Sicherheitsdienstleistungen bei Karten-Zahlungssystemen

Sandro Amendola[1]
Waldemar Grudzien[2]

Kurzfassung:
Die deutsche Kreditwirtschaft wird künftig vermehrt Chipkarten auf der Grundlage des EMV-Standards ausgeben. Auf Protokollebene wird die Sicherheit dabei durch die in EMV definierten kryptographischen Abläufe gewährleistet. Die Veröffentlichung legt nach einer einführenden Betrachtung der Historie und einer kurzen Darlegung der Ziele der Kartengesellschaften die grundlegenden Sicherheitsmechanismen von EMV dar.

Stichworte: EMV, Chipkarte, chipbasierte Zahlungssysteme

Abstract:
The German banking industry issues more and more smart cards based on the EMV standard. EMV mechanisms ensure the security on cryptographic protocol layer. After a description of the history of EMV and the objectives of the card organisations this lectures explains the security mechanisms of EMV.

Key words: EMV, Smart Card, Smart Card based payment schemes

1 Einleitung

Sicherheit hat von jeher in der deutschen Kreditwirtschaft einen hohen Stellenwert. So werden in Karten-Zahlungssystemen sicherere kryptographische Verfahren sowie sichere Komponenten, wie Sicherheitsmodule in Terminals und in Hintergrundsystemen, verwendet.

Die Zahlungssysteme Europay, Mastercard und Visa (EMV) haben 1994 eine erste Version des gemeinsam entwickelten Standards für Chipkarten-Applikationen und Chipkarten-Terminals vorgelegt. Mit der Version 3.1.1 von 1998 wurde ein stabiler Stand erreicht. Im Dezember 2000 wurde die Version 4.0 unter dem Namen „EMV 2000“ veröffentlicht. Die Änderungen und Anpassungen, die zwischenzeitlich in Form von Bulletins veröffentlicht wurden, begründeten sich meist aus Erfahrungen aus der laufenden Implementierungsphase. An der grundlegenden Architektur von EMV hat sich jedoch nichts geändert. Eine konsolidierte Version 4.1 ist im Mai 2004 bereitgestellt worden.

Europay hatte, auch mit Zustimmung der deutschen Vertreter, im Jahr 1998 beschlossen, dass alle Terminals im Bereich von Europay mit Zieldatum 31. Dezember 2004 EMV-

[1] SRC Security Research & Consulting GmbH, Bonn
[2] Bundesverband Deutscher Banken e.V., Berlin

kompatibel sein sollen. Bis zu diesem Zeitpunkt sollten außerdem alle Karten, die das Zahlungssystem „Maestro“ unterstützen, mit einem Chip ausgestattet sein, der eine EMV-Anwendung trägt. Gleichlautende Beschlüsse gibt es auch für Mastercard und Visa. Im Vordergrund stand dabei der Wunsch, den Magnetstreifen durch Chip-Anwendungen zu ersetzen, da der Magnetstreifen das Ende seiner Entwicklungsmöglichkeiten erreicht hat und zusätzliche Anwendungen nur mit Hilfe der Chipkartentechnik verwirklicht werden können. Als gutes Bespiel dafür galt zu diesem Zeitpunkt die elektronische Geldbörse, die ohne Chipkarten-Technologie nicht denkbar wäre. Zwischenzeitlich entscheiden Issuer (Kartenausgeber) und Acquirer (Betreiber) flankiert durch *Incentives* und *Liability Shift* als Entscheidungsparameter selbständig, wann sie mit der Migration zu EMV beginnen.

Chipbasierte Transaktionen auf der Grundlage von EMV kommen bereits heute international beim Geldabheben am Automaten, beim Bezahlen am POS-Terminal (Point Of Sale) mittels Kreditkarte (z.B. „VISA“) sowie im Ausland mittels der Debit-Karte der deutschen Kreditwirtschaft („Maestro“) zum Einsatz.

Transaktionen mit der Debit-Karte der deutschen Kreditwirtschaft im Inland („electronic cash“ und GA) werden heute dagegen auf der Grundlage deutscher Standards durchgeführt, die wie EMV ein sehr hohes Sicherheitsniveau gewährleisten.

Der Einsatz der Chip-Technik geht – verglichen mit der Magnetstreifentechnik – mit höheren Kosten beim Kartenausgeber und beim Betreiber der Terminal-Infrastruktur einher. Die Einführung von EMV verursacht beim Kartenausgeber Kosten durch die notwendige Ausgabe von Chipkarten und beim Betreiber durch die Umstellung der Terminals auf chipbasierte Transaktionen. Hinzu kommen Änderungen der Hintergrundsysteme. Nicht alle Kartenausgeber und Betreiber sind daher heute bereit, EMV zu unterstützen. Die internationalen Kartenorganisationen begegnen dieser Herausforderung im Wesentlichen mit zwei Instrumenten: *Liability Shift* und *Incentives*. Beim *Liability Shift* handelt es sich um eine Umkehr der Haftung. Mit *Incentives* sollen Betreiber zur Aufstellung von EMV-fähigen Geldautomaten bewegt werden.

1.1 Liability Shift

Zur Förderung der zeitgerechten Umsetzung wurde eine ab 2005 gültige Umkehrung der Haftungsrisiken (*Liability Shift*) beschlossen. Das bedeutet, dass der Betreiber eines nicht EMV-fähigen Terminals – Geldautomat oder ein POS-Terminal – für alle Schäden einstehen muss, die auf die nicht mögliche Chipverarbeitung zurückzuführen sind. Dies zielte zunächst vor allem auf den Einsatz von Karten-Duplikaten, da mit EMV eine wirksame grenzüberschreitende Kartenechtheitsprüfung möglich wird.

