



Protección de Datos en Transacciones de Pago y el Ambiente Móvil

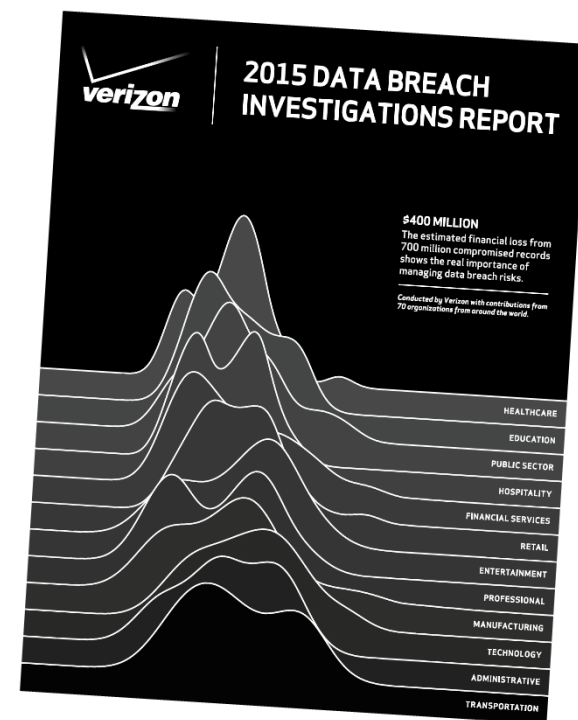
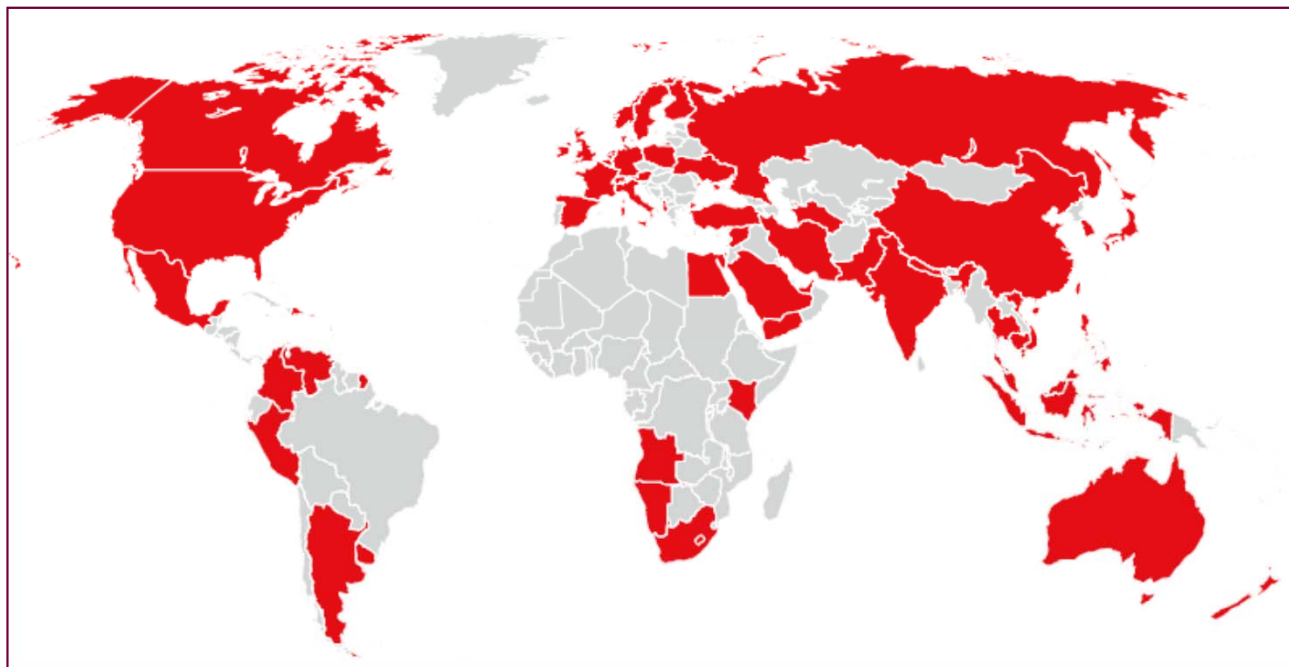
JOSE DIAZ
DIRECTOR, DESARROLLO DE NEGOCIOS
Y ALIANZAS TÉCNICAS

