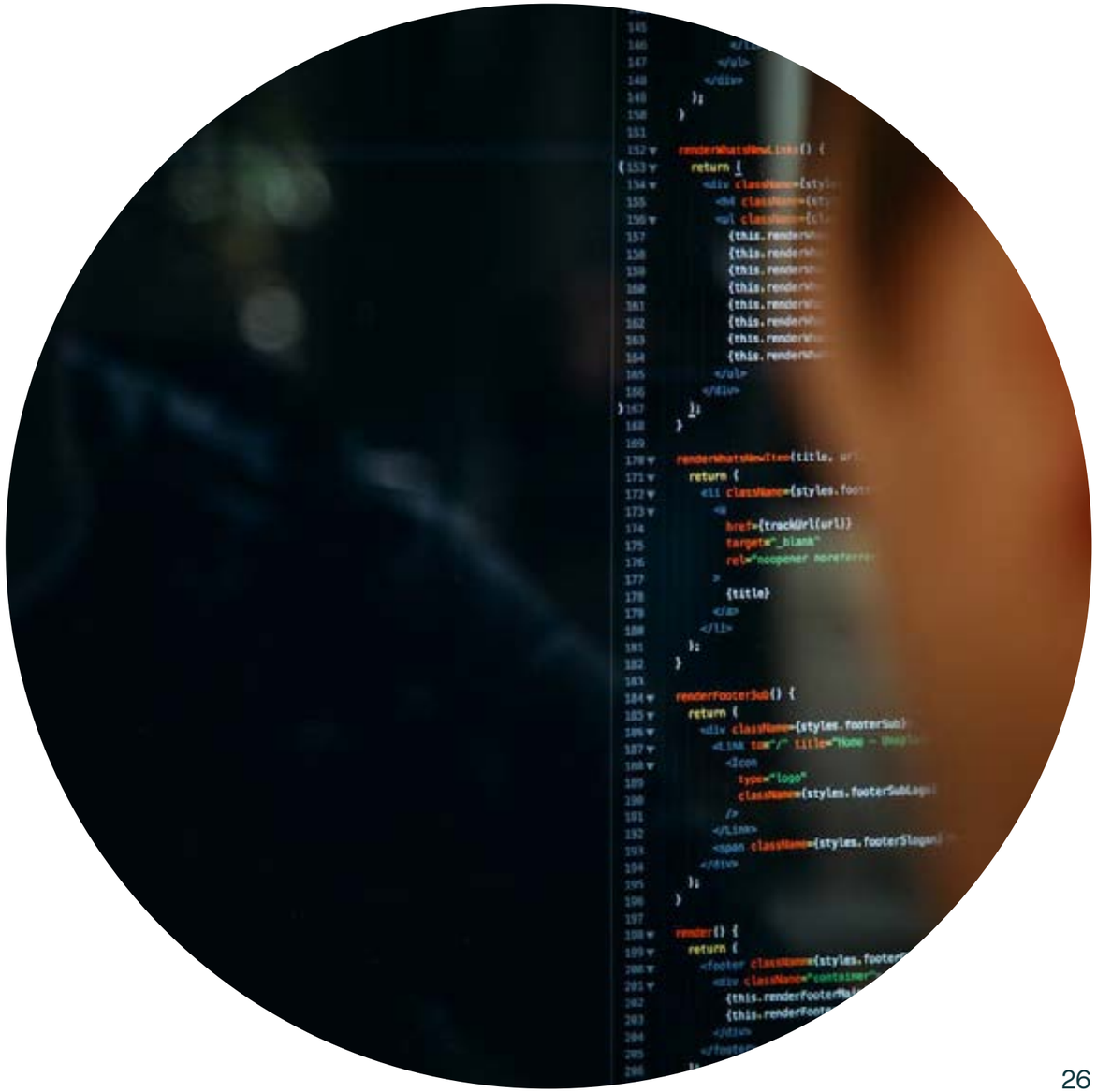
back to contents

These requirements are tested in line with the payment schemes' Level 2 requirements. This certification addresses the software's ability to implement payment functionality on COTS devices to validate the payment correctly.

