



Payment Card Industry (PCI) Datensicherheitsstandard

PCI-DSS-Gültigkeit in einer EMV-Umgebung Ein Leitfaden Version 1.0

Freigabedatum: 14. September 2010

Inhalt

1 Zusammenfassung für die Geschäftsleitung.....	3
1.1 Die Rolle von EMV	3
1.2 Die Rolle von PCI DSS	4
1.3 Schlussfolgerungen	4
2 Umfang.....	5
3 EMV-Sicherheit und PCI DSS	6
3.1 Die Zahlungskartenumgebung.....	7
3.1.1 <i>Magnetstreifentransaktionen</i>	7
3.1.2 <i>Technisches Fallback</i>	8
3.1.3 <i>Eingabe des PAN-Schlüssels</i>	8
3.1.4 <i>Transaktionen bei Post-/Telefonbestellungen</i>	8
3.1.5 <i>EMV-Transaktionen</i>	8
3.2 PCI DSS und die derzeitige EMV-Umgebung	9
3.3 Zukünftige Entwicklungen für die Transaktionssicherheit.....	9
3.4 Zusammenfassung	10
4 Referenz und Glossar	11
4.1 Referenzen	11
4.2 Abkürzungen und Glossar	12
4.3 Danksagung.....	12

1 Zusammenfassung für die Geschäftsleitung

Dieses Dokument vergleicht die aktuellen Funktionen von EMV zur Betrugsreduzierung im Sicherheitsrahmen des PCI DSS (Payment Card Industry Data Security Standard, Datensicherheitsstandard der Zahlungskartenindustrie) und stellt sie gegenüber. Außerdem werden die Gründe dafür betrachtet, weshalb die Umsetzung von PCI DSS in heutigen EMV-Umgebungen weiterhin nötig ist.

1.1 Die Rolle von EMV

EMV-Smartkarten wurden entwickelt und eingeführt, um Betrugsfälle bei Zahlungen mit Magnetstreifenkarten im persönlichen Zahlungsverkehr zu reduzieren. In ihnen kommen integrierte Chips (ICs) zum Einsatz, die Authentifizierungs- und Autorisierungsdaten mithilfe kryptografischer Schlüssel codieren. Durch den zuverlässigen Einsatz der EMV-Spezifikationen kann die Nutzung kompromittierter Kartendaten zum Betrug im persönlichen Zahlungsverkehr vermindert werden. EMV-Implementierungen, bei denen auf dem Chip andere Prüfwerte als auf dem Magnetstreifen gespeichert werden, bieten effektiven Schutz vor der Erstellung gefälschter Magnetstreifenkarten aus kompromittierten Daten des EMV-Magnetstreifenabbilds. Wird EMV zudem in Verbindung mit PIN-Eingabe zur Identifikation des Karteninhabers eingesetzt, lassen sich die Auswirkungen von Betrugsfällen mit verlorenen, gestohlenen oder niemals erhaltenen Kreditkarten einschränken. Es gibt in Ländern, in denen EMV genutzt wird, klare Belege für eine messbare und signifikante Reduzierung von Betrugsfällen im persönlichen Zahlungsverkehr¹.

EMV alleine schützt jedoch nicht die Vertraulichkeit von oder den unangemessenen Zugriff auf sensible Authentifizierungs- bzw. Karteninhaberdaten. In aktuellen Zahlungsumgebungen werden unter Umständen sowohl Transaktionen mit EMV als auch solche ohne EMV durchgeführt (z. B. mit Magnetstreifen oder einer aus technischen Gründen erforderlichen Eingabe der primären Kontonummer (PAN)). Transaktionen, welche die EMV-Spezifikationen nicht erfüllen, bieten nicht denselben Schutz vor Betrug wie EMV-Transaktionen. Deshalb sind zusätzliche Schutzmechanismen erforderlich. Außerdem muss beachtet werden, dass die PAN in EMV-Umgebungen nicht geheim gehalten wird. Vielmehr ist es zur Durchführung wichtiger Schritte von EMV-Transaktionen sogar notwendig, dass das Point-of-Sale-Terminal die PAN als Klartext verarbeiten kann. Das Ablaufdatum und andere Karteninhaberdaten werden ebenfalls als Klartext übertragen.