www.thales-esecurity.com

THALES GROUP CONFIDENTIAL

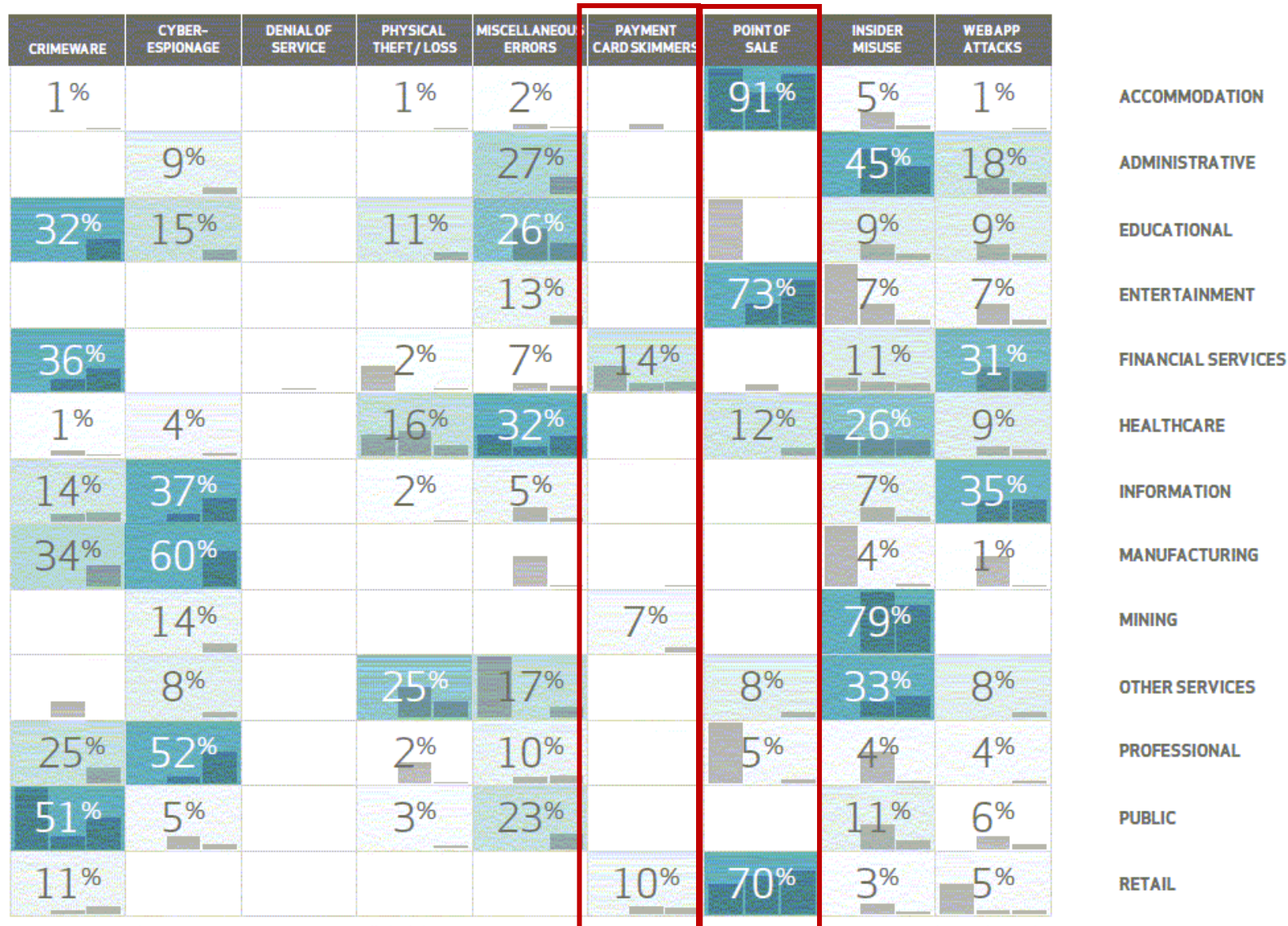


Reporte de Verizon sobre Brecha de Datos



"2013 puede ser recordado como el "año de las brechas de comercios", pero una evaluación comprensiva sugiere que fue un año de transición de ataques geopolíticos a ataques de gran escala en sistemas de tarjetas de pago "

Industrias Victimas



Que Tienen en Común?



Brecha de Target – Impacto en Penalidades

Target indicó recientemente en documentos financieros que hasta el momento había tenido \$252 Millones en gastos relacionados a la brecha



- En Marzo, Target acordó a pagar \$10 Millones para cerrar un demanda legal sometida por consumidores
- MasterCard llegó a un acuerdo de \$19 Millones para rembolsar a los bancos miembros por los gastos acumulados debido a la brecha en 2013
- Visa, mientras tanto, todavía esta negociando con Target sobre el reembolso a bancos emisores de Visa