4. Security: protecting payments.

One of the flagship benefits of SoftPOS is its **flexibility**. Any NFC-capable device can become a SoftPOS terminal.

This hardware-agnostic approach means they can support as many different devices as possible. However, they cannot utilize the hardware-backed security foundations that are built into traditional POS terminals. The device could therefore potentially be infected with malware or attacked, exposing valuable payment processing data and keys.



Therefore, strong security measures[7] must be incorporated into software from the beginning.

The application must work seamlessly alongside the back-end system to bring additional security. Attestation and Monitoring features can scan the security and integrity of the solution to ensure it has not been corrupted. If necessary, it can mitigate any detected threats.

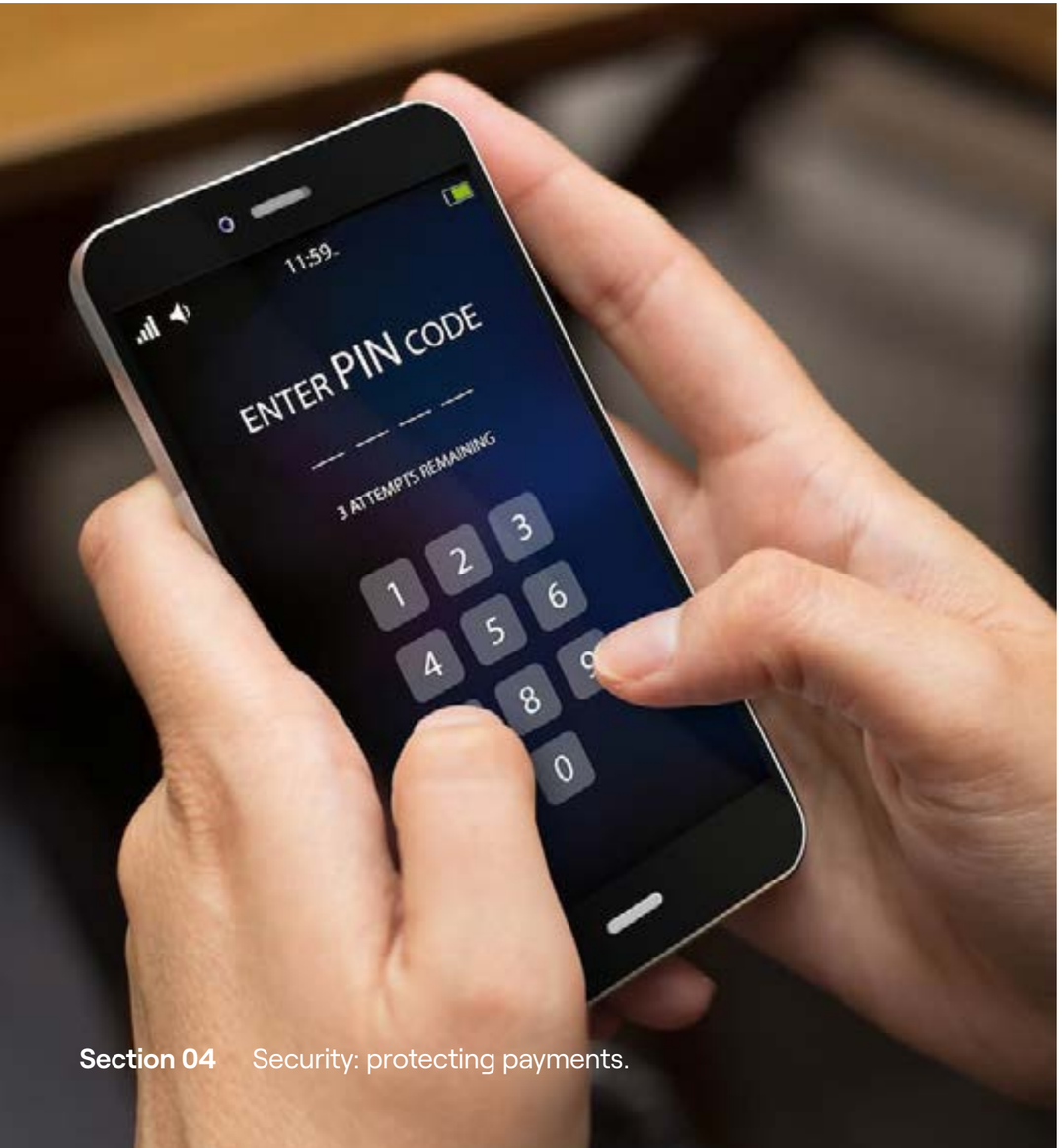
7 Read our blog > Top tips for securing SoftPOS payments.

