Inhaltsverzeichnis

Einleitung

Das vorliegende Dokument ist wie folgt gegliedert:

- In Kapitel 1 werden die Kriterien, die die kryptographischen Verfahren erfüllen müssen, beschrieben.
- In Kapitel 2 werden die Kriterien für das Schlüsselmanagement aufgelistet.
- In Kapitel 3 werden die Kriterien, die im Zusammenhang mit der PIN erfüllt werden müssen, aufgezählt.
- In Kapitel 4 werden Kriterien für die sichere Umgebung, Sicherheitsmodule und sichere PIN-Eingabegeräte beschrieben.
- Im Annex werden die Kriterien für die organisatorischen Rahmenbedingungen beschrieben.

Im vorliegenden Kriterienkatalog sind lediglich symmetrische Verschlüsselungsverfahren berücksichtigt. Die in einigen Kriterien angegebenen absoluten Zahlenwerte für die Dimensionierung der Verfahren in Kapitel 1 entsprechen dem Stand von Anfang 1997 und sollten in entsprechenden Abständen aktualisiert werden.

Die im Folgenden verwendeten Begriffe "sichere Umgebung", "Sicherheitsmodul" und "sicheres PIN-Eingabegerät" sind in Kapitel 4 erläutert.

1 Kryptographische Verfahren

In diesem Kapitel werden Anforderungen und Kriterien für kryptographische Verfahren formuliert.

Die eingesetzten kryptographischen Verfahren müssen gegen alle bisher bekannten Angriffe hinreichend sicher sein. Auf der Basis der vorhersehbaren technischen Entwicklung sollte die Sicherheit der Verfahren genügend weit in die Zukunft reichen. Dies kann durch die Wahl von Verfahren erreicht werden, die in der öffentlich zugänglichen Literatur analysiert worden sind, ohne daß relevante Schwachstellen festgestellt werden konnten.

1.1 Kryptographische Algorithmen

Kryptographische Algorithmen, insbesondere Verschlüsselungsalgorithmen und Hashfunktionen, dienen als Grundbausteine für verschiedene Sicherheitsverfahren. Die Sicherheit dieser Grundbausteine hat daher einen wesentlichen Einfluß auf die Sicherheit, aber auch auf die Leistungsfähigkeit einer Anwendung. Bei der Dimensionierung dieser Algorithmen, insbesondere bei den Schlüssellängen, muß daher besondere Sorgfalt gelten.

Da bei jedem der heute gebräuchlichen Kryptoalgorithmen stets die Gefahr besteht, daß sich dessen Sicherheit durch neue oder wesentlich verbesserte Angriffstechniken kurzfristig geringer als erwartet darstellt, müssen die eingesetzten Algorithmen zudem bei Bedarf auf möglichst einfache Art ausgewechselt werden können. Bereits beim Entwurf und insbesondere in der Implementierung ist deshalb darauf zu achten, daß in einem solchen Fall nicht das ganze System völlig neu konzipiert werden muß.

Kriterien

K. 1-1 Es dürfen nur solche kryptographischen Algorithmen verwendet werden, deren Details (z.B. in Standards) öffentlich bekannt gemacht wurden und die in der öffentlich zugänglichen Literatur ausreichend diskutiert und analysiert worden sind, ohne daß bislang relevante Schwachstellen festgestellt wurden.

K. 1-2 Die eingesetzten kryptographischen Algorithmen müssen nach dem Kenntnisstand zum Zeitpunkt der Inbetriebnahme des Systems für mindestens weitere 10 Jahre als sicher gelten. Als Maßstab gilt, daß der Zeitaufwand für eine erfolgreiche Attacke bei einer Investition in der Größenordnung von 300 Mio. USD für eine realistische Anzahl bekannter Klartexte 10 Jahre nicht unterschreiten darf.

- Für eine symmetrische Blockchiffre ergibt sich daraus die Forderung nach einer effektiven Schlüssellänge von mindestens 90 Bit (siehe [KeyLength]).

  Beispiele für symmetrische Blockchiffren sind Triple-DES (siehe [ANSI X9.52]) und IDEA (siehe [IDEA]).

- Für eine Hashfunktion bei einer Anwendung, die keine Birthday-Attacke ermöglicht, ergibt sich daraus die Forderung nach einer Länge des Hashwertes von mindestens 128 Bit[1].

  Ein Beispiel für eine 128-Bit-Hashfunktion ist RIPEMD-128 (siehe [ISO /IEC DIS 10118-3]).

[1] Als Faustregel gilt: die Sicherheit einer Hashfunktion mit einem n-Bit-Hashwert (ohne Berücksichtigung von Birthday-Attacken) entspricht der Sicherheit einer symmetrischen Blockchiffre mit n Bits.

- Für eine Hashfunktion bei einer Anwendung, bei der Birthday-Attacken möglich sind, ergibt sich daraus die Forderung nach einer Länge des Hashwertes von mindestens 160 Bit[2].

  Beispiele für 160-Bit-Hashfunktionen sind SHA-1 (siehe [FIPS PUB 180-1]) und RIPEMD-160 (siehe [ISO /IEC DIS 10118-3]).

K. 1-3 Kryptographische Algorithmen müssen korrekt implementiert und während Installation, Wartung und Betrieb gegen unbemerkte Veränderung geschützt werden.

K. 1-4 Die kryptographischen Algorithmen müssen in einer sicheren Umgebung oder in einem Sicherheitsmodul ausgeführt werden.

1.2 Authentifikation

Die sichere gegenseitige Authentifikation ist der grundlegende Sicherheitsdienst in einem Netz von kommunizierenden Komponenten. Wenn die Identität des Kommunikationspartners nicht zweifelsfrei nachgewiesen werden kann, ist in der Regel jede weitere Absicherung des Datenaustauschs sinnlos. Die Sicherheit von kryptographischen Verfahren basiert auf der Voraussetzung, daß die eingesetzten Schlüssel nicht nur vertraulich, sondern auch authentisch verteilt wurden.

Kriterien

K. 1-5 Alle Systemkomponenten, von deren Unterscheidbarkeit die Sicherheit des Systems abhängt, müssen sich gegenseitig durch kryptographische Verfahren authentisieren. Dabei können sich auch Gruppen von Komponenten derselben Identität bedienen, wenn diese untereinander nicht unterscheidbar sein müssen.

K. 1-6 Dazu muß jede dieser sicherheitsrelevanten Komponenten oder Komponentengruppen über einen eindeutigen Identifikator und einen komponenten(gruppen)spezifischen Schlüssel verfügen, die in einer Initialisierungsprozedur in die Komponente eingebracht werden können. Der Identifikator darf nicht unbemerkt verändert, der Schlüssel nicht unbemerkt verändert oder ausgelesen werden können.

K. 1-7 Wenn die Integrität der zwischen zwei Systemkomponenten ausgetauschten Daten mit kryptographischen Verfahren geschützt ist, kann die Authentifikation implizit durch die korrekte Ausführung der kryptographischen Operationen erfolgen.

K. 1-8 Wenn die Integrität der zwischen zwei sicherheitsrelevanten Systemkomponenten ausgetauschten Daten (ausnahmsweise) nicht mit kryptographischen Verfahren geschützt ist, muß eine explizite gegenseitige Authentifikation durch den Austausch von verschlüsselten, sich nicht wiederholenden Elementen (Zufallszahlen, Sequenznummern, Zeitangaben) erfolgen.

K. 1-9 Die für die Authentifikation benötigten kryptographischen Operationen müssen in einer sicheren Umgebung oder in einem Sicherheitsmodul ausgeführt werden.

K. 1-10 Das Authentifikationsverfahren soll unabhängig von den verwendeten Algorithmen implementiert werden, damit bei neuen Erkenntnissen zu den eingesetzten Algorithmen ein späterer Übergang auf andere Algorithmen möglich ist.

---

[2] Als Faustregel gilt: die Sicherheit einer Hashfunktion mit einem n-Bit-Hashwert (mit Berücksichtigung von Birthday-Attacke) entspricht mindestens der Sicherheit einer symmetrischen Blockchiffre mit n/2 Bits.

1.3 Datenübertragung und -speicherung

Sicherheitsrelevante Daten müssen während der Übertragung und während der Speicherung außerhalb einer sicheren Umgebung oder eines Sicherheitsmoduls durch kryptographische Verfahren gegen unbefugte Kenntnisnahme und/oder gegen unautorisierte Veränderung geschützt werden.