Das Potenzial, dass diese Transaktionsarten und/oder Daten im persönlichen Zahlungsverkehr oder bei Zahlungen ohne vorliegende Karte offengelegt und für betrügerische Zwecke missbraucht werden, ist der Grund, weshalb die Umsetzung von PCI DSS auch heute in EMV-Transaktionsumgebungen notwendig ist.

¹ Financial Fraud Action UK und die UK Cards Association. „Fraud The Facts 2010 – The Definitive Overview of Payment Industry Fraud and Measures to Prevent it“ (Betrug, die Fakten 2010 – der definitive Überblick über Betrug im Zahlungsverkehr und Gegenmaßnahmen). Online verfügbar: http://www.theukcardsassociation.org.uk/files/ukca/fraud_the_facts_2010.pdf

1.2 Die Rolle von PCI DSS

Der Datensicherheitsstandard der Zahlungskartenindustrie PCI DSS umfasst 12 grundlegende technische und betriebliche Anforderungen, die vom PCI Security Standards Council (PCI SSC) festgelegt wurden. Anstelle einer Fokussierung auf eine spezifische Betrugs-kategorie soll PCI DSS den Karteninhaber und vertrauliche Authentifizierungsdaten überall dort schützen, wo diese Daten im Zahlungssystem vorhanden sind. Auf diese Weise wird Betrügern der Zugang zu diesen Daten so weit wie möglich verwehrt. PCI DSS erreicht dieses Sicherheitsziel auf zwei Wegen:

- Integritätssicherung von Systemkomponenten, die als Bindeglied zu vertraulichen Authentifizierungs- und Karteninhaberdaten dienen, und deren Schutz vor physischen und Hacker-Angriffen.
- Wahrung der Vertraulichkeit von Karteninhaberdaten, wenn diese in einer bestimmten Umgebung gespeichert werden, oder von Karteninhaber- und vertraulichen Authentifizierungsdaten bei der Übertragung über öffentliche und offene Netzwerke.

1.3 Schlussfolgerungen

In Zahlungsumgebungen mit effektiver Nutzung von EMV lassen sich Betrugsfälle im persönlichen Zahlungsverkehr erheblich reduzieren. Wie oben jedoch bereits detailliert beschrieben wurde, erfüllen derzeit implementierte EMV-Umgebungen nicht automatisch die Anforderungen von PCI DSS. Zudem wird die Vertraulichkeit von Karteninhaber- und Authentifizierungsdaten nicht geschützt. Kommt noch die Möglichkeit von Händlern hinzu, Transaktionen sowohl mit als auch ohne EMV zu bearbeiten, wird klar, dass der Schutz vertraulicher Karteninhaber- und Authentifizierungsdaten nötig ist.

Konzeptionell bedingt unterscheidet PCI DSS nicht zwischen den Sicherheitsmechanismen der zugrunde liegenden Transaktion. Stattdessen steht der Schutz der PAN und anderer vertraulicher Authentifizierungsdaten im Vordergrund, ohne dass das bestehende Betrugsrisiko bei Kompromittierung dieser Daten überprüft wird. Sollte sich EMV als alleiniges Zahlungsmittel in einem bestimmten Bereich des persönlichen Zahlungsverkehrs durchsetzen und zudem mit einem global eingeführten Prozess für die zuverlässige Authentifizierung bei Transaktionen ohne vorliegende Karte (CNP-Transaktion) gekoppelt werden, sänke zukünftig die Notwendigkeit erheblich, die PAN und andere vertrauliche Authentifizierungsdaten geheim zu halten. Infolge dessen würde PCI DSS aktualisiert werden, um sich mit den dann bestehenden neuen Bedrohungen auseinanderzusetzen. Sein Geltungsbereich bezüglich EMV würde sich dann entsprechend reduzieren. Bis dahin bilden EMV und PCI DSS zusammen einen leistungsstarken zweigleisigen Ansatz für die Zielsetzungen der Betrugsreduzierung und der Sicherheitsverbesserung.