back to contents

Other potential security mechanisms include:

- Anti-Tampering
- Anti-Rooting
- Anti-Instrumentation
- Anti-Emulation
- Anti-Debugging
- Device-Binding
- Obfuscation
- White-box Cryptography

Many of these are available from specialist software technology providers. They allow developers to adopt solutions which have already passed the complex security evaluation.



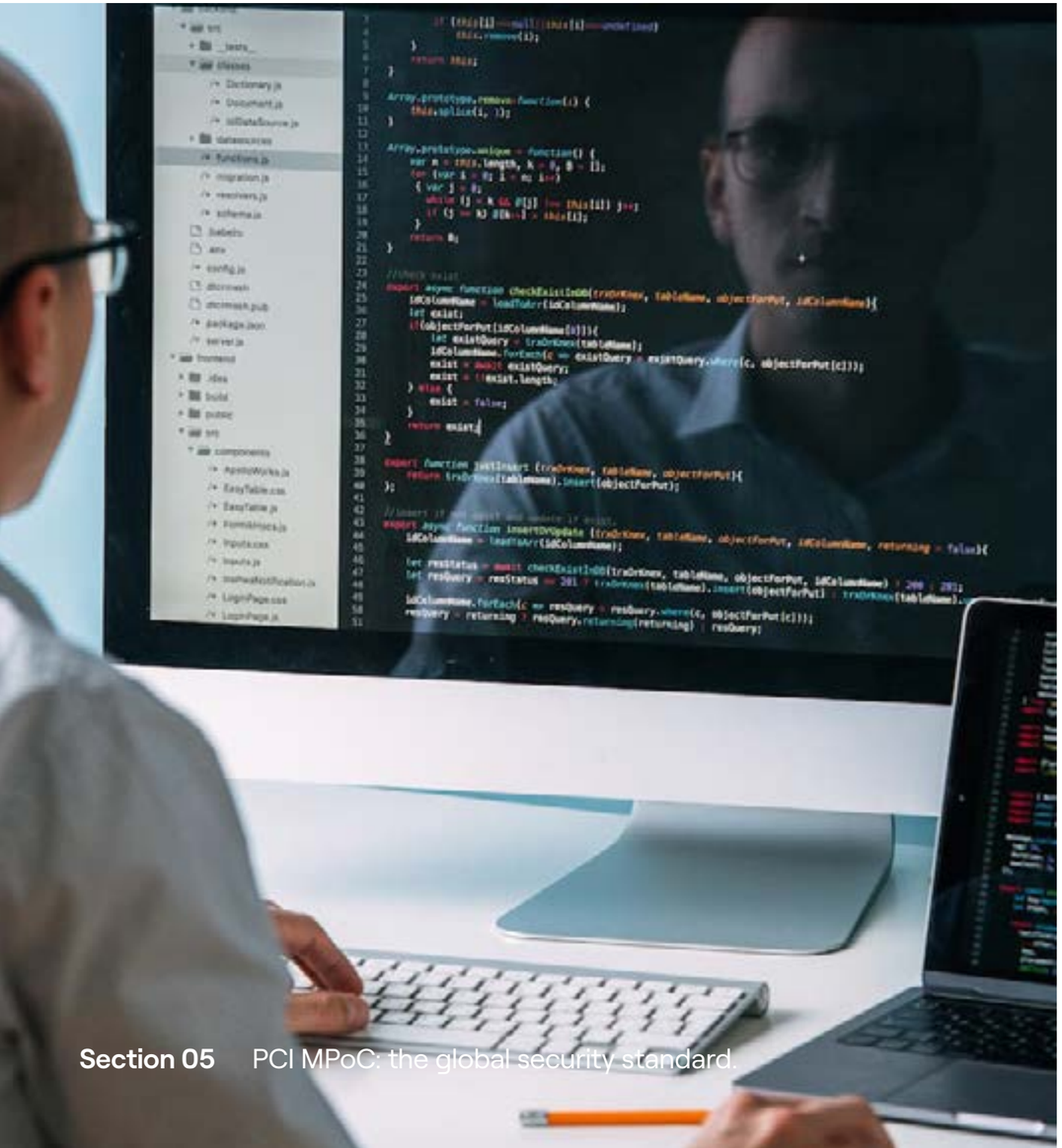
Paths to certification.