Kriterien

K. 1-11 In der Systemspezifikation muß für alle Datenelemente festgelegt werden, ob sie gegen Abhören und/oder gegen Veränderung geschützt werden müssen. Es können verschiedene Grade des Schutzbedarfs definiert werden (etwa für Schlüssel unterschiedlicher Hierarchiestufen).

K. 1-12 Der Schutz von Datenelementen gegen unbefugte Kenntnisnahme während der Übertragung oder der Speicherung außerhalb einer sicheren Umgebung oder eines Sicherheitsmoduls muß durch Verschlüsselung mit einem sicheren Blockchiffrieralgorithmus (gemäß 1.1) erfolgen. Falls das zu verschlüsselnde Datenelement länger ist als die Blocklänge des Verschlüsselungsalgorithmus, muß der Cipher Block Chaining (CBC) Mode gemäß ISO 10116 zum Einsatz kommen. Für den Schutz speziell von Schlüsseln und PINs während der Speicherung und Übertragung gelten außerdem die in den Kapiteln 2.3, 2.4, 3.2 und 3.3 formulierten Kriterien. Schlüssel doppelter Blocklänge dürfen auch im ECB-Modus verschlüsselt werden.

K. 1-13 Der Schutz von Datenelementen gegen unautorisierte Veränderung während der Übertragung oder der Speicherung außerhalb einer sicheren Umgebung oder eines Sicherheitsmoduls muß mit einer der folgenden Methoden erfolgen. Der Schutz kann dabei entweder auf den Daten selbst oder auf einem aus diesen mit Hilfe einer sicheren Hashfunktion (gemäß 1.1) berechneten Hashwert erfolgen.

- Bilden und Anfügen eines Message Authentication Codes (MAC) auf der Basis eines sicheren Blockchiffrieralgorithmus (gemäß 1.1) gemäß ISO 9797.
- Verschlüsselung mit einem sicheren Blockchiffrieralgorithmus (gemäß 1.1) im Cipher Block Chaining Mode gemäß ISO 10116, falls die Nachricht ausreichend Redundanz aufweist, um eine Manipulation mit hoher Zuverlässigkeit zu erkennen.

K. 1-14 In den Integritätsschutz müssen Datenelemente einbezogen werden, mit deren Hilfe die Integrität der Nachrichtenfolge bewahrt werden kann (z.B. Sequenznummern).

K. 1-15 Die für die sichere Übertragung und Speicherung benötigten kryptographischen Operationen müssen in einer sicheren Umgebung oder in einem Sicherheitsmodul ausgeführt werden.

K. 1-16 Die Verfahren zum Schutz gegen unbefugte Kenntnisnahme und gegen unautorisierte Veränderung von Daten sollen unabhängig von den verwendeten Algorithmen implementiert werden, damit bei neuen Erkenntnissen zu den eingesetzten Algorithmen ein späterer Übergang auf andere Algorithmen möglich ist.

1.4 Zufalls- und Pseudozufallsgeneratoren

Die Anwendung kryptographischer Verfahren erfordert häufig die Bestimmung von Zufallszahlen (z.B. für Schlüssel). Da die Bestimmung dieser Zufallszahlen in den meisten Fällen nicht zu einer anderen Zeit oder an einem anderen Ort wiederholt zu werden braucht, ist es aus Sicherheitssicht zu bevorzugen, die Zufallszahlen durch einen wirklichen Zufallsprozeß zu erzeugen. Falls kein geeigneter Hardware-Zufallsgenerator zur Verfügung steht, können in den meisten Fällen auch Pseudozufallsgeneratoren zum Einsatz kommen.

Kriterien

K. 1-17 Die von einem Zufallsgenerator oder einem Pseudozufallsgenerator erzeugten Werte müssen möglichst gleichverteilt und statistisch unabhängig sein. Abweichungen dürfen mit Hilfe statistischer Testverfahren nicht signifikant nachweisbar sein.

K. 1-18 Die von einem Zufallsgenerator erzeugten Werte dürfen nicht reproduzierbar sein.

K. 1-19 Ein Zufallsgenerator oder Pseudozufallsgenerator muß in einer sicheren Umgebung oder einem Sicherheitsmodul, insbesondere so implementiert sein und betrieben werden, daß keine unbemerkte Beeinflussung seiner Ergebnisse von außen erfolgen kann.

K. 1-20 Die statistischen Eigenschaften eines Zufallsgenerators müssen im Betrieb regelmäßig überprüft werden.

K. 1-21 Initialwerte und Schlüssel eines Pseudozufallsgenerators müssen echt zufällig gewählt und geheimgehalten werden. Der Zufallsgenerator, der für diesen Zweck eingesetzt wird, muß selbst die in diesem Abschnitt genannten Kriterien erfüllen.

K. 1-22 Der Pseudozufallsgenerator muß so gestaltet sein, daß ohne Kenntnis des Schlüssels die erzeugten Pseudozufallszahlen nicht besser erraten werden können als bei echt zufälliger Erzeugung, auch wenn alle bereits erzeugten Pseudozufallszahlen bekannt sind. Gegebenenfalls muß der Schlüssel entsprechend häufig gewechselt werden.

K. 1-23 Der Pseudozufallsgenerator muß so gestaltet und betrieben werden, daß auch bei Kenntnis des Schlüssels aus bekannten Pseudozufallszahlen die vorangehenden und nachfolgenden Pseudozufallszahlen nicht präzise berechnet werden können.

2 Schlüsselmanagement

In einem System, dessen Sicherheit zu einem wesentlichen Teil auf dem Einsatz kryptographischer Verfahren beruht, stellt das sichere Management der Schlüssel eine sehr wichtige Aufgabe dar. Die wichtigsten Teilaufgaben des Schlüsselmanagements sind Schlüsselerzeugung, Schlüsselspeicherung, Schlüsselverteilung, Schlüsselbenutzung, Schlüsselwechsel und Schlüsselzerstörung.

Im Rahmen dieses Dokuments können nicht alle Anforderungen an das Schlüsselmanagement jeder möglichen Ausprägung eines PIN-Verfahrens im Detail beschrieben werden. Grundsätzlich gilt, daß die Auswahl der einzusetzenden Verfahren nach den relevanten Standards und den dort niedergelegten Maßgaben für die Anwendung dieser Verfahren erfolgen muß.

2.1 Schlüsselhierarchie

Der Sinn einer Schlüsselhierarchie liegt darin,

- einen automatischen Wechsel von häufig gebrauchten und möglicherweise kompromittierbaren Schlüsseln zu ermöglichen;
- zu verhindern, daß durch erfolgreiche Angriffe auf Teile des Systems (z.B. auf eine oder mehrere Terminals oder Chipkarten) das Gesamtsystem oder größere Teile davon betroffen werden.

Kriterien

K. 2-1 Die Schlüsselhierarchie muß eindeutig definiert sein, wobei ein Schlüssel K_1 eine höhere Stufe hat als ein Schlüssel K_2, wenn K_2 mit Hilfe von K_1 verschlüsselt oder abgeleitet wird.

K. 2-2 Ein Schlüssel höherer Hierarchiestufe muß mindestens die maximale Länge aller ihm in der Schlüsselhierarchie untergeordneten Schlüssel aufweisen. Falls es sich dabei um Schlüssel für unterschiedliche Algorithmen handelt, muß dies sinngemäß für die effektiven Schlüssellängen gelten.

K. 2-3 Nur Schlüssel der untersten Hierarchiestufen dürfen zum Schutz von Daten, die selbst keine Schlüssel sind, verwendet werden.

K. 2-4 Die Kompromittierung von Schlüsseln niedrigerer Hierarchiestufen darf nicht oder nur unter einem Aufwand, der dem Brechen des zugrundeliegenden Verschlüsselungsalgorithmus gemäß 1.1 entspricht, zu einer Kompromittierung von Schlüsseln höherer Hierarchiestufen führen.

2.2 Schlüsselerzeugung

Kriterien

K. 2-5 Schlüssel mit langer Lebensdauer müssen mit Hilfe eines unbeeinflußbaren (echten) Zufallsprozesses gleichverteilt und statistisch unabhängig erzeugt werden.