Prinzipiell gilt der *Liability Shift* aber auch für Karten, die keine EMV-Anwendung tragen. Hier hat der Kartenausgeber alle Schäden zu tragen, die beim Einsatz von EMV nicht

entstanden wären. Allerdings sind mögliche zusätzliche Lasten für die Kartenausgeber differenziert zu betrachten. Schließlich ist jeder Kartenausgeber bereits heute für jede von ihm positiv autorisierte Transaktion verantwortlich. Vom *Liability Shift* werden alle Karten betroffen sein, deren Laufzeiten über Dezember 2004 hinausgehen.

MasterCard Europe (MCE) hat Mitte 2004 beschlossen, den ab 1. Januar 2005 eintretenden *Liability Shift*, der bis dahin nur *Counterfeit* umfasste, auf die Kategorien *„Lost And Stolen“* sowie *„Never Received“* auszuweiten.

Hintergrund ist das Ziel von MasterCard, die Nutzung *von PIN mit Chip* (EMV) noch stärker als bisher zu fördern und Debit- und Kredit-Verfahren weiter anzugleichen. Für Kreditkarten wird die Nutzung der PIN an POS-Terminals zwar noch nicht verpflichtend, aber stark empfohlen. Der erweiterte *Liability Shift* trifft also nicht-EMV-fähige Terminals und EMV-Terminals ohne PIN-Pad (Acquirer). Chipkarten werden gegenüber reinen Magnetstreifen-Karten besser gestellt (Issuer). Die Maßnahme soll auch dazu beitragen, die Unterschrift als Karteninhaber-Prüfung langfristig unattraktiv werden zu lassen. Da Visa Europe für alle Karten und alle EMV-Terminals ebenfalls per 1. Januar 2005 einen *Liability Shift* für Chip/PIN-Transaktionen beschlossen hat, fand insoweit eine Angleichung der Rahmenbedingungen statt.

Ab Januar 2005 wird also in den Fällen, in denen eine Seite — Karte oder Terminal — nicht EMV-fähig ist, für missbräuchliche Transaktionen mit einer gefälschten Karte (*Counterfeit*) der *Liability Shift* angewendet. Die Haftung ist dann immer von der Seite zu übernehmen, die nicht EMV-fähig ist. Da es bei dieser Missbrauchsart darauf ankommt, die gefälschte Karte als solche zu erkennen, spielt die PIN eine untergeordnete Rolle. Gliedert man den *Liability Shift* nach Art der möglichen Transaktionen, ergibt sich daraus das folgende Bild:

		Terminal-Fähigkeiten		
		Nur Magnetstreifen	Chip ohne PIN-Pad	Chip mit PIN-Pad
Eigenschaften der Karte	Nur Magnetstreifen	Kein *Liability Shift*	Issuer haftet	Issuer haftet
	Chip	Acquirer haftet	Kein *Liability Shift*	Kein *Liability Shift*
	Chip und PIN	Acquirer haftet	Kein *Liability Shift*	Kein *Liability Shift*

Für die Missbrauchskategorien *Lost and Stolen* sowie *Never Received* stellt sich die Tabelle etwas anders dar. Eingesetzt wird hier die Karte des Karteninhabers, so dass als wichtigstes Mittel zur Verhinderung von Missbrauch die Nutzung bzw. die Akzeptanz der

PIN herangezogen wird. Da systematisch Offline-PIN-Prüfungen vorkommen, ist die Kombination Chip und PIN für den *Liability Shift* maßgeblich.

		Terminal-Fähigkeiten		
		Nur Magnetstreifen	Chip ohne PIN-Pad	Chip mit PIN-Pad
Eigenschaften der Karte	Nur Magnetstreifen	Kein *Liability Shift*	Kein *Liability Shift*	Issuer haftet
	Chip	Kein *Liability Shift*	Kein *Liability Shift*	Issuer haftet
	Chip und PIN	Acquirer haftet	Acquirer haftet	Kein *Liability Shift*

Für deutsche POS-Terminals sind die Kombinationen ohne PIN-Pad nicht relevant. Da die meisten Terminals, die Maestro- und/oder Kreditkarten akzeptieren, in Deutschland gleichzeitig electronic cash unterstützen, besitzen sie ein sicheres PIN-Pad. Für Maestro als dezidiertes PIN-basiertes Zahlungssystem hat diese Kombination zumindest in Deutschland ebenfalls keine Bedeutung.

Wichtig ist noch der Hinweis auf die so genannten Fallback-Transaktionen, die magnetstreifenbasiert ablaufen. Sofern es sich um einen echten Fallback handelt, also der Chip aus technischen Gründen nicht genutzt werden kann, obwohl Karten und Terminal chipfähig sind, tritt der *Liability Shift* nicht in Kraft.

1.2 Incentives

Um die Migration zu beschleunigen, wurde für die Betreiber von Geldautomaten ein *Incentive* geschaffen. Dieses sieht seit 1999 eine zunehmende Absenkung der *Interchange* vor, wenn ein Geldautomat nicht EMV-kompatibel ist. Sobald ein Geldautomat umgerüstet ist, erhält er die normale *Interchange*. Vor dem Hintergrund der eher zögerlich angelaufenen Ausgabe von EMV-Karten hat MasterCard Europe neben einer erneuten Absenkung der *Interchange* eine Erweiterung des bisherigen Systems beschlossen. Zu den bisherigen zwei Fällen eines reinen magnetstreifenfähigen und eines EMV-fähigen Geldautomaten tritt als dritte Variante der Fall, dass an einen EMV-fähigen Geldautomaten eine EMV-Karte per Chip verarbeitet wird. Diese neue Variante wird als *„Full Chip EMV ATM“* bezeichnet. Hintergrund ist die Absicht, zukünftig nicht nur einen Anreiz zur Umstellung der Geldautomaten zu geben, sondern auch den Issuern von EMV-Karten einen Vorteil anzubieten. Daraus ergibt sich insgesamt folgende Systematik:

- *„Combined Chip EMV and Magnetic Stripe ATM“* – Die Transaktion muss an einem EMV-zugelassenen Geldautomaten stattfinden, bei der der Magnetstreifen gelesen wird, weil die eingesetzte Karte entweder keinen Chip besitzt oder der Chip nicht lesbar ist *(Fall Back)*.
- *„Full Chip EMV ATM“* – Die Transaktion muss an einem EMV-zugelassenen Geldautomaten stattfinden und sie muss auf Basis eines EMV-fähigen Chips auf der Karte ablaufen.
- *„Magnetic Stripe Only ATM“* – Die Transaktion muss an einem reinen magnetstreifenbasierten Geldautomaten stattfinden, wobei es unerheblich ist, welche Technik die eingesetzte Karte aufweist.

