Industria de tarjetas de pago (PCI)
Norma de seguridad de datos

Aplicabilidad de la norma de seguridad de datos de la industria de tarjetas de pago (PCI DSS) en un entorno EMV
Documento de guía
Versión 1.0

Fecha de publicación: 14 de septiembre de 2010

Contenido

1 Resumen ejecutivo

Este documento compara y contrasta las posibilidades de reducción del fraude que ofrece EMV dentro del marco de la norma de seguridad de datos de la industria de tarjetas de pago (PCI DSS), así como explica por qué sigue siendo necesario implementar la norma PCI DSS en los entornos EMV que existen en la actualidad.

1.1 El papel que desempeña EMV

Las tarjetas inteligentes EMV se diseñaron e introdujeron para reducir los casos de fraude en las transacciones presenciales en las que usan tarjetas con banda magnética basadas en circuitos integrados (IC) que emplean claves criptográficas secretas para generar los datos de autenticación y autorización. Así, si se implementan firmemente las especificaciones EMV, se puede conseguir mitigar el riesgo de que se emplee una tarjeta interceptada para cometer una fraude presencial. Las implementaciones de EMV que utilizan diferentes valores de verificación de tarjetas en el chip, en comparación con los alojados en la imagen de la banda magnética, imponen una eficaz barrera frente a la creación de tarjetas de banda magnética falsas a partir de datos de imágenes de bandas magnéticas EMV interceptadas. Además, cuando se implementa junto con un PIN para verificar al titular de la tarjeta, EMV limita el impacto de las categorías de fraude de pérdida, robo o no recepción de la tarjeta. Es un hecho probado que, en aquellos países en los que se ha implementado EMV, se ha conseguido reducir de forma medible y significativa el fraude presencial.[1].

No obstante, EMV no puede proteger por sí solo la privacidad de, o el acceso improcedente a, datos de autenticación confidenciales o a los datos de los titulares de las tarjetas. Los entornos actuales de EMV de procesamiento y aceptación pueden procesar transacciones EMV y no EMV (como de banda magnética o introducción de claves PAN cuando motivos técnicos así lo requieran). Estas transacciones no EMV no ofrecen las mismas capacidades de reducción de fraude que las transacciones EMV y, en consecuencia, requieren protección adicional. Además, es importante tener presente que, en un entorno EMV, el número PAN no permanece confidencial en ningún punto de la transacción. De hecho, es necesario que el terminal de punto de venta procese el PAN sin cifrado alguno para poder llevar a cabo ciertos pasos clave en el proceso de transacción de EMV. La fecha de vencimiento y otros datos del titular de la tarjeta se transmiten también sin cifrar.

El potencial para que estos tipos de transacciones u otros elementos puedan peligrar y se usen fraudulentamente dentro del canal presencial y el canal en el que no está presente la tarjeta hace necesario implementar la norma PCI DSS en los entornos de aceptación de EMV actuales.

[1]Financial Fraud Action UK y la UK Cards Association. “Fraud The Facts 2010 – The Definitive Overview of Payment Industry Fraud and Measures to Prevent it”. Disponible en línea: http://www.theukcardsassociation.org.uk/files/ukca/fraud_the_facts_2010.pdf

1.2 El papel que desempeña la norma PCI DSS

La norma de seguridad de datos de la industria de tarjetas de pago (PCI DSS) incluye 12 requisitos operacionales y técnicos clave definidos por el Consejo sobre Normas de Seguridad de la PCI (Industria de tarjetas de pago). En lugar de centrarse en una forma específica de fraude, la norma PCI DSS busca proteger los datos del titular de la tarjeta y los datos de autenticación confidenciales allí donde estos datos estén presentes dentro del ecosistema de pago, limitando así su disponibilidad para los estafadores. La norma PCI DSS cumple con sus objetivos de seguridad de dos maneras:

- Garantizando la integridad de los componentes del sistema que puedan llevar a los datos del titular de la tarjeta y a los datos de autenticación confidenciales frente a posibles ataques físicos y lógicos.
- Protegiendo la confidencialidad de los datos del titular de la tarjeta al almacenarse en un entorno concreto, o datos confidenciales de autenticación y del titular de la tarjeta al transmitirse a través de una red pública o abierta.

