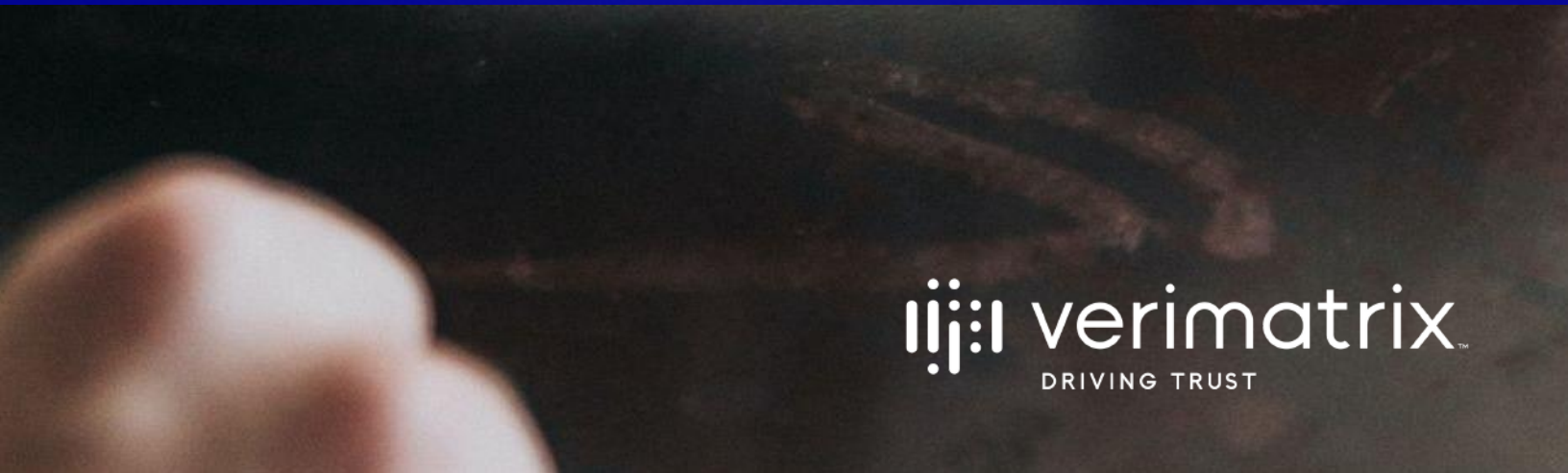
EBOOK

POINT OF SALE 5.0

Enabling Card Acceptance with Software Security

April 2021



verimatrix
DRIVING TRUST

Executive Summary

One of the fastest moving and most exciting parts of the payment chain today is that of Point of Sale – the place brick-and-mortar merchants engage with their customers.

Payment card acceptance has historically been a hardware-intensive and complex process – highlighted by EMV migration in the United States. This has been due to the need for high security standards. Payments, like many industries, is realizing those high standards can be met with modern software security. This brings new flexibility in deployment models.

Change is being driven by a demand for card acceptance amongst new segments of retailers, as well as desire to reduce costs.

It has been almost a decade since Digital Wallets started adopting software security. This has given a safe platform for imaginations to flourish and innovations to come to market quickly. By embracing new security models, the same is possible on the acceptance side for Point of Sale through SoftPOS.

This poses opportunities and challenges in equal measure; opportunities for new players to come through and build a successful business, and challenges for first- and second-generation companies who have built their businesses on "traditional" models.

Executive Summary

This paper focuses on the technologies, standards and security challenges that are arising as a result.

To keep transaction and card data safe, it is critical to prevent:

- **Reverse engineering of the application**
- **“Man in the device” style attacks**
- **Side channel attacks to extract cryptographic keys**

By leveraging Verimatrix’s many years’ experience building approved and certified mobile payment solutions, the paper demonstrates how App Shielding technology resolves many of the challenges a vendor will encounter when undergoing PCI security certification for their Contactless Payments on COTS (Tap-to-Phone) and Software-based PIN Entry (PIN-on-Glass) products.

Payment acceptance will evolve rapidly in the next few years. The flexibility of SoftPOS provides the platform to enable innovation. By using Application Shielding as a solid security foundation, not only is SoftPOS certification easier to achieve, but it becomes the basis for the vendor’s point of sale solutions for many years to come.