Für die beschriebenen drei Klassen wurden unterschiedliche *Interchanges* festgelegt, die für den innereuropäischen Betrieb gelten *(Intra-European ATM Fallback Service Fee)*. Der variable Anteil wurde durchgängig von 0,25 % auf 0,20 % abgesenkt. Für die Jahre 2006 bis 2007 wurden weitere Absenkungen erörtert, aber noch nicht beschlossen.

2 Sicherheitsmechanismen von EMV

EMV definiert ein System, bei dem im Terminal asymmetrische und in der Karte symmetrische und asymmetrische kryptographische Verfahren zum Einsatz kommen. Die Absicherung der Schnittstelle zwischen Terminal und Hintergrundsystem ist nicht Bestandteil von EMV, sondern muss vom Betreiber festgelegt werden. EMV legt kryptographische Mechanismen zum Schutz von Nachrichten fest, die

- zwischen der Karte und dem Terminal und
- zwischen der Karte und dem Hintergrundsystem ausgetauscht werden.

Ein grundlegendes Sicherheitsziel bei Karten-Zahlungssystemen ist das Erkennen von gefälschten Kundenkarten. Zur Abwehr dieser Angriffe bietet EMV nun international nutzbare kryptographische Sicherheitsmechanismen zur *Kartenechtheitsprüfung* an.

Dabei stellt das Terminal bzw. das Hintergrundsystem sicher, dass die Transaktion mit einer echten Karte durchgeführt wird. Soll eine Transaktion offline durchgeführt werden, d.h. ohne dass das Terminal mit dem Hintergrundsystem kommuniziert, dann stellt das Terminal durch die sogenannte *„Dynamische Datenauthentikation“* sicher, dass es sich um eine echte Karte handelt (dieses Verfahren gibt es gemäß Kap. 5 und 6 in [EMV B2] in drei Varianten). Bei der Variante *Dynamic Data Authentication (DDA)* sowie *Combined DDA/Application Cryptogram Generation CDA* authentisiert sich die Karte gegenüber dem Terminal mittels eines Challenge-Response-Protokolls auf der Grundlage des asymmetrischen Verfahrens RSA. Wird die Transaktion online durchgeführt, dann prüft das Hintergrundsystem die Kartenechtheit auf der Grundlage von Daten, die von der Karte

erzeugt wurden. In diesem Fall kommt ein symmetrisches Verfahren („Triple-DES“) zum Einsatz (vgl. Kap. 8 in [EMV B2]).

Neben der Kartenechtheitsprüfung ist die *Benutzer-Authentikation mittels PIN* ein weiterer Sicherheitsmechanismus, der von EMV chipbasiert unterstützt wird. Zwar wird dieser Sicherheitsmechanismus auch bei Transaktionen verwendet, die mit Magnetstreifenkarten ohne Chip durchgeführt werden, jedoch wird dabei die PIN online geprüft, was eine sichere Datenübertragung zwischen Terminal und Hintergrundsystem voraussetzt.

EMV erlaubt nun auch eine Benutzer-Authentikation, bei der das Terminal die PIN offline prüft. Dabei wird die PIN an die Karte übertragen, von dieser geprüft und das Ergebnis der Verifikation dem Terminal mitgeteilt. Insbesondere bietet EMV damit den Kartenausgebern die Möglichkeit die Benutzer-Authentikation mittels Unterschrift durch sichere Benutzer-Authentikation mittels PIN zu ersetzen.

Die Maestro-Karte unterstützt nur eine verschlüsselte PIN-Prüfung. Dabei wird die PIN vom Terminal innerhalb des sicheren Bereichs der Hardware verschlüsselt und als Geheimtext an die Karte übertragen. Die Offline-PIN-Prüfung spielt am deutschen GA keine Rolle, da dort die PIN nie an die Karte übertragen, sondern immer online verifiziert und auf dem Weg zum Hintergrundsystem immer verschlüsselt gesendet wird.

Bei Magnetstreifenkarten muss die Transaktionsnachricht vom Terminal erzeugt werden, da die Karte über keine Logik verfügt. EMV-Chipkarten können hingegen selber Kryptogramme generieren, so dass der Karteninhaber sozusagen über sein eigenes Sicherheitsmodul verfügt. Dabei berechnet die Karte ein sicheres „*Application Cryptogram AC*“, das die Authentizität der Transaktionsdaten sicherstellt. Dieses *AC* wird bei einer Online-Autorisierung an das Hintergrundsystem gesendet und dort geprüft. Das Hintergrundsystem sendet im Gegenzug eine kryptographisch gesicherte Antwortnachricht an die Karte zurück. EMV erlaubt damit eine sichere Ende-zu-Ende-Absicherung zwischen Karte und Hintergrundsystem.

