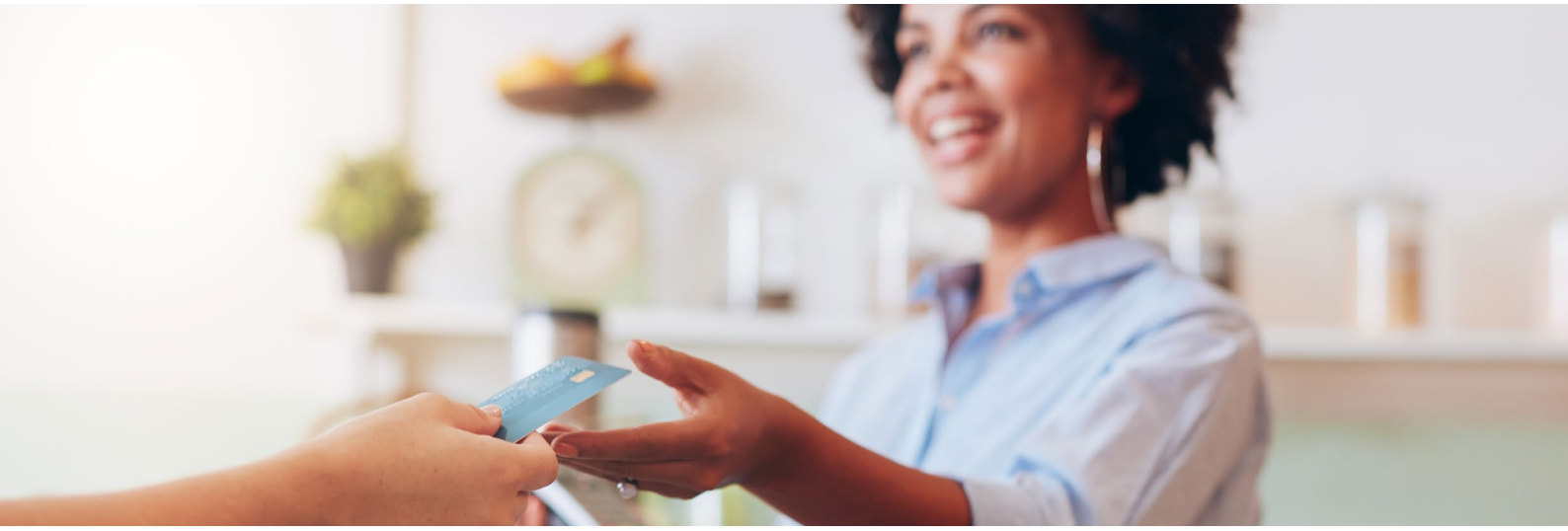
IMPLEMENTING SMART POINT OF SALE (SMARTPOS) DEVICES

INSIGHTS FROM TECHNOLOGIES TO APPLICATION MARKETPLACES

EXECUTIVE SUMMARY



Since they were first introduced, POS terminals have evolved into powerful devices that intend not only to accept payment cards and process transactions, but offer a broad range of non-payment services helping merchants in their business. These new types of POS are usually called SmartPOS.

SmartPOS terminals are intended to offer not only standard payment applications but also provide merchants access to a range of applications to support their business. However, POS vendors and acquirers are not always able to offer a range of payments technologies or value added services flexible and diverse enough to suit the needs of each and every merchant. Merchants are extremely diverse in their nature, and it is difficult to understand their businesses well enough to offer specific value added services and applications.

This white paper takes a closer look at SmartPOS terminals. We will define the main components and features of SmartPOS, discuss the main consideration points in regards of change in business models, security risks, and architecture implementation. In addition, we will discuss the different models of implementing the POS App Marketplace and the need and approach of an application validation process.

IMPLEMENTING SMART POINT OF SALE (SMARTPOS) DEVICES

INSIGHTS FROM TECHNOLOGIES TO APPLICATION MARKETPLACES

INTRODUCTION

Point-of-sale (POS) terminals have become popular for delivering a range of new services for merchants and customers. What were once simple card-reading and transaction capture machines are now complex computing devices. They are capable of not only performing transactions, but also managing inventories and running business applications. Nowadays, POS terminals are required to communicate faster and easier, to support several concurrent applications, and handle different card types (credit and debit cards, loyalty cards, etc.). Modern POS terminals have an attractive design, touch-screen interface, and offer connectivity features that facilitate their integration into the merchant's environment. In much the same way feature phones evolved to smartphones by gaining functionalities that go far beyond simply making calls, POS terminals have evolved into the so called "SmartPOS", allowing merchants to benefit from features far beyond simply performing transactions.

SmartPOS terminals are intended to offer not only standard payment applications but also provide merchants access to a range of applications to support their business. However, POS vendors and acquirers are not always able to offer a range of payments technologies or value added services flexible and diverse enough to suit the needs of each and every merchant. Merchants are extremely diverse in their nature, and it is difficult to understand their businesses well enough to offer specific value added services and applications. Even if POS vendors and acquirers do understand such needs, there is a natural limitation on the number of applications that they can develop per year. Additionally, the costs for specifying, developing, testing, and maintaining a complete portfolio of POS value added applications may be economically unfeasible. This is just one of the reasons why it is difficult for POS vendors and acquirers to serve small and medium sized merchants with uniquely tailored services and solutions.

To overcome this limitation, SmartPOS terminals enable merchants to use not only applications provided by the POS vendors and/or by acquirers but to download applications developed by 3rd party providers that are tailored to their needs. This is facilitated by creating a platform for POS applications - The POS Application Marketplace. Through opening the SmartPOS to 3rd party providers there is a many-to-many mapping of developers to merchants, increasing the collective manpower and creativity to design relevant services for merchants and eventually for the customers. This approach enables an ecosystem which drives innovation in commerce and nurtures business, similar to what happened with the app stores for smartphones.

This white paper takes a closer look at SmartPOS terminals. We will define the main components and features of SmartPOS, discuss the main consideration points in regards of change in business models, security risks, and architecture implementation. In addition, we will discuss the different models of implementing the POS App Marketplace and the need and approach of an application validation process.

1. WHAT IS SMARTPOS?

Before diving into SmartPOS specifics, we need to align the definition of SmartPOS and to understand how it differs from a typical POS. To begin, we will briefly discuss the evolution of POS. We will then discuss the additions to a typical POS, introduced by SmartPOS, which will form our understanding of the nature of SmartPOS.

1.1 POS HISTORY AND DEFINITION

Much has changed in the way customers pay in shops or restaurants. POS terminals have undergone several transformations before reaching the functionality and look we are so familiar with now. Prior to the development of payment terminals, merchants used the so called manual imprinters. With the help of these machines merchants imprinted the information of the payment card onto a paper slip and then mailed this slip to the customer's bank for processing. This process was time consuming and did not offer the instant transfer capabilities that are now standard. The first payment card authorizations were done over the phone. This usually took up to 5 minutes. Due to the wait, this solution was not a preferred one either.

The first point-of-sale (POS) terminal emerged in 1979, when Visa introduced a bulky electronic data capturing terminal. This was the first credit card terminal, very similar to the ones we know today.

In 1983 an electronics company from Hawaii, currently known as Verifone, introduced the ZON terminal series. This terminal set the standard for all credit card terminals, and is still being used by many merchants to this day; Verifone is now one of the largest manufacturers of processing terminals in the world.