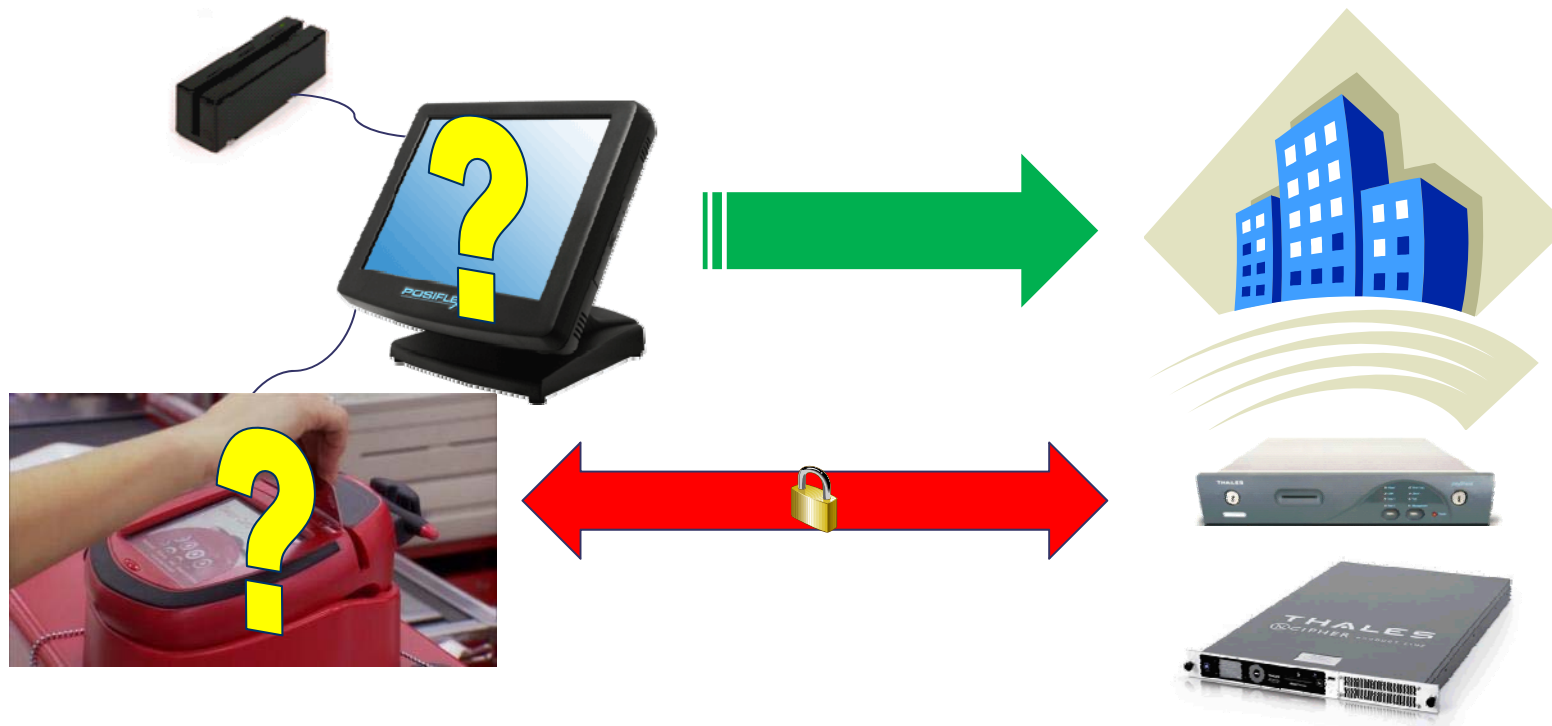


Finextra 16 Abril 2015

El Ambiente de un Comercio

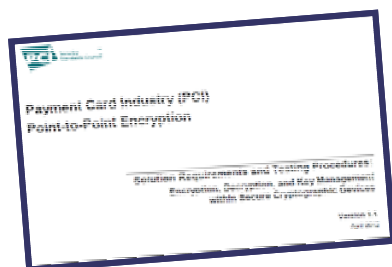
Comercio

Adquiriente /
Switch en Comercio

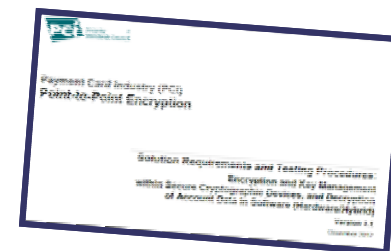


Descripción de
Datos (PCI P2PE)

Uso de P2PE para Reducción de Ámbito



PCI Point-to-Point Encryption Solution Requirements



Define requerimientos para soluciones P2PE con el propósito de reducir el ámbito de evaluaciones PCI DSS en comercios utilizando dicha solución

“Los datos cifrados está fuera del ámbito si, y sólo si, se ha verificado que la entidad que posee los datos cifrados del tarjetahabiente no tiene los medios para descifrarlos.”



Y que Sobre PCI y Móvil?



AT A GLANCE
MOBILE PAYMENT
ACCEPTANCE SECURITY
Revised 2014

Accepting Mobile Payments with a Smartphone or Tablet

Many merchants seek innovative ways to engage customers and enhance the payment experience. The ever-expanding capabilities of mobile devices now includes payment acceptance. Along with the increased convenience, mobile payment acceptance can also bring new risks. Securing account data at the point of capture is one of the most important in controlling these risks. Validated Point-to-Point Encryption (P2PE) is available on the PCI Council (PCI SSC) website. If you choose to accept mobile payments, help you in your responsibilities under PCI DSS.

This *At a Glance* provides an example of a P2PE solution that leverages a mobile device's display and communication functions to secure mobile payments. Central to the example is the use of an approved hardware accessory in conjunction with a validated P2PE solution. Combining a validated P2PE solution with tablets helps to maintain data security throughout the transaction.



PROTECT CARDHOLDER DATA

The PCI Data Security Standard (PCI DSS) requires merchants to protect cardholder data. You must protect any payment card information, whether it is printed, processed, transmitted or stored.

FOR MERCHANTS INTERESTED IN BUILDING THEIR OWN MOBILE PAYMENT ACCEPTANCE SOLUTION:

Partner with a Provider of a Validated Solution

Validated P2PE solutions ensure that cardholder data is encrypted before it enters a mobile device. Using a validated and properly implemented P2PE solution greatly reduces the risk that a malicious person could intercept and use cardholder data.

Solution providers will often provide you with a card reader that works with your mobile device. Validated solution providers will have a list of approved card readers (also called Point of Interaction or POI) that have been tested to work securely with their solution. The solution provider is responsible for ensuring that any POI used with their solution has been validated as compliant with the appropriate PCI SSC security requirements, including the Secure Reading and Exchange of Data (SRED).

Your solution provider will also tell you how to safeguard your mobile payment system. This guidance is contained in a *P2PE Instruction Manual (PIM)*. Your acquirer or payment brand may ask you to complete a *P2PE Self-assessment Questionnaire* as part of your annual PCI DSS validation – including confirming that you are following the solution provider's PIM. You should coordinate with your acquirer or payment brand.