Table of Contents

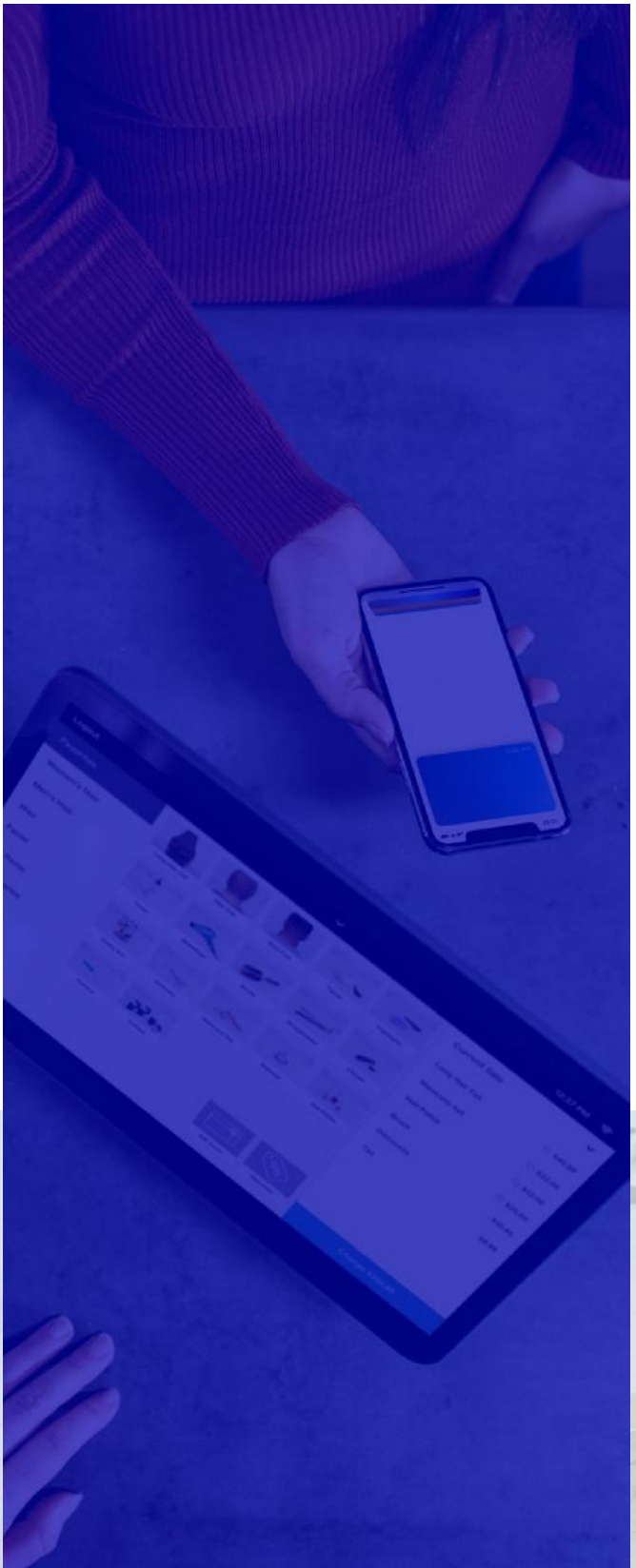
Introduction

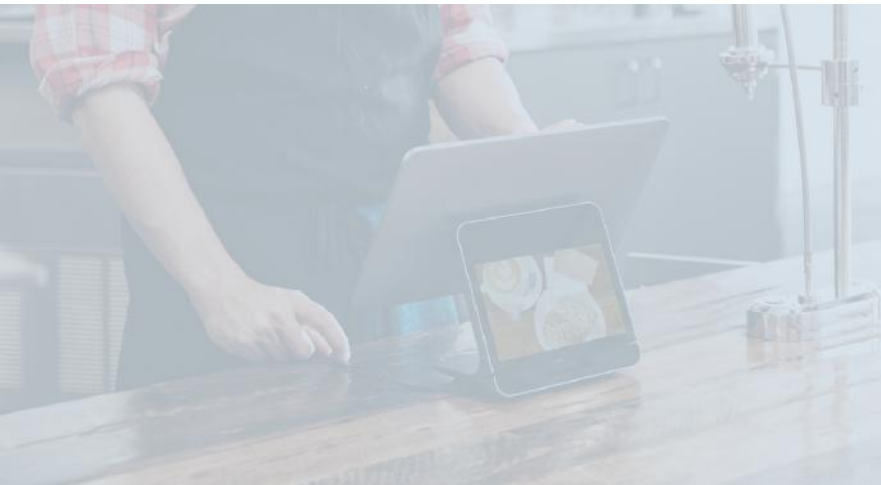
Software Point of Sale (SoftPOS) is one of the most exciting areas in Payments right now (and no, it doesn't feature Blockchain or AI - yet anyway). There are a plethora of companies developing SoftPOS systems and software, many of these are small start-ups, but in addition, the large incumbent players are increasingly active.

What makes SoftPOS exciting is that it is being driven by a real market need. A desire to lower costs, yes; but also, a requirement to enable card payments in new markets and industries. This need has accelerated in the current pandemic.

SoftPOS can be seen as extension of the mPOS trend.

This eBook will be of interest to anyone responsible for delivering a certified SoftPOS product to market.





mPOS to SoftPOS

It is fair to say that Square pretty much invented the mPOS category, providing small merchants (and some very large ones) with innovative and attractive hardware and software, backed up by systems and services. Of course, this has been primarily in the United States before the EMV migration started and simple mag stripe (and no security whatsoever) was allowable.

In other parts of the world where EMV was already deployed, the original Square solution was not allowed. This created space for new entrants in the market, like iZettle, to develop EMV compliant mPOS products. These use dedicated “Pin Entry Devices” (PEDs); and could be considered a hybrid, combining traditional POS devices with some of the benefits of Square’s approach.

Thus the mPOS market has grown and it is now common to see a vendor at a farmers' market in California taking Square payments or a food-cart cashier in Stockholm taking chip and pin payments via an iZettle terminal; use-cases where the larger EMV PEDs from established players are simply too expensive to make sense.

Of course, nothing stays still. Inspired by HCE[1] Payment Wallets, start-ups and payment processors began innovating to create pure software Point of Sale solutions that could accept contactless payments on any Android smartphone. Even traditional POS terminal manufacturers soon got in on the act.

In payment acceptance, standard smartphones are often referred to as Consumer Off The Shelf devices (COTS).

Motivated to support the industry trend, the Card Schemes, EMVCo and PCI have developed standards for SoftPOS. The two headline standards are both from PCI: Contactless Payments on COTS (CPOC) and Software-based PIN entry on COTS (SPOC). These standards are not yet interoperable, so the Card Schemes have developed a waiver program to allow PIN entry with CPOC.

[1]Host Card Emulation is the interface on Android phones that allows banks and digital wallet providers to turn mobile phones into payment cards.

Evolution of Card Acceptance

There is a consistent trend in the world of computing: moving from dedicated hardware to off-the-shelf components with software defined use cases. This trend extends to the world of security, which is moving from hardware guarded perimeters to intelligent software protection.

Innovation in payment technology is driven by two questions:

1

How do we get more people to make payments on our network?

This means making it easier and more convenient to pay.

