Qualcomm

Enabling Secure Payment on Enterprise Devices

Adding hardware-level security for contactless payment acceptance on commercial, off-the-shelf enterprise devices

May 2023

Ketal Gandhi - Senior Director, Business Development, Qualcomm Technologies, Inc.
Le Vu Dinh - Senior Manager, Business Development, Qualcomm Technologies, Inc.

SoftPOS and contactless payments

Merchants, consumers, and the payment card industry are always ready to make retail transactions as frictionless and contactless as possible. But most of that friction and contact results from the inevitable trade-off between ease of use and transaction security. The search never ends for a digital payment system that is secure and easy to implement without the need for dedicated hardware at the point of sale (POS).

SoftPOS (Software Point of Sale) is gaining traction as a viable alternative for small, medium, and large businesses. Unlike traditional payment terminals that rely on dedicated hardware to protect the payment information, SoftPOS solutions enable COTS devices (smartphones and tablets) to accept contactless payments through a software app over near-field communication (NFC). Many pilot programs are underway, but all stakeholders are concerned about the overall security of the software-based solution.

This brief explores Qualcomm Technologies' hardware root of trust-based security technologies for accepting payments on commercial, off-the-shelf enterprise (COTS) devices. On a vast install base of Android enterprise devices powered by Qualcomm's System on a Chip, in-built security foundations include technologies—such as the Qualcomm® Trusted Execution Environment (TEE), Qualcomm® wireless edge services (WES), and Trusted User Interface—to provide hardware-based security assurances, paving the way to adoption of SoftPOS retail payment acceptance at scale for various scenarios.

The bright future of SoftPOS and contactless payments

Reducing friction at POS is a desirable goal for merchants, consumers, and the entire payment industry. Currently, contactless payments are the brightest prospect for achieving that goal and SoftPOS has emerged as a popular option for conducting contactless retail transactions. According to a global study conducted by research and advisory firm Aite-Novarica, significant investment has been going on in this space—with pilots live in 74 countries involving 200 acquirers and almost a million phones in the field.

- SoftPOS can improve the customer experience at check-out in retail stores and restaurants, especially during spikes in sales volume and customer traffic. Store associates and restaurant staff can use a SoftPOS payment acceptance application running on an associate's enterprise Android devices. That way, businesses enable payments acceptance on handheld devices that are currently available to their workers, avoiding bottlenecks from a limited quantity of dedicated payment terminals.
- SoftPOS has a role to play in speeding the transition to digital forms of payment, especially in markets where COD (cash on delivery) and cash-based transactions still dominate. The use case for delivery drivers and gig workers, for example, is squarely within the capabilities of a SoftPOS application running on an NFC-equipped, Android-based enterprise device.
- Looking to the future, SoftPOS paves the way for the continuing evolution of payment acceptance through new forms of POS, self-checkout systems and other payment-integrated devices, such AI-enabled vending machines, self-checkout/in and self-ordering kiosk terminals, smart carts, etc. It offers greater flexibility in design and mobility without relying on traditional hardware. Imagine, for example, an NFC-enabled smart mirror in a fitting room that can accept contactless payment seamlessly from a consumer's smart watch.

Juniper Research anticipates that the number of merchants using SoftPOS could reach 34.5 million globally by 2027. Juniper envisions consumer adoption of SoftPOS becoming a driver for merchants to adopt contactless-capable POS solutions.

But how to make SoftPOS secure?

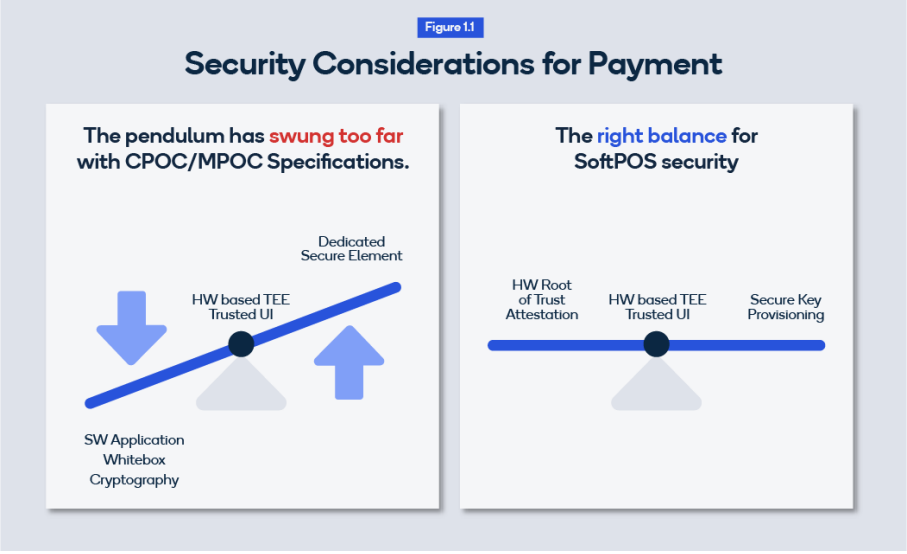
There is, however, an alternate side to the wide accessibility, ease of use, and hardware-independence—SoftPOS is based on software-based security. As an app running on an Android device, a SoftPOS solution is inherently less secure than traditional POS hardware. Inadequate security can lead to fraudulent transactions and the theft of private cardholder data.