Once the software is built, all SoftPOS solutions must pass security evaluation. This process varies based on if a solution includes PIN entry support.

- **Solutions with PIN entry** must go through PCI Mobile Payments on COTS (PCI MPoC™) security evaluation and certification.
- **Solutions that do not support PIN entry** can either take PCI Contactless Payments on COTS (CPoC™) requirements or PCI MPoC requirements security evaluation and certification.

5. PCI MPoC: the global security standard.

back to contents



A versatile standard: the Swiss army knife.

In 2022, PCI SSC issued a new standard called Mobile Payments on COTS (MPoC™), that includes new security requirements to evaluate solutions with or without PIN entry support.

The program also supports the independent evaluation and certification of payment acceptance components (e.g: Software Development Kit (SDK), Attestation and Monitoring back-end). This facilitates the security evaluation of the fragmented SoftPOS infrastructure and ensures the full scope of solutions undergo rigorous testing.

This new PCI MPoC standard brings additional implementation options which come with their own security challenges, such as: PIN entry support, offline transactions, manual entry of account data and remote kernels.

PCI SSC member schemes which require PCI MPoC.

The PCI MPoC Security and Test Requirements document was released by the Payment Card Industry Security Standards Council (PCI SSC), on November 16th, 2022 (and updated in February 2023). This was alongside the release of the PCI MPoC Program Guide in December 2022 and the latest Technical FAQs in March 2024.

back to contents

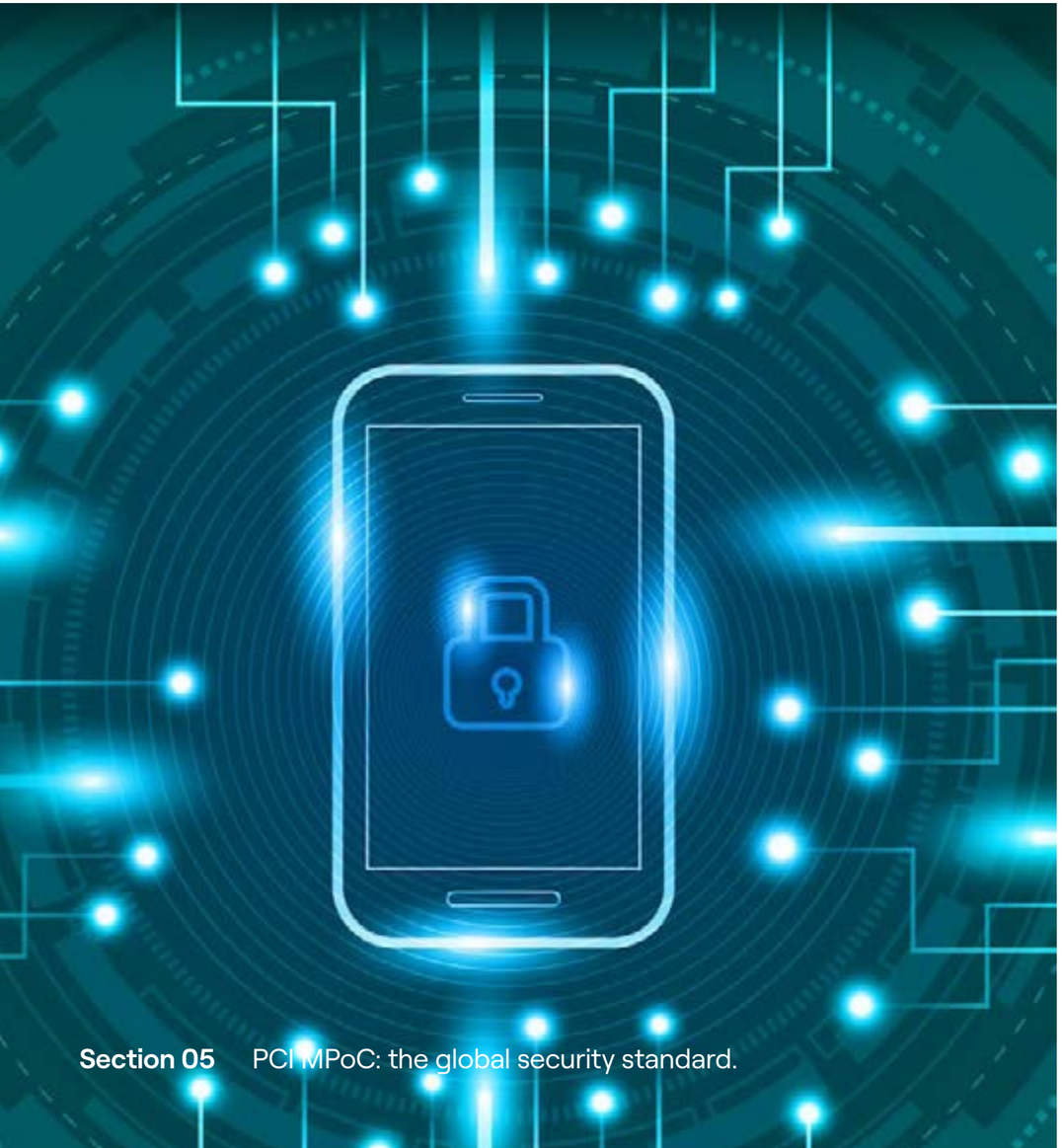
- PCI SSC is the entity in charge of the security requirements definition and acting as the Certification Body.
- PCI SSC's members are: American Express, Discover, JCB, Mastercard and Visa.
- The PCI MPoC Security and Test Requirements document is currently under revision and is being updated by PCI SSC to release PCI MPoC v1.1.