K. 2-6 Die übrigen Schlüssel können zufällig oder pseudozufällig (gemäß 1.4) erzeugt oder mit Hilfe anderer Schlüssel berechnet werden.

K. 2-7 Die Berechnung von Schlüsseln muß mit Hilfe eines kryptographischen Algorithmus gemäß 1.1 so erfolgen, daß

- der berechnete Schlüssel ohne Kenntnis des für die Berechnung benutzten Schlüssels nicht einfacher bestimmt werden kann als ein zufällig erzeugter Schlüssel;

- aus der Kenntnis des berechneten Schlüssels und der übrigen Inputdaten keine Informationen über den für die Berechnung benutzten Schlüssel abgeleitet werden können, ohne den zugrundeliegenden kryptographischen Algorithmus zu brechen.

K. 2-8 Alle Schlüssel müssen in einer sicheren Umgebung oder in einem Sicherheitsmodul mit geprüften Werkzeugen erzeugt oder berechnet werden, so daß sie nicht von Unbefugten ausgelesen oder manipuliert werden können.

K. 2-9 Die Systeme müssen jeden Versuch, einen Schlüssel unautorisiert zu erzeugen, verhindern.

2.3 Schlüsselspeicherung

Die Schlüssel dürfen während der Speicherung nicht ausgelesen, verändert, ersetzt oder unautorisiert benutzt werden.

Kriterien

K. 2-10 Kryptographische Schlüssel dürfen nur in einer der folgenden Formen gespeichert werden:

- In Klartext in einer sicheren Umgebung, in einem Sicherheitsmodul oder in einem sicheren PIN-Eingabegerät.
- Verschlüsselt mit einem Schlüssel höherer Hierarchiestufe.

K. 2-11 Wenn Schlüssel in Klartext gespeichert werden, müssen zusätzlich zu den Schlüsseln Hashwerte zur Sicherstellung der Integrität gespeichert werden.

K. 2-12 Wenn Schlüssel in verschlüsselter Form gespeichert werden, ist zusätzlich zur Vertraulichkeit auch die Authentizität und Integrität der Schlüssel durch ein geeignetes kryptographisches Verfahren sicherzustellen. Das Verfahren muß auch erlauben, das Wiedereinspielen alter Schlüssel zu erkennen.

K. 2-13 Keiner einzelnen Person darf es möglich sein, auf irgendeinen geheimen Schlüssel in voller Länge in Klartext zuzugreifen, diesen auszulesen, zu verändern oder zu ersetzen.

K. 2-14 Die Systeme müssen jeden Versuch, einen Schlüssel unautorisiert auszulesen, zu verändern, zu ersetzen oder zu benutzen, verhindern.

2.4 Schlüsselverteilung

Die Schlüssel müssen vertraulich und authentisch verteilt werden, d.h. es muß sichergestellt werden, daß jeder Schlüssel an die richtige Systemkomponente und nur an diese verteilt wird. Insbesondere dürfen Schlüssel während der Verteilung auch nicht durch alte Versionen ersetzt werden können (replay).

Kriterien

K. 2-15 Kryptographische Schlüssel dürfen nur in einer der folgenden Formen verteilt werden:

- In Klartext in mindestens zwei getrennten Komponenten. Der Schlüssel muß von jedem Bit beider Komponenten abhängen. Jede Komponente muß mindestens dieselbe Länge wie der vollständige Schlüssel aufweisen. Die Komponenten müssen getrennt verteilt werden. Unautorisierter Zugriff darauf muß mit hoher Wahrscheinlichkeit entdeckt werden.
- In Klartext in einer sicheren Umgebung oder in einem Sicherheitsmodul.
- Verschlüsselt mit einem Schlüssel höherer Hierarchiestufe.

K. 2-16 Es dürfen nur Schlüssel der obersten Hierarchiestufe, die nicht selbst verschlüsselt werden können (z.B. Transportschlüssel), im Klartext (in mindestens zwei getrennten Komponenten, vgl. K. 2-15) außerhalb eines Sicherheitsmoduls oder einer sicheren Umgebung auftreten, und nur soweit und solange dies für die Verteilung und Initialisierung unbedingt erforderlich ist. Die Verbreitung und Gültigkeitsdauer dieser Schlüssel muß so gering wie möglich gehalten werden.

K. 2-17 Wenn Schlüssel oder Schlüsselkomponenten in Klartext verteilt werden, müssen zusätzlich zu den Schlüsseln und Schlüsselkomponenten Hashwerte zur Sicherstellung der Integrität übermittelt werden.

K. 2-18 Wenn Schlüssel in verschlüsselter Form verteilt werden, ist zusätzlich zur Vertraulichkeit auch die Authentizität und Integrität der Schlüssel durch ein geeignetes kryptographisches Verfahren sicherzustellen. Das Verfahren muß auch erlauben, das Wiedereinspielen alter Schlüssel zu erkennen.

K. 2-19 In der Systemdokumentation ist genau zu bezeichnen, welcher Schlüssel in welcher Phase in den einzelnen Systemkomponenten benötigt wird. Die Schlüssel dürfen nur an diejenigen Systemkomponenten verteilt werden, in denen sie tatsächlich benötigt werden.

K. 2-20 Der Schutz der Schlüssel bei der Verteilung muß durchgehend zwischen den Sicherheitsmodulen der Quelle und des Ziels gestaltet sein. Insbesondere darf kein Schlüssel zwischen Verteilung und Installation in einem den Kriterien für die Speicherung von Schlüsseln nicht genügenden Zustand zwischengespeichert werden.

K. 2-21 Ein Schlüssel darf nur dann in ein Gerät geladen werden, wenn feststeht, daß die Speicherung des Schlüssels in diesem Gerät den dafür geltenden Kriterien entspricht.

K. 2-22 Die Systeme müssen jeden Versuch, einen Schlüssel unautorisiert zu verteilen, verhindern.

2.5 Schlüsselbenutzung und Schlüsselwechsel

Die Sicherheit einer Anwendung kann potentiell dadurch beeinträchtigt werden, daß Schlüssel auf nicht vorgesehene Art benutzt werden. Dies kann dadurch verhindert werden, daß jedem Schlüssel sein Verwendungszweck unzweideutig zugewiesen wird, und diese Zuweisung im Betrieb durchgesetzt und überwacht wird.

Auch beim Einsatz von Verschlüsselungsalgorithmen, bei denen die Bestimmung der Schlüssel durch Brechen des Verfahrens sehr unwahrscheinlich ist, muß dennoch auch weiterhin mit anderen Angriffen auf die Schlüssel, wie physischer Zugriff auf ein Sicherheitsmodul, Bestechung, Erpressung, etc., gerechnet werden. Aus diesem Grund müssen alle Schlüssel sowohl regelmäßig als auch notfallmäßig ausgewechselt werden können. Ein regelmäßiger Schlüsselwechsel begrenzt den Schaden im Falle von unentdeckten Kompromittierungen. Ein notfallmäßiger Schlüsselwechsel begrenzt den Schaden im Falle von entdeckten Kompromittierungen.

Kriterien

K. 2-23 Jeder Schlüssel darf jeweils nur für einen einzigen, in der Spezifikation des Systems eindeutig definierten kryptographischen Zweck[3] verwendet werden.

K. 2-24 Die Systeme müssen jeden Versuch, einen Schlüssel für einen anderen Zweck als den vorhergesehenen zu verwenden, erkennen und verhindern.

[3] Für Debit- und Kreditkarten sind grundsätzlich unterschiedliche Schlüssel zu verwenden, auch wenn der Zweck der gleiche ist.

K. 2-25 Es müssen hinreichende Vorkehrungen oder Möglichkeiten zum regelmäßigen Schlüsselwechsel aller Schlüssel getroffen werden.

K. 2-26 Es müssen hinreichende Vorkehrungen oder Möglichkeiten zum notfallmäßigen Schlüsselwechsel aller Schlüssel existieren.

K. 2-27 Die Systeme müssen jeden Versuch, einen Schlüssel unautorisiert auszuwechseln, verhindern.

K. 2-28 Im Fall einer erkannten (oder angenommenen) Kompromittierung müssen geeignete Maßnahmen ergriffen werden können, um die Verwendung des kompromittierten Schlüssels und aller davon abgeleiteten Schlüssel zu beenden.