1.3 Conclusiones

Los entornos de aceptación que hacen un uso eficaz de EMV pueden reducir sustancialmente el fraude en entornos presenciales, si bien, como se ha indicado anteriormente, el entorno EMV, tal y como se implementa hoy en día, no cumple automáticamente con los requisitos de la norma PCI DSS ni protege la confidencialidad del titular de la tarjeta ni los datos de autenticación personales. Si a esto le añadimos la opción de los comerciantes de procesar transacciones EMV y no EMV, resulta obvio que proteger la confidencialidad del titular de la tarjeta y los datos de autenticación personales es fundamental.

El diseño de la PCI DSS no distingue entre los mecanismos de seguridad de las transacciones subyacentes, sino que tiene por objetivo proteger el PAN y otros datos de autenticación confidenciales en sí, sin examinar el riesgo de fraude subyacente en caso de ponerse en riesgo estos datos. En el futuro, si EMV llegara a ser el único medio de pago en un canal presencial concreto, acompañado de un proceso de autenticación potente y adoptado a nivel global para transacciones sin presencia de tarjeta (CNP), la necesidad de mantener la confidencialidad del PAN y de otros datos de autenticación personales se vería reducida significativamente. Esto conllevaría la actualización de la PCI DSS para alinearla con el panorama de amenazas vigentes; en consecuencia, su aplicabilidad en relación con EMV se reduciría. Hasta entonces, EMV y PCI DSS conforman juntos un potente acercamiento de doble vertiente a los objetivos de reducción del fraude e incremento de la seguridad.

Así pues, a la hora de proteger el entorno de aceptación presencial actual, no deberá pensarse en EMV o en PCI DSS, sino más bien en una combinación de EMV y PCI DSS. Ambos son elementos esenciales en la lucha contra el fraude y la desprotección de los datos. Juntos proporcionan el mayor nivel de seguridad de los datos del titular de la tarjeta a lo largo de todo el proceso de transacción.

2 Ámbito de competencia

Este documento va dirigido a quien adopte la tecnología EMV, incluidos pero sin limitarse a ellos, vendedores, compradores, procesadores y emisores, o quienes validen los entornos PCI DSS, como un QSA (Evaluador de seguridad certificado) y un ISA (Evaluador de seguridad interna).

Se entiende y acepta que diferentes mercados en distintas regiones del mundo se encuentran en etapas diferentes en cuanto a madurez y despliegue de EMV. Estos mercados, aún inmaduros, trabajarán con el objetivo de cumplir con las recomendaciones de las marcas de tarjetas de pago y EMVCo.

El documento no proporciona detalles técnicos acerca de EMV ni de PCI DSS, ni tampoco instrucciones sobre cómo implementar EMV o PCI DSS, sino que da por hecho que el lector está familiarizado con ambos estándares. También se asume que la tarjeta IC y los fabricantes del terminal habrán incorporado las últimas directrices de EMV en sus productos. Se entiende que la mejor seguridad es la que proporcionan los terminales conformes con la última versión del programa de pruebas de seguridad de transacciones de PIN de la PCI.

Si le interesa, podrá obtener información detallada acerca de los estándares y las especificaciones EMV y PCI en los sitios web relevantes (*www.emvco.com y www.pcisecuritystandards.org*), así como en los documentos y guías propios de las diferentes marcas.

Se recuerda al lector que el papel del Consejo sobre Normas de Seguridad de la PCI es generar estándares de seguridad y otros documentos de guía y apoyo. Todos los aspectos relacionados con el cumplimiento, aplicación y adopción de estos estándares, incluidas todas las cuestiones relacionadas con posibles riesgos, son responsabilidad de los distintos planes de tarjeta individuales. Las preguntas de los lectores al respecto habrán de dirigirse a su contacto relevante en PCI DSS.

3 Seguridad de EMV y la norma PCI DSS

Para comprender la relación de los entornos actuales de procesamiento y aceptación EMV con la norma PCI DSS, es necesario analizar los elementos de datos presentes en las transacciones EMV, al igual que entender cómo podría usarse esta información con fines fraudulentos. Además, es importante entender la protección limitada inherente en las transacciones no EMV y cómo se puede usar fraudulentamente esta información si llegara a revelarse.