3 Nachweis der Sicherheitseigenschaften

In Abbildung 1 ist die Struktur des kartengestützten Zahlungsverkehrs dargestellt. Dessen zentrale Einheit stellt die durch eine Bank emittierte Karte dar. Die Kundenbank (in Abbildung 1 die **Bank des Zahlungspflichtigen**) ist der Kartenausgeber (Issuer) der Karte. Mit Hilfe der Karte kann der Kunde (**Zahlungspflichtiger**) an einem Terminal über das Geld des mit der Karte verbundenen Kontos verfügen. Der verfügte Geldbetrag kann einem anderen Konto – zum Beispiel dem eines Händlers (**Zahlungsempfänger**) – gutgeschrieben werden. Hierzu benötigt wiederum der Händler eine Bank (**Bank des Zahlungsempfängers**). Ein Terminal kann ein Selbstbedienungsgerät wie Kontoauszugsdrucker und Geldautomat einer Bank, ein Kartenterminal bei einem Händler (POS-Terminal) oder auch ein Kundenterminal für das Internet-Banking sein.

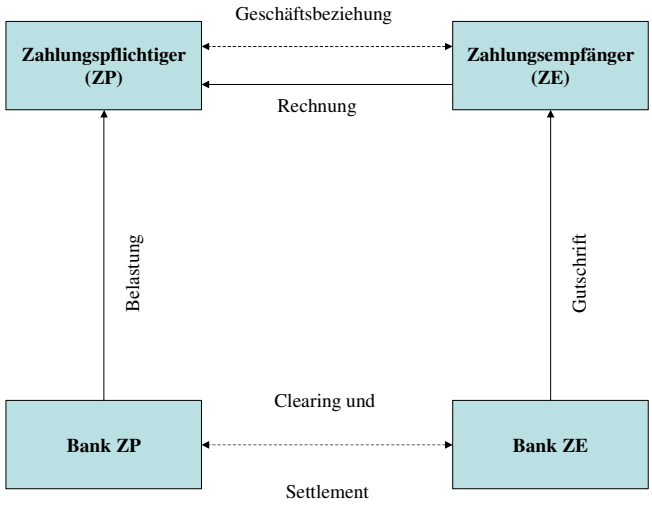

Abbildung 1: Struktur des kartengestützten Zahlungsverkehrs

3.1 Sicherheitsziele

Die Sicherheitsziele, die mit den in EMV definierten kryptographischen Abläufe (kryptographischen Protokolle) zu erreichen sind, lassen sich wie folgt formulieren:

Karteninhaber-Sicherheit: Eine gültige Transaktion kann nur zustande kommen, wenn der Kunde eine gültige Karte und die zugehörige PIN verwendet. Ein *TC*, der ein positives Transaktionsergebnis anzeigt, wird nur über den Betrag berechnet, den der Kunde vorher bestätigt hat. Eine Online-Autorisierung erfolgt ebenfalls nur über einen solchen Betrag.

Händler-Sicherheit bzw. GA-Betreiber-Sicherheit: Dem Händler wird ein positives Transaktionsergebnis nur dann angezeigt (bzw. im Fall des GA: Geld wird nur dann ausgegeben), wenn ein gültiger *TC* über den vereinbarten Betrag vorliegt oder eine gültige Online-Autorisierungsantwort zu diesem Betrag empfangen wurde.

Diese Sicherheitsziele ergeben sich daraus, dass ein auf EMV basierendes Karten-Zahlungssystem genau dann sicher ist, wenn sich alle Streitfälle klären lassen. Dies ist auf der Ebene des kryptographischen Protokolls genau dann der Fall, wenn ein positives Transaktionsergebnis, das sich in der Ausgabe eines *TC* durch die Karte ausdrückt, den beiderseits erwarteten Betrag enthält und die Berechtigung des Kunden nachgewiesen ist.

Nachfolgend wird begründet, dass die kryptographischen Protokolle keine Manipulationen durch einen Angreifer zulassen, die bewirken würden, dass ein Transaktionsergebnis zustande kommt, durch das ein nicht zu klärender Streitfall entstehen würde. Dabei werden zwei Varianten – ein Offline- und eine Online-Variante – beschrieben, welche den vereinbarten Betrag für alle Parteien sicherstellen.

Bei der Betrachtung wird folgendes vorausgesetzt. Es handelt sich um ein echtes Terminal, das bei der Offline-PIN-Prüfung die PIN immer verschlüsselt an die Karte sendet und im Online-Fall die Transaktion über ein Netz abgewickelt, das eine gegenseitige Authentikation von Karte und Hintergrundsystem unterstützt.

Wollte man die Sicherheit des Gesamt-Systems nachweisen, dann bliebe zu begründen, dass es keine Schwachstellen in den grundlegenden kryptographischen Algorithmen, in den beteiligen Komponenten oder im organisatorischen Umfeld gibt. Solche Schwachstellen werden zwar durch geeignete Maßnahmen ausgeschlossen, dies zu begründen ist jedoch nicht Gegenstand des vorliegenden Dokuments. Wenn auf der Ebene der kryptographischen Protokolle ein Streitfall entsteht, dann muss sich der Streitfall anhand der vorliegenden Transaktions- und Protokolldaten oder anderer Tatsachen klären lassen.

3.2 Offline-Autorisierung mit CDA und verschlüsselter Offline-PIN-Prüfung

In diesem Abschnitt wird der Ablauf einer Offline-Autorisierung mit CDA und verschlüsselter Offline-PIN-Prüfung untersucht, der nachfolgend kurz dargelegt ist:

1. Reset der Karte
2. Selektion der Maestro-Anwendung
3. Betragsbestätigung
4. Anwendungsinitialisierung durch das Kommando GET PROCESSING OPTIONS
5. Lesen und Prüfen der Anwendungsdaten
6. Verschlüsselte Offline-PIN-Prüfung
7. Kombinierte Dynamische Datenauthentikation CDA
8. Offline-Autorisierung durch das Kommando GENERATE AC (Die Karte erzeugt ein *„Transaction Certificate TC“*, das in die Erstellung der Signatur *Signed Dynamic Application Data* eingeht.)
9. Karte entnehmen
10. Beleg entnehmen

