AG Chipkarten
des AK Technik
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder[1]

Anforderungen zur informationstechnischen Sicherheit bei Chipkarten[2]

I. Einleitung

Chipkarten sind miniaturisierte IT-Komponenten, meist in der genormten Größe einer Kreditkarte. Sie haben Eingang ins tägliche Leben gefunden, gewinnen zunehmend an gesellschaftlicher Bedeutung und bedürfen aus der Sicht des Datenschutzes zur Wahrung der informationellen Selbstbestimmung und der informationstechnischen Sicherheit größter Aufmerksamkeit.

Die derzeit bekannteste Chipkarten-Anwendung ist die Telefonkarte, die ein Guthaben enthält, das beim Gebrauch der Chipkarte in einem Kartentelefon reduziert wird, bis das Konto erschöpft ist und die Chipkarte unbrauchbar wird. Ebenfalls allgemein bekannt ist die Krankenversicherungskarte (KVK), die lediglich einen gesetzlich vorgegebenen Inhalt hat und zur Identifizierung des Patienten sowie zur Abrechnung ärztlicher Leistungen verwendet wird. Sie ist ein Beispiel für eine Chipkarte, die lediglich die dem Versicherten erkennbare Oberfläche einer umfassenden IT-Infrastruktur ist. Was unterhalb dieser Oberfläche geschieht, ist für die Betroffenen nicht transparent.

Weitere neue Anwendungsbereiche von Chipkarten sind derzeit in der Diskussion bzw. in der Erprobung, z.B.:

---

[1] In der Arbeitsgruppe haben mitgewirkt: Walter Ernestus (Der Bundesbeauftragte für den Datenschutz), Hanns-Wilhelm Heibey (Federführung) (Berliner Datenschutzbeauftragter), Uwe Jürgens (Der Landesbeauftragte für den Datenschutz Schleswig-Holstein), Veikko Müller (Der Landesbeauftragte für den Datenschutz Brandenburg), Wolfgang Polacek (Der Landesbeauftragte für den Datenschutz Niedersachsen), Dr. Uwe Schläger (Der Hamburgische Datenschutzbeauftragte), Wilfried Seiffert (Der Landesbeauftragte für den Datenschutz Niedersachsen), Rüdiger Wehrmann (Der Hessische Datenschutzbeauftragte)

[2] Die hiermit vorgelegte Ausarbeitung entspricht dem Wissensstand von Mitte 1995. Der schnelle Fortschritt bei der Entwicklung der Chipkartentechnologien macht im Prinzip eine ständige Anpassung oder Fortschreibung erforderlich. Die Arbeitsgruppe hat jedoch beschlossen, zunächst ein fertiges Papier mit festgelegtem Aktualitätsstand vorzulegen, da sonst die Gefahr besteht, nie zu einem Abschluß zu kommen. Jedoch ist es geeignet, in weiteren Arbeitsschritten fortgeschrieben zu werden.
Zur besseren Lesbarkeit der Ausarbeitung wird sie durch ein **Abkürzungsverzeichnis** ergänzt.

- die Chipkarte im bargeldlosen Zahlungsverkehr

- Gesundheits- oder Patientenchipkarten zur Speicherung und Übermittlung medizinischer Daten.

Von der Technik her sind reine Speicherchipkarten zur Aufnahme von Daten (meist in Halbleiter-Technologie oder optischer Speichertechnik) von solchen Karten zu unterscheiden, in die Mikroprozessoren und speichernde Bauteile integriert sind. Solche Prozessorchipkarten sind als Kleinstcomputer ohne Mensch-Maschine-Schnittstelle anzusehen. Ihre Verwendung bedarf also zusätzlicher technischer Systeme zum Lesen der gespeicherten Daten, zum Aktivieren der Funktionen der Mikroprozessoren und zum Beschreiben der Speicher.