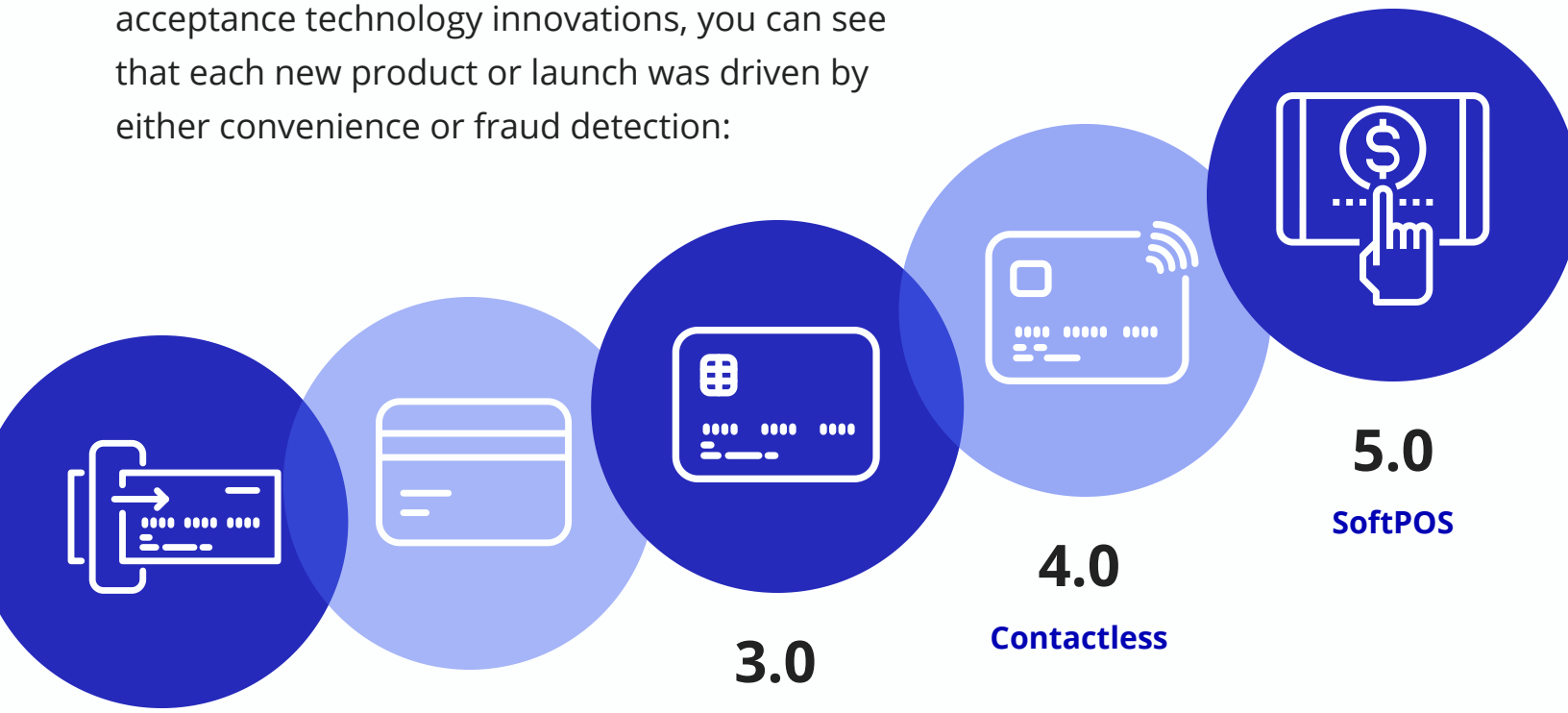
2

How do we reduce fraud?

By making payments more secure, cost is driven out of the system and consumer trust is increased (which, in turn, means that more people will make payments on a trustworthy, secure platform).

Evolution of Card Acceptance

Looking at this timeline of card payment acceptance technology innovations, you can see that each new product or launch was driven by either convenience or fraud detection:



1.0
Zip zap

2.0[2]
Magstripe

3.0
EMV Chip

4.0
Contactless

5.0
SoftPOS

At each stage of evolution, industry stakeholders are tasked with defining the rules and specification to maintain the security and interoperability of the payment networks. Given SoftPOS changes from an established and trusted security model to a new approach, this is more important than ever.

[2] The original mPOS products can be considered evolutions of Magstripe, EMV or Contactless acceptance

Contactless Payments on COTS (AKA Tap-To-Phone)

As the name suggests, Tap-to-Phone is a Point of Sale implementation that allows any Android phone to take tap-to-pay NFC payments from a contactless card (or device) for goods and services, under the contactless transaction value limit. In this use-case, the transaction values are restricted and therefore a further level of authentication (PIN) is not required, there is no provision for PIN-entry in the software or on the device.