WHY SECURING MOBILE PAYMENTS IS IMPORTANT

- Current mobile devices have limited security safeguards for payment acceptance

FOR MERCHANTS INTERESTED IN BUILDING THEIR OWN MOBILE ACCEPTANCE SOLUTION:

Use an Approved Point of Interaction (POI) Device

Mobile devices are not necessarily designed to be secure input or storage devices for cardholder data. Your mobile payment solution thus requires additional technology, including encryption, to secure cardholder data acceptance. The first part of a secure mobile payment solution is an approved "point of interaction," which is a technical term for an approved PIN entry device (PED) or approved secure card reader. The diagram above shows two options: one is a Secure Card Reader that reads the magnetic stripe of a payment card; the other is an approved POI for reading a card and manually entering a PIN. All these devices have the same purpose: to safely capture and encrypt cardholder data. As of July 2014, some approved, they will be listed on the Council's website.

PCI Data Security Standard

Implementing a validated P2PE solution for mobile payment security is a key requirement of the PCI DSS. This means that a validated and properly implemented solution for mobile payments may lessen the requirements for your annual assessment against the PCI DSS. Scope reduction can dramatically reduce the cost of compliance. You will still be responsible for compliance with the PCI DSS. You must also be responsible for merchant policies and procedures, for contractual obligations to your P2PE solution provider, for physical protection of payment systems, and for following the *P2PE Instruction Manual*.

PCI Security Standards Council

The PCI Security Standards Council is an open global forum, launched in 2006, that is dedicated to the development, management, education, and awareness of the PCI Security Standards, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements.

The Council's five founding global payment brands -- American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. -- have agreed to incorporate the PCI DSS as the technical requirements of each of their data security compliance programs. Each founding member also recognizes the QSAs, PA-QSAs and ASVs certified by the PCI Security Standards Council.

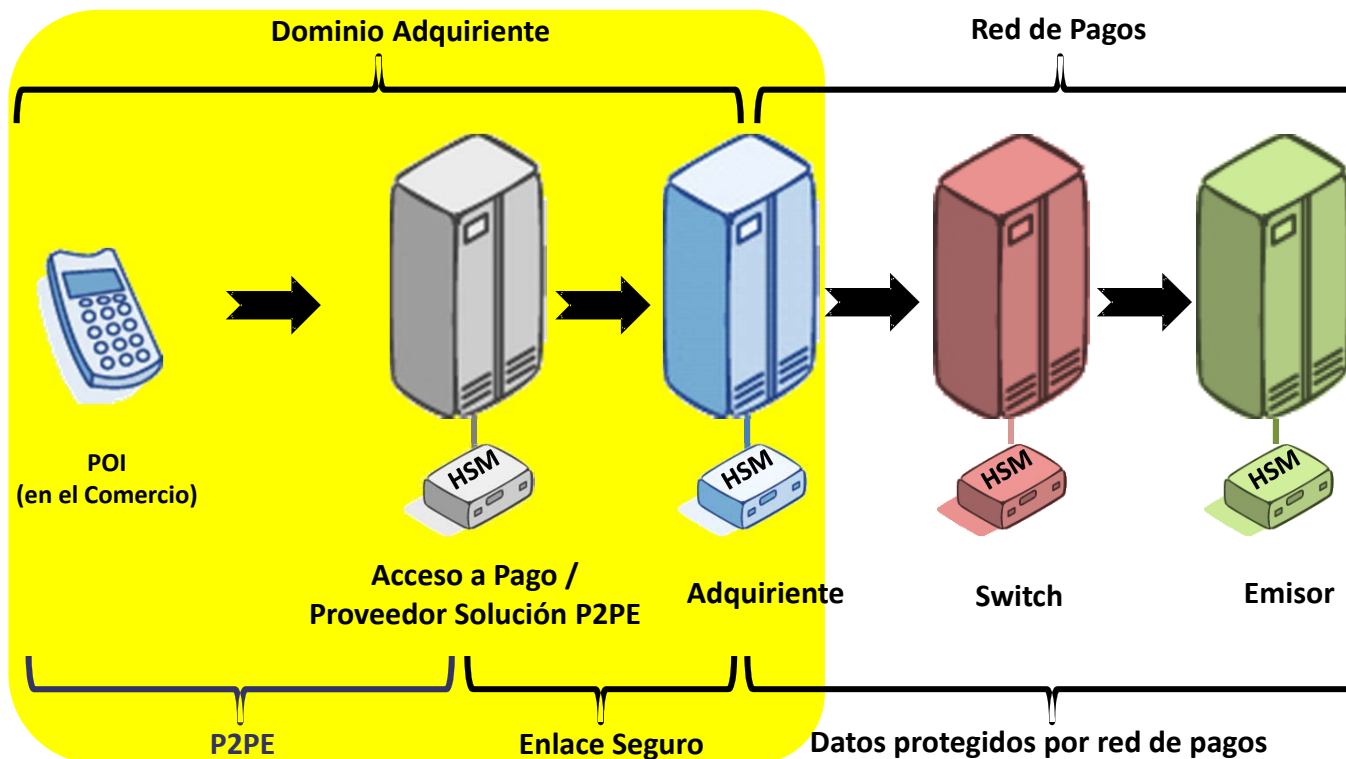


change the random data back into the original data (a process called decryption).



The key must be protected from unauthorized access or disclosure.