Verifone's primary global competitor was Hypercom. In 1982 Hypercom started producing dedicated payment terminals and became the largest terminal vendor in the South Pacific region. Another big player emerged in 1994, Israeli based Lipman Electronic Engineering, Ltd. Verifone later acquired both of these major competitors, acquiring Lipman in 2006 and the payment part of the Hypercom business in 2011.

Verifone, Hypercom, and Lipman were the big three equipment manufacturers, but there were other important companies that produced processing equipment. Thales, Ingenico, Schlumberger, and Linkpoint are a few of the larger companies.

Apriva, Comstar, and eProcessingNetwork were smaller and specialized in wireless technologies.

Since 1979, POS terminals have only improved, particularly in the areas of security, performance, and reliability. However, while in the changes in TVs, mobile phones, tablets and wearables are clearly visible, POS devices from the 1990s look very similar to those found on store shelves today. Starting in the 2010s, POS vendors began looking into improving user interface and developing additional services to enrich their offer, leading to mPOS and SmartPOS.

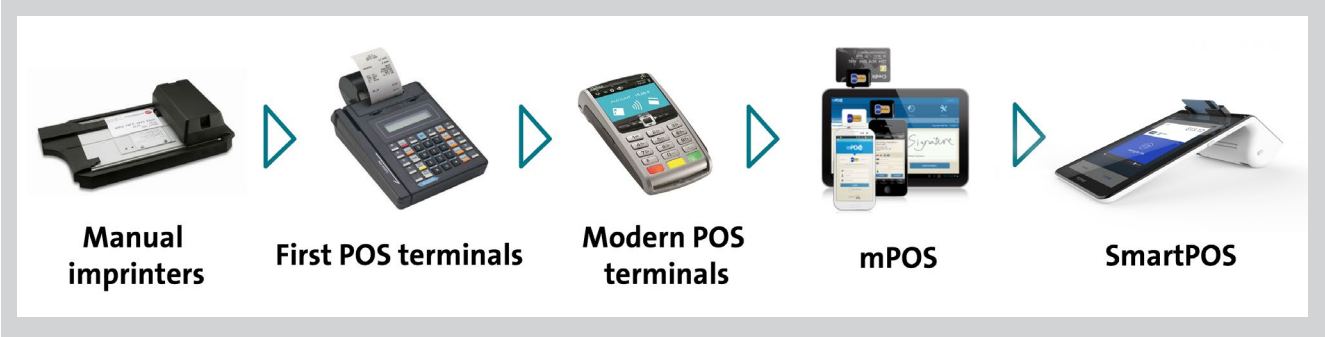


Figure 1. Checkout process from the customer point of view

Nowadays we refer to a POS terminal as a device that interfaces with a payment card to make electronic funds transfer. A more formal definition of POS is provided by EMVCo[1]:

"The device used in conjunction with ICC (A/N: that is an EMV compliant chip based payment card) at the point of transaction to perform a financial transaction. The terminal incorporates the interface device and may also include other components and interfaces such as host communications".

Modern POS terminals, usually called SmartPOS terminals, offer services that are far beyond typical POS services. This change in functionality and role in the merchant's business is clearly indicated by the new terminology introduced by Payment Card Industry Security Standards Council - PCI SSC (more details about PCI SSC can be found in Section 3.3). To incorporate the expanded functionalities of SmartPOS, PCI SSC now refers to the POS terminal as Point-Of-Interaction (POI) systems. The definition of POI is the following[2]:

"A POI is an electronic-transaction-acceptance product. A POI consists of hardware and software and is hosted in acceptance equipment to enable a cardholder to perform a card transaction. Thereby the POI may be attended or unattended. POI transactions include IC, magnetic-stripe, and contactless payment-card-based payment transactions".

However, neither of these definitions fully represent the nature of SmartPOS.

SmartPOS is inherently a POS device and embraces all its requirements and functionalities. Furthermore, SmartPOS offers services beyond payments. This adds further requirements to its hardware and software, and introduces new security considerations and increases integration efforts.

The following sections provide a more detailed description of the main components and features of SmartPOS and how it compares to a typical POS.

1.2 MAIN COMPONENTS OF POS

A typical POS terminal, as well as SmartPOS, consists of two main components: hardware and software (see Figure 2). In the following sections we will discuss each of the components and list the additional hardware and/or software components that were introduced by SmartPOS.

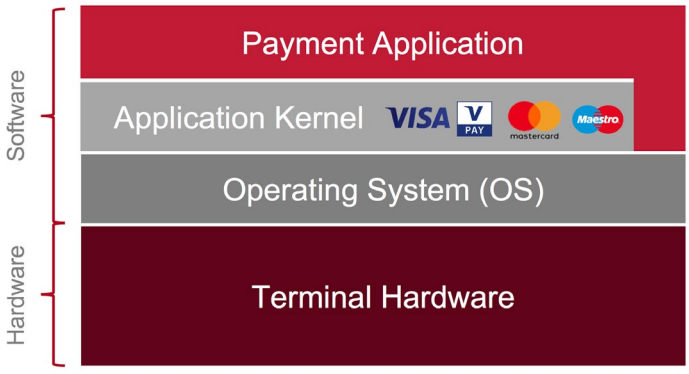


Figure 2. Typical POS components

[1] Source: https://www.emvco.com/
[2] Source: https://www.pcisecuritystandards.org/

1.2.1 Hardware Components

Typically, the POS terminal includes hardware components such as card readers, PIN Pad, receipt printer, and display as shown in Figure 3.

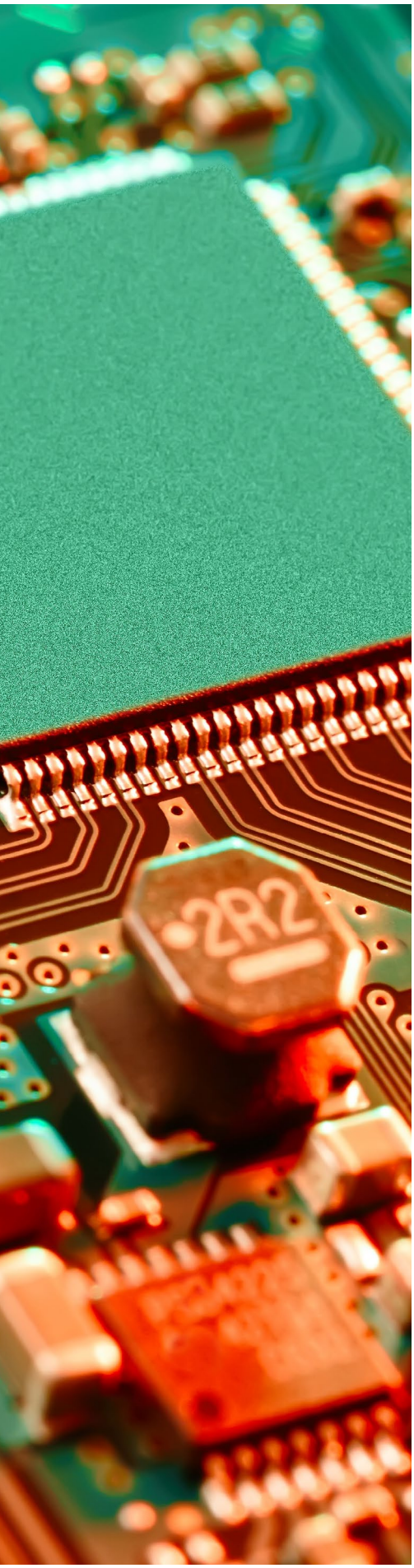
Figure 3. Typical POS terminal hardware components

Looking more broadly at the merchant's environment, a typical POS terminal is just one of many devices that are utilized. Other devices that are usually present in the merchant's environment are:

- Cash register that is an electronic device for registering and calculating transactions. The amount of a transaction is transferred to the POS terminal for the electronic payment transactions. Modern cash registers allow merchants to perform product and inventory management, employee management, sales reporting, and other functions.
- Additional customer facing devices that display the product database. It may also enable other services, such as employee clock-in and viewing sales reports.
- Any other devices like computers and tablets.