Deshalb sollte die Sicherung der aktuellen Umgebung im persönlichen Zahlungsverkehr nicht als einzelne Aufgabe von entweder EMV oder PCI DSS, sondern vielmehr als gemeinsames Ziel von sowohl EMV als auch PCI DSS betrachtet werden. Beides sind wichtige Elemente im Kampf gegen Betrug und die Gefährdung von Daten. Über den gesamten Transaktionsvorgang hinweg bieten beide zusammen den größten Schutz für die Karteninhaberdaten.

2 Umfang

Dieses Dokument richtet sich an Anwender von EMV-Technologie, einschließlich, jedoch nicht begrenzt auf, Einzelhandel, Erwerb, Verarbeitung und Herausgabe, oder die Prüfung von PCI-DSS-Umgebungen wie durch Qualified Security Assessors (QSA) und Interne Sicherheitsberater (Internal Security Assessors, ISA).

Es wird verstanden und akzeptiert, dass sich die EMV-Einführung und -Systemreife weltweit je nach Region und Markt in unterschiedlichen Phasen befinden. In Märkten, in denen die Systemreife noch nicht erreicht wurde, wird auf das Einhalten der Empfehlungen von Kreditkartenunternehmen und EMVCo hingearbeitet.

In diesem Dokument sind keine technischen Details zu EMV oder PCI DSS oder Anweisungen zur Umsetzung von EMV oder PCI DSS enthalten. Vom Leser werden aber Kenntnisse beider Standards vorausgesetzt. Es wird angenommen, dass die Produkte von IC-Karten- und Terminal-Herstellern die neuesten EMV-Richtlinien erfüllen. Es besteht Einvernehmen darüber, dass Terminals, die gemäß der neuesten Version des Testprogramms für PCI-PIN-Transaktionen geprüft worden sind, die beste Sicherheit bieten.

Interessierte Leser können Details zu den EMV- und PCI-Standards und -Spezifikationen sowie markenspezifische Richtlinien und Dokumente auf den entsprechenden Websites www.emvco.com und www.pcisecuritystandards.org finden.

Die Leser werden an die Rolle des PCI Security Standards Council erinnert, Sicherheitsstandards und andere Richtlinien dokumente als Hilfestellung zu verfassen. Für alle Aspekte in Bezug auf die Konformität, Durchsetzung und Übernahme dieser Standards, einschließlich aller Probleme im Hinblick auf Risiken, sind die Verantwortlichen des jeweiligen Zahlungskartensystems zuständig. Bei Fragen diesbezüglich sollten sich Leser direkt an ihre zuständige PCI-DSS-Kontaktperson wenden.

3 EMV-Sicherheit und PCI DSS

Um zu verstehen, wie derzeitige EMV-Akzeptanz- und Verarbeitungsumgebungen mit PCI DSS in Verbindung stehen, müssen zuerst die Datenelemente von EMV-Transaktionen betrachtet werden. Außerdem muss verstanden werden, wie diese Daten von Betrügern missbraucht werden können. Zudem muss der begrenzte Schutz bei Transaktionen ohne EMV verstanden und zudem erkannt werden, wie die dabei verarbeiteten Informationen bei Offenlegung anfällig für betrügerische Aktivitäten sind.