Implementación P2PE



Disminuye la inquietud del comercio en cumplir con evaluaciones

- Elimina datos de tarjetahabiente en el ambiente del comercio
- Protege los datos desde el PDV hasta el punto de Acceso o Adquiriente
- Oportunidad de ingreso para proveedor de servicio P2PE!

Que esta Motivando la Protección de Datos?

PCI DSS



- Redes y Sistemas Seguros, Proteger Datos de Tarjetahabiente, Administración de Vulnerabilidad, Control de Acceso, Supervisar y Evaluar Redes, Política de Seguridad
- HSMs ayudan a cumplir con algunos de estos requerimientos

PCI P2PE

- Protección de datos punto a punto entre terminal de pago en comercio y adquiriente
- Simplifica cumplimiento con PCI DSS
- HSMs juegan parte importante en la solución – Requeridos para descifrar los datos y administración de claves

PCI PIN Security

- Guía para auditorias en procesadores de PIN
- HSMs igualmente juegan parte importante – Requeridos para traducción/verificación de PINs y administración de claves

THALES

| Pagos Móvil

www.thales-esecurity.com

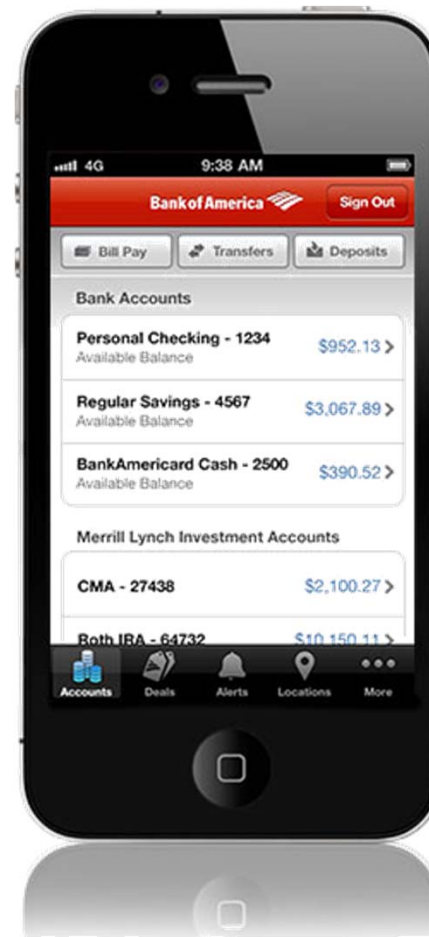
OPEN
THALES GROUP INTERNAL
THALES GROUP CONFIDENTIAL
THALES GROUP SECRET



Banca Móvil

Banca Móvil no es igual a Pagos Móvil

- Es una relación directa entre uno y su banco
- Permite acceso a balance de cuentas
- Se puede pagar cuentas, pero:
 - Mayoría son cuentas que uno se registro para pagar directamente (electricidad, teléfono, etc.)
- Uno puede transferir fondos entre sus cuentas
 - Pero no transferir fondos a un amigo si no tiene información sobre su banco y numero de cuenta
- Tal vez es posible depositar un cheque tomando una fotografía del cheque y enviando al banco
- Uno no puede pagar por compras en un comercio con una aplicación de banca móvil



Panorama Tradicional de Pagos

Modelo tradicional de 'Cuatro' puntas define un ambiente bien controlado



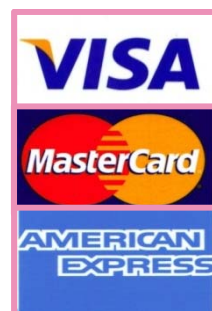
Tarjeta Consumidores



Sistema de Comercio



Banco de Consumidor



Red



Banco de Comercio

Pago Móvil Amplia el Panorama

Modelo tradicional de 'Cuatro' puntas define un ambiente bien controlado



Tarjeta Consumidores



Red



Banco de Consumidor



Banco de Comercio

Dispositivos de Pago Móvil



**Banda
Magnética**

EMV

Aceptación Pagos Móvil (mPOS)