K. 2-29 Im Fall einer erkannten (oder angenommenen) Kompromittierung müssen geeignete Maßnahmen ergriffen werden können, um alle Daten und Schlüssel zu bestimmen, die mit dem kompromittierten Schlüssel oder davon abgeleiteten Schlüsseln geschützt wurden.

2.6 Schlüsselzerstörung

Kriterien

K. 2-30 Es müssen Vorkehrungen getroffen werden, nicht mehr benötigte Schlüssel oder aktive Schlüssel im Fall der drohenden Kompromittierung so zerstören zu können, daß es nicht mehr möglich ist, die Schlüssel ganz oder teilweise zu rekonstruieren, z.B. gemäß ISO 9564-1, Annex G.

3 PIN

3.1 PIN-Erzeugung

3.1.1 PIN-Länge

Die Länge der PIN hat großen Einfluß auf die Sicherheit des PIN-Verfahrens. Damit das Erraten und Ausprobieren einer PIN (auch bei Vorliegen gewisser Teilinformationen) möglichst schwierig ist, sollte die PIN möglichst viele Stellen haben. Damit sich die Benutzer die PIN jedoch auswendig merken können, muß hier ein Kompromiß geschlossen werden. Falls die Benutzer die PIN selbst wählen können, ist es möglich, mehr als die heute üblichen vier Dezimalstellen zuzulassen. Dies ist außerdem sehr empfehlenswert, da bei Selbstwahl-PINs die Gleichverteilung nicht mehr gewährleistet ist und sich somit die Sicherheitsproblematik bezüglich der PIN-Länge verschärft.

Es ist jedoch zu beachten, daß viele internationale Systeme nicht mehr als 4 Ziffern akzeptieren und /oder keine alphanumerische PIN-Eingabe unterstützen.

Kriterien

K. 3-1 Eine zugewiesene PIN darf nicht weniger als 4 und nicht mehr als 6 Zeichen lang sein[4].

K. 3-2 Eine durch den Kunden gewählte PIN soll nicht weniger als 6 und nicht mehr als 12 Zeichen lang sein[5]. Bis zur Verarbeitung von PINs mit mehr als 4 Stellen in allen Endgeräten kann eine durch den Kunden gewählte PIN nur 4 Stellen lang sein.

3.1.2 PIN-Auswahl

Die Auswahl einer PIN kann entweder durch den Karteninhaber erfolgen oder durch den Herausgeber, der sie dem Karteninhaber zuweist.

Falls der Herausgeber die PINs zuweist, so können die PINs entweder (pseudo-)zufällig erzeugt oder aus Kartendaten abgeleitet werden. In beiden Fällen müssen die erhaltenen PINs möglichst gleichverteilt sein, um das Erraten und Ausprobieren einer PIN nicht zu vereinfachen.

Kriterien

K. 3-3 Die PIN-Auswahl muß gemäß einer der folgenden Techniken erfolgen:

- zugewiesene echt zufällige PIN
- zugewiesene pseudozufällige PIN
- zugewiesene abgeleitete PIN

---

[4] Die Mindestlänge von 4 Zeichen ist (für alle PINs) in [ISO 9564-1] vorgeschrieben. Die Maximallänge von 6 Zeichen wird dort für zugewiesene numerische PINs empfohlen und wird für zugewiesene alphanumerische PINs analog festgelegt.

[5] Die Mindestlänge von 6 Zeichen ist (für durch Kunden gewählte alphanumerische PINs) in [ISO 9564-1] empfohlen. Für durch Kunden gewählte numerische PINs wird dies analog festgelegt. Die Maximallänge von 12 Zeichen ist (für alle PINs) in [ISO 9564-1] vorgeschrieben.

- durch Kunden gewählte PIN

K. 3-4 Falls die PINs zufällig oder pseudozufällig erzeugt werden, so muß der dabei verwendete Zufalls- oder Pseudozufallsgenerator die Kriterien aus 1.4 erfüllen.

K. 3-5 Falls die PINs aus Kartendaten abgeleitet werden, darf die abgeleitete PIN ohne Kenntnis des benutzten Schlüssels nicht einfacher bestimmt werden können als eine zufällig erzeugte PIN. Insbesondere darf der Ableitungsprozeß nicht spezielle PIN-Werte bevorzugt erzeugen.

K. 3-6 Falls die PINs aus Kartendaten abgeleitet werden, müssen sie kryptographisch von vollständigen Kartenidentifikationsdaten abgeleitet werden .

K. 3-7 Falls die PINs aus Kartendaten abgeleitet werden, dürfen aus der Kenntnis der PIN und der Inputdaten keine Informationen über den benutzten Schlüssel effizient abgeleitet werden können. Es müssen die Kriterien aus 1.1 erfüllt werden.

K. 3-8 Falls die PINs durch die Kunden gewählt werden, so muß der Herausgeber den Kunden Auswahlanweisungen und Warnungen geben (für nähere Hinweise hierzu siehe z.B. ISO 9564-1, Annex H).

K. 3-9 Zugewiesene PINs müssen möglichst gleichverteilt sein, um das Erraten einer PIN zu erschweren.

K. 3-10 Die PINs müssen in einer sicheren Umgebung oder in einem Sicherheitsmodul mit geprüften Werkzeugen erzeugt oder abgeleitet werden, so daß sie nicht von Unbefugten ausgelesen oder manipuliert werden können.

3.2 PIN-Speicherung

Die Speicherung von PINs beim Herausgeber ist notwendig, wenn die PINs nicht aus Kartendaten abgeleitet werden, sondern (pseudo-)zufällig erzeugt werden. Außerdem kann es notwendig sein, die PIN (bzw. einen davon abgeleiteten Wert) auf der Karte zu speichern.

Die gespeicherte PIN darf nicht abgehört oder unbemerkt manipuliert werden können. PINs dürfen nur innerhalb sicherer Umgebungen oder Sicherheitsmodule (inkl. PIN-Briefe) im Klartext vorliegen.

Kriterien

K. 3-11 Wenn die PIN außerhalb einer sicheren Umgebung oder eines Sicherheitsmoduls gespeichert wird, so muß sie verschlüsselt sein. Die dabei verwendeten Algorithmen müssen die Kriterien aus 1.1 erfüllen.

K. 3-12 Wenn die PIN außerhalb einer sicheren Umgebung oder eines Sicherheitsmoduls gespeichert wird, so muß die Integrität der PIN geschützt sein. Die dabei verwendeten Algorithmen müssen die Kriterien aus 1.1 erfüllen.

K. 3-13 Die Referenz-PIN darf nur innerhalb einer sicheren Umgebung oder eines Sicherheitsmoduls (inkl. PIN-Briefe) im Klartext erscheinen. Die Transaktions-PIN darf nur innerhalb einer sicheren Umgebung, innerhalb eines Sicherheitsmoduls oder innerhalb eines sicheren PIN-Eingabegeräts im Klartext erscheinen. Die sichere Umgebung, das Sicherheitsmodul bzw. das sichere PIN-Eingabegerät müssen die jeweiligen Kriterien aus 4 erfüllen.

K. 3-14 Die PIN-Speicherung muß die Kriterien aus 1.3 erfüllen.

K. 3-15 Auch wenn zwei PINs zufällig den gleichen Wert aufweisen, dürfen sie für die Verschlüsselung während der Speicherung beim Herausgeber nicht auf den gleichen verschlüsselten Wert abgebildet werden.

K. 3-16 Für das Verschlüsseln der PIN bei Transport und Speicherung als Referenz-PIN müssen unterschiedliche Schlüssel verwendet werden.

K. 3-17 Das Schlüsselmanagement für die PIN-Speicherung muß die Kriterien aus 2 erfüllen.

3.3 PIN-Verteilung

Eine Verteilung der PIN innerhalb des Systems ist zu verschiedenen Zwecken notwendig. Dazu gehört z.B. die Mitteilung der PIN an den Karteninhaber durch den Herausgeber (bzw. umgekehrt, wenn der Kunde die PIN selber wählt). Außerdem muß bei der PIN-Prüfung je nach gewähltem Verfahren (siehe dazu Kapitel 3.4) die vom Kunden eingetippte PIN (Transaktions-PIN) oder die vom Herausgeber geforderte Referenz-PIN (oder jeweils daraus abgeleitete Daten) an die Prüfstelle übermittelt werden.