In der unteren Tabelle sind die Daten aufgelistet, die auf einer EMV-Chipkarte gespeichert bzw. während der Bearbeitung von EMV-Transaktionen verfügbar sind. Außerdem werden Gründe für die Speicherung dieser speziellen Daten angegeben. Dabei muss beachtet werden, dass sowohl die Daten auf einem EMV-fähigen Chip sowie die bei EMV-Transaktionen gesendeten Daten Karteninhaberinformationen sowie vertrauliche Authentifizierungsdaten umfassen, die mithilfe von PCI DSS geschützt werden sollen.

	Datenelement	Grund für Speicherung
Karteninhaberdaten	Primary Account Number (PAN)	<p>Wird aus folgenden Gründen im Klartext für EMV-Transaktionen benötigt:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Identifikation des Karteninhabers und Durchführung der Transaktion <input type="checkbox"/> Vereinfachtes Transaktions-Routing <input type="checkbox"/> Datenauthentifizierung am Point-of-Sale <input type="checkbox"/> Ermöglichung der Schlüsselableitung durch den Emittenten
	Name des Karteninhabers	Auf einem EMV-Chip gespeichert Übertragung in einer Autorisierungsmeldung nicht erforderlich
	Servicecode	In den Spur 2 entsprechenden Daten auf dem Chip vorhanden. Ermöglicht dem Emittenten bei EMV-Transaktionen die Überprüfung des Kartenprüfcodes oder -werts, sofern ebenfalls in den Spur 2 entsprechenden Daten enthalten.
	Ablaufdatum	<p>Immer auf EMV-Karten im Klartext mit speziellem Tag gespeichert.</p> <p>Bei Online-Autorisierung wird das Ablaufdatum, das in den Spur 2 entsprechenden Daten gespeichert ist, in die Autorisierungsmeldung aufgenommen. Diese Daten sind im Klartext verfügbar.</p>

	Datenelement	Grund für Speicherung
Vertrauliche Authentifizierungsdaten	Vollständige Magnetstreifendaten	Optional kann EMV Spur 1 und Spur 2 entsprechende Daten enthalten. Diese Daten entsprechen den Feldern eines Magnetstreifens. Aus Gründen der Abwärtskompatibilität werden in EMV-Transaktionen die Spur 2 entsprechenden Daten bei Online-Autorisierungsanfragen übermittelt. Diese Daten sind im Klartext verfügbar. Wird hingegen ein eindeutiger Kartenprüfcode oder -wert verwendet, unterscheiden sich die Spur 2 entsprechenden Daten von den auf Spur 2 eines Magnetstreifens gespeicherten Daten. Daher können diese Daten nicht zur Fälschung von Magnetstreifenkarten herangezogen werden. In diesem Fall sind lediglich die oben beschriebenen Karteninhaberdaten anfällig.
	CAV2/CVC2/CVV2/CID	Nicht Teil der EMV-Spezifikation. EMV-Chips enthalten diese Daten nicht. Dieser Code ist lediglich auf die Karte aufgedruckt.
	PIN/PIN-Block	Die EMV-Spezifikation ermöglicht die Offline-Verifizierung des Karteninhabers durch die Nutzung einer im Chip gespeicherten PIN, sodass der PIN-Block die Point-of-Sale-Umgebung niemals verlässt. Andere Methoden für die Kartenprüfung werden ebenfalls unterstützt, unter anderem Online-PIN.

3.1 Die Zahlungskartenumgebung

Heutzutage werden EMV-Transaktionen am häufigsten in Hybridumgebungen durchgeführt, in denen neben Transaktionen mit EMV auch solche ohne EMV abgewickelt werden. Unter diesen Umständen ist der Schutz der Karteninhaber- und vertraulichen Authentifizierungsdaten weiterhin für die Integrität der Zahlungskette unerlässlich.