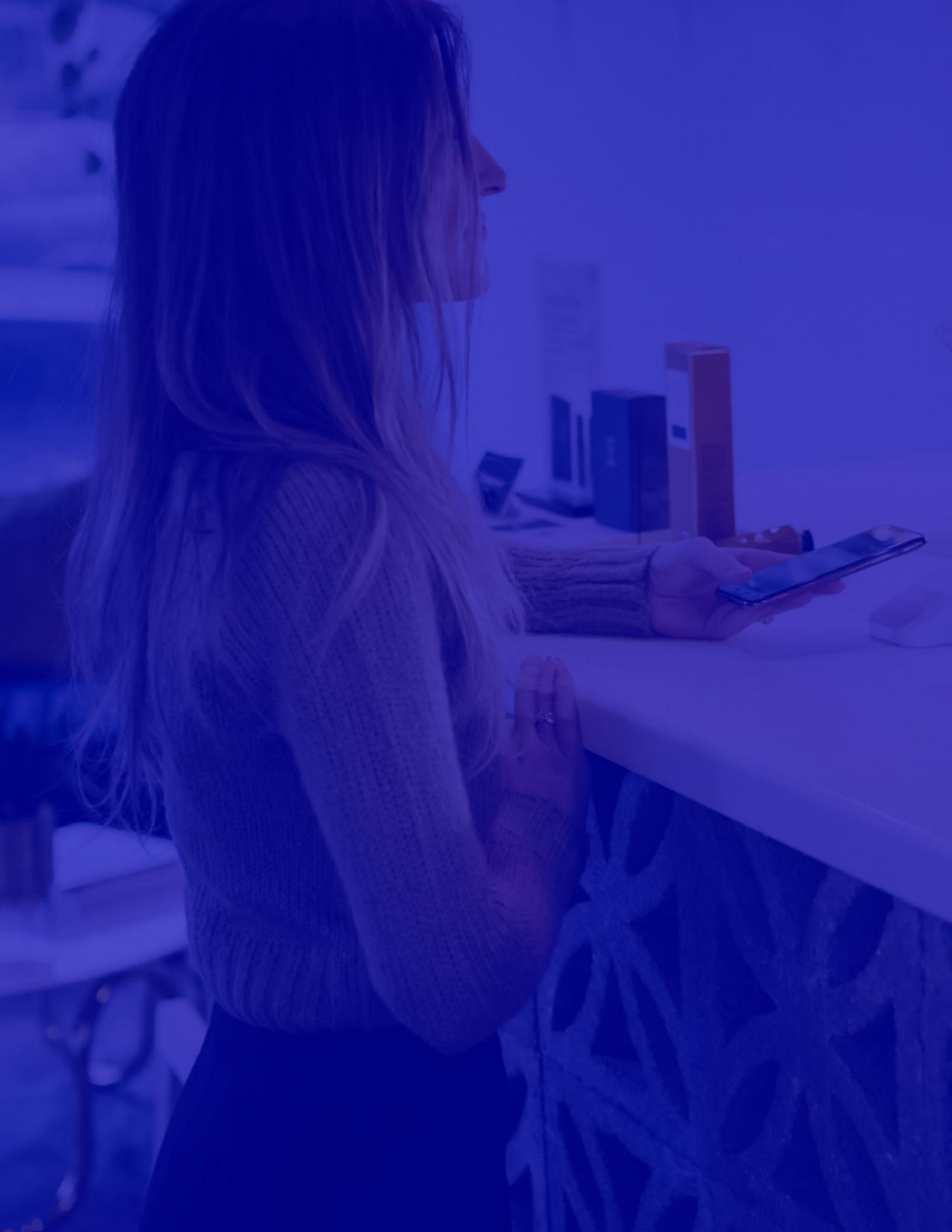
Contactless payment is now the preferred way for consumers to pay in-store – a trend that has accelerated quickly due to the global pandemic. Reducing the need for merchants to be compelled to accept magstripe or contact-chip transactions.

Given the transaction value limits, the most likely retail uses initially for Tap-to-Phone will be for low value, fast transactions: coffee shops and food trucks, newspaper stands, market traders and even charity donations.

There is an exception to transaction value limits. This is when the payment device supports verifying the cardholder. This is a technique known as Consumer Device-Cardholder Verification Method (CD-CVM). This is possible from mobile wallets and the new generation of credit cards that have a built-in fingerprint scanner.

Since Tap-to-Phone is a 100% software solution, there is potential for traditional buyers of POS terminals to develop solutions for themselves, rather than waiting for their traditional hardware vendors to catch up.

If we stretch the definition slightly, it is clear that many self-service panels appearing in fast-food and other high footfall, low transaction value sites, can benefit from the ability to take a contactless payment.



Protecting Transactions on COTS with App Shielding Solutions

Tap-to-phone raises massive security questions. There is a move from an established and trusted security model to a new model that has not been seen before in the POS market. Of course, mobile payments and the associated security have been proven elsewhere – such as HCE cloud-based payments.

Like HCE, Tap-to-Phone has all of the transaction processing within the mobile app, on the same mobile device which the merchant will do his own Mobile Banking, messaging via WhatsApp and play Fortnite. This demands that the transaction flows and the processing of the transaction be secure and ring-fenced. Exactly as with certified secure HCE Payment Applications.

Operating on COTS devices means that the payment processing cryptography must be performed in a pure software environment – which requires whitebox cryptography and wider app shielding technologies. Without this hardening, the SoftPOS application will be vulnerable to attack and payment processing will be exposed.

For added assurance that the components in the solution are in a secure state, an Attestation framework is required. This needs to have the ability to react and mitigate risks to the overall security of the solution – checking the application and runtime environment.

The Attestation framework is split into two parts: the application running on the COTS device and a back-end server. Firstly, the application will perform local Attestation of the runtime environment (type 1), taking action to mitigate any immediate threats – Application Shielding Environmental Checks can provide this functionality. These checks can either be run at predetermined times and events or upon request of the server with the result sent to the server as proof. Secondly, runtime monitoring data will be collected and sent to the server component for independent verification (type 2).

Software-Based PIN Entry COTS (AKA Pin-On-Glass)

The payment industry felt much excitement – and a degree of trepidation – in 2018 when PCI's Software based PIN entry on COTS specification was released. Dedicated, expensive hardware would no longer be needed to accept a cardholder's PIN and authorize a transaction. A consumer's PIN could now be entered onto the touch screen of an off-the-shelf smart device. This became known as "PIN-on-Glass".

Implementing PIN-on-Glass allows mPOS vendors to greatly reduce their bill-of-parts. The dedicated hardware can be scaled back and much more of the solution can be implemented in software.

Another market segment that will be revolutionized by PIN-on-Glass is the self-service kiosk. This market is expected to grow by $2.29bn in the next four years[4] . In the short term, this is where PIN-on-Glass can have the most impact.

The majority of self-service kiosks deployed today have two components:

1 **The large touch screen where a consumer places their order**

2 **A separate card terminal for taking payment**

The touch screen is bright, shiny and very appealing to consumers. This makes it quick and easy to place an order, while providing an interactive environment that allows the merchant to analyse how consumers interact with the platform and target directed upsell opportunities. Specialists in the space claim that they are able to increase the average transaction size by 20% to 30%.

