Grobanalyse
des neuen Verfahrens
zur PIN-Berechnung und PIN-Prüfung für ec-Karten

Inhaltsverzeichnis

1 Zusammenfassung der Resultate

Dieses Dokument enthält eine zeitlich und aufwandmässig limitierte Grobanalyse der Sicherheit des neuen Verfahrens zur PIN-Berechnung und PIN-Prüfung für ec-Karten.

Die Sicherheit des neuen Verfahrens wurde für die vorgesehende Anwendung als ausreichend beurteilt. Gegenüber dem bisherigen Verfahren wurden signifikante Verbesserungen festgestellt. Diese liegen vor allem in den folgen Punkten:

- Einsatz von Tiple-DES statt DES;
- Einsatz kartenspezifische Schlüssel;
- Möglichkeit zum Schlüsselwechsel.

Aus Sicherheitsüberlegungen werden sowohl für die PIN-Generierung wie auch für die PIN-Verifikation jeweils die Alternativen 3 empfohlen.

Die weiteren Resultate und Empfehlungen dieser Untersuchung lauten zusammengefasst wie folgt:

1. Triple-DES bietet in bezug auf die *v*oraussehbaren technischen Entwicklungen eine Sicherheitsreserve von mehr als 10 Jahren. Dennoch sollte die Implementierung des Verfahrens so gestaltet werden, dass zu einem späteren Zeitpunkt der Ersatz des Chiffrieralgorithmus problemlos möglich ist.

2. Durch den Einsatz kartenspezifischer Schlüssel kann ein erfolgreicher kryptoanalytischer Angriff auf den Hauptschlüssel zwar nicht völlig ausgeschlossen werden, er ergibt sich jedoch ein nennenswerter Sicherheitsgewinn, der die zusätzliche Komplexität mehr als rechtfertigt.

3. Die Trennung der Verfahren für PIN-Generierung und PIN-Verifikation bringt per se keinen bedeutenden Zuwachs an Sicherheit. Die Trennung ist vor allem deshalb sinnvoll, weil sie die Möglichkeit der zufälligen Erzeugung von PINs un der späteren Einführung einer Selbstwahl-PIN bietet.

4. Die Berechnung der PINs aus den Kartendaten stellt unter Sicherheitsgesichstspunkten eine überflüssige, potentielle Schwachstelle dar. Wenn möglich ist Alternative 3 der PIN-Erzeugung durch einen Pseudozufallsgenerator vorzuziehen. Noch besser wäre die wirklich zufällige Erzeugung der PINs durch einen geeigneten Prozess.

5. Für die zukünftige Einführung von Selbstwahl-PINs sollten folgende Punkte berücksichtigt werden:

   - Die Möglichkeit von Selbstwahl-PINs mit mehr als vier Stellen, wie sie in den Alternativen 2 und 3 der PIN-Verifikation gegeben ist, sollte von Angang an vorgesehen werden
   - Der durch den Einsatz kartenspezifischer Schlüssel erzielte Sicherheitsgewinn geht durch die Einführung der Selbstwahl-PIN verloren, falls das Verfahren modifiziert wird.

6. Zusätzlich zum regulären Schlüsselwechsel auf der Basis des Verfallsjahres der Karte sollte die Möglichkeit für einen notfallmässigen Schlüsselwechsel geschaffen werden. Dies ist bei Verzicht auf die Ersatzautorisierung mit den Alternativen 3 auch leicht möglich.

7. Falls die Möglichkeit der Ersatzautorisation offen gehalten werden soll, wird vorgeschlagen, für die Berechnung der Prüfwerte auf der Karte separate Schlüssel zu verwenden, die nur im Bedarfsfall verteilt werden.

2 Das neue Verfahren

Das vorgeschlagene neue Verfahren zur PIN-Berechnung und PIN-Prüfung [1, 2] unterscheidet sich in seinen sicherheitsrelevanten Aspekten vom bisherigen Verfahren vor allem in den folgenden Punkten:

- Trennung von PIN-Berechnung und PIN-Prüfung;
- Einsatz kartenspezifischer Schlüssel;
- Ersatz von DES durch Triple-DES als Chiffrierverfahren;
- Möglichkeit zum Schlüsselwechsel;
- Option auf Selbstwahl-PIN.