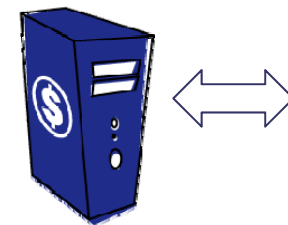
POS Tradicional



Comercio

Proveedor Servicio de Pagos

Dispositivos, aplicaciones y redes confiadas



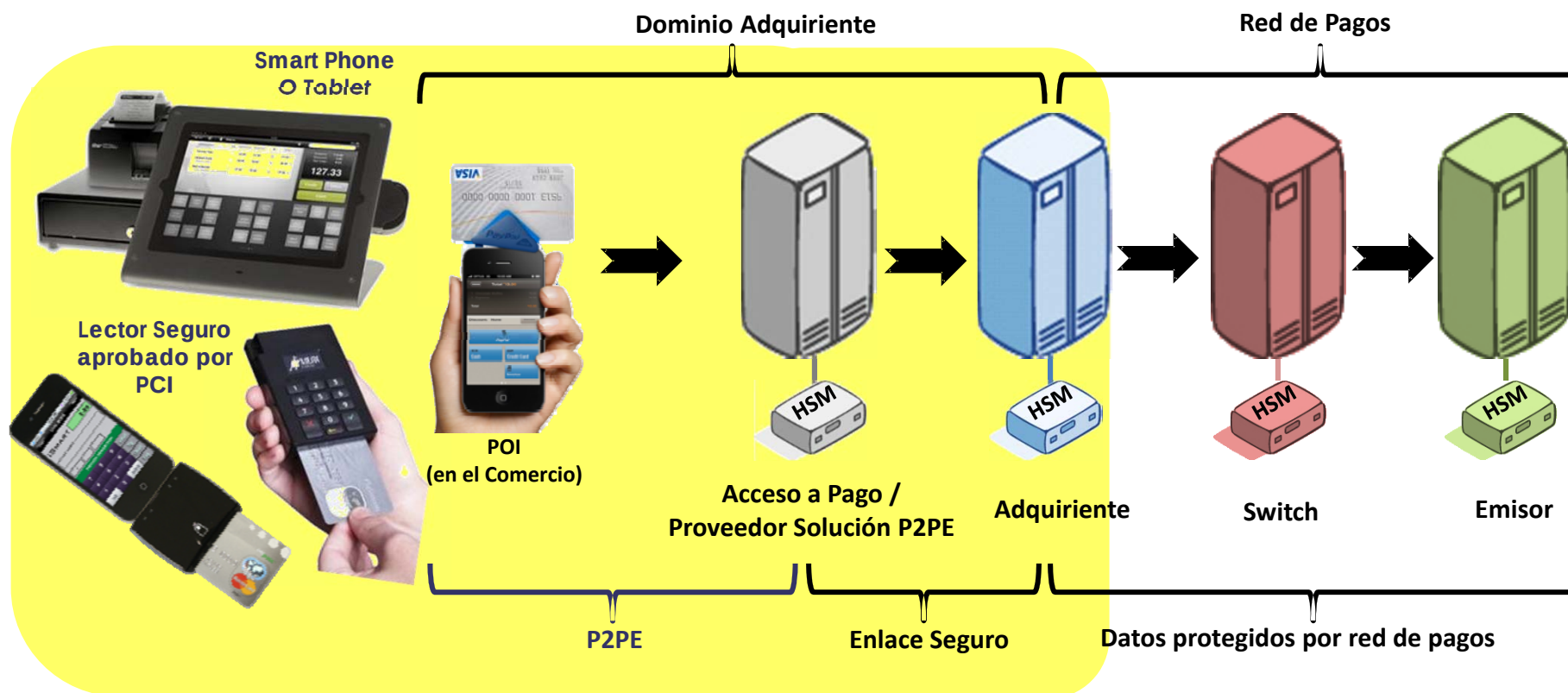
POS Móvil



Portal de Pagos

Dispositivos, aplicaciones y redes sin confianza

Protección de Datos en Aceptación Móvil (mPOS)

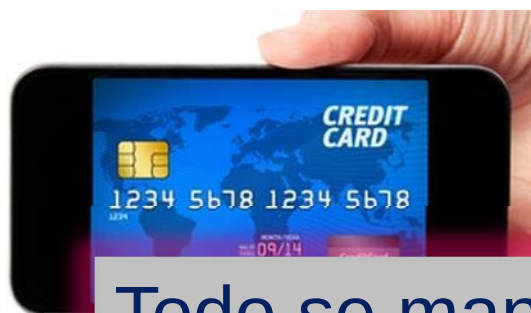


Permite seguridad de datos en transacciones mPOS

- Elimina datos de tarjeta habiente del dispositivo móvil y ambiente del comercio
- Utiliza P2PE para protección de datos
- Un elemento importante en transacciones mPOS!

Pagos con Móvil Introduce Nuevos Desafíos

Modelo tradicional de 'Cuatro' puntas define un ambiente bien controlado



Sistema de Comercio



Todo se mantiene igual – pero...

- Teléfono móvil es inseguro
- Son controlados por consumidor
- No los pueden 'leer' el comercio