Es wird untersucht, welche Schlüsse man daraus ziehen kann, dass ein POS-Terminal eine Transaktion der Art „Offline-Autorisierung mit CDA und verschlüsselter Offline-PIN-Prüfung“ mit positivem Ergebnis abschließt. Der Fall, dass eine Transaktion nicht erfolgreich abgeschlossen wird, muss nicht im Detail untersucht werden, denn in diesem Fall könnte ein Streitfall nur dadurch entstehen, dass der Händler versucht, Daten zu dieser fehlgeschlagenen Transaktion einzureichen. Da das POS-Terminal aber in diesem Fall

nicht über ein gültiges *Transaction Certificate TC* verfügt, würde ein Nachprüfen der eingereichten Daten deren Fehlerhaftigkeit zeigen, so dass der Streitfall geklärt werden kann.

3.2.1 Authentizität der Transaktionsdaten

Das POS-Terminal schließt die Transaktion als erfolgreich ab, wenn es von der Karte eine Antwort auf das Kommando GENERATE AC erhält, die ein *TC* und eine gültige Signatur *Signed Dynamic Application Data* enthält (vgl. Kap. 6 in [EMV B2]).

Aus der Tatsache, dass alle Prüfungen, die das POS-Terminal für diese Nachricht durchführt, positiv sind, lassen sich dann die folgenden Feststellungen ableiten: Der vom POS-Terminal im Kommando GENERATE AC übergebene Betrag geht mit in die Daten ein, die zur Berechnung des Hashwertes *Transaction Data Hash Code* verwendet werden, denn er ist in der Liste *Card Risk Management Data Object List 1 (CDOL1)* spezifiziert. Der *Transaction Data Hash Code* geht wiederum in die Erstellung des Signaturwertes *Signed Dynamic Application Data* ein, den die Karte dem POS-Terminal in der Antwort auf das Kommando GENERATE AC sendet. Aufgrund der kryptographischen Eigenschaften der Hash-Funktion und der Signatur-Funktion kann die Prüfung der Signatur im POS-Terminal nur dann erfolgreich sein, wenn das POS-Terminal zur Berechnung denselben Betrag verwendet wie die Karte bei der Signatur-Erzeugung. Damit wird sichergestellt, dass das POS-Terminal die Transaktion nur dann als erfolgreich abschließt, wenn der vom POS-Terminal selbst an die Karte gesandte Betrag mit dem von der Karte verarbeiteten Betrag übereinstimmt. Unter der Voraussetzung, dass das POS-Terminal intern sicherstellt, dass es nur einen vom Kunden bestätigten und auch vom Händler akzeptierten Betrag verwendet, gilt: **Ein positives Transaktionsergebnis kann nur zustande kommen, wenn der darin enthaltene Betrag von Händler und Kunde akzeptiert wurde.**

Auch der Wert *Unpredictable Number UN*, die Zufallszahl des POS-Terminals, ist in der *CDOL1* als Teil der Daten spezifiziert, die in die Signaturberechnung eingehen (siehe Kap. 6.6.1 in [EMV B2]). Damit kann das POS-Terminal feststellen, dass der Signaturwert *Signed Dynamic Application Data* zur aktuellen Transaktion gehört. **Dies verhindert das Wiedereinspielen alter positiver Antworten auf das Kommando GENERATE AC.**

Der Wert *Cryptogram Information Data CID*, der angibt, ob die Transaktion durch die Karte erfolgreich abgeschlossen wurde, und das *Transaction Certificate TC* gehören zu den Daten, die in die Signaturberechnung des *Signed Dynamic Application Data* eingehen (siehe Kap. 6.6.1 in [EMV B2]). Damit ist sichergestellt, dass dem POS-Terminal eine negative Antwort der Karte nicht als eine positive vorgespiegelt werden kann und dass der Wert *TC* tatsächlich der von der Karte berechnete Wert ist und nicht verfälscht wurde. Damit ist sichergestellt: **Dem Händler wird ein positives Transaktionsergebnis nur dann angezeigt, wenn ein gültiger *TC* über den vereinbarten Betrag vorliegt.**

Die Karte muss so konfiguriert sein, dass wesentliche Tatsachen über die Transaktion authentisch vorliegen und dadurch die Berechtigung der Einreichung dieser Transaktion in einem eventuellen Streitfall nachweisbar ist. Insbesondere gehen z.B. gemäß [GA MAESTRO] in die Berechnung des *AC* ein: der Transaktionsbetrag und die Währung, ein eindeutiger Transaktionszähler der Karte *(ATC)*, so dass ein *TC* nur einmal eingereicht werden kann, *Cryptogram Information Data CID*, die zeigen, dass tatsächlich ein positives Ergebnis der Transaktion vorlag sowie die *Card Verification Result CVR*, die zeigen, dass eine PIN-Prüfung in der Karte erfolgreich war.

3.2.2 Kartenechtheitsprüfung

Da die Signatur *Signed Dynamic Application Data* mit einem privaten RSA-Schlüssel berechnet wird, dessen Echtheit anhand geeigneter Zertifikate geprüft wird, ist das Berechnen eines solchen Wertes ohne Besitz der korrekten Karte nicht möglich. Dabei wird vorausgesetzt, dass die Implementierung der Karte einerseits und ein sicheres Schlüsselmanagement im Zusammenhang mit der Personalisierung andererseits die Preisgabe des geheimen Schlüssels einer Karte verhindern. **Damit ist sichergestellt, dass die Transaktion mit einer echten Karte durchgeführt wurde.**

Damit die Sicherheitseigenschaften von *CDA*, die oben abgeleitet wurden, sicher zum Tragen kommen, muss noch folgendes sekundäres Ziel erreicht werden: **Wenn POS-Terminal und Karte über die Fähigkeit *CDA* verfügen, wird unter den verschiedenen Offline-Verfahren tatsächlich *CDA* ausgewählt (und nicht *SDA* oder *DDA*).**