2.1 PIN-Generierung

2.1.1 PIN-Generierung aus Karteninformationen

Die PIN wird aus Karteninformationen (X) und einem 16-Byte langen kartenspezifischen Schlüssel KK_{PINGEN} abgeleitet, wobei KK_{PINGEN} selbst aus den Informationen der Spur 3 und dem institutsweiten Schlüssel KGK_{PINGEN_INST} berechnet wird. Der Prozess der PIN-Generierung ist in Abbildung 2.1. dargestellt.

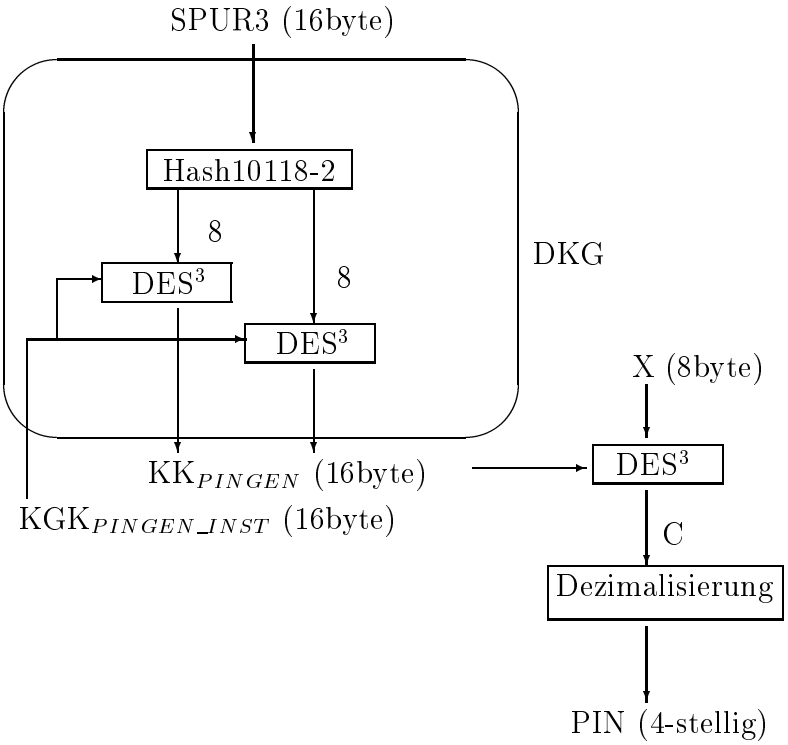

Abbildung 1: PIN-Generierung

Erläuterung:

- KK_{PINGEN} = DKG(SPUR3,KGK_{PINGEN_INST})
- C = e*KK_{PINGEN}(X)
- PIN = Dezimalisierung (C)

2.1.2 Dezimalisierung Alternative 1 (ZKA)

Die PIN ist eine 4-stellige Dezimalzahl, welche aus $C=C_{1x}C_{2x}\cdots C_{16x}$ berechnet wird:

1. Suchen von Links nach Rechts:
   - $PIN_i := C_{kx}$, wenn $C_{kx} \in \{0,1,\ldots,9\}$;
2. Falls weniger als 4 Ziffern gefunden werden:
   - $PIN_i := C_{kx} - 10$, mit $C_{kx} \in \{A,B,C,D\}$.
3. Eine führende Null wird durch die Ziffer "6", "7", "8" oder "9" ersetzt.

2.1.3 Dezimalisierung Alternative 2

C wird als Integer interpretiert. (C modulo 9000) + 1000 ergibt die PIN.

2.1.4 PIN-Generierung durch Pseudozufallsgenerator

Als weitere Alternative zu den beiden oben beschriebenen Verfahren kann die PIN auch unabhängig von den Kartendaten durch den folgenden Prozess bestimmt werden:

1. Initialisierung: Startwert z_0 Schlüssel K (jeweils 8 Byte) frei wählen.
2. Bestimmen der jeweils nächsten Pseudozufallszahl z_i:
   - z_i := eK('00..00', z_{i-1}) durch eine Verschlüsselung mit DES im CBC-Mode mit Schlüssel K und ICV='00..00'.
3. Bestimmen der PIN aus der Pseudozufallszahl $z_i = (z_{i,1}, z_{i,2}, \ldots, z_{i,16})$ durch die Suche von Links nach Rechts:
   - $PIN_1 := z_{i,x}$, wenn $z_{i,x} \in \{1,2,\ldots,9\}$
   - $PIN_k := z_{i,x}$, wenn $z_{i,x} \in \{0,1,\ldots,9\}$ für $k = 2,3,4$

2.2 PIN-Verifikation

2.2.1 PVN-Berechnung

Die beiden nationalen PIN Verification Values (PVN$j, j = 1, 2$) sind zwei 4-stellige Dezimalzahlen. Sie werden auf dem Magnetstreifen der ec-Karte und/oder in einer Positiv-Datei des Autorisierungssystems gespeichert.