Banco de Consumidor

Red

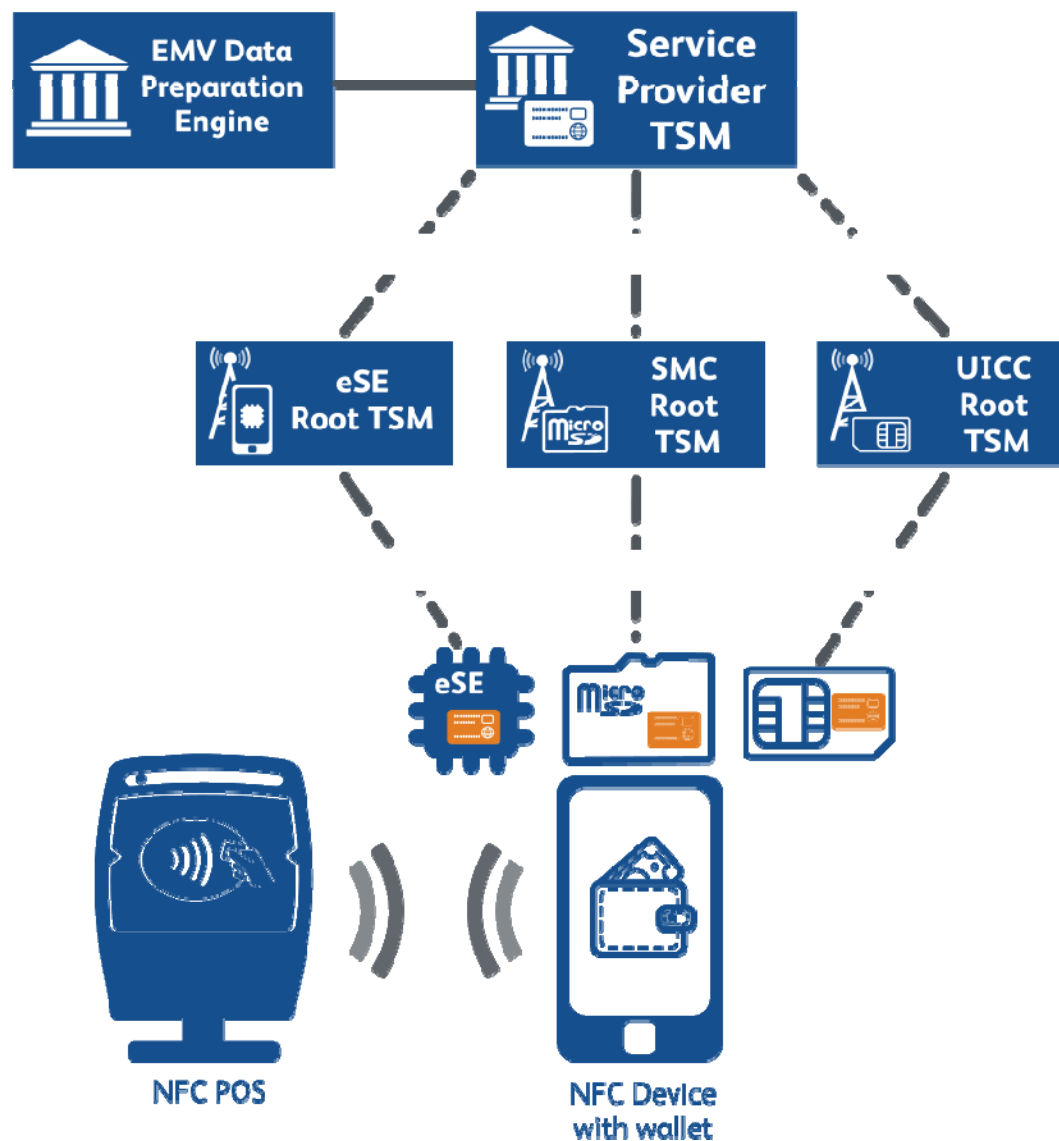


Banco de Comercio

Ambiente Ampliado – Muchos Actores



Elemento Seguro (SE)



Cortesía de Bell ID

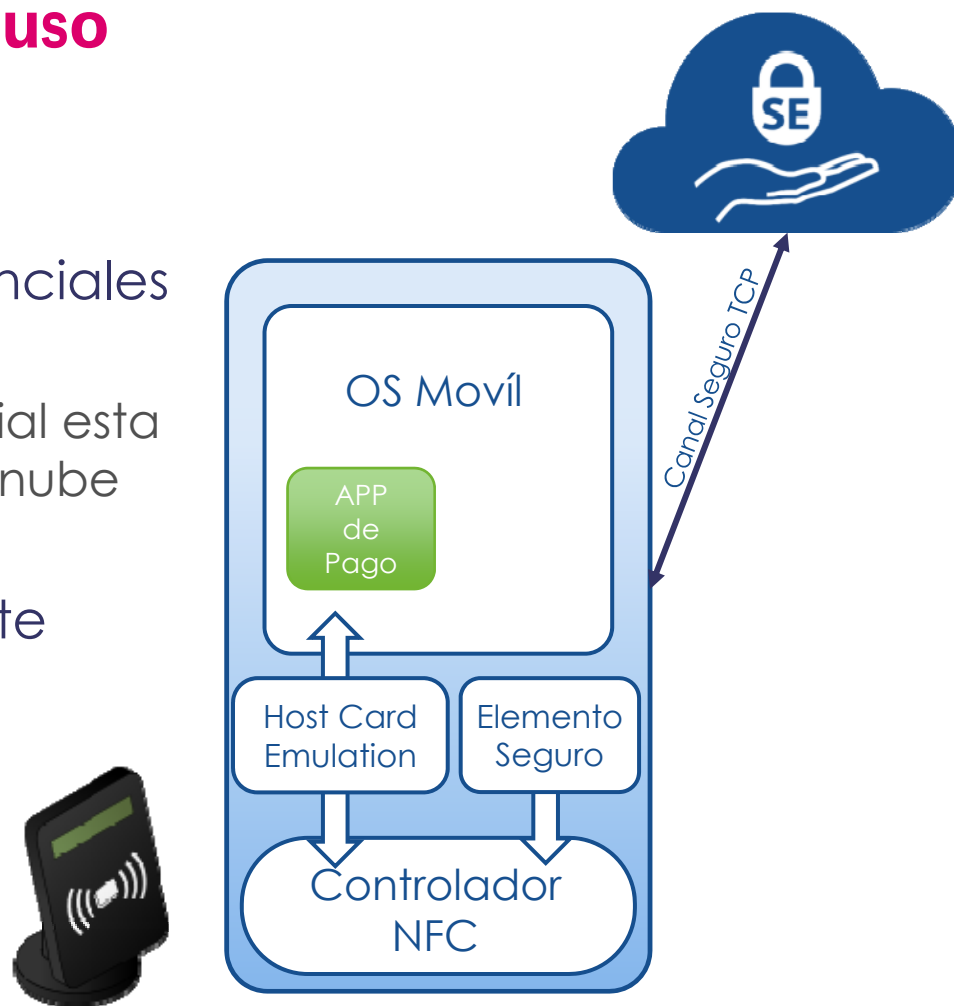
Host Card Emulation (HCE)