With this variety of devices any usual customer has faced at least one situation in a store when first they were directed to a monitor to check if a desired product is in stock. Later, they had to follow the store employee to a different place to provide the information needed for a delivery service, and then finally go to the cashier to pay for the purchase. SmartPOS intends to combine all the above devices into one device as shown in Figure 4.

Figure 4. SmartPOS hardware components



By combining all the devices present at the merchant's counter into a single device with a modern design and powerful and feature-rich hardware capabilities, SmartPOS provides evident benefits to merchants like:

- Aggregates all the functionality that is typically offered by the cash register and other merchant's devices into a single device. This facilitates the customer buying experience, introduces new services to the customer, and optimizes the merchant process.
- Modern design enhances user experience.
- Mobility enables the cashier to bring the POS to the customer and accept orders anywhere in or even out of the merchant's store.

1.2.2 Software Components

Typical POS software components, as well as those found in SmartPOS, include operating system, application kernel and payment application layers (see Figure 2). The operating system is a set of programs that manage the POS or SmartPOS hardware components and provide common services for application software. Application kernel and payment application implement all functions associated with accepting and processing transactions, including storage and transmission of sensitive card data.

Beyond payment services offered by SmartPOS are enabled by non-payment applications. These applications can be developed by SmartPOS vendors and acquirers as well as by 3rd party developers. Usually, non-payment applications are grouped in the POS App Marketplace. Introducing the POS App Marketplace may affect the SmartPOS architecture - we'll discuss these possible architecture options in Section 3.2. Examples of possible services that can be offered with SmartPOS are listed below:

- Product management including automatic sales price calculation based on rules, tracking stock counts, automatically stop selling products when inventory runs out, and ability to offer different versions of the products (such as multiple sizes, colors, materials, expiry dates, etc.).
- Product information including in-depth information about the products with references to related items, cross-selling and up-selling suggestions, and sales tips.
- Know-your-customer services including customers' order histories of both in-store or online shopping, customer loyalty programs, customer information, and more.
- Real-time analytics including unlimited number of KPIs and customized reports that would allow management to analyze and gain insight into the store's growth and analyze sales by staff members, location, time period, or customers.
- Employee management including setting employees' schedules, assign permissions, and allow them to clock in and out of work on the POS system.
- Inventory management including monitoring stock levels and low stock alerts.

2. SMARTPOS: TECHNICAL AND BUSINESS CONSIDERATIONS

By offering new services and opening SmartPOS for 3rd party application developers, some additional security risks need to be taken into account and the POS architecture and business rules must be reconsidered. In this section we first discuss the security risks that the SmartPOS introduces, then we will look at the impact on the POS architecture, and finally we will discuss whether SmartPOS has any additional requirements to the POS certification.

2.1 SECURITY RISKS IN SMARTPOS

Being effectively an enhanced POS terminal and maintaining the same core functionality, SmartPOS is subject to the same security risks as a typical POS, such as skimming, forced offline authorization, API attacks, tampering attacks, disassembling, spoofing, etc.

The enhanced functionalities of SmartPOS may also impose additional security risks. One of the most important points to consider is that SmartPOS allows installation and usage of 3rd party applications. This certainly increases the risk of installation of malicious applications. To eliminate this risk, the following actions should be taken into account:

- The applications that are downloaded and installed on the SmartPOS should be downloaded only from a trusted source like the POS App Marketplace. SmartPOS vendors should ensure that it is not possible to load applications from other sources. SmartPOS vendors may also consider implementation of application whitelisting tools that allow to run only applications that are included in the whitelist.
- The applications that are available on the POS App Marketplace shall be validated by the POS App Marketplace owner to ensure that they do not break security of the SmartPOS (see Section 4 for more details about application validation process).
- The merchant should have policies in place that would describe who is allowed to load, install and use applications on the SmartPOS. For this, SmartPOS vendors should consider a permission management system on their devices.
- The architecture of SmartPOS terminals should be developed in a way that separates the payment and non-payment applications to ensure the minimum interactions between these applications (see Section 3.2 for more details on possible SmartPOS architecture models).
- SmartPOS vendors should allow merchants to restrict the SmartPOS connection to the Internet by applying rules for internet access only for those applications and services that are explicitly allowed.

Another possible area of vulnerability concerns the integration of SmartPOS in the merchant's business. Merchants should take into account the following points while setting up the SmartPOS:

- SmartPOS configurations. Merchants should ensure SmartPOS is properly configured. In addition, merchants should avoid using default usernames and passwords on SmartPOS.
- Access management. Merchants should develop and maintain security processes and SmartPOS access management. This should include a list of employees that are allowed to load, install and use applications on the SmartPOS. Merchants should also remove access for terminated users in a timely fashion.

2.2 IMPACT ON TERMINAL ARCHITECTURE

One of the main requirements to SmartPOS remains security of the payment processing and payment sensitive data. As discussed in the previous section an important area of security consideration is allowing non-payment applications used on SmartPOS. SmartPOS vendors need to ensure that these applications do not affect the security of payment sensitive data (e.g. PAN, PIN, track1, track 2 data, etc.) which are stored, processed or transmitted by the payment application. According to PCI SSC requirements (see Section 3.3 for more details), payment and non-payment applications need to be separated to ensure that the security of the payment applications is not adversely impacted by the non-payment applications installed on the SmartPOS. There are three possible architecture models that would allow this separation:

1. Separation on the hardware level
2. Separation on the operating system (OS) level
3. Separation on the application level

Below we discuss all three options in more detail.