PCI MPoC is a flexible, objective-oriented standard. It provides a set of modular security requirements to certify secure payment acceptance solutions on COTS devices in a merchant-attended environment.

Flexibility and versatility as a foundation.

PCI MPoC includes new use cases such as online PIN, offline transactions, manual entry of card data on the mobile device, remote kernels, as well as SDK and Attestation and Monitoring service separate certifications, which were not supported under PCI CPoC. It supports external Magnetic Stripe Reader (MSR) and external Secure Card Reader, either with or without PIN entry support.

Note: As with all other PCI standards, any mandates, regulations, or rules regarding these requirements are provided by the participating payment brands.



Payment schemes proprietary security certification programs discontinued.

Mastercard and Visa discontinued their Tap-on-Phone pilot security programs for solutions without PIN entry support and switched to a PCI CPoC mandate 13 months after the PCI CPoC v1.0 standard was officially released.

Since the release of the PCI MPoC v1.0 standard, it has been announced that the Mastercard Tap-on-Phone with PIN pilot security program and the Visa Tap-to-Phone with PIN pilot security program will both be sunset and replaced by PCI MPoC after a few months (by the end of 2024 at the latest).

Migration towards PCI MPoC certification is required.

For solutions which support PIN entry, the only options for vendors were the Tap-on-Phone with PIN pilot security programs from the schemes (Mastercard, Visa, American Express, etc). As these were pilot programs, there were some deployment restrictions in terms of the geographies addressed and number of licenses deployed.

These are being phased out and replaced by PCI MPoC, which allows full deployment with no restrictions. Mastercard and Visa have issued official communications regarding phasing out their pilot security programs and the mandated migration towards PCI MPoC.

back to contents

Discover Visa latest communication on PCI MPoC.

Visa has recognized the burden of the current PCI requirements regarding submitting Tap-to-Phone applications for MPoC Solution evaluation.

Therefore, in lieu of complete MPoC Solution certification, Visa accepts three types of PCI MPoC certification:

- MPoC Solution (any variant).
- MPoC Software Application.
- MPoC Software SDK Isolated.