HCE es una alternativa al uso del Elemento Seguro en dispositivo móvil

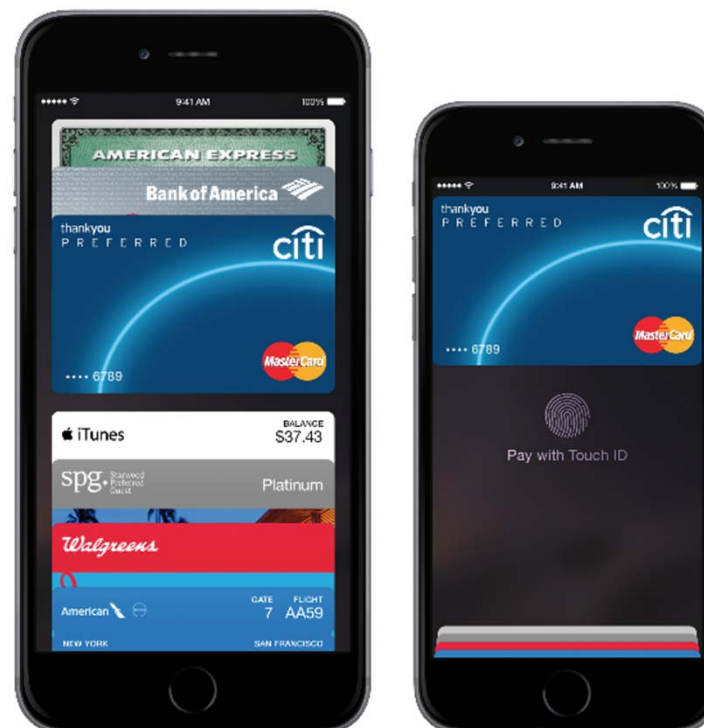
- Aplicación móvil tiene credenciales de pago
 - Solamente información esencial esta en el móvil, el resto esta en la nube
- Cada marca tiene especificaciones sobre soporte para implementaciones HCE

Riesgo mitigado a por utilización de:

- Claves dinámicas
- Tokenización del PAN



Y Entonces Llego Apple Pay



Creo infraestructura entre Emisores de Tarjetas, Marcas de Tarjetas y Apple permitiendo la carga de credenciales de pago en el Elemento Seguro del iPhone (6)

- Permite pagos sin contacto (basado en NFC) entre el teléfono móvil y la terminal punto de venta

Esquemas de Pagos Móvil

Origen: CNN Money

    				
Apple Pay	Samsung Pay	Google Wallet	PayPal	Bitcoin
AVAILABILITY				
Only iPhone 6.	Only Samsung Galaxy S6.	Any device with the app.	Any device with the app.	Any device with the app.
HOW YOU USE IT				
 Fingerprint OK for tap-to-pay (at new registers) and online purchases.	 Fingerprint OK for tap-to-pay (at new registers)	 Tap-to-pay (at new registers, only on NFC-enabled Android phones). Send money via app or email.	 Send money via email or phone number.	 Scan QR code
HOW IT WORKS				
 Uses NFC (radiowaves) to send your encrypted payment information.	Uses NFC. At old credit card machines, uses MST (magnetic fields).	Like a debit card. You recharge it. At new registers, uses NFC.	Uses PayPal network to transmit credit card or debit transactions.	Totally independent money system.

Esquemas de Pagos Móvil (2)

 Apple Pay	 Samsung Pay	 Google Wallet	 PayPal	 Bitcoin
SECURITY				
 Most secure. Retailers don't even get your credit card.	 Most secure. Retailers don't even get your credit card.	 Secure. Retailers don't get your credit card, but Google does.	 Secure. Retailers don't get your credit card, but PayPal does.	 Tricky. Secure, but you're on your own. Lose a password? Get hacked? Your money is gone.
PROS				
Quick and easy.	Quick and easy. Works everywhere.	Easy. Great for sending money to friends.	Easy. Great for sending money to friends.	Very private. Easy. Great for sending money to friends.
CONS				
Doesn't work everywhere. Only some places have NFC-enabled registers.	Magnetic option is annoying. You must hold it a certain way above the magnetic stripe reader.	Doesn't work everywhere. Only some places have NFC-enabled registers.	Only works at merchants who accept PayPal. It's a bit rare in person.	Difficult to obtain bitcoins. Rarely ever accepted. Few merchants use this.

Resumen

- Datos de tarjeta son peligrosos, protección de acuerdo a PCI es necesario, y un beneficio
 - Riesgo de brecha todavía es alto en el mercado
- No hay duda que la tecnología móvil es de gran interés para pagos
 - Proyecciones del mercado son enormes
- La tecnología móvil ha creado disrupción en el ambiente 'tradicional' de pagos
 - mPOS ha sido el impulso primario en el uso de móvil para pagos
- No debemos pensar en pagos móvil, debemos pensar en comercio móvil
 - Este es el interés primario de comerciantes
- Seguridad de datos es un componente crítico en despliegues para confiabilidad
 - Es la expectativa de consumidores



Preguntas (envíe por móvil)?



THALES



Gracias

JOSE DIAZ
THALES E-SECURITY
JOSE.DIAZ@THALESESEC.COM

ING. JORGE CAÑIZARES
ELECTRODATA
JCANIZARES@ELECTRODATA.COM.EC

www.thales-esecurity.com

THALES GROUP CONFIDENTIAL