2.2.1 Application segregation on hardware level

One of the possible ways to ensure that the payment application's performance and processed data are not altered by any (malicious) applications is to implement a multi-platform architecture on the SmartPOS. In this case, all the sensitive payment data and payment processing should be isolated from other possible activities on the hardware level. Figure 5 shows a high level architecture of

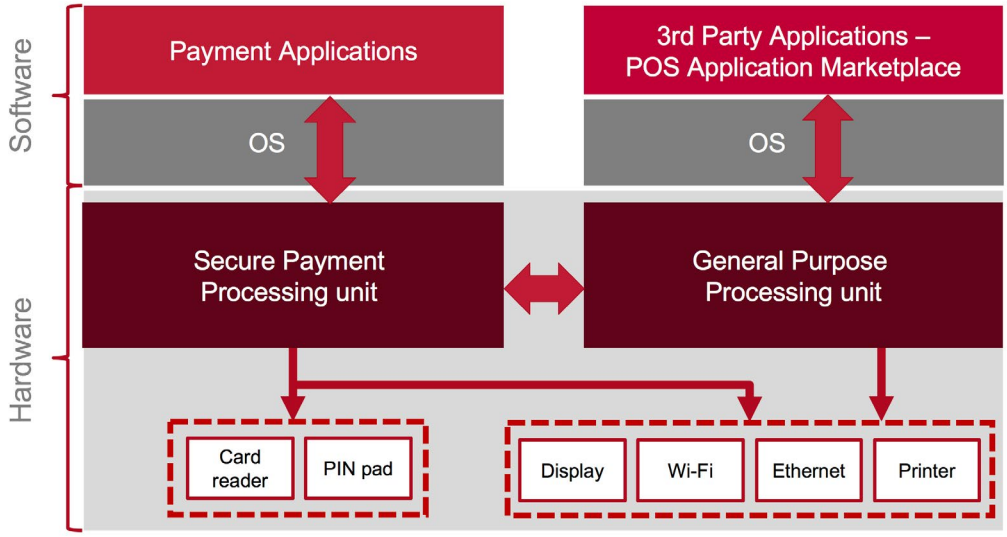


Figure 5. SmartPOS hardware segregation architecture model

the multi-platform implementation.

In this case, payment processing is performed in a completely isolated environment and non-payment applications do not have access to the sensitive payment data, card reader, and PIN pad. Some of the hardware components may be shared between both platforms like SmartPOS display, Wi-Fi, Ethernet, Printer, etc.

SmartPOS vendors may develop an interface between secure payment and general purpose processing units. This interface is usually proprietary for SmartPOS vendors and may include a limited number of functionalities. To use this interface, 3rd party providers would need to get a permission from the SmartPOS vendor.

2.2.2 Application segregation on operating system (OS) level

Separation of payment and non-payment applications on the operating system level implies using two operating systems that run on the same SmartPOS hardware. A good example of this type of architecture is using a Trusted Execution Environment

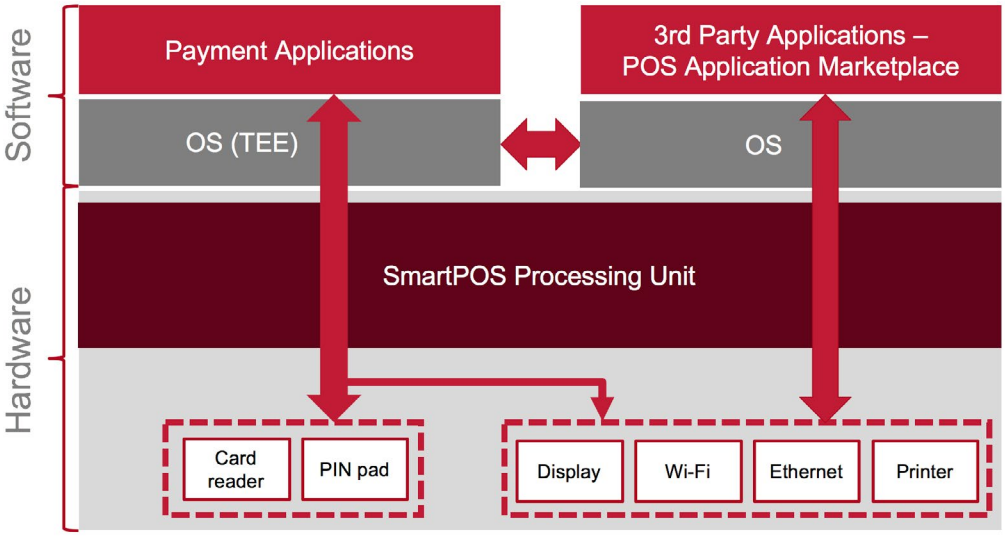


Figure 6. SmartPOS operating system segregation architecture model

(TEE). With this solution, payment data and payment processing are isolated from other applications on the operating system level. Figure 6 shows a high level architecture of this implementation.

There may be a limited application programming interface (API) between two environments that would allow to use some of the payment data for authorized non-payment applications. Similarly, to the hardware segregation approach, the use of this API will need a permission from the SmartPOS vendors.

This type of implementation is fairly common in the payment industry. There are different implementation efforts in this area (like GlobalPlatform, Trusted Computing Group, etc.). The idea of this implementation is to create an isolated environment to run the payment application and process the transaction.

2.2.3 Application segregation on software level

Another possible option to implement co-existence of payment and non-payment applications on one SmartPOS is to ensure that payment applications by themselves are robust to any tampering by other applications.

Use of APIs that would allow to communicate with payment applications should be highly secured and allowed only for authorized parties with explicit permission.

In this case, the process of loading and using of non-payment applications developed by 3rd party providers requires much higher validation and control level compared to the other SmartPOS architecture options. Figure 7 demonstrates this type of implementation.

The SmartPOS vendors should apply additional security mechanisms to ensure that the payment applications cannot be tempered by other applications installed on the device. This mechanism may include permission management system, access management system, strong antivirus and firewalls, etc.

To ensure that only authorized applications have access to the payment data, SmartPOS vendors would usually provide an SDK that is developed and signed by the SmartPOS vendors. Only this SDK would be allowed to access the payment data. In the case a non-payment application requires access to the payment data, this SDK should be embedded in this application.

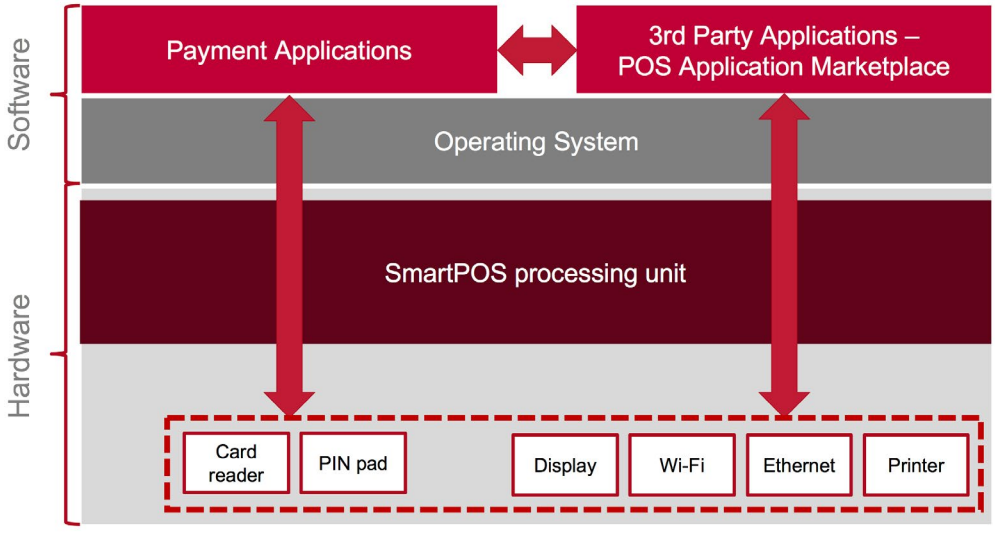


Figure 7. SmartPOS application segregation architecture model

ARCHITECTURE MODEL	SECURITY	USER EXPERIENCE	APPLICATION DEVELOPMENT
HARDWARE LEVEL SEGREGATION	Provides a better logical segregation of applications. Generally speaking, segregation on the hardware level brings less security risks than other implementations.	May impact the user experience. Payment processing and any other additional services operating on different operating systems. Smooth switch between two operating systems that is not obvious for the end user may be challenging.	Brings complexity in the application development. There may be non-payment applications that would require payment data for their services. For example, some specific loyalty calculation that is incorporated in the payment process or report and analytics services. In this case, development of such applications may become complex and in some case quite limited.
OPERATING SYSTEM LEVEL SEGREGATION	Payment applications are isolated from other applications.	Smooth switch between two environments may be challenging.	To enable authorized applications using payment data, SmartPOS should specify API between two environments. The application development may be limited by the APIs that are offered by the SmartPOS vendor.
APPLICATION LEVEL SEGREGATION	Additional security mechanisms need to be considered to ensure that the payment applications are not compromised.	Communication between applications is usually fast and smooth and does not affect user experience.	Third party applications can be easily integrated with the payment applications that may bring many added value services to the merchants

Table 1. SmartPOS architecture models comparison

Table 1 summarizes the three architecture models previously discussed.