Der PVNj wird aus Karteninformation (X) und einem 16-Byte langen kartenspezifischen Schlüssel $KK_{PVNGENj}$ abgeleitet, wobei $KK_{PVNGENj}$ selbst aus den Informationen der Spur 3 und dem institutsweiten Schlüssel $KGK_{PVNGENj\_INST}$ berechnet wird. Der Prozess der PVNj-Berechnung ist in Abbildung 2.1.1 dargestellt.

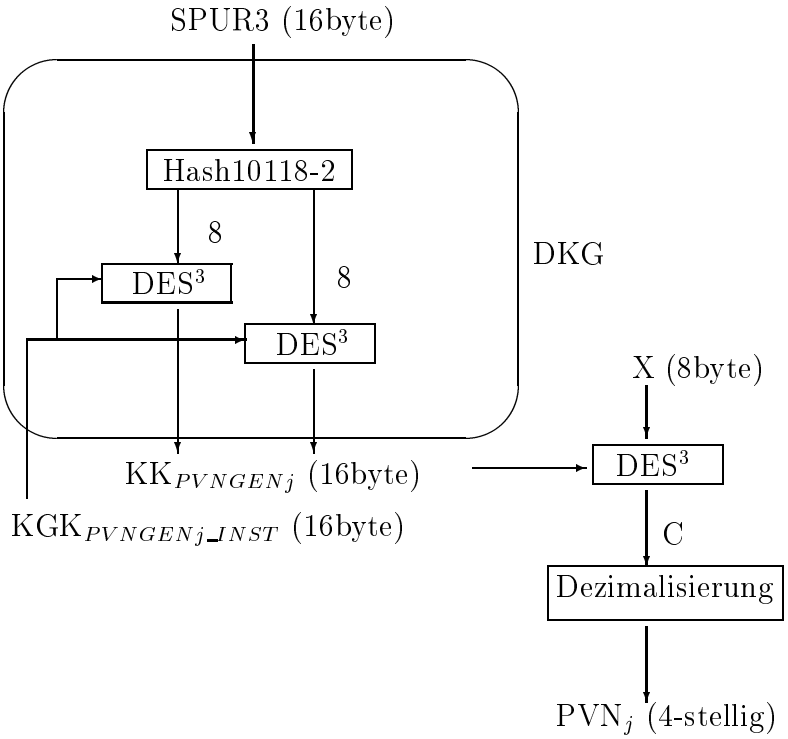

Abbildung 2: PVN-Berechnung

Erläuterung:

- $KK_{PVNGENj}$ =DKG(CID2, $KGK_{PVNGENj\_INST}$)

- PVNj = Dezimalisierung (C_j)
- $j = 1, 2$

2.2.2 Dezimalisierung

Die Dezimalisierung erfolgt wie in Abschnitt 2.1.4 beschrieben, jedoch ohne die Korrektur der ersten Ziffer, d.h. führende Nullen bleiben erhalten.

2.2.3 Alternative 1 (ZKA)

In den Wert X zur Bestimmung der beiden PVNs gehen neben dem Verfallsdatum und Teilen der Kontonummer die vier Stellen der Klartext-PIN ein.

2.2.4 Alternative 2

In den Wert X zur Bestimmung der beiden PVNs gehen neben dem Verfallsdatum und Teilen der Kontonummer die Länge L der PIN im Bereich $3 < L < 11$ und die L vorhandenen Stellen der Klartext-PIN ein.

2.2.5 Alternative 3

Auf die Dezimalisierung und Speicherung der Werte PVNj auf der Karte wird verzichtet. Statt dessen werden die vollständigen Werte C_j in der Positiv-Datei gespeichert. Die Berechnung erfolgt in diesem Fall mit dem in 2.2.4 definierten Inputwert.