La tabla a continuación presenta los elementos de datos presentes en una tarjeta con chip EMV o disponibles al procesar una transacción EMV, así como por qué están ahí. Es importante resaltar que tanto los datos almacenados en un chip para EMV como los datos enviados durante una transacción EMV contienen elementos de datos correspondientes al titular de la tarjeta y a datos de autenticación confidenciales que PCI DSS pretende proteger.

	Elemento de datos	Motivo de su presencia
Datos del titular de la tarjeta	PAN (Número de cuenta principal)	Necesario en datos sin cifrar para que las transacciones EMV puedan: ▪ identificar al titular de la tarjeta y resolver la transacción; ▪ facilitar el curso de la transacción; ▪ autenticar los datos en el punto de venta; ▪ habilitar la derivación de claves por parte del emisor.
	Nombre del titular de la tarjeta	Presente en un chip EMV. No es necesario transmitirlo en un mensaje de autorización.
	Código de servicio	Presente en los datos equivalentes a la pista 2 en el chip. Su propósito en EMV es permitir al emisor validar el valor o el código de verificación de la tarjeta si se incluye también en los datos equivalentes a la pista 2.
	Fecha de vencimiento	Siempre aparece en las tarjetas EMV sin cifrar y con una etiqueta de fecha de vencimiento específica. En caso de autorización en línea, la fecha de vencimiento incluida en los datos equivalentes a la pista 2 se transmitirán en el mensaje de autorización. Estos datos aparecen sin cifrar.

	Elemento de datos	Motivo de su presencia
Datos de autenticación confidenciales	Datos integrales en banda magnética	EMV puede opcionalmente contener datos equivalentes a la pista 1 y 2, con los mismos campos que los de una banda magnética. Con fines de continuidad, los datos equivalentes a la pista 2 se incluyen generalmente en solicitudes de autorización en línea de EMV. Estos datos aparecen sin cifrar. No obstante, cuando se usa un valor o un código de verificación de chip único, los datos equivalentes a la pista 2 difieren de los datos de la pista 2 de las bandas magnéticas y no se pueden utilizar para crear tarjetas de banda magnética fraudulentas. Solo en este caso los elementos de datos del titular de la tarjeta, tal y como se han descrito anteriormente, permanecen confidenciales.
	CAV2/CVC2/CVV2/CID	No entra en las especificaciones EMV. Los chips EMV no contienen esta información. Este código solo aparece impreso en la propia tarjeta.
	PIN/Bloqueo del PIN	La especificación EMV permite verificar al titular de la tarjeta sin que sea necesario estar en línea gracias al PIN almacenado en el propio chip; esto hace que, en caso de bloquearse el PIN, este no salga nunca del entorno del punto de venta. También se admiten otros métodos de verificación de la tarjeta (CVM), entre ellos el PIN en línea.

3.1 El entorno de la tarjeta de pago

La mayor parte de los entornos que actualmente procesan transacciones EMV son entornos híbridos que gestionan transacciones tanto EMV como no EMV. En estas circunstancias, proteger la confidencialidad del titular de la tarjeta y los datos de autenticación personales sigue siendo fundamental para garantizar la integridad de la cadena de pago.

3.1.1 Transacciones con banda magnética

En una transacción con banda magnética, los datos del titular de la tarjeta y los datos de autenticación personales se obtienen a partir de datos estáticos codificados dentro de la banda magnética de la tarjeta, y se envían al emisor (generalmente sin cifrar) para su autorización. La naturaleza estática de estos datos hace que se puedan copiar fácilmente bien directamente desde la tarjeta o interceptándolos al procesar la transacción. Los datos interceptados de la banda magnética se podrían después utilizar para crear tarjetas de banda magnética falsas que podrían emplearse en operaciones presenciales y en cajeros automáticos. Además, también es posible extraer de los datos de la banda magnética el número PAN y la fecha de vencimiento y utilizarlos en fraudes sin presencia de tarjeta (CNP), en aquellos casos en los que el canal CNP no utilice otros datos de autenticación diferentes a los disponibles en el canal presencial.