2.2 IMPACT ON TERMINAL ARCHITECTURE

POS terminals are a target for hackers, which is why it is important to have a properly certified POS solution. The ultimate goal of these certifications is to ensure interoperability and to have a secure, robust, and reliable POS/SmartPOS terminal that can perform trouble-free transactions within the merchant's payment infrastructure.

POS certification requirements apply also to SmartPOS and can be grouped into three main groups as shown in Figure 8:

- Regulatory requirements
- Functional certification requirements
- Security certification requirements

REGULATORY REQUIREMENTS

- Legal hardware requirements for major global regions such as FCC (North America), CE (Europe), C-Tick (AUS/NZ) and also specific "incountry" requirements for countries such as Brazil, Japan, China and Korea. In general, these requirements cover radio performance, EMC and safety testing. However, the exact standards that are applied depend on the radio technology used, such as Bluetooth, Wi-Fi, RFID, NFC or Cellular (GSM/UMTS).

FUNCTIONAL CERTIFICATION REQUIREMENTS

- EMVCo (Level 1 and Level 2 type approval)
- Payment scheme specific requirements (American Express, Discover, MasterCard, Visa and other)
- Acquirer and country specific certification

SECURITY CERTIFICATION REQUIREMENTS

- PCI SSC (PCI PTS, PCI P2PE)
- Common Criteria certification (for some markets)

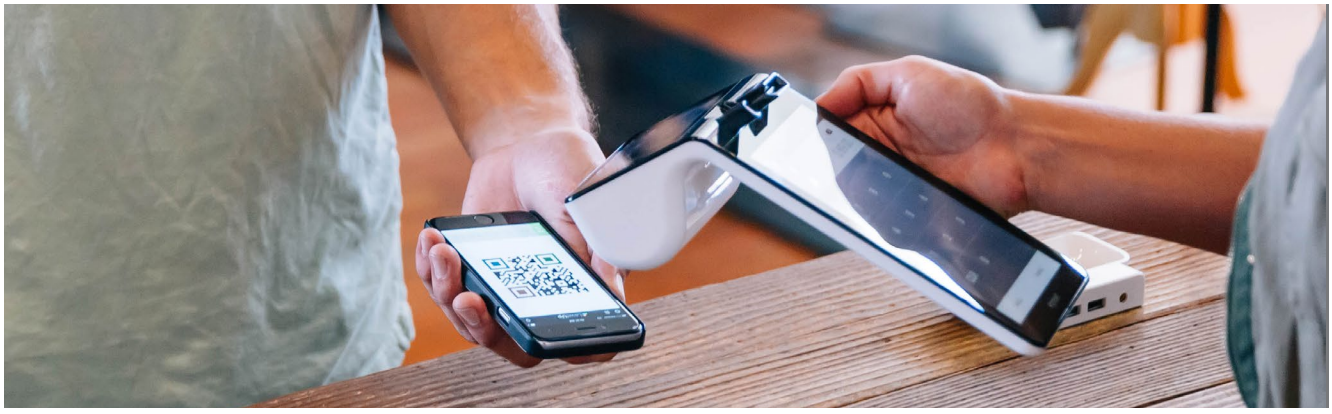
Figure 8. POS/SmartPOS certification and standards overview

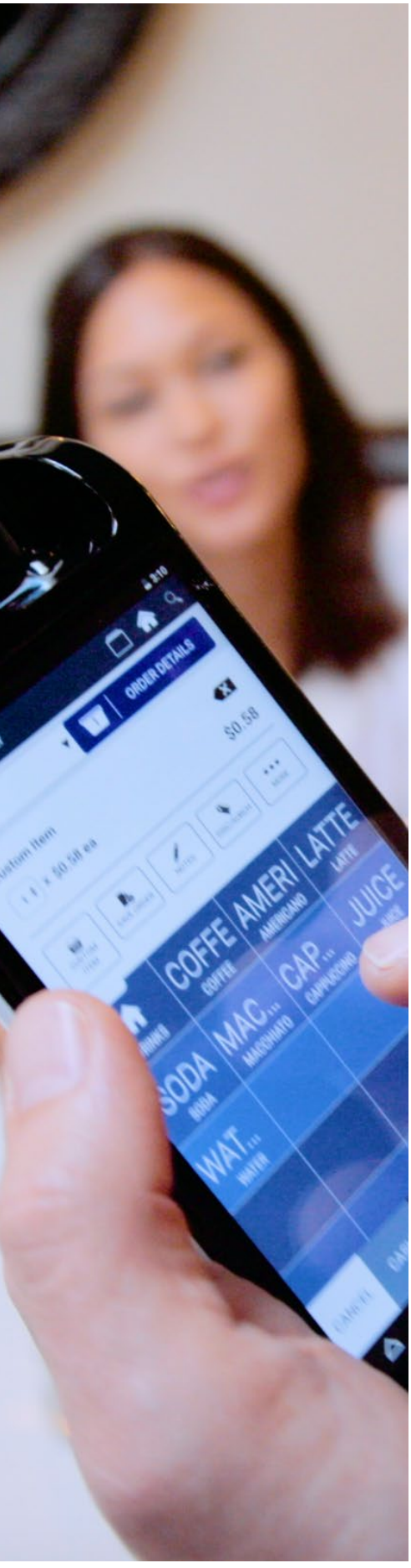
For the regulatory and functional POS certification requirements, no impact is expected for SmartPOS certification. However, depending on the business model and development of new innovative services the requirements to SmartPOS regulatory and functional certification may be changed in the future.
As discussed in Section 3.1 additional services that are offered by SmartPOS affect security requirements that are mainly covered by the PCI Security Standards Council. The following section discusses additional PCI SSC requirements that are applicable to SmartPOS.