3 Analyse

3.1 Sicherheit der eingesetzten Mechanismen

3.1.1 Triple-DES

Die Sicherheit des Triple-DES[1] wurde im Rahmen dieser Analyse nicht eigens untersucht. Nach dem Stand der in der zugänglichen Literatur dokumentierten Forschung ist das derzeit effizienteste Verfahren zum Brechen von Triple-DES die vollständige Sucher durch den Raum der 2^{112} möglichen Schlüssel.

Man geht heute davon aus, dass die vollständige Suche nach einem 56-bit Schlüssel (DES) bei vertretbaren Investitionen im Zeitraum von einigen Stunden oder wenigen Tagen möglich ist. Daher gelten heute 80-bit Schlüssel bei der Konzeption sicherer Systeme selbst im Bereich der taktischen Sicherheit als die untere Grenze.

Unter *diesen* Gesichtspunkt und unter Berücksichtigung des absehbaren technischen Fortschritts können die 112-bit Schlüssellänge des Triple-DES als heute und für mindestens weitere 10 Jahre als ausreichend gelten. Leider ist der Effekt auf die Sicherheit durch zukünftige Entwicklungen neuartiger Kryptoanalysetechniken nicht seriös vorhersagbar. Durch den Einsatz eines öffentlich bekannten und weit verbreiteten Chiffrierverfahren wie Triple-DES ist die Chance jedoch hoch, dass derartige Entwicklungen frühzeitig bekannt werden.

Aus diesem Grund wird dringend empfohlen, die Implementierung der Verfahren zur PIN-Generierung und PIN-Prüfung so zu gestalten, dass zu einem späteren Zeitpunkt der Ersatz des Chiffrieralgorithmus problemlos möglich ist.

3.1.2 Dynamische Schlüsselgenerierung

Die Ableitung der kartenspezifischen Schlüssel erfolgt mit demselben Mechanismus, der auch bei der ec-Karte mit Chip zum Einsatz kommt. Es wurde im Rahmen der Sicherheitsanalyse der ec-Karte mit Chip untersucht und nicht beanstandet. Auch hier gilt die oben formulierte Empfehlung, das Verfahren so zu gestalten, dass bei Bedarf ein Wechsel des Mechanismus möglich ist.

[1] Mit Triple-DES ist der sogenannte Two-Key Triple-DES nach ANSI X9.52 gemeint.

3.1.3 Dezimalisierung

1. Dezimalisierung der PIN nach Alternative 1

   Es ist offensichtlich und wohlbekannt, dass die Dezimalisierung nach Alternative 1 (2.1.1) zu einer signifikanten Ungleichverteilung der möglichen PIN-Werte führt. Dies bringt jedoch nach unserer Kenntnis in der Praxis keine wesentliche Beeinträchtigung der Sicherheit mit sich.

   Aus prinzipiellen Erwägungen ist es jedoch vorzuziehen, eine möglichst hohe Anzahl möglicher Werte möglichst gleichverteilt zu erzeugen. Eine Verbesserung könnte in diesem Sinne dadurch erreicht werden, dass auch PINs mit führenden Nullen zugelassen werden. Falls dies nicht erwünscht ist, kann die Verteilung immer noch dadurch verbessert, werden, dass vor jeder Generierung einer PIN eine Ziffer zwischen '1' und '9' statt zwischen '6' und '9' festgelegt wird, mit der eine allfällige führende '0' ersetzt wird.

   Es ist jedoch unklar, was die Aussage in [1] "beliebig, aber fest" bedeutet:

   - Erfolgt die Auswahl dieser Ziffer deterministisch oder zufällig?
   - Wird vor jeder Generierung der Wert neu gewählt, oder geschieht die Festlegung z.B. täglich?

   Durch die Einführung eines zufälligen Elementes in die PIN- Generierung würde der Sinn der Ableitung aus Kartendaten eigentlich zunichte gemacht. Eine vollständig zufällige oder pseudozufällige Generierung wäre in diesem Fall sinnvoller. (Der Satz "Eine führende Null wird durch die Ziffer Eins ersetzt." am Ende der Beschreibung von Alternative 1 in [1] sollte gestrichen werden.)

2. Dezimalisierung der PIN nach Alternative 2

   Die Dezimalisierung der PIN nach Alternative 2 (2.1.2) ist wegen der ausgeglicheneren Verteilung der Alternative 1 vorzuziehen.