All SoftPOS solutions must adhere to the PCI Mobile Payments on COTS (MPoC) standard, which defines security requirements, test requirements, and guidance for mobile payment acceptance using COTS devices and card networks—like Visa and Mastercard—to require adherence to the standard for certification. Because MPoC offers security options at both the software and hardware levels, the market is embracing the option that is easier to implement, i.e., the software option. The problem with this approach is that a software application conducting contactless payment transactions is not secure enough to provide adequate protection from cyberthreats and fraud, especially as the SoftPOS solution scales from micro merchants to SMB to large enterprise customers; from micro transactions to a higher amount and a larger number of transactions; from consumer mobile COTS devices to Android enterprise mobile and fixed devices; and from attended to semi-attended and unattended scenarios. Software-based security will just not be sufficient.

The risk is even greater in markets like the European Union and for debit card transactions, where the transaction combines contactless payment with a PIN (personal identification number). That is because it is easy to hack PIN entry on a smartphone screen with software-based security. Furthermore, mobile devices and the applications running on them are becoming highly favored targets of bad actors. According to the Mobile Security Index report from Verizon, 45% of organizations have recently experienced mobile-related compromise, with almost three-fourths of them describing that compromise as "major".

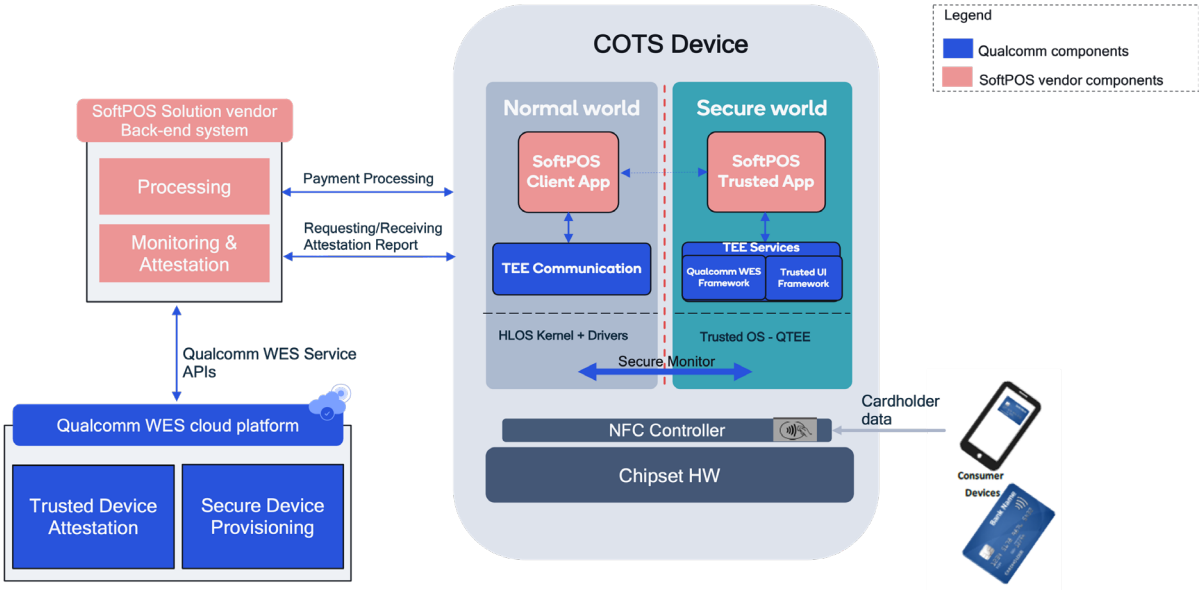
In such a hostile climate, card networks have not authorized SoftPOS to scale up to the volume needed for mass-market adoption. Meanwhile, the payment card industry is fine-tuning the security framework. The most recent version of the MPoC standard was released in November 2022, providing more comprehensive guidance and requirements to address SoftPOS security.

But true security for SoftPOS calls for protection at both the software and hardware levels. For example, on dedicated payment terminals, the payment transactions and PIN entry are secured with a dedicated secure element, while SoftPOS solutions are implementing pure software application-level security. It is as if the pendulum has swung completely in the opposite direction. There needs to be a balance, which can be offered through pre-integrated hardware root of trust-based security on COTS devices—even for software-based payment acceptance solutions.



Qualcomm's hardware-based security technologies to secure SoftPOS payments

The essence of Qualcomm's solution to hardware-based security for SoftPOS is to use existing hardware in the device to create a secure and isolated environment, preventing unauthorized access and modification of applications and data, as well as providing attestation service to enable relying parties to establish hardware-based trust in the devices. On Qualcomm chipsets, we achieve this hardware-based security by leveraging technologies such as Qualcomm TEE, Trusted UI Framework, and Qualcomm WES.