2.3.1 Security certification requirements

PCI SSC was formed by the major payment schemes brands (American Express, Discover, JCB, MasterCard and VISA) to ensure secure handling of sensitive cardholder data and has defined PCI PTS compliance (Device Testing and Approval Program Guide) which is mandatory for any solution that allows for customer PIN entry, and is also a foundation of the PCI Point to Point Encryption (P2PE) standard. Having both payment and non-payment applications running on the SmartPOS at the same time imposes additional security concerns to SmartPOS. PCI PTS has additional requirements to this type of POS terminals that includes:

- SmartPOS must enforce the separation between multiple applications. It must not be possible that one application interferes or tampers with another application or the OS of the device including, but not limited to, modifying data objects belonging to another application or the OS. It should be ensured that the device has isolated firmware from applications; applications are authenticated by the firmware; and that the processor and the firmware are able to provide separation between applications. Specifically, it should be ensured that:
    - Any application cannot adversely affect the security features of SmartPOS.
    - Any application cannot modify any of the cryptographic functionality of the SmartPOS or introduce new primitive cryptographic functionality.
    - An application is strongly authenticated to the SmartPOS secure controller by digital signature.
    - Applications shall not be able to see any plaintext key. A key is selected by an application through passing a valid key index to the firmware and the firmware will handle the rest. The application will only obtain encrypted data from the firmware at the end.
- If the SmartPOS relies upon the use of a multi-platform architecture model (see Figure 5) or a multi-operating system architecture model (see Figure 6) the SmartPOS vendor should document the method of communications provided between these processors, including any physical interface and API(s).
- If the SmartPOS enforces isolation on the processor level (see Figure 7), SmartPOS vendors should provide mechanisms to ensure that code and data objects of different applications/firmware are kept separate.
- SmartPOS vendors should provide a defined and documented process containing specific details on how applications should be signed. This must include any “turnkey” systems required for compliance with the management of display prompts, or any mechanisms used for authenticating any application code.
- SmartPOS vendors should provide documentation (i.e., specifications, schematics, block diagrams, etc.) containing information that relates to application loading and application/configuration updates, including remote access, to determine whether it supports the assertions made by the vendor.





The security assessment requirements to the payment and non-payment applications from PCI SSC perspective are also different. For example, payment applications in a P2PE solution will require P2PE Domain 2 assessment while non-payment applications will only require P2PE Domain 1 assessment. The payment application might be subject to PCI DSS assessment if the application is used as part of authorization/settlement at a merchant location if the application is not part of a P2PE solution listed on PCI SSC website. The application vendor might wish to get the payment application validated to PCI PA-DSS requirements to assist with the merchant's PCI DSS assessment.

Distinction between payment and non-payment applications cannot come solely based on the application developer statement. There is a clear need of a regulator and in Section 4 we discuss further which party could develop or adopt this role. Below are some PCI SSC requirements that non-payment applications MUST NOT do on the SmartPOS. Otherwise the non-payment applications would need to be treated as payment applications.

- The non-payment application must not store, process, or transmit sensitive payment data (e.g. PAN, track 1, track 2, PIN, etc.)
- The non-payment application must not display "Enter PIN"
- The non-payment application must not create communication protocol (IP/wireless)
- The non-payment application must not create separate execution environment
- The non-payment application must not have its own key management
- The non-payment application must not handle keys in the clear
- In a P2PE solution, the non-payment application must not violate the security guidelines provided by the device and payment application vendors

3. SMARTPOS APPLICATION MARKETPLACE OWNERSHIP AND APPLICATION VALIDATION PROCESS

The possibility to develop, load, and use multiple non-payment applications on the SmartPOS brings many additional benefits to the merchant but also brings additional considerations for acquirers in terms of offering this terminal to the market.

As we described previously, the terminal vendors and acquirers need to ensure that the applications that are loaded to the SmartPOS are approved and secure. Ideally, the possibility to load the application from an untrusted source should not be possible. To prevent loading applications from untrusted sources, SmartPOS solutions should only allow installation of applications through the associated POS App Marketplace. This is comparable to what we see in the world of smartphones, where trusted applications are available via the Google Play Store for Android devices or Apple's App Store for iOS devices. In this case the merchant can be sure that the application loaded to the device is secure and verified.

However, before apps can reach their application marketplaces, they should be properly verified to ensure that they were securely developed and will not compromise the SmartPOS and the consumer's security and privacy. Therefore, a new role in this ecosystem needs to be introduced which will be responsible for performing app validation. Naturally, this role should be taken by the party who owns the POS App Marketplace. But who is the owner of the marketplace?

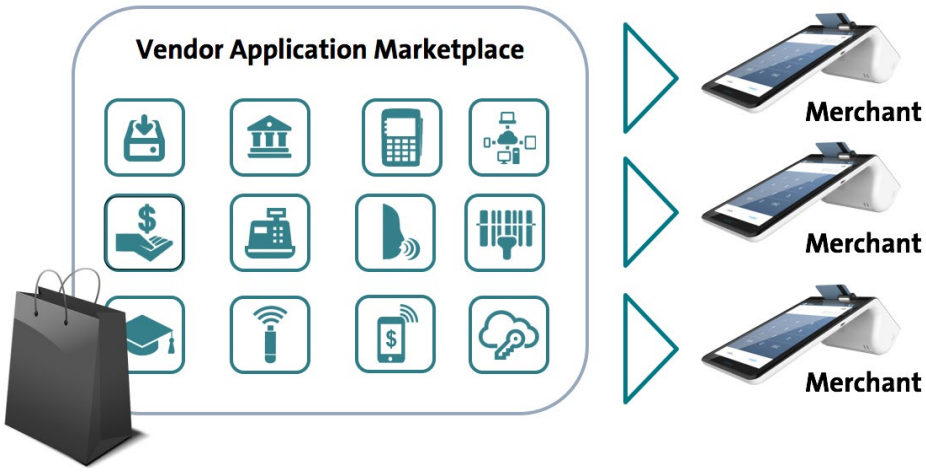


Figure 9. Full SmartPOS vendor ownership model overview

3.1.1 Full SmartPOS vendor ownership

A possible POS App Marketplace model is when the owner of the marketplace is the SmartPOS vendor as shown in Figure 9. This model is very similar to a model observed in the modern smartphone devices when the owner of the marketplace is the owner of the OS, i.e. Google or Apple. The applications that are included in the POS App Marketplace can be developed by the SmartPOS vendor itself, a 3rd party provider or an acquirer. Any application that intends to be included in the POS App Marketplace needs to pass the validation process of the SmartPOS vendor. After successful validation, it is published in the marketplace and can be available for any merchant that uses this SmartPOS from this vendor.

The full control of the POS App Marketplace belongs to the SmartPOS vendors. Usually acquirers or merchants do not have any impact on what appears in the marketplace and do not have direct connection with application developers. The SmartPOS vendor is also responsible for ensuring that the applications that appear in the marketplace are secure and do not tamper the payment data.

3.1.2 SmartPOS vendor and acquirer partial ownership

With a partial POS App Marketplace ownership, the SmartPOS vendor is responsible for validating and adding the applications to a database. However, the acquirer is able to choose what applications should appear in their marketplace. In this way different acquirers may have their selected set of the applications (Figure 10).