3. Dezimalisierung des PVN

   Der Einfluss der Bytes in C auf PVN ist nicht gleichverteilt, z.B. gilt:

- Die Wahrscheinlichkeit, dass das sechzehnte Byte C_{16x} den PVN beeinflusst, ist kleiner als $(3/8)12 = 8 \times 10^{-6}$.
- Die Wahrscheinlichkeit, dass das erste Byte C_{1x} den PVN beeinflusst, ist grösser als 5/8.

Darin ist jedoch kein unmittelbares Sicherheitsproblem zu erkennen.

4. Verzicht auf Dezimalisierung der Prüfwerte

   Falls möglich, sollte auf die Dezimalisierung der Prüfwerte ganz verzichtet werden und diese statt dessen, wie in Alternative 3 (2.2.4) vorgesehen, in voller Länge in der Positiv-Datei abgelegt werden. Dieses Vorgehen bietet wichtige Vorteile für die PIN-Generierung (siehe 3.1.4) und die Möglichkeit zum Wechseln von Schlüsseln (siehe 3.3.3). Die parallele Prüfung von zwei verschiedenen Prüfwerten pro Karte erscheint - im Gegensatz zu den Alternativen mit dezimalisierter PVN - in diesem Fall überflüssig. Der zweite Prüfwert könnte sinnvoller als Vorbereitung für einen schnellen Schlüsselwechsel benutzt werden.

3.1.4 Zufallsgenerierung der PIN

Aus Sicherheitsgründen ist es vorzuziehen, auf die Berechnung der PIN aus den Kartendaten vollkommen zu verzichten, da die PINs im Prinzip auch zufällig oder pseudozufällig (wie in 2.1.4) gewählt werden könnten. Dadurch wird ein potentieller Angriffspunkt aus dem System eliminiert. Um weiterhin neue Karten mit alter PIN ausgeben zu können, ist es jedoch notwendig, dass die PIN einer Karte in bestimmten Fällen zurückgerechnet werden kann. Aus den PVN-Werten ist dies nur sehr umständlich durch Ausprobieren aller möglichen PINs möglich. Wenn jedoch die vollständigen Prüfwerte C_j (bzw. einer davon) in der Positiv-Datei vorhanden sind, ist dies gleichbedeutend mit einer verschlüsselten Speicherung der PIN und es ist möglich, in der Sicherheitsbox Funktionen für die Neuberechnung des Prüfwertes bei Karten- oder Schlüsselwechsel zu implementieren.

Eine wirklich zufällig Erzeugung wäre für diese Anwendung prinzipiell einer pseudozufälligen Erzeugung vorzuziehen, da die Berechnung nicht zu einer anderen Zeit oder an einem Ort wiederholt werden muss - und in der Tat gar nicht wiederholbar sein sollte. Wenn aus Gründen der Implementierung

dennoch eine pseudozufällige Erzeugung gewählt wird, ist gegen das beschriebene Verfahren (2.1.4) aus kryptologischer Sicht nichts einzuwenden. Es ist jedoch zu beachten, dass der Initialwert und der Schlüssel (wie alle anderen kryptographischen Schlüssel) echt zufällig gewählt und geheim gehalten werden müssen.

3.2 Trennung von PIN-Generierung und PIN-Verifikation

Der Sicherheitsgewinn durch die Trennung der Verfahren und der Schlüssel zur PIN-Generierung und zur PIN-Verifikation ist nicht offensichtlich und hängt von den Details der relevanten Bedrohungen ab.

Da die Anzahl der möglichen PINs (notwendigerweise) so gering ist, dass eine maschinell unterstützte vollständige Suche mit geringem Aufwand möglich ist, kann sowohl der Schlüssel für die PIN-Generierung, wie auch der Schlüssel für die PIN-Verifikation dazu dienen, zu einer vorhandenen Karte die zugehörige PIN zu bestimmen.

Die Situation stellt sich anders dar, wenn man die Fälschung von Karten in Betracht ziehen muss. Der Schlüssel für die PIN-Generierung kann nicht verwendet werden, um den korrekten PVN zu beliebigen Kartendaten zu bestimmen. Falls diese Bedrohung daher nicht durch die Verwendung einer Positiv-Datei aufgefangen wird, ergibt sich ein Vorteil aus einer begrenzten Verbreitung des Schlüssels für die PIN-Verifikation.