MPoC Software SDK Non-Isolated are not accepted by Visa Ready Tap-to-Phone.

6. What’s the next step?

back to contents

SoftPOS solutions give small businesses opportunities to accept payments in ways that were previously unavailable to them due to high costs.

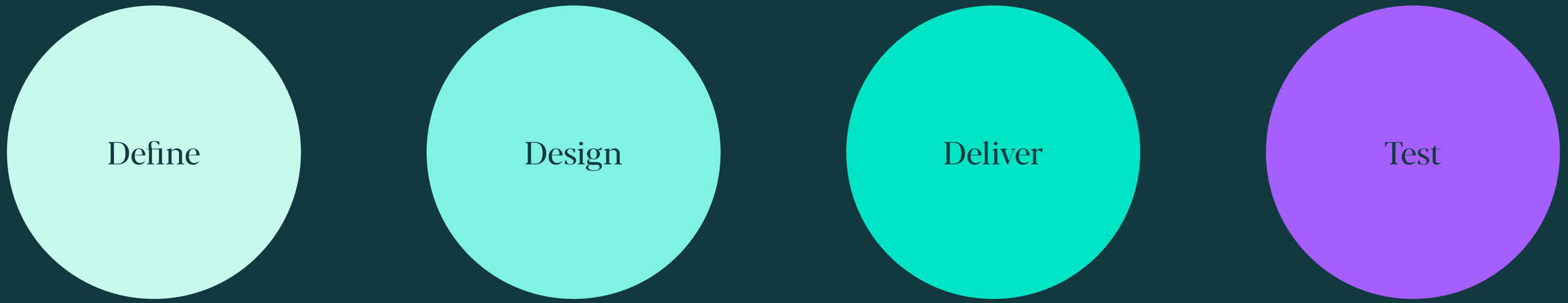
Merchants and consumers need to be confident that every possible step has been taken to protect sensitive payments data. Developers cannot be expected to be abreast of all the intricacies of the market, new specifications, upskilling and the constantly evolving requirements.

Dedicating time, money and people to such a project would require a large investment from any enterprise. Thankfully, Fime's experts are on hand to provide extensive technical expertise in defining, designing, delivering and testing solutions.

back to contents

Throughout the process, Fime supports stakeholders in four different stages.

Checklist to ensure a smooth integration project.



Define Design Deliver Test

Define

Stage one – Define to get ahead.

SoftPOS for solution vendors, fintechs, merchants, PSPs and banks

- Market study, competitive landscape and local context.
- SoftPOS service considerations and lifecycle.
- “Make or Buy” analysis.
- Business model, post launch ROI.
- Investment models, fees and ROI.

Training & workshop

- Best practices.
- SoftPOS Technology training.
- Solution security considerations.
- PCI MPoC security requirements and security evaluation process training.

Define Design Deliver Test

Design

Stage two – Design to improve efficiency.

Training & workshop

- EMV® training mandates / specifications for SoftPOS.
- Scope and description for development project.
- Dos and Don’ts.
- Impact and risk analysis.

System requirements & architecture

- Local requirements.
- International requirements per scheme.
- Implementation options.
- Mobile benchmarking architecture review.
- Software architecture support including security.

Security design review

Define Design **Deliver** Test

Stage three – Deliver to make it happen.

Support for development

- Latest schemes specifications.
- Anticipate certification requirements.
- Dedicated kernel per scheme supported.

Security modules

- Secure PIN entry module.
- White-box cryptography / Obfuscation of the code.
- Runtime application self-protection solution.

PCI MPoC documentation writing support

Test tools for SoftPOS debug

Define Design Deliver Test

Stage four – Test to ensure trust.

Lab testing & services

- EMVCo Level 1 program for COTS (optional).
- Level 2 per scheme: debug and certification sessions.
- Level 3 terminal integration testing.
- Remote expertise.
- Ticketing expertise.

Pre-assessment & security evaluation

- Without PIN Entry: PCI CPoC or PCI MPoC.
- With PIN entry: PCI MPoC.

Share your challenge.

Our Fime experts are here to help you make innovation possible, from defining, designing to delivering and testing your products and services.

- visit fime.com
- or contact sales@fime.com