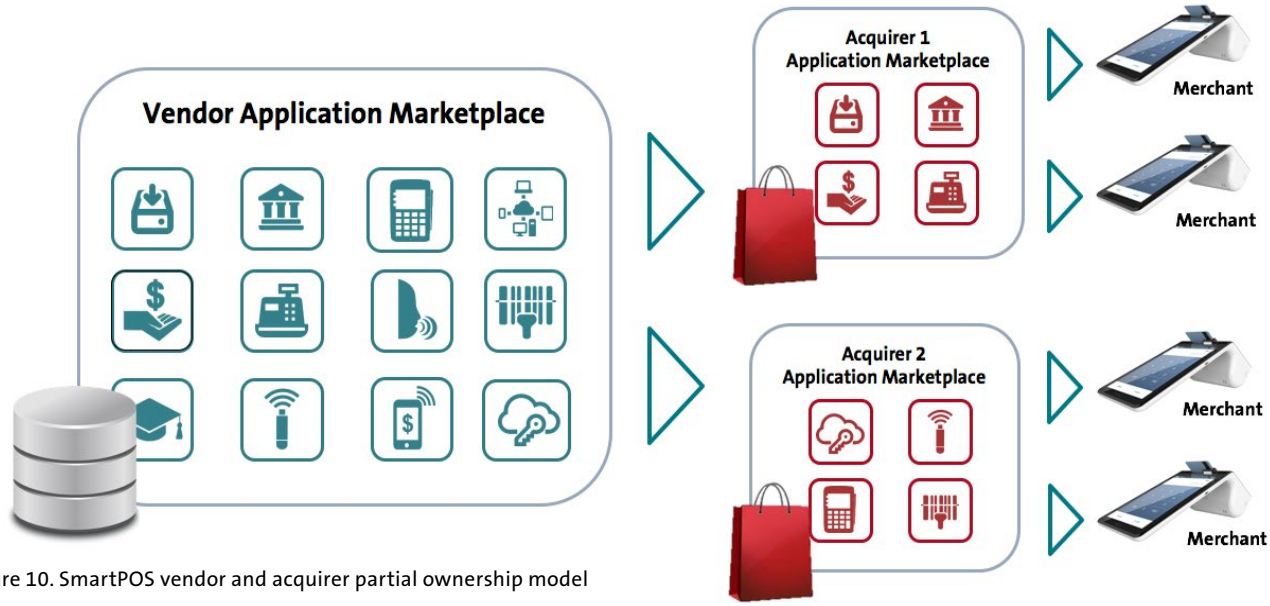


Figure 10. SmartPOS vendor and acquirer partial ownership model

This model gives some control on the content of the POS App Marketplace to acquirers. At the same time the ultimate responsibility for the validation of the applications is still on the SmartPOS vendors. This model also implies that acquirers do not have a direct connection with the application developers.

3.1.3 No SmartPOS vendor ownership

In this model the SmartPOS vendor provides a white labeled POS App Marketplace and grants the rights to use it to the acquirers. It is completely up to the acquirer to decide on the applications that should be included in this marketplace (Figure 11). This implies that acquirers can develop the applications themselves or offer 3rd party providers applications. Acquirers are also responsible for the validation process of the applications that appear in the POS App Marketplace.

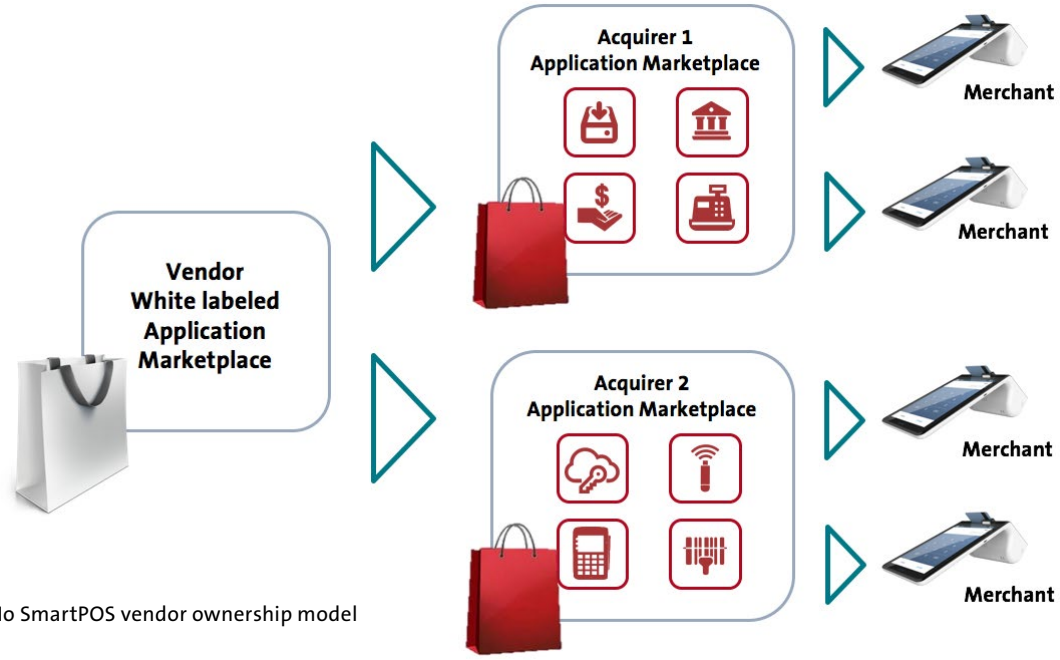


Figure 11. No SmartPOS vendor ownership model

This model may be attractive for big acquirers that are interested to keep the ownership of the POS App Marketplace in their premises and are able to fill the marketplace with useful and relevant applications. For this, acquirers should consider the way to attract application developers to develop new services for their marketplace. Additionally, acquirers are also responsible for establishing a good validation process of these applications.

3.2 APPLICATION VALIDATION PROCESS

According to PCI PTS requirements any application loaded on the POS needs to be signed by an authorized party. This will prevent loading of malicious applications, mitigate arbitrary code execution and will ensure clear path to liability. The signing party should be the owner of the POS App Marketplace. Depending on the ownership model it may be either SmartPOS vendor or acquirer.

Regardless of the type of the application (payment or non-payment) that is added to the POS App Marketplace the application validation process must assess the functionality, security, and compliance of the application. The POS App Marketplace owner may consider three main activities during the validation process:

- Reverse engineering of the application that recreates a binary code to trace it back to the original source code
- Static analysis that includes review of the code and API used by the application
- Dynamic analysis that evaluates security of the application during runtime on the SmartPOS

The above listed activities would allow detection of any vulnerabilities of the application that may include but not limited to:

- Hardcoded credentials to access SmartPOS and steal sensitive data
- Weak cryptography
- Hardcoded secret keys
- Lack of use encryption protocols like TLS
- Account harvesting
- Permission to download external applications etc.