Die Trennung von Generierung und Verifikation ist schon deshalb vorteilhaft, weil dadurch die Möglichkeit der zufälligen Erzeugung von PINs (siehe 3.1.4) und der späteren Einführung einer Selbstwahl-PIN geschaffen wird. Da für eine Selbstwahl-PIN jedoch u.U. mehr als vier Stellen vorzuziehen sind, sollte für die PIN-Verifikation eine Variante gewählt werden, die diese Möglichkeit zulässt, d.h. Alternative 2 (2.2.3) oder 3 (2.2.4).

3.3 Einsatz kartenspezifischer Schlüssel

3.3.1 Bestimmung des Schlüssels im heutigen Verfahren

Es ist bekannt, dass beim heutigen Verfahren, bei dem die PIN mit einem globalen Schlüssel aus bestimmten Kartendaten abgeleitet wird, der globa-

le Schlüssel mit der Kenntnis von fünf Paaren von zusammengehörenden Kartendaten und PIN und fünf Klartestangriffen auf DES berechnet werden kann. Ein Klartextangriff mit vollständiger Schlüsselsuche benötigt dabei im Mittel 2^{55} Verschlüsselungsoperationen. Der Schlüssel kann demnach mit durchschnittlich 5×2^{56} Verschlüsselungsoperationen bestimmt werden.

Die Notwendigkeit der Kenntnis von fünf PINs erklärt sich darauf, dass aus der Kenntnis einer einzigen PIN der Schlüssel noch nicht eindeutig gestimmt werden kann. Allerdings kann man durch die vollständige Suche die Menge der $2^{56}/9000 = 2^{43}$ Schlüssel bestimmen, die die gegebenen Kartendaten auf die gegebene PIN abbilden. Durch eine zweite PIN kann der Angreifer eine zweite Menge von 2^{43} möglichen Schlüsseln bestimmen. Der gesuchte Schlüssel liegt im Schnitt dieser beiden Mengen, die im Mittel etwa 2^{30} Schlüssel umfasst. Nach etwa fünf derartigen Versuchen ist zu erwarten, dass die Schnittmenge mit hoher Wahrscheinlichkeit[2] nur noch einen einzigen, also den gesuchten Schlüssel enthält.

3.3.2 Bestimmung von $\mathrm{KGK}_{PINGEN\_INST}$ und $\mathrm{KGK}_{PVNGENj\_INST}$ im neuen Verfahren

Wie die folgende Überlegung zeigt, kann auch durch den Einsatz kartenspezifischer Schlüssel der beschriebene Angriff nicht verhindert werden. Der Aufwand für die Durchführung wird aber durch die Massnahme deutlich erhöht.

Aus der ersten bekannten PIN werden, wie oben beschrieben, die 2^{43} möglichen Kandidaten für den kartenspezifischen Schlüssel dieser Karte $\mathrm{KK}_{PINGEN1}$ errechnet (unter Annahme, dass weiterhin DES zum Einsatz käme). Da aus der Kenntnis eines kartenspezifische Schlüssels und der Kartendaten der zugehörige globale Schlüssel $\mathrm{KGK}_{PINGEN\_INST}$ durch vollständige Suche eindeutig bestimmt werden kann, ergeben sich daraus 2^{43} mögliche Kandidaten für $\mathrm{KGK}_{PINGEN\_INST}$. Nach dem gleichen Verfahren werden aus einer zweiten, zu einer anderen Karte gehörenden PIN zunächst 2^{43} Kandidaten für $\mathrm{KK}_{PINGEN2}$ und damit 2^{43} mögliche Werte für $\mathrm{KGK}_{PINGEN\_INST}$ bestimmt. Mit fünft verschiedenen PINs und $5 \times 2^{43} \times 2^{56} = 2^{101}$ Verschlüsselungsoperationen wäre also trotz der zweistufigen Schlüsselhierarchie die Bestimmung des globalen Schlüssels weiterhin möglich.

[2]Die genaue Bestimmung dieser Wahrscheinlichkeit in Abhängigkeit von der Anzahl der PINs ist relativ aufwendig und für die vorliegende Betrachtung unnötig.