Dies sieht man wie folgt: Die Fähigkeit der Karte, *CDA* durchzuführen, ist im Datum *AIP* codiert, welches in der Antwort auf GET PROCESSING OPTIONS an das POS-Terminal gesandt wird. Zunächst könnte dieser Wert bei der Übertragung verfälscht werden, da er in dieser Nachricht nicht kryptographisch abgesichert ist. Dies würde aber im Schritt *SDA* (falls *SDA* gewählt würde) bzw. Ableitung des öffentlichen Schlüssels der Karte (falls *DDA* gewählt würde) auffallen, da das Datum *AIP* bei der deutschen Karte zu den in die Signaturberechnung eingehenden Daten gehört (siehe [SECCOS DC], Kap. 7.2). Daher würde hier das POS-Terminal die Transaktion als fehlerhaft abbrechen, wenn der *TAC (Terminal Action Code)* so eingestellt ist, dass das Fehlschlagen von *CDA* zum Fehlschlag der Gesamttransaktion führt. Dies ist für deutsche POS-Terminals [DC POS] der Fall.

3.2.3 PIN-Prüfung

Im Rahmen von EMV soll die RSA-Verschlüsselung der PIN auch das Wiedereinspielen eines alten PIN-Blocks verhindern. Für die Eignung der gewählten Verschlüsselung zu diesem Zweck gelten die folgenden Ausführungen: Die Fragestellung ist, ob das RSA-Verfahren die Sicherheit der verschlüsselten PIN-Eingabe gemäß Kap. 7.2 in [EMV B2] garantieren kann.

Der Ablauf ist wie folgt: Die Karte sendet eine Zufallszahl *RND* in der Größe von acht Byte an das POS-Terminal. Das Terminal sendet eine nach dem RSA-Verfahren ver-

schlüsselte Nachricht *C* an die Karte, wobei der öffentliche Schlüssel *K* der Karte benutzt wird. Die verschlüsselte Nachricht *C* ist von der Form

$$C = e_{RSA,K}\ 7F \,||\, PIN \,||\, RND \,||\, Random\text{-}Padding,$$

wobei PIN für einen formatierten PIN-Block der Größe acht Byte steht und Random-Padding für vom POS-Terminal angehängte Zufallszahlen steht, die *C* bis zur Länge des Modulus auffüllen. Das hier betrachtete Angriffsszenario besteht darin, dass der Angreifer zunächst in der Lage ist, eine verschlüsselte PIN-Eingabe *C* zwischen POS-Terminal und Karte abzuhören, wobei der Karteninhaber die richtige PIN eingegeben hat und danach sich in den Besitz der Karte bringen kann. Die Frage ist jetzt, ob der Angreifer in der Lage ist, durch Kenntnis von *C* zu einer neuen Zufallszahl *RND'* eine Nachricht *C'* der Form

$$C' = e_{RSA,K}\ 7F \,||\, PIN \,||\, RND' \,||\, Random\text{-}Padding$$

zu produzieren, ohne die Nachricht *C* entschlüsseln zu müssen. Das verwendete Padding-Verfahren stellt gegen bisher bekannte Attacken, die die Homomorphie der RSA-Verschlüsselung ausnutzen, einen ausreichenden Schutz dar. Im Ergebnis lässt sich also feststellen, dass nach dem heutigen Stand der Wissenschaft **keine Methoden bekannt sind, die es erlauben würden, das Verfahren zur Übertragung der verschlüsselten PIN im Rahmen der Offline-PIN-Prüfung erfolgreich anzugreifen.**

Die Karte muss so konfiguriert sein, dass ein *TC* im Kommando GENERATE AC nur dann berechnet wird, wenn eine erfolgreiche Offline-PIN-Prüfung vorausgegangen ist. Das Bit 1 „Offline-PIN-Prüfung nicht durchgeführt" in Byte 1 im *Card Issuer Action Codes (CIAC)* „online" muss auf 1 gesetzt sein, d.h. die Karte muss eine Online-Autorisierung erzwingen, wenn keine Offline-PIN-Prüfung erfolgte. Die Karte darf außerdem nur eine verschlüsselte Offline-PIN-Prüfung zulassen. Dadurch wird nach dem heutigen Stand der kryptographischen Forschung sichergestellt, dass die PIN bei der Übertragung geheim gehalten wird, dass die Übertragung authentisch erfolgt und dass insbesondere keine früher aufgezeichnete verschlüsselte PIN übertragen werden kann. Dies ist bei der deutschen Maestro-Karte der Fall [GA MAESTRO]. **Also muss sich der Karteninhaber durch Kenntnis der PIN authentisiert haben.**

3.3 Online-Autorisierung mit gegenseitiger Authentikation

Nachfolgend ist der Ablauf der Online-Autorisierung mit gegenseitiger Authentikation kurz dargelegt:

1. Reset der Karte
2. Selektion der Maestro-Anwendung
3. Betragsbestätigung
4. Anwendungsinitialisierung durch das Kommando GET PROCESSING OPTIONS

5. Lesen und Prüfen der Anwendungsdaten
6. PIN-Eingabe, Vorbereitung der verschlüsselten Online-PIN-Prüfung in Schritt 8.
7. Vorbereitung der Online-Autorisierung durch die Karte (*„Authorisation Request Cryptogram ARQC“*; 1. GENERATE AC)
8. Onlinekommunikation mit dem Autorisierungssystem (PIN-Prüfung, Autorisierung, *„Autorisation Response Cryptogram ARPC*“)
9. Übergabe des einzureichenden Zertifikats an das Terminal durch die Karte (*„Transaction Certificate TC“*; 2. GENERATE AC)
10. Karte entnehmen