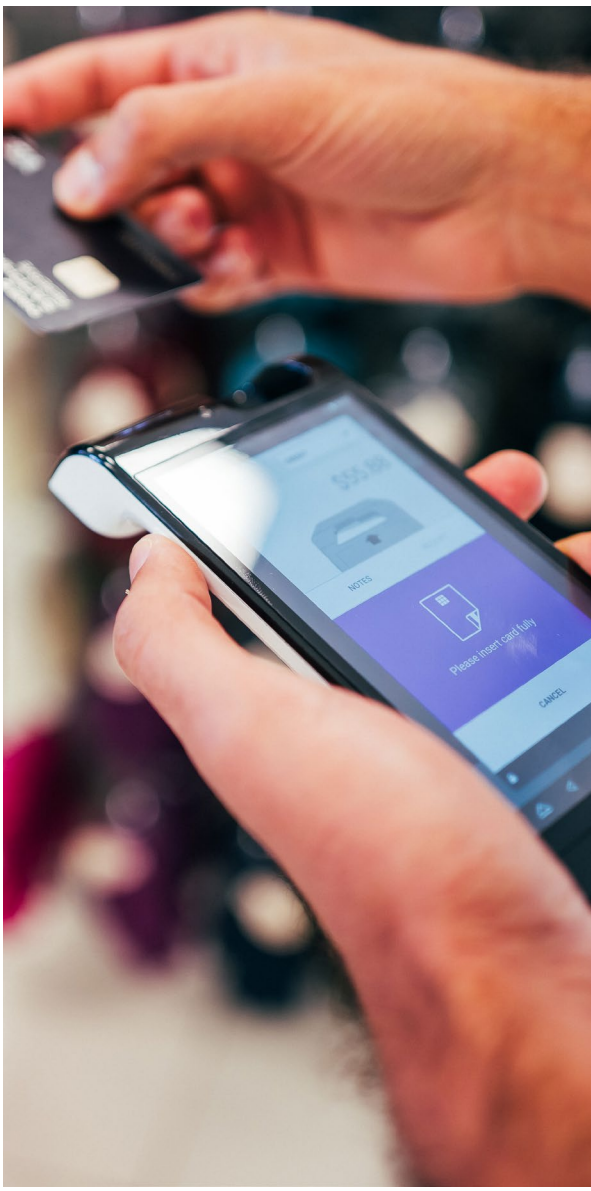
SUMMARY + CONCLUSION

Since they were first introduced, POS terminals have evolved into powerful devices that intend not only to accept payment cards and process transactions, but offer a broad range of non-payment services helping merchants in their business. These new types of POS are usually called SmartPOS.

SmartPOS is inherently a POS device and it embraces all its requirements and functionalities. The main addition of SmartPOS is a possibility to develop, load and use multiple non-payment applications on the same device. This of course brings many additional benefits to the merchant but also additional security, integration, and business considerations.

On the technical level, SmartPOS vendors need to ensure that payment applications are not tampered in any way by other applications installed on the SmartPOS. This may be achieved by segregation of the payment and non-payment applications on of the following levels: hardware level, operating system (OS) level, application level.

Applications that are allowed to be installed on a SmartPOS can be downloaded only from a trusted source. This source is usually the POS App Marketplace. However, before applications get to the POS App Marketplaces, they should be properly verified to ensure that they are secure and will not compromise payment processing and data storage on SmartPOS. This verification is performed by the party who is the POS App Marketplace owner. SmartPOS vendors may consider several options for the marketplace ownership such as full SmartPOS vendor ownership, ownership shared between SmartPOS vendor and acquirers, and acquirer's ownership. Regardless of the ownership model the application validation process must assess the functionality, security, and compliance of the application.



For further information on SmartPOS, please contact:
TRANSACTIONSECURITY@UL.COM or visit **UL-TS.COM**

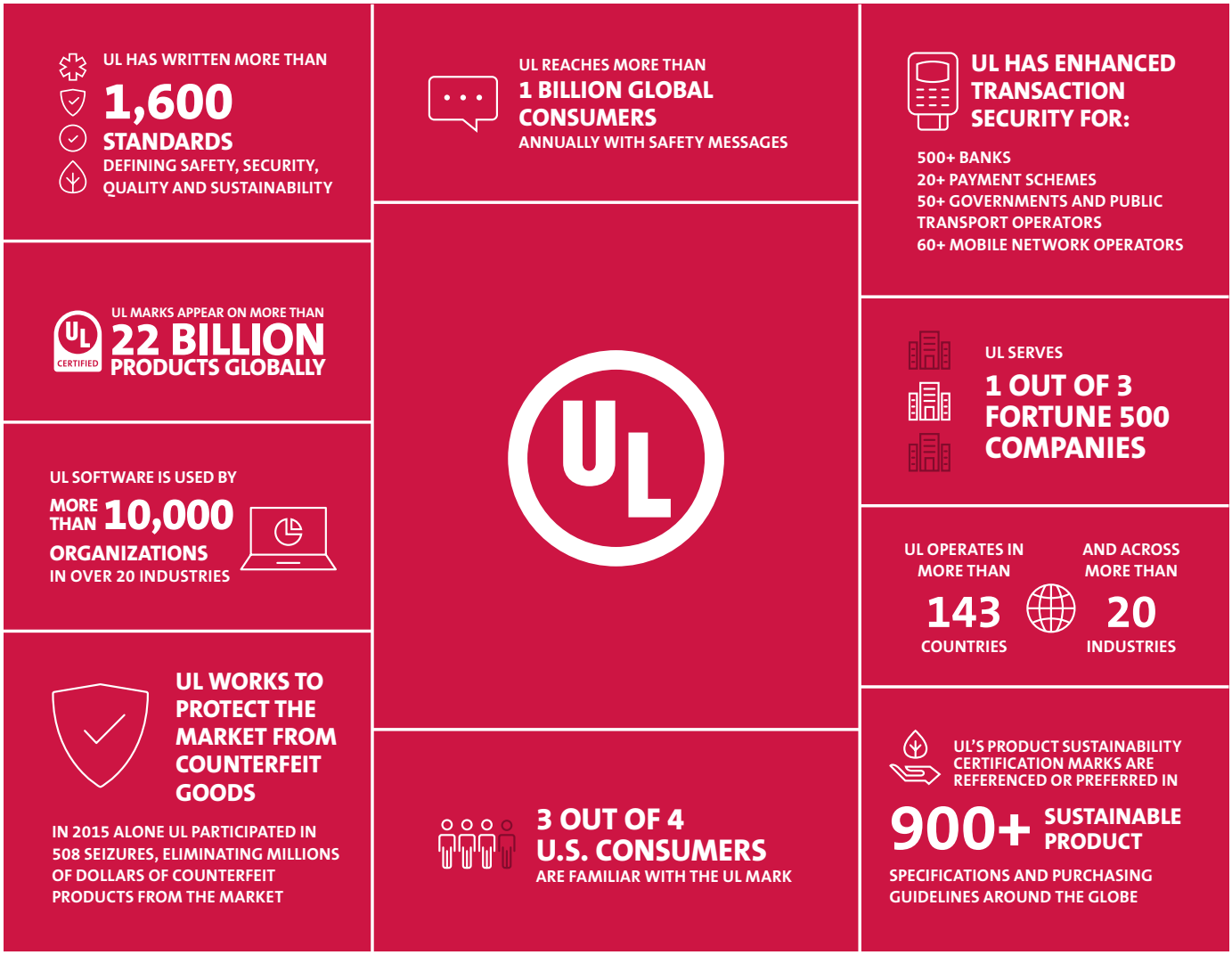
ABOUT US

UL fosters safe living and working conditions for people everywhere through the application of science to solve safety, security and sustainability challenges. The UL Mark engenders trust enabling the safe adoption of innovative new products and technologies. Everyone at UL shares a passion to make the world a safer place. We test, inspect, audit, certify, validate, verify, advise and train and we support these efforts with software solutions for safety and sustainability.

UL's Transaction Security division guides companies within the mobile, payments, and transit domains through the complex world of electronic transactions.

UL is the global leader in safeguarding security, compliance, and global interoperability. Offering advice, training, compliance and interoperability services, security services, and test tools, during the full life cycle of your product development process or the implementation of new technologies.

UL's people proactively collaborate with industry players to define robust standards and policies. Bringing global expertise to your local needs. UL has accreditations from industry bodies including Visa, Mastercard, Discover, JCB, American Express, EMVCo, UnionPay International, PCI, GCF, GlobalPlatform, NFC Forum, and many others. To learn more about us, visit UL-TS.com.



UL-TS.COM