3.1.2 Derivación técnica alternativa

La mayoría de las tarjetas EMV contienen una banda magnética que ofrece compatibilidad con entornos previos no EMV o para garantizar respaldo técnico si el chip para EMV no pudiera leerse. La "derivación técnica alternativa" describe un proceso de excepción por el cual un dispositivo con capacidad EMV lee la banda magnética de la tarjeta EMV en lugar de los datos en el chip. En estos casos, los mecanismos de seguridad proporcionados por EMV se omiten y la seguridad de la transacción revierte a la de una banda magnética. En muchos mercados EMV maduros, no obstante, esta derivación técnica alternativa queda generalmente restringida y controlada, con lo que este tipo de fraude es limitado.

3.1.3 Introducción de clave PAN

La introducción de una clave PAN se usa como derivación técnica alternativa cuando no se puede leer una banda magnética o un chip. Para completar una transacción de introducción de clave PAN solo hace falta el número PAN, la fecha de vencimiento y la firma del cliente, con lo que esta técnica es fácilmente susceptible de fraude si se interceptan los datos del titular de la tarjeta en cualquier canal de aceptación. Si bien para introducir la clave PAN es necesario falsificar la firma del titular de la tarjeta, este método de verificación del titular es potencialmente menos fiable, ya que el comerciante podría verificar la firma incorrectamente, o simplemente no hacerlo. Este método de introducción de datos está restringido y controlado, y no se usa mucho en los entornos EMV maduros, lo cual limita el fraude por introducción de clave PAN.

3.1.4 Transacciones basadas en pedidos por teléfono o por correo

Los comerciantes a menudo utilizan este método para aceptar transacciones remotas en sus entornos de aceptación EMV. Como con la introducción de la clave PAN, el vendedor introducirá manualmente el número PAN y la fecha de vencimiento; no obstante, además de estos datos, el vendedor a menudo introducirá el código de seguridad de la tarjeta (el código de tres dígitos impreso en la tarjeta física) como parte del proceso de autorización de la transacción.

3.1.5 Transacciones EMV

En los entornos de aceptación EMV, la transacción EMV contiene datos valiosos para un estafador. Las situaciones de riesgo de los datos se pueden categorizar de la siguiente manera:

- El CVV/CVC del chip no es único: Si el CVV/CVC de la tarjeta EMV es igual que el de la banda magnética, los datos equivalentes a la pista 2 interceptados se podrían usar para crear tarjetas de banda magnética con objeto de utilizaras en fraudes presenciales y de cajero automático.

- Lectura pormenorizada: Cuando se inserta íntegramente una tarjeta en un lector, como en un cajero automático, la banda magnética en sí se puede leer y los datos capturados se pueden utilizar para crear tarjetas de banda magnética.

- Desprotección del número PAN y fecha de vencimiento: EMVCo no exige que el número PAN y la fecha de vencimiento permanezcan confidenciales al procesar transacciones EMV. En la infraestructura de aceptación de pagos actual, es posible que se presenten transacciones de pago para su aprobación cuya autorización se base exclusivamente en el número PAN y la fecha de vencimiento. Esta información suele aparecen sin cifrar en las transacciones con banda magnética y EMV, y puede usarse fraudulentamente en otros canales de aceptación de pagos, como canales sin

presencia de tarjeta (CNP), que no utilizan datos de autenticación adicionales aparte de los disponibles en el canal presencial.

Estas amenazas hacen que los datos nativos de las transacciones EMV requieran más protección aparte de la que inherentemente proporciona EMV.

3.2 La norma PCI DSS y el entorno EMV actual

El estándar EMV ofrece seguridad en las transacciones e interoperabilidad global dentro de un entorno de transacción EMV. Las implementaciones de EMV que utilizan valores de verificación de tarjetas diferentes a los incluidos en la banda magnética mitigan el riesgo de que se intercepten datos de transacciones EMV con objeto de usarlos para crear tarjetas falsas. De la misma manera, EMV evita activamente que se produzcan ataques de clonación de tarjetas mediante el uso de métodos de autenticación de tarjetas mejorados y, al implementarse conjuntamente con un PIN como método de verificación del titular de la tarjeta, limita el impacto de las categorías de fraude por pérdida, robo o no recepción de la tarjeta. No obstante, EMV no protege la confidencialidad ni evita que se puedan interceptar ciertos elementos de datos de las transacciones.