[4] https://www.researchandmarkets.com/reports/4894510/global-self-service-kiosk-market-2020-2024

Software-Based PIN Entry COTS (AKA Pin-On-Glass)

One example of an upsell opportunity enabled by this technology is a fast food restaurant that rearranges menus to direct diners into purchasing combinations for larger profits.

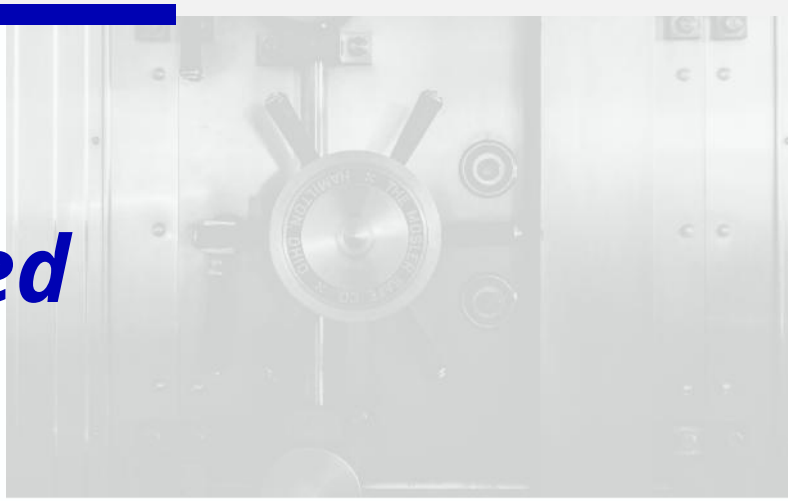
However, the separate card reader is an awkward addition to this scenario. It's expensive, adding a hefty amount to the bill of parts. More importantly, it breaks the consumer's eye contact with touch screen. Any UX expert will tell you that the split screen approach is detrimental to user engagement.

"One of the basic foundational design principles is KISS (Keep it Simple Stupid) and Less is More. A good user experience is one where anyone can easily find what they need to do." says Verimatrix's resident UX expert Renee Testa. "This is difficult to accomplish when a user has to shift focus between multiple devices to perform an action, such as placing an order and paying for it. Having a single device to interact with allows the customer to focus in one place and maintain context throughout their experience. Contextualization helps prevent users from getting lost in their interactions and enables them to complete the experience quickly and successfully. When consumers experience a positive interaction with any product, this results in a positive brand awareness – and increased revenue."

With PIN-on-Glass, there is no need to separate a keypad and screen for accepting payments. Scaling the dedicated POS terminal down to a simple secure card reader and utilising the kiosk's touch screen for PIN entry not only reduces costs but creates a much stronger experience for the consumer. The confusing redirection is eliminated, and the consumer remains engaged on the touch screen.

Rules & Regulations

PCI is the industry body tasked with defining and enforcing the security standards for PIN-on-Glass[5]. Before any solution can be deployed, it must first be approved by PCI. This includes evaluation by an independent security lab.



The PCI security objective is stated very clearly as:

"...to provide reasonable assurance that Software-based PIN CVM Solutions provide adequate security mechanisms, controls and mitigations to protect the consumer's cardholder data, PIN and other assets - e.g., cryptographic keys, correlatable data, etc.—from unauthorized disclosure, modification or misuse by providing an attack surface that may be perceived as uneconomic for an attacker to penetrate.

It is recognized that an attacker may have other objectives - e.g., self-promotion, nation-state attack, etc. - and may expend more resources to circumvent established controls than is warranted by the direct financial fraud payback.

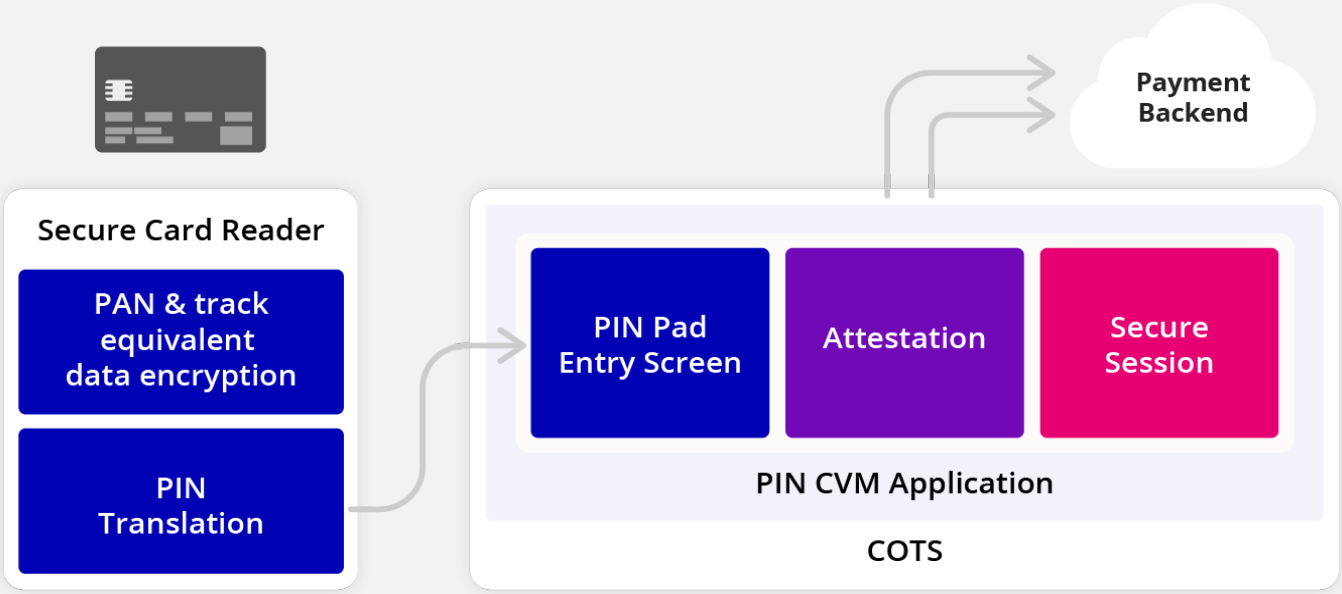
For the COTS components, the objective of these security requirements is to provide reasonable assurance that these components have been kept up to date and have not been modified from what had been deployed by the COTS provider."