Während der PIN-Verteilung darf die PIN nicht abgehört oder unbemerkt manipuliert werden können. Außerdem muß sichergestellt werden, daß die PIN nicht von Unbefugten dem zugehörigen Konto zugeordnet werden kann.

Kriterien

K. 3-18 Während der elektronischen PIN-Verteilung außerhalb einer sicheren Umgebung oder eines Sicherheitsmoduls muß die PIN verschlüsselt sein. Die dabei verwendeten Algorithmen müssen die Kriterien aus 1.1 erfüllen.

K. 3-19 Während der elektronischen PIN-Verteilung außerhalb einer sicheren Umgebung oder eines Sicherheitsmoduls muß die Integrität der PIN geschützt sein. Die dabei verwendeten Algorithmen müssen die Kriterien aus 1.1 erfüllen.

K. 3-20 Die PIN darf nur innerhalb einer sicheren Umgebung oder eines Sicherheitmoduls im Klartext erscheinen.

K. 3-21 Die Datenübertragung bei der PIN-Verteilung muß die Kriterien aus 1.3 erfüllen.

K. 3-22 Für das Verschlüsseln der PIN bei Transport und Speicherung der Referenz-PIN müssen unterschiedliche Schlüssel verwendet werden.

K. 3-23 Wenn die PIN während des Verteilungsprozesses einem Kundenkonto zugeordnet werden kann, darf sie nicht in Klartext erscheinen.

K. 3-24 Die Verschlüsselung von PINs während der Verteilung muß so erfolgen, daß jede PIN mit einem anderen Schlüssel verschlüsselt wird. Die Wahl dieser Schlüssel muß so erfolgen, daß bei Kenntnis aller zu einem Zeitpunkt benutzten Schlüssel nicht die vorher benutzten Schlüssel abgeleitet werden können.

K. 3-25 Für die Verschlüsselung von PINs während der Verteilung muß gelten:

- Falls dieselbe PIN wiederholt verschlüsselt wird, so müssen die entsprechenden verschlüsselten Werte unterschiedlich sein.
- Auch wenn zwei PINs zufällig den gleichen Wert aufweisen, dürfen sie nicht auf den gleichen verschlüsselten Wert abgebildet werden.

K. 3-26 Das Schlüsselmanagement für die PIN-Verteilung muß die Kriterien aus 2 erfüllen.

K. 3-27 Für den Schutz der Referenz-PIN und der Transaktions-PIN während der Verteilung müssen verschiedene Verschlüsselungsschlüssel verwendet werden.

K. 3-28 Alle Funktionen während der PIN-Herausgabe, die die Zuordnung einer PIN zu einer Karte oder zu einem Konto betreffen und die Personal des Herausgebers benötigen, müssen dem Vieraugenprinzip gehorchen.

K. 3-29 Alle Funktionen, die das Rücksetzen des Fehlbedienungszählers betreffen und die Personal des Herausgebers benötigen, müssen dem Vieraugenprinzip gehorchen.

K. 3-30 Wenn der Herausgeber die PIN zuweist, muß er diese in einem PIN-Brief an den Kunden versenden. Dabei müssen die Kriterien in ISO 9564-1, 7.3.1, erfüllt werden.

K. 3-31 Wenn die PIN vom Kunden gewählt wird, muß die Auswahl beim Herausgeber erfolgen. Dabei müssen die Kriterien aus ISO 9564-1, 7.3.2.1, erfüllt werden.

K. 3-32 Es muß sichergestellt sein, daß die verschlüsselte PIN nur in Zusammenhang mit den vom Kunden gewünschten Transaktionen benutzt werden kann. Mehrere Transaktionen pro PIN-Eingabe sind in bestimmten Fällen erlaubt, jedoch muß dann bei jeder Transaktion die PIN neu verschlüsselt werden.

3.4 PIN-Prüfung

Die Prüfung der PIN kann prinzipiell auf zwei Arten erfolgen. Im einen Fall wird mit der eingegebenen PIN eine Berechnung durchgeführt und das Ergebnis mit einem Prüfwert verglichen. Im anderen Fall wird die PIN-Ableitung erneut durchgeführt und die dabei erhaltene PIN mit der eingegebenen PIN verglichen. Im letzteren Fall sind die Verfahren für PIN-Generierung und PIN-Prüfung identisch.

Falls die Prüfung mittels eines Prüfwertes erfolgt, muß sichergestellt sein, daß die Vielfalt der PINs nicht zusätzlich dadurch eingeschränkt wird, daß mehrere PINs auf denselben Prüfwert abgebildet werden und damit bei der Prüfung nicht unterschieden werden können. Aus dem Prüfwert darf ohne Kenntnis eines Schlüssels nicht die zugehörige PIN, aus PIN und Prüfwert nicht der Schlüssel bestimmbar sein.

Kriterien

K. 3-33 Die folgenden Prüfungsverfahren sind zulässig:

- PIN-Prüfung im Chip der Karte

  Die vom Kunden eingegebene PIN (oder davon abgeleitete Daten) wird im Chip seiner Karte mit den dort vorliegenden Referenzdaten verglichen. (Die PIN-Übertragung zwischen Tastatur und Chip muß die Kriterien der PIN-Verteilung aus 3.3 erfüllen.)

- PIN-Prüfung beim Herausgeber

  Die vom Kunden eingegebene PIN (oder davon abgeleitete Daten) muß zum Herausgeber übermittelt werden, bei dem der Vergleich mit Referenzdaten stattfindet, die dort vorliegen oder dorthin übermittelt werden.

- PIN-Prüfung bei einer anderen Institution

  Die Institution muß sowohl die vom Kunden eingegebene PIN (oder davon abgeleitete Daten) als auch die Referenzdaten (die von Informationen auf der Karte abgeleitet werden, oder vom Herausgeber übermittelt werden) erhalten, um die PIN-Prüfung durchführen zu können.

  Die hierbei notwendige Verteilung der PIN (oder davon abgeleiteter Daten) zwischen Terminal und Prüfstelle durch das System muß die Kriterien aus 3.3 erfüllen.

K. 3-34 Falls die PIN-Prüfung mittels eines Prüfwertes erfolgt, muß sichergestellt sein, daß die Wahrscheinlichkeit, daß zwei unterschiedliche PINs auf denselben Prüfwert abgebildet werden und damit bei der Verifikation nicht unterschieden werden können, vernachlässigbar klein ist.

K. 3-35 Aus dem Prüfwert darf ohne Kenntnis eines Schlüssels nicht die zugehörige PIN, aus PIN und Prüfwert nicht der Schlüssel bestimmbar sein.

K. 3-36 Die vollständigen Kartenidentifikationsdaten müssen so in die Bildung des Prüfwertes einbezogen werden, daß der Verifikationsprozeß die Ersetzung eines Wertes durch einen anderen gespeicherten Wert mit hoher Wahrscheinlichkeit erkennen würde.

3.5 PIN-Änderung

Eine Änderung einer PIN kann aus mehreren Gründen notwendig sein:

- der Kunde möchte die PIN wechseln,
- der Kunde hat die PIN vergessen,
- die PIN ist (tatsächlich oder angenommenerweise) kompromittiert.

Die Änderung einer PIN durch den Kunden kann an einem bedienten Terminal oder an einem unbedienten Terminal im System des Herausgebers erfolgen. Generell gilt, daß dabei die Verfahren zur Änderung einer PIN analog zu den Verfahren der PIN-Auswahl sein sollten.

Neben der Änderung von PINs kann auch die Deaktivierung von PINs notwendig werden. Dabei muß sichergestellt werden, daß die deaktivierte PIN später nicht mehr mit der zugehörigen Kontonummer verwendet werden kann.

Kriterien

K. 3-37 Die Verteilung der PIN bei der PIN-Änderung muß gemäß den Kriterien aus 3.3 geschehen.

K. 3-38 Wenn ein Kunde eine PIN an einem bedienten Terminal ändert, so muß dies auf die gleiche Art erfolgen, wie die Auswahl einer PIN durch den Kunden beim Herausgeber. Dabei müssen die Kriterien aus ISO 9564-1, 7.3.2.1, erfüllt werden.