En todos los entornos de aceptación, tal como se ha descrito en la sección 3.1 anterior, las transacciones de pago presentadas para su aprobación basándose exclusivamente en datos estáticos (como banda magnética, datos de claves introducidas manualmente, transacciones basadas en pedidos telefónicos o por correo, números PAN y fechas de vencimiento) tienen valor en sí y, a menos que se tomen las medidas adecuadas para impedir el acceso a los datos, se pueden usar para efectuar transacciones fraudulentas. Por estas razones, la norma PCI DSS sigue constituyendo una herramienta fundamental para proteger los datos estáticos.

La norma PCI DSS se aplica a todos los canales de pago posibles y a todas las maneras en las que puedan usarse datos de titulares de tarjetas para llevar a cabo una transacción.

3.3 Desarrollos futuros en la seguridad de las transacciones

El desarrollo de cambios, mejoras y nuevas oportunidades de pago es continuo. El uso de los métodos de autenticación que proporciona EMV y la introducción de otros datos de autenticación en el canal CNP, el número PAN y la fecha de vencimiento, ya no pueden por sí mismos ser suficientes para poder completar una transacción. Entre los futuros cambios podríamos ver la aparición de procedimientos mejorados de autenticación y procesos para todos los canales de las transacciones donde:

- EMV sea el único método de pago eficaz en un canal presencial. En un entorno EMV maduro, esto podría conllevar una migración a una tarjeta solo EMV, lo cual reduciría la amenaza del entorno híbrido permitiendo al mismo tiempo transmitir el número PAN del titular de la tarjeta, junto con otros datos confidenciales, sin cifrar.
- En los entornos que no migren a una tarjeta solo EMV, pero en los cuales EMV constituya el único métodos de pago presencial, resulta fundamental utilizar valores de verificación de la tarjeta alojados en el chip y en la banda magnética.
- El canal sin presencia de tarjeta utiliza datos de autenticación adicionales para verificar al titular de la tarjeta que no se pueden obtener en caso de interceptación del entorno de aceptación presencial.

En este caso, la necesidad de mantener la confidencialidad del número PAN y de otros datos de autenticación personales es significativamente menor. Por ello, la norma PCI DSS deberá

actualizarse para alinearse con el panorama de amenazas que pudiera existir, y su aplicabilidad en relación con EMV se reduciría en consecuencia.

3.4 Resumen

EMV ha de entenderse en el contexto de los entornos actuales de procesamiento de transacciones, donde la confidencialidad de los datos del titular de la tarjeta procedentes de transacciones EMV, junto con datos de autenticación personales procedentes de transacciones no EMV, sigue siendo fundamental para garantizar la integridad del sistema de pago.

Mientras que EMV es capaz de reducir substancialmente el fraude en las transacciones con presencia de tarjeta, no puede automáticamente satisfacer los requisitos de la norma PCI DSS en cuanto a protección de los datos del titular de la tarjeta y los datos de autenticación personales. Dado este contexto en las implementaciones actuales de EMV, la necesidad de proteger la confidencialidad del titular de la tarjeta y sus datos de autenticación personales de acuerdo con lo estipulado en la norma PCI DSS sigue siendo crítica en el esfuerzo global del sector por evitar el uso de datos en transacciones fraudulentas en otros entornos.

En el futuro, si EMV pasara a convertirse en el único medio de pago en un canal presencial concreto, juntamente con un proceso de autenticación robusto adoptado globalmente para transacciones sin presencia de tarjeta (CNP), la necesidad de mantener la confidencialidad del número PAN y otros datos de autenticación personales sería significativamente menor. Por ello, la norma PCI DSS deberá actualizarse para alinearse con el panorama de amenazas que pudiera existir, y su aplicabilidad en relación con EMV se reduciría en consecuencia.