In diesem Abschnitt wird für den Fall der Online-Autorisierung geprüft, inwieweit ein nicht zu klärender Streitfall entsteht. Der Einfachheit halber wird hier zunächst der Fall betrachtet, dass nur eine Online-Autorisierung mit Online-PIN-Prüfung ohne zusätzliche Offline-Kartenechtheitsprüfung durchgeführt wird (Fall am deutschen GA). Eine mögliche Kombination von Online- und Offline-Verfahren wird anschließend kommentiert. Das Terminal schließt die Transaktion als erfolgreich ab, wenn es von der Karte eine Antwort auf ein zweites GENERATE AC erhält, die ein vom Terminal angefordertes *TC* enthält. Man kann nun wie im Offline-Fall eine Reihe von Schlussfolgerungen ziehen:

3.3.1 Authentizität der Transaktionsdaten

Die Karte berechnet ein *TC* nur dann, wenn ein solcher vom Terminal im zweiten GENERATE AC angefordert wurde. Dies geschieht wiederum in einem von zwei Fällen: Das Terminal hat eine korrekte Nachricht des Kartenausgebers erhalten, die einen Antwortcode mit positivem Ergebnis enthält oder die Online-Autorisierung konnte nicht durchgeführt werden (es wurde keine korrekte Antwort erhalten) und das Terminal versucht eine Offline-Autorisierung durchzuführen. Dieser zweite Fall wird unten unter den Nachträgen zu Sonderfällen behandelt. Da nach [MRL], Kap. 8.7, ein Integritätsschutz der Nachrichten zwischen Terminal und Kartenausgeber verlangt wird, der unter anderem den Antwortcode der Nachricht beinhaltet, ergibt sich: **Das Terminal fordert ein *TC* nur dann an, wenn der Kartenausgeber die Online-Anfrage mit einem positiven Antwortcode beantwortet hat.**

Der Kartenausgeber erzeugt einen positiven Antwortcode nur dann, wenn er sich von der Korrektheit der PIN überzeugt hat (für den Fall, dass keine Online-PIN-Prüfung erfolgt, siehe Nachträge). Unter der Voraussetzung, dass das Terminal intern sicherstellt, dass nur der vom Kunden bestätigte und auch vom Händler akzeptierte Betrag verwendet, gilt: **Ein positives Transaktionsergebnis kann nur zustande kommen, wenn der in der Online-Anfrage enthaltene Betrag von Händler und Kunde akzeptiert wurde.**

Insofern kann in einem eventuellen Streitfall der verbindliche Betrag immer anhand der Online-Nachrichten rekonstruiert werden. Dabei ist zu beachten, dass der Transaktionsbetrag jedenfalls in die Integritätsabsicherung der Nachrichten eingeht (siehe Kap. 8.7 in [MRL]).

Dem Händler wird ein positives Transaktionsergebnis nur dann angezeigt, wenn der Kartenausgeber die Online-Anfrage über den vereinbarten Betrag mit einem positiven Antwortcode beantwortet hat. Anhand der im Autorisierungssystem gespeicherten Daten der Online-Anfrage ist daher auch die Berechtigung der Einreichung dieser Transaktion in einem eventuellen Streitfall nachweisbar. **Das Wiedereinspielen alter positiver Antworten auf eine Online-Anfrage wird gemäß Kap. 8.7 in [MRL] durch Verwendung eines eindeutigen Sitzungsschlüssels oder eines eindeutigen Zählers verhindert.**

Deutsche Karten lehnen im GA-Maestro-System die Berechnung eines *TC* im zweiten GENERATE AC ab, wenn entweder

- die Online-Autorisierung gar nicht erfolgte (das Terminal hat keine korrekte Autorisierungsantwort erhalten). Dies wird dadurch sichergestellt, das Bit 8 in Byte 3 des *CIAC Offline* den Wert 1 hat;
- oder die Online-Autorisierung erfolgte, aber die Karte keine Autorisierungsdaten des Kartenausgebers erhält. Dies wird dadurch sichergestellt, dass Bit 7 in Byte 3 von *CIAC Offline* den Wert 1 hat und dass Bit 0 des Bytes *Anwendungssteuerung* den Wert 0 hat (wäre letzteres nämlich 1, so würde sich die Karte eventuell so verhalten, als habe eine erfolgreiche Kartenausgeber-Authentikation stattgefunden, auch ohne dass sie dies geprüft hat);
- oder die Online-Autorisierung erfolgte, aber das *ARPC* fehlerhaft ist. Dies wird dadurch sichergestellt, dass Bit 6 in *CIAC Offline* gesetzt ist.

Damit ist sichergestellt, dass die Karte ein *TC* nur dann berechnet, wenn sich der Kartenausgeber korrekt mittels *ARPC* authentisiert hat.

Bei deutschen Karten geht im GA-Maestro-System gemäß [GA MAESTRO] der Transaktionsbetrag in die Berechnung des *ARQC* und in die Berechnung des *TC* in Rahmen des zweiten GENERATE AC ein. Der Kartenausgeber stellt bei der Prüfung des *ARQC* fest, dass derjenige Transaktionsbetrag verwendet wurde, den ihm das Terminal integritätsgeschützt übermittelt hat, und die Karte verifiziert implizit durch die Prüfung des *ARPC*, dass alle Prüfungen des Kartenausgebers erfolgreich waren. **Damit ist auch sichergestellt, dass ein *TC* nur über den Betrag berechnet wird, den der Kunde vorher bestätigt hat.**

3.3.2 Kartenechtheitsprüfung

Die Echtheit der Karte kann vom Kartenausgeber dadurch festgestellt werden, dass er den von der Karte berechneten Wert *ARQC* prüft. Da dieser mit einem kartenindividuellen