Natürlich liegt der entsprechende Aufwand für Triple-DES noch weit höher, nämlich bei schätzungsweise $9 \times 2^{99} \times 2^{111} = 2^{213}$ Verschlüsselungsoperationen. Der Faktor 2^{111} gilt unter der Annahme, dass die vollständige Suche die effizienteste Möglichkeit zur Bestimmung des Schlüssels aus einem(!) bekannten Klartext darstellt. Der Faktor 9×2^{99} bliebe dagegen auch für den Fall erhalten, dass in Zukunft ein wesentlich leistungsfähigeres Kryptoanalyseverfahren für Triple-DES entdeckt werden sollte.

Eine analoge Überlegung führt im Fall, dass der Schlüssel $\mathrm{KGK}_{PVGENj\_INST}$ aus bekannten Paaren von PIN und PVNj bestimmt werden sollen, auf dasselbe Resultat.

3.3.3 Einfluss der Selbstwahl-PIN

Die obigen Überlegungen gelten nur unter Voraussetzung einer unveränderlichen PIN. Falls der Karteninhaber, wie es als Option vorgesehen ist, seine PIN ändern kann, benötigt er nicht fünf bzw. neun verschiedene Karten mit bekannter PIN, um den Schlüssel eindeutig zu bestimmen, sondern muss lediglich entsprechend oft eine neue PIN wählen. Da er lediglich eine zusätzliche Schlüsselsuche nötig um aus dem eindeutigen KK auch KGK zu bestimmen. Daraus ist zu folgern, dass es sinnvoll sein könnte, bei Einführung der Selbstwahl-PIN vorzusehen, dass sich der kartenspezifische Schlüssel beim Wechsel der PIN ändert. Dazu könnten etwa die drei Byte des Fillers dienen, indem man sie bei jedem PIN-Wechsel hochzählt und be Überlauf weitere PIN-Änderungen unterbindet.

3.4 Möglichkeit zum Schlüsselwechsel

Obwohl durch den Einsatz von Triple-DES und kartenspezifischer Schlüssel die direkten Möglichkeiten für die Kompromittierung der globalen Schlüssel eingeschränkt werden, ist dennoch mit anderen Angriffen, wie physischer Zugriff auf ein Sicherheitsmodul, Bestechung, Erpressung etc. zu rechnen. Aus diesem Grund ist die Möglichkeit zum Wechseln globaler Schlüssel eine unverzichtbare Anforderung. Dies gilt in besonderem Masse für Schlüssel, die zum Zwecke der Ersatzautorisierung an mehrere Stellen weitergegeben werden müssen oder sogar in Geldausgabeautomaten vor Ort installiert werden.

Neben dem vorgesehenen Verfahren für einen regelmässigen Schlüsselwechsel

auf der Basis der Verfallsjahre der Karten, wäre ein zusätzlicher Mechanismus für einen notfallmässigen Schlüsselwechsel von Vorteil.

Falls die PIN-Verifikation, wie in Abschnitt 2.2.4 beschrieben, ausschliesslich auf der Basis der vollständigen Prüfwerte in der Positiv-Datei erfolgt, ist ein Schlüsselwechsel jederzeit möglich. Für die Ersatzautorisierung mit Hilfe der PVNs auf der Karte sollte ein separater Schlüssel vorgesehen werden, der erst dann verteilt werden müsste, wenn sich herausstellen sollte, dass Ersatzautorisierungen auch weiterhin notwendig sind. Es sollte dabei vorgesehen werden, dass die PVNs auf den Karten für den Fall der Kompromittierung dieses Schlüssels durch die Geldgabeautomaten sicher (d.h. unter Umständen mehrfach) gelöscht oder überschrieben werden können.

Der Wechsel des Schlüssels für die PIN-Generierung ist dagegen nicht möglich, ohne auch gleichzeitig die PINs zu ändern und somit u.U. die Kartenbenutzer zu alarmieren. Dies könnte ein weiterer Grund sein, auf die Berechnung der PIN aus den Kartendaten zugunsten einer Zufallserzeugung zu verzichten.

Literatur

[1] "Neues Verfahren zur PIN-Berechnung und PIN-Prüfung für ec-Karten", Version 5.

[2] "Rahmenbedingungen und -planung zur Einführung eines neuen PIN-Verfahrens für ec-kartengestützte Zahlungssysteme", Version 0.9 vom 05.06.1996.