5 https://blog.pcisecuritystandards.org/new-pci-software-pin-entry-on-cots-standard

Rules & Regulations

The card's PIN is a highly valuable security asset. PIN-on-Glass starts from the principle of "separating church & state".

The "church" in this case is the PIN and the "state" being the credentials for the card managed by that PIN. If an attacker can't know both at the same time, the risk is greatly reduced.



This is the same reason PCI's Tap-to-Phone specifications do not yet allow PIN entry.

When it comes to PIN-on-Glass. The transaction (and so card details) are handled by a Secure Card Reader; and so never seen by the device and software controlling the "glass".

This approach leaves the software free to focus on managing the user interaction and capturing the PIN entry.

Protecting Transactions on SPOC with App Shielding Solutions

Operating on COTS devices means that the cryptography must be performed in a pure software environment – which requires whitebox cryptography and wider app shielding technologies. Without this hardening, the SoftPOS application will be vulnerable to attack and payment processing will be exposed.

Ensuring the runtime environment has not been compromised is an important component ensuring that malicious software is not recording PIN entry. Environment Checks provided by App Shielding allows the SPOC software to monitor the environment directly. The SPOC security requirements go further and mandate Device Attestation. This is where an external server monitors the security of the device. This is achieved through a security agent in the software sending analytics data to server for processing. App Shielding is required to protect the integrity of the security agent, stopping a malicious actor from spoofing the data and so compromising the integrity of the client software and device.

Combining SPOC & CPOC

As the specifications currently stand, Contactless Payments on COTS and Software-based PIN Entry on COTS are mutually exclusive.

That does not stop vendors seeing the target as quickly merging PIN-on-Glass and Tap-to-Phone functionality to create a fully-featured SoftPOS. Essentially, this would allow a smartphone to fully replace a dedicated POS terminal for all contactless payments. This is particularly compelling in markets that support Online PIN; where any value of transaction could be approved with a PIN after a contactless payment “tap”.

With it not being possible to combine CPOC and SPOC today, the payment schemes have been running waiver programs to support the vendors and the wider market. This gives vendors special dispensation to support PIN entry with CPOC. The vendor still has to go through extensive security evaluation with an independent lab to demonstrate that they have made their best efforts to keep the account and the PIN data separate within the implementation.

Maintaining Security & Minimizing Fraud

The good news is that the principles of POS running on a software platform is pretty much the flipside of the existing, proven and certified mobile payments (HCE) technology. Exactly the same tools that are able to deliver certifiable solutions, without additional hardware on the mobile device, can be used.

Verimatrix has brought its expertise to banks building issuer wallets over the last 8 years; and the company now brings these solutions to technology vendors, Point of Sale manufacturers, and payment processors who are making the switch to SoftPOS.

Application Hardening

A fundamental requirement from both PCI and the payment schemes is to harden the mobile application implementing the CPOC and PIN Entry functionality.

Amongst other things, this is to stop:

- Reverse engineering of the application
- "Man in the device" style attacks
- Side channel attacks to extract cryptographic keys

Code Protection and Whitebox have been used in the mobile payment space for many years and have demonstrated their ability to meet the security level requirement here through repeated independent lab evaluations.

To meet these tough requirements, protection needs to be injected directly into the code so it integrates tightly with functional logic.

The required protection includes:

- Strong obfuscation of code logic;
- Environmental checks that are constantly running (including during any on-device transaction processing) validating the runtime environment as the code executes – allowing for detection of dynamic (asynchronous) compromises.
  These include checking for:
  - Rooted devices (including Magisk Hide)
  - Emulation
  - Debuggers attaching to the process
    Hooking frameworks (e.g. Frida)
- Anti-tamper check network interleaved with functional code to constantly check the integrity of the app package, code and security measures.

Cryptographic Protection

Modern payment infrastructure is based on cryptographic challenge-response to sign (authorize) transactions.

By definition, building a true SoftPOS means the terminal side cryptography must be performed in purely software while keeping the cryptographic algorithms and cryptographic keys safe.

The keys are the secret to unlocking the payment cryptography. Therefore, they must not be exposed to an attacker. The proven approach for this is Whitebox Cryptography.

Not all Whiteboxes are created equal, so it is important to consider how the chosen solution performs in the real world. For SoftPOS, there are three factors to look at:

PERFORMANCE

1 Transaction speed is very important to the payment experience – a slow transaction leaves consumers feeling awkward waiting for the confirmation screen. It is critical to make sure that the whiteboxes are designed and tuned to match the use case to avoid wasted code or CPU cycles.

SECURITY

2 Certification will not be achieved if the whiteboxes cannot withstand attack. Therefore, it is important that the chosen solution can withstand the attacks the security labs will subject it to – typically lifting, reverse engineering, Differential Fault Injection (DFI) and Differential Computational Analysis (DCA). A vendor having previous experience with payment certification is often invaluable for smoothing the security certification.

CONTROL

3 The entity that generates the whitebox “owns” the static key (sometimes called the root key) dissolved into the whitebox. That means the chain of trust stops with the whitebox generator. It is good security practice to ensure that the chain stops with the SoftPOS developer and not the whitebox technology vendor.

PIN Entry

Security requirements around PIN Entry require that it be kept logically separated from card data. This is tricky within a single mobile app that is also implementing CPOC. It is one of the reasons that PIN Entry is under waiver when combined with CPOC.