Schlüssel berechnet wird und einen MAC über verschiedene Daten darstellt, kann er nur von der echten Karte erzeugt worden sein (vorausgesetzt, dass die Geheimhaltung der Schlüssel durch Implementierung der Geräte und Sicherheit der organisatorischen Abläufe gewährleistet ist.) Bei deutschen Karten gehen gemäß [GA MAESTRO] eine Zufallszahl des Terminals und der Wert *CID* in die Berechnung des *ARQC* ein. **Damit kann der Kartenausgeber sicherstellen, dass eine positive Antwort auf eine Online-Anfrage nur dann erfolgt, wenn sich der Karteninhaber durch Besitz der Karte authentisiert hat.**

3.3.3 PIN-Prüfung

Die PIN wird verschlüsselt an den Kartenausgeber übertragen und so in die Integritätssicherung einbezogen, dass keine alte PIN wiedereingespielt werden kann (vergleiche Kap. 8.7 in [MRL]). Wenn dagegen eine Online-Autorisierung ohne PIN-Prüfung erfolgt, kann das Autorisierungssystem anhand der *CVR* (die bei deutschen Karten im *ARQC* kryptographisch abgesichert ist) erkennen, dass keine Offline-PIN-Prüfung erfolgt ist. Insofern ist es nicht möglich, dem Kartenausgeber eine erfolgreiche Offline-PIN-Prüfung vorzuspiegeln, wenn diese nicht wirklich erfolgt ist. **Also muss sich der Karteninhaber durch Kenntnis der PIN authentisiert haben.**

3.3.4 Nachträge zu Sonderfällen und Varianten

Im Fall, dass eine Transaktion nicht erfolgreich abgeschlossen wird (d.h. es liegt kein gültiger *TC* vor), könnte ein Streitfall nur dadurch entstehen, dass der Händler bzw. GA-Betreiber versucht, Daten zu dieser fehlgeschlagenen Transaktion dennoch einzureichen. Ist bereits die Online-Autorisierung fehlgeschlagen oder hat sie gar nicht stattgefunden, so ist diese Tatsache den Protokolldaten der Autorisierungsstelle zu entnehmen und der Streitfall damit geklärt. War die Online-Autorisierung erfolgreich und die Transaktion wurde erst danach von der Karte oder Terminal abgelehnt, so muss das Terminal ein Storno (vergleiche [MRL]) abschicken. War dies der Fall, so ist die Situation wieder anhand der Protokolldaten der Autorisierungsstelle zu klären. War dies nicht der Fall, so liegt in jedem Fall eine Manipulation vor: Entweder muss der Händler das Terminal manipuliert haben, damit es trotz fehlgeschlagener Transaktion kein Storno durchgeführt hat oder es muss jemand die Antwort der Karte auf das zweite GENERATE AC so manipuliert haben, dass die Nachricht formal eine korrekte Transaktion angezeigt hat, aber der Wert des *TC* inkorrekt war. Es ist in einem solchen Fall also zu untersuchen, ob das Terminal manipuliert wurde (dies sollte deshalb feststellbar sein, weil die Terminals „tamper evident“ sein müssen). Ist es manipuliert worden, so ist dies weiterzuverfolgen, was außerhalb der hier gemachten Protokollbetrachtung liegt. Ist es nicht der Fall, so ist davon auszugehen, dass die Zahlung auch vom Terminal am Ende der Transaktion als korrekt gemeldet wurde. Dies bedeutet, dass zum Zeitpunkt der Transaktion diese für Kunde und Händler als erfolgreich angezeigt wurde.

Wenn Karte und Terminal in dem Fall, dass eine Online-Autorisierung misslungen ist, noch eine Offline-Autorisierung zulassen (dies ist bei deutschen GA-Maestro-Karten al-

lerdings nicht der Fall), so gelten dafür dieselben Aussagen, die in Abschnitt 3.2 für einen reinen Offline-Ablauf gemacht wurde: Genau dann, wenn die bereits dort genannten Voraussetzungen erfüllt sind, ist eine solche Form der Autorisierung geeignet, Sicherheit für Karteninhaber und Händler zu gewährleisten (insbesondere nur dann, wenn sowohl Karte als auch Terminal *CDA* unterstützen und keine Offline-Autorisierung ohne *CDA* zulassen).

4 Nutzung von EMV durch andere Anwendungen

Die Mechanismen von EMV können nicht nur von internationalen Zahlungssystemen – so soll das Zahlungssystem electronic cash ebenfalls auf EMV umgestellt werden – sondern z.B. auch für die TAN-Generierung verwendet werden. Die deutsche Kreditwirtschaft hat einen Standard [TAN D] definiert, über den mittels der Chipkarte der deutschen Kreditwirtschaft und einem Kartenleser TANs erzeugt werden können. Der Bankkunde hat mit seiner Karte und einem Leser damit auch immer seine TAN-Liste verfügbar. Dabei wird die TAN aus dem „*Application Cryptogram AC*“ abgeleitet, der über das EMV-Kommando GENERATE AC berechnet wird.

5 Referenzen

[DC POS] EMV-Debit-/Credit-POS-Terminals, Version 2.0, 16.11.2004

[EMV B2] Europay International, MasterCard International and Visa International, Integrated Circuit Card Specification for Payment Systems, Book 2, Security and Key Management, Version 4.1, May 2004

[GA MAESTRO] Schnittstellenspezifikation für die ZKA-Chipkarte, Geldautomaten- und Maestro-Anwendung, Version 2.0, 10.09.2003

[MRL] Maestro Global Rules, 07/2004

[MeOoVa96] Handbook of Applied Cryptography, A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, 1996

[SECCOS DC] Schnittstellenspezifikation für die ZKA-Chipkarte, EMV-Kommandos, Version 1.0, 19.11.2001

[TAN D] Schnittstellenspezifikation für die ZKA-Chipkarte, TAN-Anwendung (Debit), Version 1.0, 15.04.2003