K. 3-39 Wenn ein Kunde eine PIN an einem unbedienten Terminal im System des Herausgebers ändert, so muß die aktuelle PIN eingegeben und verifiziert werden, bevor die vom Kunden gewählte neue PIN ausgewählt und aktiviert wird. Die neue PIN muß vom Kunden zweimal identisch eingegeben werden.

K. 3-40 Alle Funktionen während der PIN-Änderung, die Personal des Herausgebers benötigen, müssen dem Vieraugenprinzip gehorchen.

K. 3-41 Beim Ersatz einer vergessenen PIN müssen die Kriterien für die PIN-Auswahl aus 3.1.2 erfüllt werden.

K. 3-42 Wenn eine zugewiesene PIN vergessen worden ist, muß für den Kunden mit dem selben Verfahren wie bei der Kartenneuausgabe eine neue PIN bestimmt werden (die zufällig den gleichen Wert wie die alte PIN haben kann). Eine Ersatz-PIN darf nicht absichtlich die gleiche sein wie die originale PIN.

K. 3-43 Wenn eine zugewiesene PIN vergessen worden ist, und die neue PIN mittels eines PIN-Briefes an den Kunden gesendet werden soll, muß dies auf die gleiche Art erfolgen, wie beim Senden eines PIN-Briefes bei der Auswahl einer PIN. Dabei müssen die Kriterien aus ISO 9564-1, 7.3.1, erfüllt werden.

K. 3-44 Wenn von einer PIN angenommen wird, daß sie kompromittiert ist, muß sie so schnell wie möglich deaktiviert werden. Der Kunde muß über einen Ersatzwert informiert werden oder die Möglichkeit erhalten, einen zu wählen. Eine Ersatz-PIN darf nicht absichtlich die gleiche sein wie die originale PIN.

K. 3-45 Wenn angenommen wird, daß eine zugewiesene abgeleitete PIN kompromittiert ist, muß mindestens ein Datenelement, das bei der Ableitung der PIN verwendet wird, geändert und herausgegeben werden.

Anmerkung: Dies kann erfordern, daß eine zugehörige Karte neu herausgegeben oder neu codiert werden muß und daß die alte Karte gesperrt wird.

K. 3-46 Eine PIN muß in den folgenden Fällen deaktiviert werden:

- die PIN ist kompromittiert (oder die Kompromittierung wird angenommen),
- alle zur PIN gehörenden Konti des Kunden werden aufgelöst,
- der Kunde fordert die Deaktivierung der PIN,
- die Lebenszeit der PIN endet.

Die Deaktivierung der PIN kann z.B. erfolgen durch das Entfernen der zu deaktivierenden PIN aus den Datensätzen des Herausgebers, durch das Sperren des Zugangs zum Konto oder durch das Sperren der Karte.

K. 3-47 Falls eine PIN wegen (angenommener oder tatsächlicher) Kompromittierung deaktiviert wird, muß dies dem Kunden mitgeteilt werden.

3.6 PIN-Vernichtung

Die PINs, die im System des Herausgebers gespeichert werden, müssen von den Stellen, an denen sie nicht mehr benötigt werden, gelöscht werden.

Hinweise für die Löschung und Zerstörung von sensitiven Daten auf unterschiedlichen Speichermedien sind in ISO 9564-1, Annex G, enthalten.

Kriterien

K. 3-48 Es müssen Vorkehrungen getroffen werden, nicht mehr benötigte Klartext-PINs so zerstören zu können, daß es nicht mehr möglich ist, die PINs ganz oder teilweise zu rekonstruieren, z.B. gemäß ISO 9564-1, Annex G. Insbesondere müssen die Herausgeber geeignete Sicherheitsmaßnahmen treffen in Bezug auf die interne Handhabung und Beseitigung von zurückgesendeten PIN-Briefen und von jedem überflüssigen Material, das mit dem ursprünglichen Druck der PIN-Briefe verbunden ist.

Anmerkung: Im Falle von Nicht-Zustellbarkeit müssen Karte und PIN-Briefe an verschiedene Adressen zurückgesendet werden.

4 Sichere Umgebungen, Sicherheitsmodule und sichere PIN-Eingabegeräte

Es ist nicht möglich, stets alle Schlüssel und PINs nur verschlüsselt zu verarbeiten. Um dennoch sicherzustellen, daß diese geheimen Daten nicht von Unbefugten in Erfahrung gebracht werden können, darf die Verarbeitung von Schlüsseln und PINs im Klartext nur in einer sicheren Umgebung, in Sicherheitsmodulen oder in sicheren PIN-Eingabegeräten erfolgen.

Außerdem muß sichergestellt werden, daß sicherheitsrelevante Funktionen nicht manipuliert oder gestört werden können. Es darf weder möglich sein, die Implementierung von sicherheitsrelevanten Funktionen zu manipulieren, also z.B. von außen zu Fehlern zu veranlassen, noch auf Zwischenergebnisse, Teilschlüssel etc. zuzugreifen. Diese Funktionen dürfen also nur in einer sicheren Umgebung, in Sicherheitsmodulen oder in sicheren PIN-Eingabegeräten betrieben werden, die diese Anforderungen erfüllen.

Die detaillierten Anforderungen an die sichere Umgebung, das Sicherheitsmodul oder das sichere PIN-Eingabegerät können sich dabei je nach der sicherheitsrelevanten Funktion unterscheiden. Auf diese Unterschiede wird in diesem Kapitel jedoch nicht explizit eingegangen.

In diesem Kapitel werden die Begriffe "sichere Umgebung", "Sicherheitsmodul" und "sicheres PIN-Eingabegerät" erläutert. Dazu werden Kriterien angegeben, die die für PIN-Verfahren notwendigen Punkte abdecken. Für eine eigentliche Prüfung, ob eine Umgebung, ein Modul oder ein PIN-Eingabegerät hinreichend sicher ist, sind die im folgenden genannten Kriterien nicht ausreichend detailliert. Dazu kann auf spezialisierte Kriterien, wie z.B. auf ISO 13491-2, zurückgegriffen werden.

Eine sichere Umgebung kann z.B. ein Rechnerraum mit Panzerglas, Schlössern und strikter Zugangsregelung und -überwachung sein. Ein Sicherheitsmodul kann z.B. ein Hardware-Modul sein, dessen Öffnen schwierig ist und das bei Angriffsversuchen die Schlüssel löscht.

4.1 Sichere Umgebung

In einer sicheren Umgebung dürfen Schlüssel und PINs im Klartext bearbeitet werden. Die wichtigste Eigenschaft einer sicheren Umgebung ist, daß geeignete Maßnahmen existieren, um den unbefugten Zugang zu diesen Schlüsseln und PINs zu verhindern.

Kriterien

K. 4-1 Eine sichere Umgebung muß mit einer Zugangskontrolle oder anderen Mechanismen ausgestattet sein, die die Kenntnisnahme von Schlüsseln oder PINs (oder Teilen davon), die in der sicheren Umgebung verarbeitet werden, verhindern. Auch darf es weder möglich sein, die Implementierung von sicherheitsrelevanten Funktionen zu manipulieren, also z.B. von außen zu Fehlern zu veranlassen, noch auf Zwischenergebnisse, Teilschlüssel etc. zuzugreifen.

K. 4-2 Die Zugangskontrollen zu einer sicheren Umgebung (oder die gleichwertigen anderen Mechanismen) müssen solange wirksam sein, bis alle Schlüssel, PINs und nützliche Rückstände von Schlüsseln und PINs aus der sicheren Umgebung vernichtet worden sind. Bei der Vernichtung von Schlüsseln und PINs müssen die Kriterien aus 2.6 und 3.6 erfüllt werden.

4.2 Sicherheitsmodule

In einem Sicherheitsmodul dürfen Schlüssel und PINs im Klartext verarbeitet werden. Eine wichtige Eigenschaft eines Sicherheitsmoduls ist, daß Mechanismen existieren, um den unbefugten Zugang zu den gespeicherten Daten zu erschweren.

Dazu müssen Sicherheitsmodule gegen Angriffe besonders geschützt sein. Dies bedeutet z.B., daß das Anbringen einer Abhörvorrichtung unmöglich ist oder zumindest solche Schäden am Gerät bewirkt, daß es mit hoher Wahrscheinlichkeit entdeckt wird. Auch die Kenntnisnahme von Schlüsseln und PINs darf im normalen Betrieb nicht möglich sein.