The solution consists of three parts:

Qualcomm Trusted Execution Environment (TEE)

The Qualcomm TEE is a controlled and isolated execution environment, also known as "secure world", that runs alongside the main operating system of the device, such as Android. Based on the standardized technology and hardware-based access control, Qualcomm TEE provides several security services and securely hosts third-party trusted applications that manage sensitive assets, like authentication credentials and keys. Qualcomm TEE is designed to execute only trusted pre-approved code and is tamper-resistant to protect against external attacks and malware, ensuring sensitive information is protected even if the operating system is compromised.

With the Qualcomm TEE, a device can accept payments securely while performing a variety of common functions typical for COTS hardware. Qualcomm TEE also enables service providers and software developers to create trusted applications to perform security sensitive functions, such as authentication, privacy sensitive data processing, and more.

Qualcomm Wireless Edge Services (WES)

Qualcomm WES is Qualcomm's chip-to-cloud service that enables relying parties, such as service providers and applications, to establish hardware-based trust in the end point devices that are being remotely managed and establish secure communication with them. Qualcomm WES leverages SOC unique hardware credentials to establish device trust.

With the hardware-based attestation and device provisioning services, Qualcomm WES provides service providers/apps with the ability to verify the unique identity, device health (integrity and authenticity), and connection health of the device when the payment transaction is being processed. Qualcomm WES attestation service can also help verify the integrity and authenticity of the payment processing application on the device.

Trusted User Interface (TUI)

Trusted User Interface is a security feature that allows the application/service provider to verify the identity of a user by verifying the PIN during the payment transaction. TUI on Qualcomm chipsets leverages Qualcomm TEE and is designed to be tamper-resistant, allowing processing of sensitive payment credentials. Trusted User Interface, when integrated with Qualcomm TEE and hardware-based attestation service, can provide a secure and tamper-proof environment for processing payment transactions with PIN on glass.

SoftPOS has unquestionable benefits for merchants, consumers, and the payment card industry. But to enable widespread adoption of SoftPOS, it is important to leverage hardware-based security frameworks present on Android devices.

What industry leaders are saying:

As the market seeks out cost-effective ways to accept payments with broad-reaching capabilities, Mastercard is unlocking new ways to modernize physical and digital acceptance. As software-based point of sale gains momentum, SoftPOS offers greater functionality and seamlessly integrates with other business systems, bringing innovation, trust, and access to the point-of-sale ecosystem. Our ecosystem partners are exploring different ways of securing SoftPOS solutions to meet industry standards and we are excited to see the benefits that each security framework can bring to the industry.

Jerome Guibal, Director, Product Management at Mastercard

Innovation and security are priorities for the development of all solutions at Worldline. We are in constant dialogue with partners like Qualcomm Technologies, Inc. to improve our solutions on both security and reliability. The SoftPOS market is evolving rapidly and Worldline is always looking for potential future solutions. For that, we are in close contact with Qualcomm to evaluate new ways to securely manage SoftPOS and mobile payments.

Karel-Lodewyck Lefere, Director, Global Strategic Partnerships at Worldline

Aligned with Qualcomm's vision for SoftPOS implementation, Datalogic has worked to enable TUI and TEE for the SoftPOS applications on our flagship enterprise PDA, Memor 20, based on SD660 chipsets, to demonstrate the utmost secure way to execute payment transactions. As a trusted advisor to our enterprise customers, enabling new features with highest security is paramount for us.

Mangaraju Vuppala, Director, Mobile Product Management at Datalogic

Qualcomm and Aurus' collaboration on SoftPOS is bound to be a win for retailers and their customers. Hardware layer security and next-gen NFC technology is paramount in SoftPOS adoption with enterprise retailers. Enterprise merchants can now accept payment on common Android tablets which run mPOS Endless Aisle inventory management software without the need for a payment terminal. Retailers who adopt SoftPOS solutions will be able to repurpose existing devices, reduce CAPEX, and delight customers with the ability to pay with a simple tap of their card or phone. Aurus provides a specialized payments platform to Tier-1 retailers that automatically incorporate new innovations in payments like SoftPOS.

Parag Shirnamé, Vice President, Client Relations at Aurus

Qualcomm's hardware-based security technologies provide the services needed to secure SoftPOS payment acceptance on COTS and enterprise devices. Qualcomm provides SDKs for Qualcomm TEE, Qualcomm WES, and TUI to ease the development and implementation of contactless payment methods and securely protect human interactions. Already installed in billions of devices, Qualcomm Technologies' solutions provide an easy path to secure and scale contactless payments acceptance for merchants while reducing the total cost of their check-out solution.

If you're interested in finding out more about what Qualcomm is doing in the retail space, please visit: https://www.qualcomm.com/products/internet-of-things/industrial/retail