3.1.1 Magnetstreifentransaktionen

Bei Magnetstreifentransaktionen werden die Karteninhaber- und vertraulichen Authentifizierungsdaten aus den statischen Daten ausgelesen, die auf dem Magnetstreifen der Karte verschlüsselt sind, und an den Emittenten zur Autorisierung übermittelt (normalerweise als Klartext). Die statischen Daten lassen sich leicht entweder direkt von der Karte oder durch Abfangen der Daten während des Transaktionsvorgangs kopieren. Magnetstreifendaten können zur Fälschung von Magnetstreifenkarten verwendet und zum Betrug im persönlichen Zahlungsverkehr oder an Geldautomaten missbraucht werden. Außerdem lassen sich die PAN und das Ablaufdatum aus den Magnetstreifendaten extrahieren und für den Betrug bei CNP-Transaktionen einsetzen, wenn für die Zahlung keine weitere Authentifizierung verwendet wird, die über die im persönlichen Zahlungsverkehr verfügbaren Daten hinausgeht.

3.1.2 Technisches Fallback

Die meisten EMV-Karten enthalten auch einen Magnetstreifen, damit sie auch in Zahlungsumgebungen ohne Unterstützung von EMV eingesetzt werden können und damit bei Unlesbarkeit des EMV-Chips ein technisches Fallback möglich ist. Als technisches Fallback wird eine Ausnahme bezeichnet, bei der von einem EMV-fähigen Gerät der Magnetstreifen anstatt des EMV-Chips ausgelesen wird. In diesem Fall werden die Sicherheitsmechanismen von EMV umgangen und die Sicherheit der Transaktion fällt auf das Niveau von Magnetstreifen zurück. In vielen Märkten mit zunehmender Verbreitung von EMV findet ein technisches Fallback jedoch nur begrenzt und kontrolliert statt, damit es keine Grundlage für Betrug bietet.

3.1.3 Eingabe des PAN-Schlüssels

Die Eingabe des PAN-Schlüssels dient als Fallback, wenn ein Magnetstreifen oder Chip nicht gelesen werden kann. Um eine Transaktion mit der Eingabe eines PAN-Schlüssels durchzuführen, sind lediglich die PAN, das Ablaufdatum und die Unterschrift des Kunden erforderlich. Deshalb ist dieses Verfahren sehr anfällig für den Betrug mit Karteninhaberdaten in allen Akzeptanzverfahren. Bei Betrugsfällen unter Eingabe eines PAN-Schlüssels wird die Unterschrift des Karteninhabers gefälscht. Die Identifikation des Karteninhabers anhand der Unterschrift ist potenziell weniger zuverlässig, da der Händler Schwierigkeiten haben kann, die Fälschung zu erkennen, oder aber die Unterschrift womöglich erst gar nicht überprüft. Diese Methode der Dateneingabe wird begrenzt und kontrolliert sowie in Märkten mit zunehmender Verbreitung von EMV nur noch selten eingesetzt, wodurch sich der Betrug mithilfe von PAN-Eingabe in Grenzen hält.

3.1.4 Transaktionen bei Post-/Telefonbestellungen

Händler nutzen diese Methode manchmal, um entfernte Transaktionen in ihrer EMV-Umgebung zu akzeptieren. Wie bei der Eingabe des PAN-Schlüssels muss der Händler die PAN und das Ablaufdatum manuell erfassen. Allerdings gibt der Händler zusätzlich zu diesen Daten im Rahmen der Transaktionsautorisierung noch den Sicherheitscode der Karte (dreistelliger, auf der Karte aufgedruckter Code) ein.

3.1.5 EMV-Transaktionen

In EMV-Akzeptanzumgebungen umfasst die EMV-Transaktion Daten, die für betrügerische Zwecke missbraucht werden können. Szenarien, in denen ein Risiko für die Daten besteht, lassen sich weitgehend folgendermaßen kategorisieren:

- Fehlen eines eindeutigen Kartenprüfcode/-werts: Wird für eine EMV-Karte derselbe Kartenprüfcode/-wert wie für den Magnetstreifen verwendet, können die der Magnetspur 2 entsprechenden Daten erfasst werden und mit deren Hilfe eine Magnetstreifenkarte für den Betrug im persönlichen Zahlungsverkehr und an Bankautomaten erstellt werden.
- Auslesen des tatsächlichen Magnetstreifens: Wird die Karte vollständig in ein Lesegerät wie einen Geldautomaten eingeführt, kann der Magnetstreifen selbst ausgelesen und die erfassten Daten zur Fälschung von Magnetstreifenkarten verwendet werden.
- Gefährdung durch PAN und Ablaufdatum: EMVCo erfordert bei EMV-Transaktionen nicht die Geheimhaltung von PAN und Ablaufdatum. In der heutigen Infrastruktur für die Zahlungsakzeptanz ist es möglich, dass Transaktionen ausschließlich auf Grundlage der PAN und des Ablaufdatums genehmigt und autorisiert werden. Diese Informationen liegen normalerweise sowohl bei EMV- als auch

Magnetstreifentransaktionen als Klartext vor und könnten deshalb in anderen Zahlungskännen für betrügerische Handlungen missbraucht werden, zum Beispiel bei CNP-Transaktionen, bei denen keine weiteren Daten als die, die auch im persönlichen Zahlungsverkehr genutzt werden, zur Authentifizierung herangezogen werden.

Infolge dieser Bedrohungen müssen native EMV-Transaktionsdaten über die von EMV vorgesehenen Mechanismen hinaus geschützt werden.

3.2 PCI DSS und die derzeitige EMV-Umgebung

Der EMV-Standard bietet Transaktionssicherheit und globale Interoperabilität in einer EMV-Transaktionsumgebung. EMV-Systeme, bei denen Kartenprüfwerte zum Einsatz kommen, die sich von den auf dem Magnetstreifen gespeicherten Werten unterscheiden, senken das Risiko, dass kompromittierte EMV-Transaktionsdaten zur Erstellung gefälschter Karten verwendet werden. Gleichmaßen schützt EMV dank verbesserter Methoden zur Kartenauthentifizierung aktiv vor Angriffen durch geklonte Karten und schränkt zudem die Auswirkungen von Betrugsfällen mit verlorenen, gestohlenen oder niemals erhaltenen Kreditkarten ein, wenn zur Überprüfung des Karteninhabers zudem eine PIN-Eingabe erforderlich ist. EMV schützt jedoch nicht die Vertraulichkeit bestimmter Transaktionsdaten bzw. vor deren Gefährdung.

In allen Akzeptanzumgebungen wie oben in Abschnitt 3.1 angegeben sind Zahlungstransaktionen, die allein auf Basis statischer Daten zur Genehmigung vorgelegt werden, – z. B. Magnetstreifen, manuell per Tastenfeld eingegebene Daten, auf Post-/Telefonbestellungen basierte Transaktionen sowie PAN und Ablaufdaten – mit der Übermittlung wertvoller Daten verbunden. Diese können für Betrugszwecke ausgenutzt werden, wenn der Zugriff auf die Daten nicht durch entsprechende Maßnahmen unterbunden wird. Aus diesen Gründen bleibt PCI DSS weiterhin ein grundlegendes Mittel für den Schutz von statischen Daten.

PCI DSS gilt für alle möglichen Zahlungskännen und -weisen, bei denen Karteninhaberdaten zur Durchführung der Transaktion verwendet werden.

3.3 Zukünftige Entwicklungen für die Transaktionssicherheit

Änderungen und Verbesserungen werden kontinuierlich vorgenommen; zugleich vollzieht sich die Entwicklung neuer Zahlungsmöglichkeiten. Durch den Einsatz der von EMV bereitgestellten Authentifizierungsmethoden und die Einführung zusätzlicher Authentifizierungsmethoden für CNP-Zahlungsvorgänge ohne vorliegende Kreditkarte würden die PAN und das Ablaufdatum alleine nicht mehr zur Durchführung einer Transaktion ausreichen. Zu weiteren Änderungen könnte die Einführung verbesserter Authentifizierungsverfahren und -prozesse für alle Transaktionskännen zählen, damit Folgendes zutrifft:

- In einem bestimmten Vertriebskanal mit persönlichem Zahlungsverkehr ist EMV die einzige Zahlungsmethode. Bei entsprechender Verbreitung von EMV könnte dies die Migration auf eine Karte beinhalten, die nur noch EMV unterstützt. Auf diese Weise ließe sich die Bedrohung durch Umgebungen reduzieren, in denen parallel zu EMV-Transaktionen noch weitere Methoden mit Übertragung der PAN des Karteninhabers und anderer vertraulicher Informationen im Klartext zulässig sind.

- In Umgebungen, in denen die Migration zur ausschließlichen Nutzung einer EMV-Karte nicht durchgeführt wird, EMV aber im persönlichen Zahlungsverkehr als einzige Methode eingesetzt wird, ist es wichtig, dass sich die auf dem Chip und Magnetstreifen gespeicherten Werte zur Kartenüberprüfung unterscheiden.
- Bei Zahlung ohne vorliegende Karte werden zusätzliche Authentifizierungsdaten zur Überprüfung des Karteninhabers herangezogen. Diese zusätzlichen Daten können über die Nutzung der Karte im persönlichen Zahlungsverkehr nicht kompromittiert werden.

Unter diesen Umständen ist die Geheimhaltung der PAN und anderer vertraulicher Authentifizierungsdaten nicht mehr so stark von Bedeutung. Infolge dessen würde PCI DSS aktualisiert werden, um sich mit den dann bestehenden neuen Bedrohungen auseinanderzusetzen. Sein Geltungsbereich bezüglich EMV würde sich dann entsprechend reduzieren.

3.4 Zusammenfassung

EMV muss im Zusammenhang mit der derzeit bestehenden Umgebung für die Transaktionsbearbeitung betrachtet werden. Deshalb ist bei EMV-Transaktionen die Vertraulichkeit der Karteninhaberdaten sowie bei Transaktionen ohne EMV die Geheimhaltung vertraulicher Authentifizierungsdaten von grundlegender Bedeutung, damit die Integrität des Zahlungssystems gewahrt bleibt.

Während EMV das Betrugsrisiko bei Transaktionen mit vorliegender Kreditkarte erheblich senken kann, erfüllt es nicht automatisch die PCI-DSS-Anforderungen an den Schutz der Karteninhaberdaten und vertraulichen Authentifizierungsdaten. In Hinblick auf die derzeitigen EMV-Implementierungen ist der Schutz von Karteninhaberdaten und vertraulichen Authentifizierungsdaten, wie durch PCI DSS vorgeschrieben, weiterhin ein wichtiger Teil der Bemühungen in der Branche, dem Gebrauch dieser Daten bei betrügerischen Transaktionen in anderen Zahlungsumgebungen einen Riegel vorzuschieben.

Sollte sich EMV als alleiniges Zahlungsmittel in einem bestimmten Bereich des persönlichen Zahlungsverkehrs durchsetzen und zudem mit einem global eingeführten Prozess für die zuverlässige Authentifizierung bei CNP-Transaktionen gekoppelt werden, sänke zukünftig die Notwendigkeit erheblich, die PAN und andere vertrauliche Authentifizierungsdaten geheim zu halten. Infolge dessen würde PCI DSS aktualisiert werden, um sich mit den dann bestehenden neuen Bedrohungen auseinanderzusetzen. Sein Geltungsbereich bezüglich EMV würde sich dann entsprechend reduzieren.

Heute ergänzen sich EMV und PCI DSS sowie die PA-DSS- und PTS-Standards und bilden wichtige Elemente eines ganzheitlichen Ansatzes hinsichtlich der Zielsetzungen für die Betrugsreduzierung und den Schutz von Karteninhaberdaten in der Zahlungsverkehrsbranche. In Märkten, in denen die Migration zu EMV vollzogen wurde oder derzeit durchgeführt wird, sollten EMV und PCI DSS im Zahlungsverkehr gemeinsam eingesetzt werden, um gegen Betrug vorzugehen und die Sicherheit zu erhöhen.