Je nach Anwendung und Umgebung, in denen ein Sicherheitsmodul betrieben wird, sind die Anforderungen an das Sicherheitsmodul unterschiedlich. Ein Sicherheitsmodul, das in exponierter Lage betrieben wird, muß z.B. physisch stärker geschützt sein, als ein Sicherheitsmodul, das innerhalb einer geschützten Umgebung betrieben wird. Die folgenden Kriterien gelten für alle Sicherheitsmodule, sind jedoch relativ zur beabsichtigten Betriebsweise und Umgebung formuliert.

Kriterien

K. 4-3 Wenn ein Sicherheitsmodul in der beabsichtigten Weise und Umgebung betrieben wird, so muß sichergestellt sein, daß die Kenntnisnahme von gespeicherten Schlüsseln oder PINs (oder Teilen davon) verhindert wird.

K. 4-4 Wenn ein Sicherheitsmodul in der beabsichtigten Weise und Umgebung betrieben wird, darf es weder möglich sein, die Implementierung von sicherheitsrelevanten Funktionen zu manipulieren, also z.B. von außen zu Fehlern zu veranlassen, noch auf Zwischenergebnisse, Teilschlüssel etc. zuzugreifen.

K. 4-5 Wenn ein Sicherheitsmodul in der beabsichtigten Weise und Umgebung betrieben wird, so müssen beim Eindringen in das Sicherheitsmodul automatisch und sofort alle enthaltenen Schlüssel, PINs, und nützlichen Rückstände von Schlüsseln und PINs vernichtet werden. Bei der Vernichtung von Schlüsseln und PINs müssen die Kriterien aus 2.6 und 3.6 erfüllt werden.

K. 4-6 Ein Sicherheitsmodul darf nur dann betrieben werden, wenn sichergestellt ist, daß es nicht verändert worden ist, um ein Eindringen zu ermöglichen (z.B. Einbringen eines Abhörmechanismus).

K. 4-7 Sicherheitsmodule müssen so entworfen sein, daß sie keine Kenntnisnahme von geheimen Daten durch Abstrahlung ermöglichen.

K. 4-8 Ohne spezielle Ausrüstung und Kenntnisse, die nicht allgemein vorhanden sind, darf es nicht möglich sein, die geheimen Daten, die in einem Sicherheitsmodul gespeichert sind, in Erfahrung zu bringen oder zu verändern oder eine Abhörvorrichtung innerhalb des Moduls einzurichten oder die Hard- oder Software des Sicherheitsmoduls zu verändern. Solche Angriffe müssen am Modul physischen Schaden in der Art anrichten, daß er vor der Wiederinbetriebnahme des Moduls mit hoher Wahrscheinlichkeit entdeckt wird.

4.3 Sicheres PIN-Eingabegerät

Ein sicheres PIN-Eingabegerät muß die Eingabe der PIN ermöglichen und diese dann verschlüsselt an die Stelle weiter senden, die die PIN-Prüfung durchführt. Die wichtigste Forderung an ein sicheres PIN-Eingabegerät ist, daß es nicht möglich sein darf, vorher eingegebene PINs in Erfahrung zu bringen. Hinweise zum Design von sicheren PIN-Eingabegeräten sind in ISO 9564-1, Annex D und F, gegeben.

Kriterien

K. 4-9 In einem sicheren PIN-Eingabegerät darf es weder möglich sein, die Implementierung von sicherheitsrelevanten Funktionen zu manipulieren, also z.B. von außen zu Fehlern zu veranlassen, noch auf Zwischenergebnisse, Teilschlüssel etc. zuzugreifen.

K. 4-10 Ein sicheres PIN-Eingabegerät muß die Transaktions-PIN gemäß den Kriterien aus 3.3 verschlüsseln. Die Klartext-PIN darf das Gerät nicht verlassen. Nach Verschlüsselung der PIN muß die Klartext-PIN unmittelbar überschrieben werden.

K. 4-11 Beim Eindringen in ein sicheres PIN-Eingabegerät darf keine Kenntnisnahme irgendeiner zuvor eingegebenen Transaktions-PIN möglich sein. Dies muß auch dann gelten, wenn der betreffende Datenaustausch zum /vom PIN-Eingabegerät abgehört worden ist.

K. 4-12 Ohne spezielle Ausrüstung und Kenntnisse, die nicht allgemein vorhanden sind, darf es nicht möglich sein, die geheimen Daten, die im sicheren PIN-Eingabegerät gespeichert sind (Schlüssel und PINs), in Erfahrung zu bringen oder zu verändern oder eine Abhörvorrichtung innerhalb des Gerätes einzurichten oder die Hard- oder Software des sicheren PIN-Eingabegerätes zu verändern. Solche Angriffe müssen am Gerät physischen Schaden in der Art anrichten, daß er vor der Wiederinbetriebnahme des Gerätes mit hoher Wahrscheinlichkeit entdeckt wird.

K. 4-13 Selbst wenn im sicheren PIN-Eingabegerät gespeicherte Daten in Erfahrung gebracht werden, dürfen diese nicht in andere PIN-Eingabegeräte transferiert werden können.

K. 4-14 Bei der Eingabe der PIN in das sichere PIN-Eingabegerät darf die PIN nicht im Klartext angezeigt oder durch hörbaren Feedback enthüllt werden. Die verwendeten akustischen und /oder sichtbaren Signale, die notwendig sind, um die Dateneingabe anzuzeigen, müssen von der gedrückten Taste unabhängig sein.

K. 4-15 Es muß möglich sein, daß der Karteneigentümer unbeobachtet von anderen die PIN in das sichere PIN-Eingabegerät eingeben kann.

K. 4-16 Das sichere PIN-Eingabegerät darf keine vollständige PIN-Suche ermöglichen.

Annex A: Organisatorische Rahmenbedingungen

A.1 Korrektheit und Integrität von Hard- und Software

Die Sicherheit des PIN-Verfahrens hängt nicht nur von der Auswahl der geeigneten Algorithmen und Prozeduren, sondern auch von deren korrekten Umsetzung in Hard- und Software ab. Ebenso wichtig ist, daß sicherheitskritische Hard- und Software während aller Phasen der Entwicklung, der Installation und des Betriebs gegen unbemerkte Veränderungen geschützt wird.

Dies stellt Anforderungen an

- den Entwicklungsprozeß,
- die Implementierung und Wartung,
- die Installation, sowie
- den Betrieb

der Hard- und Software und an die Wirksamkeit der Kontrollverfahren. Die Sicherheitsanforderungen an den Betrieb sind in Abschnitt A.2 enthalten.

A.1.1 Entwicklungsprozeß

Kriterien

K. A-1 Die Hersteller von Geräten oder Programmen müssen nachweisen, daß sie nach einer bewährten Entwicklungsmethodik arbeiten, die mindestens die folgenden drei (oder zu diesen äquivalente) Stufen umfaßt:

- Funktionale Spezifikation
- Architekturentwurf (oder Grobentwurf)
- Feinentwurf

K. A-2 Die sicherheitsrelevanten Komponenten und Schnittstellen, sowie deren Abgrenzung zu nicht sicherheitsrelevanten Komponenten müssen klar bezeichnet werden. Die in der angewandten Entwicklungsmethodik definierten Stufen müssen zumindest für jede sicherheitsrelevante Komponente und Schnittstelle ausführlich und nachvollziehbar dokumentiert sein. Die Dokumentation muß den zuständigen Stellen zur Prüfung der Sicherheit zur Verfügung gestellt werden.

K. A-3 Die Entwicklungsunterlagen müssen während ihrer Erstellung, Speicherung, Übermittlung und Lagerung und Prüfung gegen unbefugten Zugriff und insbesondere gegen unbemerkte Veränderung geschützt werden.

A.1.2 Implementierung und Wartung

Kriterien

K. A-4 Die Implementierung muß in einer Weise strukturiert erfolgen und dokumentiert werden, daß die im Feinentwurf identifizierten sicherheitsrelevanten Komponenten und Schnittstellen im Gerät oder Programm eindeutig identifizierbar sind.

K. A-5 Softwareimplementierungen sind in einer gut dokumentierten Programmiersprache durchzuführen. Der dokumentierte Quellcode ist den zuständigen Stellen zur Prüfung zur Verfügung zu stellen.