El entorno EMV actual y la norma PCI DSS, junto con los estándares PA-DSS y PTS, son complementarios y ocupan cada uno un importante lugar a la hora de ofrecer un acercamiento integral a los objetivos de reducción global del fraude y protección de los datos del titular de la tarjeta en el sector de pagos. En los mercados que han migrado a EMV o están en proceso de hacerlo, las partes interesadas de la industria de pago deberán usar EMV y PCI DSS conjuntamente para reducir el fraude y aumentar la seguridad.

4 Referencia y glosario

4.1 Referencias

1. *EMV 4.2 Book 2 Security* (Libro 2 de EMV 4.2 Seguridad): www.emvco.com

2. *EMV 4.2 Book 3 Application Specification* (Libro 3 de EMV 4.2 Especificaciones de la aplicación): www.emvco.com

3. *PCI Data Security Standard, v1.2* (Estándar de seguridad de datos en PCI, v1.2): www.pcisecuritystandards.org

4. *EMV Issuer and Application Security Guidelines, v2.2 (Emisor de EMV y directrices de seguridad de la aplicación) de mayo de 2009*: www.emvco.com

5. *EMV 4.2 Book 4 Cardholder, Attendant, and Acquirer Interface Requirements* (Libro 4 de EMV 4.2 Requisitos de interfaz de comprador, asistente y titular de cuenta): www.emvco.com

6. *Glosario de términos, abreviaciones y siglas de PCI DSS y PA-DSS*

7. *Requisitos de seguridad PTS en PCI*

8. *Recommendations for EMV Processing for Industry-Specific Transaction Types (Recomendaciones para procesamiento EMV en tipos de transacciones específicas de la industria) de diciembre de 2008, v1.1*: www.emvco.com

9. Financial Fraud Action UK y la UK Cards Association. “Fraud The Facts 2010 – The Definitive Overview of Payment Industry Fraud and Measures to Prevent it.” Disponible en línea en: http://www.theukcardsassociation.org.uk/files/ukca/fraud_the_facts_2010.pdf

4.2 Abreviaciones y glosario

Puede consultar abreviaciones y definiciones en el *Glosario de términos, abreviaciones y siglas de PCI DSS y PA-DSS*.

A continuación incluimos algunas abreviaciones y definiciones adicionales.

Término	Definición
CNP	Sin presencia de tarjeta
CVM	Métodos de verificación de tarjeta
CVR	Resultados de verificación de tarjeta
DAC	Código de autenticación de datos
EMV	Formalmente Europay, MasterCard y Visa. Tarjeta de circuito integrado. Especificaciones para sistemas de pago. www.emvco.com
ICC	Tarjeta de circuito integrado
iCVV	Valor de verificación de tarjeta ICC
MO/TO	Pedidos por correo y pedidos telefónicos
POS	Punto de venta
SEPA	Zona única de pagos en euros
TRM	Gestión de riesgos de terminales
Sin presencia de tarjeta	Un tipo de transacción de pago (realizada por ejemplo por correo, teléfono o Internet), en la que el titular de la tarjeta no presenta la tarjeta al comerciante.
Tarjeta híbrida	Una tarjeta que contiene una banda magnética y un chip EMV al mismo tiempo.
Entorno de EMV	Un entorno en el que un terminal de punto de venta lee un chip EMV y lo utiliza para llevar a cabo una transacción EMV. Esto puede formar parte de un entorno híbrido que procese también datos y transacciones con banda magnética.
Entorno híbrido	Un entorno en el que el punto de venta puede leer tanto el chip EMV como la banda magnética con objeto de procesar transacciones EMV o con banda magnética.
Derivación técnica alternativa	Estado en el cual no se puede usar un chip y se recurre a otra forma de introducir datos, como leer la banda magnética o introducir una clave PAN para completar una transacción.

4.3 Reconocimientos

Son muchas las organizaciones que han contribuido individual y colectivamente en la redacción de este documento. Entre ellas: Los miembros del Consejo de Asesores del PCI, el Grupo de Interés Especial de Ámbito de Aplicación, miembros de la comunidad QSA, EMVCo, bancos, proveedores, comerciantes y consultores independientes. A todos ellos les agradecemos enormemente sus comentarios y el apoyo prestado.