Even when operating under waiver, it is important to achieve as much separation as possible. This often involves using separate whiteboxes for PIN handling to any CPOC processing, time separating when PIN and card data are present in memory and ensuring code protection environmental checks run regularly during PIN Entry.

Device Attestation

The first line of defence should always be to terminate the application execution as soon as it is under attack – nullifying the risk. This is achieved through App Shielding and it works even when an attacker has turned off the device's internet connection.

As a second line of defence, PCI requires that all active devices are monitored through an Attestation service. This provides alerts if an attacker manages to bypass part of the built-in protection, and for additional decision-making based risk indicators that do not constitute a direct attack on the app.

Device Attestation consists of three parts: data capture on the device, a secure channel, and a back-end server to process the data.

As with any computer system, the results are only as good as the data. For Device Attestation that includes:

- Mobile application and configuration modification or tamper.
  By extension that covers:
  - The state of possible 3rd party libraries within the application
  - Code executing out-of-context (e.g. through a lifting attack)
  - The cryptographic keys (including those dissolved in whiteboxes)
  - The application signing key
- Application repackaging detection
- Application execution in debug mode
- Use of a hooking framework
- Running the application on an emulator
- Metadata about the device and application

Device Attestation

As can be seen, there are commonalities between the attestation data collected and the threats a good code protection solution will react to. Callbacks from an enterprise-grade code protection tool are often the most trustworthy source of this information – the data collection is firmly anchored to the rest of the software, making it hard for an attacker to manipulate. For Attestation to be valuable, the data integrity must be guaranteed in this way.

On the backend, the server will process the data looking for high risk SoftPOS instances. The insights gleaned from monitoring the data need to be actionable. Therefore, integration with payment processing systems is required; allowing appropriate risk management to be taken when the integrity of a transaction or the SoftPOS device it originates from is in doubt.

Point of Sale v6.0

Looking further ahead, in-store payments will change dramatically in the coming years and decades.

Today, most in-store payments run over the rails provided by the card networks. While they continue to take market share from cash and checks, the next wave of disruption is coming quickly in the form of account-to-account (A2A) payments. This is the reason Mastercard acquired Vocalink in 2016; and Visa announced a partnership with Vipps in 2020.

A2A allows an up-to-date, flexible payment infrastructure to be built using modern internet technologies. It will lower costs, speed up settlement time and empower innovation.

The challenge that A2A has is Universality.

Payments is an all-or-nothing business. Consumers will not adopt a new way of paying unless they can use it at most merchants. Where there is doubt in a consumer's mind, they will fall back to a payment method they are confident will be accepted. Equally, there is little benefit to merchants accepting a payment method if there are no customers using it. The existing card networks have universality, and it is a large hurdle for innovation to overcome.

Arguably, it is markets without incumbent electronic payment that has seen the most innovation in recent years – for example, M-Pesa in Kenya and WePay in China.

Mobile provides a migration path, a tool for achieving universality while also supporting innovation. SoftPOS has a large part to play in this.

Point of Sale v6.0

Being pure software, a SoftPOS can be upgraded over the air to accept new payment methods while maintaining support for legacy systems. Equally, a digital wallet can be easily expanded by its provider. Solutions can start by operating on existing rails; and then transparent to the user, can automatically switch to new infrastructure where it is available – making the best choice for each transaction at the point of sale. Over time, the old system will disappear, and the consumers and merchants will be none-the-wiser.

It is this vision that makes Apple's recent acquisition of MobeeWave so interesting. How does Apple Pay develop in the coming years with Apple controlling both the payment device and the acceptance terminal?