K. A-6 Die Hersteller von Geräten oder Programmen müssen nachweisen, daß sie während der gesamten Implementierungs- und Wartungsphase mit einem bewährten Konfigurationskontrollsystem arbeiten.

K. A-7 Die Hersteller müssen nachweisen, daß bei der Implementierung die Verantwortlichkeiten und Zugriffsrechte klar definiert sind und die Arbeiten in einer Umgebung und mit Werkzeugen ausgeführt werden, die eine Kontrolle von Zuständigkeiten und Zugriffsrechten jederzeit gewährleisten.

K. A-8 Die Hersteller müssen umfassende Tests der Funktionalität und Sicherheit durchführen. Insbesondere muß nachgewiesen werden, daß die beabsichtigten Funktionen nicht mißbraucht oder umgangen werden können, und daß nur die beabsichtigten Funktionen ausgeführt werden können. Die Testdaten und Testergebnisse sind zu dokumentieren und den zuständigen Stellen zur Prüfung zur Verfügung zu stellen.

K. A-9 Die Hersteller müssen nachweisen, daß sie die notwendigen Wartungsarbeiten, den Ersatz und Update von Komponenten in einer Weise organisieren und durchführen können, die eine unautorisierte Veränderung der Geräte oder Programme zuverlässig verhindern.

K. A-10 Nachfolgendes Herunterladen von Programm-Updates von sicherheitsrelevanten Diensten darf nur nach gegenseitiger kryptographischer Authentifikation der kommunizierenden Parteien stattfinden. Die Integrität der Programm-Updates muß geschützt sein.

A.1.3 Installation

Kriterien

K. A-11 Die Hersteller müssen für alle Komponenten Installationsprozeduren definieren und ggf. Werkzeuge mitliefern, die gewährleisten, daß die Geräte und Programme auf dem gesamten Weg von der Implementierung bis in die Betriebsumgebung durchgehend gegen unbemerkte Manipulationen gesichert sind.

A.2 Betriebsablauf

In diesem Kapitel werden die Kriterien, die in Bezug auf Audit und Alarmverfahren zu erfüllen sind, genannt.

A.2.1 Audit

Es ist nicht möglich, ein System vollständig gegen Angriffe abzusichern. Deshalb ist es eine wichtige Sicherheitsfunktion, zumindest das Erkennen von Angriffen und Angriffsversuchen gegen das System zu unterstützen, um die Analyse der Angriffe zu erleichtern und notwendige Alarmbehandlungen und Schadensabwehrmaßnahmen durchführen zu können. Ebenso müssen regelwidrige Handlungen von eigentlich autorisierten Personen zumindest nachträglich entdeckt und nachgewiesen werden können. Dazu ist das Führen von Audit Trails und Log-Aufzeichnungen notwendig.

Darin müssen z.B. Verletzungen von Sicherheitsregeln und Unregelmäßigkeiten im System (z.B. unkorrekte Übertragung, mehrfache Initialisierung von individuellen Systemkomponenten, mehrfache unkorrekte Eingabe von PINs, wiederholte Meldungen) aufgezeichnet werden. Diese Aufzeichnungen müssen so geführt werden, daß es möglich ist, relevante Operationen, die mit sensitiven Daten durchgeführt wurden, und die dabei betroffenen Daten zu rekonstruieren. Diese Aufzeichnungen müssen so ausgewertet werden, daß sie innert akzeptabler Frist zu geeigneten Alarmbehandlungen führen.

Kriterien

K. A-12 Die Verletzungen von Sicherheitsregeln, Unregelmäßigkeiten im System, Betrugsversuche und die unternommenen Aktionen müssen aufgezeichnet werden. Alle Daten, die notwendig sind, um die betroffenen Operationen zu rekonstruieren, müssen aufgezeichnet werden.

K. A-13 Aufgezeichnete Daten müssen so ausgewertet werden, daß innert nützlicher Frist Aktionen gegen die Verletzungen von Sicherheitsregeln und Unregelmäßigkeiten getätigt werden können.

K. A-14 Die bei diesen Aufzeichnungen gespeicherten Daten müssen so geschützt sein, daß unautorisierte Kenntnisnahme, unautorisierte Manipulation und unautorisiertes Löschen verhindert wird.

A.2.2 Alarmverfahren

Falls ein Angriff auf das System erkannt worden ist, so muß dies Alarm auslösen. Für alle definierten Alarme muß festgelegt sein, wer zuständig ist und welche Notfallprozeduren und Abwehrstrategien ablaufen sollen. Außerdem müssen Prozeduren existieren, um festzustellen, welcher Schaden angerichtet worden ist.

Dies gilt insbesondere für die Kompromittierung von Schlüsseln oder PINs. Um diese möglichst rasch zu erkennen, sollten alle Anzeichen einer Kompromittierung von Schlüsseln oder PINs, wie etwa beschädigte oder zeitweise verschwundene Sicherheitsmodule, verspätetes Eintreffen von Schlüsselkurieren, erfolglose Integritätsprüfungen, etc., zu Alarmen führen.

Auch ungewöhnliche Häufungen von Fehlversuchen bei der PIN-Eingabe müssen zu Alarmen führen. Dazu gehört der Fall, daß innerhalb kurzer Zeit für die gleiche Karte mehrere Fehlversuche an beliebigen Terminals auftreten. Außerdem muß ein Alarm ausgelöst werden, wenn sich eine generelle Häufung von drei Fehlversuchen bei einzelnen Terminals ergibt.

Kriterien

K. A-15 Es muß festgelegt sein, welche Situationen zu Alarmen führen sollen. Darauf aufbauend muß eruiert werden, welche Informationen dafür notwendig sind. Die dazu notwendigen Aufzeichnungen müssen die Kriterien aus A.2.1 erfüllen.

K. A-16 Für alle definierten Alarme muß folgendes gelten:

- es muß festgelegt sein, wer zuständig ist,
- es müssen Prozeduren existieren, um festzustellen, welcher Schaden angerichtet worden ist,
- es muß festgelegt sein, welche Notfallprozeduren und Abwehrstrategien ablaufen sollen. Insbesondere muß klar sein, ob sofortiges oder späteres Eingreifen notwendig ist.

K. A-17 In mindestens den folgenden Fällen muß ein Alarm ausgelöst werden:

- wenn Schlüssel oder PINs bei Erzeugung, Verteilung, Speicherung oder im Betrieb kompromittiert wurden,
- wenn für die gleiche Karte vier oder mehr Fehlversuche an beliebigen Terminals innerhalb von 24 Stunden auftreten,
- wenn sich eine generelle Häufung von drei Fehlversuchen bei einzelnen Terminals ergibt.

Annex B: Literatur

[ANSI X9.52]	ANSI X9.52-19xx Revision 6.0 Triple DES Modes of Operation
[FIBS PUB 180 - 1]	Secure Hash Standard, Federal Information Processing Standards Publication 180-1.
[IDEA]	Xuejia Lai, On the Design and Security of Block Ciphers, ETH Series in Information Processing, J. L. Massey (editor), vol. 1, Hartung-Gorre Verlag Konstanz, Technische Hochschule Zürich, 1992.
[ISO 9564 - 1]	Banking - Personal Identification Number Management and Security - Part 1: PIN Protection Principles and Techniques
[ISO /IEC 9796]	Information Technology - Security Techniques - Digital Signature Scheme Giving Message Recovery
[ISO /IEC 9797]	Information Technology - Security Techniques - Data Integrity Mechanism Using a Cryptographic Check Function Employing a Block Cipher Algorithm
[ISO /IEC 10116]	Information Technology - Modes of Operation for an n-bit Block Cipher Algorithm
[ISO /IEC 10118 - 3]	Information Technology - Security Techniques - Hash Functions - Part 3: Dedicated Hash-Functions, draft.
[ISO DIS 13491 - 2]	Banking - Secure Cryptographic Devices (Retail) - Part 2: Audit Check Lists for Devices used in Magnetic Stripe Card Systems
[KeyLength]	M. Blaze, W. Diffie, R. Rivest, B. Schneier, T. Shimomura, E. Thompson, M. Wiener, "Minimal key lengths for symmetric ciphers to provide adequate commercial security", a report by an ad hoc group of cryptographers and computer scientists, Jan. 1996. (http://www.bsa.org/policy/encryption/cryptographers.html)