4 Referenz und Glossar

4.1 Referenzen

1. *EMV 4.2 Book 2 Security* – www.emvco.com
2. *EMV 4.2 Book 3 Application Specification* – www.emvco.com
3. *PCI Data Security Standard, v1.2* – www.pcisecuritystandards.org
4. *EMV Issuer and Application Security Guidelines, v2.2 Mai 2009* – www.emvco.com
5. *EMV 4.2 Book 4 Cardholder, Attendant, and Acquirer Interface Requirements* – www.emvco.com
6. *PCI-DSS und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme*
7. *PCI PTS Security Requirements*
8. *Recommendations for EMV Processing for Industry-Specific Transaction Types, Dezember 2008, v1.1* – www.emvco.com
9. Financial Fraud Action UK und die UK Cards Association. „Fraud The Facts 2010 – The Definitive Overview of Payment Industry Fraud and Measures to Prevent it.“ (Betrug, die Fakten 2010 – der definitive Überblick über Betrug im Zahlungsverkehr und Gegenmaßnahmen) Online verfügbar:
http://www.theukcardsassociation.org.uk/files/ukca/fraud_the_facts_2010.pdf

4.2 Abkürzungen und Glossar

Abkürzungen und Definitionen finden Sie im *PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme*

Weitere Abkürzungen und Definitionen werden unten erklärt.

Begriff	Definition
CNP	Card Not Present, Karte nicht vorliegend
CVM	Card Verification Methods, Methoden für die Kartenprüfung
CVR	Card Verification Results, Ergebnisse der Kartenprüfung
DAC	Datenauthentifizierungscode
EMV	Ehemals Europay, MasterCard, Visa – Karte mit integriertem Chip Spezifikationen für Zahlungssysteme. www.emvco.com
ICC	Karte mit integriertem Chip
iCVV	ICC-Kartenprüfwert
MO/TO	Mail-Order/Telephone-Order, Post-/Telefonbestellung
POS	Point-of-Sale
SEPA	Einheitlicher Euro-Zahlungsverkehrsraum
TRM	Terminal-Risikomanagement
Card Not Present, Karte nicht vorliegend	Eine Zahlungstransaktion, die z. B. auf dem Postweg, per Telefon oder Internet durchgeführt wird und bei welcher der Karteninhaber die Zahlungskarte nicht dem Händler vorlegt.
Hybridkarte	Eine Karte, die sowohl mit einem EMV-Chip als auch mit einem Magnetstreifen ausgestattet ist.
EMV-Umgebung	Eine Umgebung, in der ein EMV-Chip von einem Point-of-Sale-Terminal gelesen und zur Durchführung einer EMV-Transaktion verwendet wird. Dies kann auch in einer sogenannten Hybridumgebung erfolgen, in der parallel Transaktionen und Daten von Magnetstreifenkarten bearbeitet werden.
Hybridumgebung	Eine Umgebung, in der sowohl EMV-Chips als auch Magnetstreifen vom Point-of-Sale gelesen und für EMV- und Magnetstreifentransaktionen verwendet werden können.
Technisches Fallback	Für den Fall, dass eine Nutzung des Chips nicht möglich ist, wird eine andere Eingabemethode, z. B. das Einlesen eines Magnetstreifens oder PAN-Schlüssels, verwendet, um eine Transaktion durchzuführen.

4.3 Danksagung

Viele Unternehmen haben einzeln und zusammen bei der Erstellung dieses Dokuments mitgewirkt, unter anderem: Mitglieder des PCI Board of Advisors, die Scoping Special Interest Group, Mitglieder der QSA Community, EMVCo, Banken, Anbieter, Händler und unabhängige Berater. Vielen Dank für die wertvollen Beiträge und die Unterstützung.