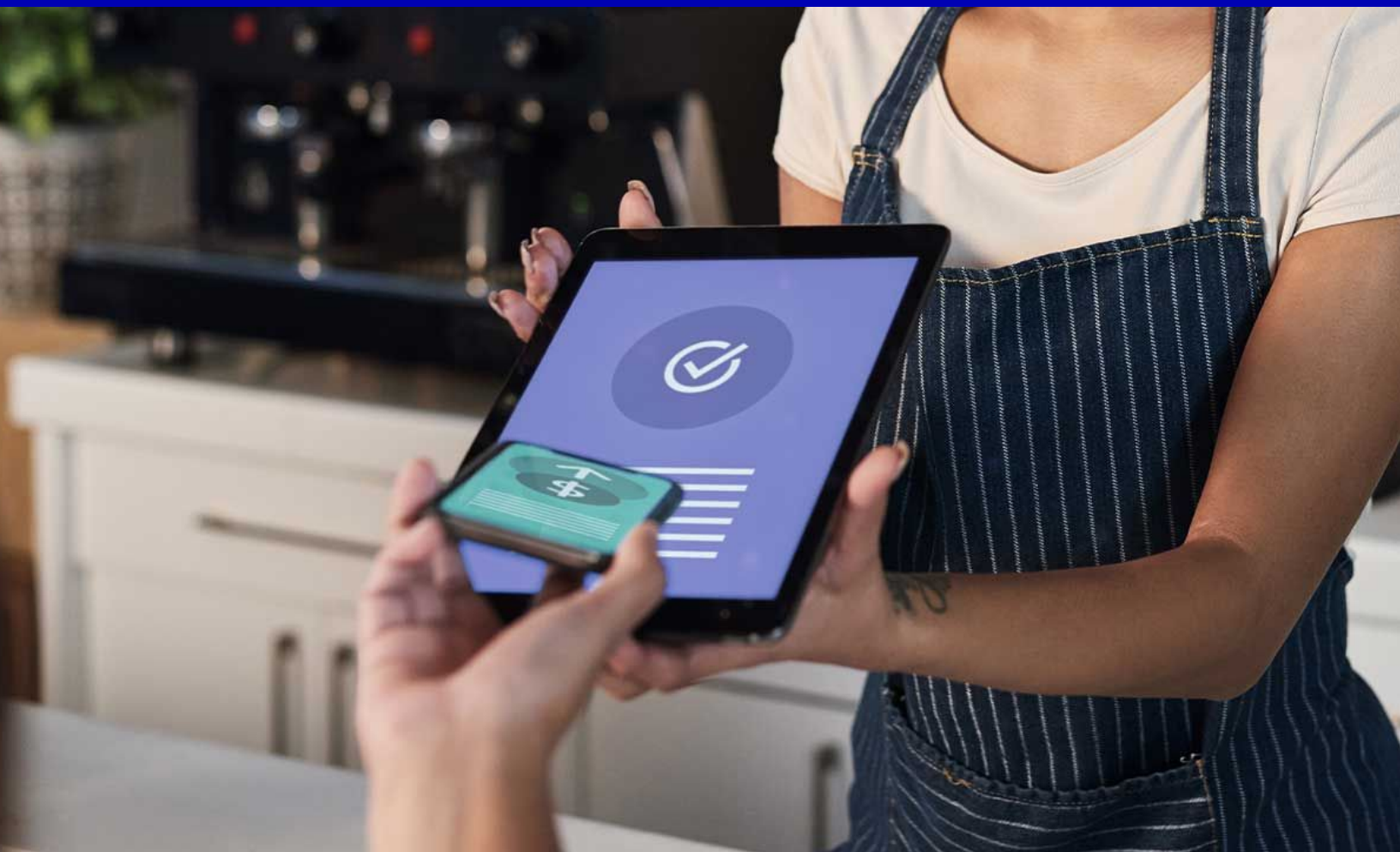
Conclusion

Driven by a demand for card acceptance amongst new segments of retailers, a whole new market has opened up on the Acquiring side of mobile payments; for small merchants through to some of the largest, and the developers supporting them.

It has almost been a decade since Digital Wallets started adopting software security. This has given a safe platform for imaginations to flourish and innovations to come to market quickly.

By embracing new security models and Application Shielding, the same is possible for the SoftPOS market.

The flexibility of software means that the current incarnation of SoftPOS specifications is only the beginning. The rate of innovation will accelerate, and it will be exciting to see how payments evolve over the next decade.



Where does Verimatrix come in?

Verimatrix's suite of shielding products empowers developers with tools that are proven against the PCI specifications, giving them confidence when it comes to security lab approvals and certification processes. While Verimatrix's experience with payment security means it is the ideal security partner for anyone developing SoftPOS solutions.

Code Protection Tool - Meet the Toughest Industries' Requirements with Proven Security:

Verimatrix Code Protection includes obfuscation, environmental checks, jailbreak and root detection, anti-tamper technology that meet the strict security requirements of the most regulated industries. This automated solution helps SoftPOS developers achieve compliance with stringent regulations such as PCI's CPOC and SPOC standards.

Our intelligent analytics platform provides real-time, in-depth analysis of the risk profile of your mobile apps. Performing early detection and alerting you when hackers attempt to attack your application. Verimatrix helps you understand the threat profile of your install base, drill down into the risk score of an individual app instance and ultimately mitigate risks before your ecosystem is compromised. Setup is easy with no-code integration to security monitoring.

Whitebox Tool - Advanced Engineering Toolkit to Enable Crypto-Security for Apps:

Exposed cryptographic keys are a known vulnerability in app code. Verimatrix's Whitebox effectively dissolves keys into the code itself and obscures algorithms to keep critical applications and data safe – even if a hacker has complete access to the device on which the algorithms are executing. This is why CTOs and chief compliance officers at many of the world's leading banks use Verimatrix Whitebox to shield their consumer-facing apps from attack. Verimatrix Whitebox provides state of the art protection crypto data as required by PCI.

About Verimatrix

Verimatrix (Euronext Paris: VMX) helps power the modern connected world with security made for people. We protect digital content, applications, and devices with intuitive, people-centered and frictionless security. Leading brands turn to Verimatrix to secure everything from premium movies and live streaming sports, to sensitive financial and healthcare data, to mission-critical mobile applications. We enable the trusted connections our customers depend on to deliver compelling content and experiences to millions of consumers around the world. Verimatrix helps partners to get to market faster, scale easily, protect valuable revenue streams, and win new business.

verimatrix
DRIVING TRUST

SoftPOS Glossary

Point of Sale (Merchant)
A generic term for systems used by merchants to manage the purchase of their goods and services. These may be as simple as a Cash Register or as complex as fully automated stores such as Amazon Go.

Point of Sale (Cards industry)
Point of Sale or (POS) in the card market refers to the mechanisms in place at merchants to read and receive payments from payment cards.

Point of Sale Terminal (Cards industry)
A POS Terminal is the device the consumer tap, inserts or swipes their debit or credit card against.

ePOS
An Electronic Point of Sale (ePOS) is a modern Cash Register that is connected to a merchant's wider systems for managing stock and customer relationships.

mPOS
Market pioneered by Square and iZettle. Mobile Point of Sale (mPOS) gives the ability to receive card payments on a standard mobile device. Traditionally this uses an accessory to securely manage a "chip" transaction and accept the card holder's PIN.

Queue Busting
Use of mobile POS devices, remote from the counter on the shopfloor at retail, entertainment and transit. Given merchants extra POS capacity at busy times without needing physical infrastructure.

Software-based PIN Entry Payments on COTS (SPOC)
Also known as PIN-on-Glass. This is a new PCI standard allowing mobile devices to become payment terminals. These can read chip-cards via a secure card-reader and take payments above the contactless limits when the PIN is entered on the device screen.

Contactless Payments on COTS (CPOC)
Also known as Tap-to-Phone. A simpler model than the traditional mPOS; allowing payments to be taken on a standard mobile device without any accessory. In this case via the NFC within the device. Payments are limited to the contactless value set by the country in which it is used.

SoftPOS
A subset of mPOS, where the Point of Sale Terminal is implemented entirely in software to provide one or both of CPOC or SPOC.

Consumer of the Shelf Device (COTS)
Standard consumer electronics hardware, rather than dedicated payment hardware. A typical example is an Android smartphone.