Systeme zur Erschließung der Funktionen von Chipkarten werden im folgenden Kartenterminals (KT) genannt. Ein KT kann einerseits als isoliertes Gerät zur Erschließung der Daten und Funktionen von Chipkarten angesehen werden. Andererseits erschließen sich die Anwendungsmöglichkeiten von Chipkarten vor allem dann, wenn das KT auch als Einheit in eine "normale" IT-Konfiguration eingebettet ist, die die Weiterverarbeitung von Daten aus einer Chipkartenanwendung bzw. die Aufbereitung von auf Chipkarten abzulegenden Daten ermöglicht. Sicherheitsbetrachtungen zum Einsatz von Chipkarten müssen deshalb auch die Sicherheit dieser Infrastrukturen einbeziehen.

Die Funktionalitäten der Chipkarten lassen sich wie folgt unterscheiden:

- Chipkarten als Speicher von Daten, die hinsichtlich ihrer Vertraulichkeit und Integrität hohen Schutzbedarf aufweisen (z. B. Kontodaten, medizinische Individualdaten);

- Chipkarten als Mittel zur Authentifizierung ihres Trägers für die Gewährung des Zugriffs auf sicherheitsrelevante Daten und Funktionen (Kontoverfügungen, Änderung medizinischer Individualdaten);

- Chipkarten als Mittel zur Signatur von Dokumenten (Verträge, Willenserklärungen, Befunde etc.).

Die weiteren Ausführungen dieses Papiers beschränken sich auf die für die Sicherheit der Informationstechnik relevanten Merkmale und Anforderungen an Chipkarten, sowohl in ihrer Funktion als Instrumente zur Herstellung von Sicherheit als auch als sicherheitsbedürftige IT-Komponenten.

Obwohl - wie die Krankenversicherungskarte zeigt - auch Speicherchipkarten datenschutzrechtlich relevant sind, beschränken sich die weiteren Ausführungen auf Prozessorchipkarten. Diese haben in Zukunft sowohl hinsichtlich ihrer Verbreitung und Anwendungen als auch in Hinblick auf datenschutzrechtliche Chancen und Risiken eine größere datenschutzrechtliche Bedeutung.

II. Empfehlungen zum Einsatz von Chipkarten

Für den datenschutzgerechten Einsatz von Chipkarten ist eine konsequente und überzeugende Sicherungstechnologie erforderlich. Datensicherungsmaßnahmen müssen in ihrer Gesamtheit einen hinreichenden Schutz der Daten vor Mißbrauch gewährleisten. Dabei ist von folgenden Gefahren auszugehen:

- unbefugte Preisgabe von Informationen (Verlust der **Vertraulichkeit**);
- unbefugte Veränderung von Informationen (Verlust der **Integrität**);
- unbefugte Vorenthaltung von Informationen oder Betriebsmittel (Verlust der **Verfügbarkeit**);
- unbefugte Änderung identifizierender Angaben (Verlust der **Authentität**).

Vor der Entscheidung über den Einsatz von Chipkarten sollte eine Technikfolgenabschätzung durchgeführt werden, so wie dies Art. 20 der EU-Datenschutzrichtlinie als Vorabkontrolle fordert. Zur Auswahl geeigneter und angemessener Sicherungsmaßnahmen ist eine systematische Einschätzung der Gefahren für das informationelle Selbstbestimmungsrecht und das Recht auf kommunikative Selbstbestimmung vorzunehmen und sind Lösungsvorschläge für eine Sicherungstechnologie zu erarbeiten.

Die Auseinandersetzung mit dem Phänomen „Chipkarte“ zwingt zur Differenzierung zwischen den technischen Systemen und den Applikationen, die sich dieser Systeme bedienen, und der Chip-

karte selbst. Genausowenig wie es „die“ Chipkarte gibt, genausowenig kann man von „der“ Chipkartenanwendung sprechen. Würde man datenschutzrechtliche und sicherheitstechnische Schlußfolgerungen ausschließlich aus einer der vielen Kombinationsmöglichkeiten ziehen, wäre eine Allgemeinverbindlichkeit der Aussagen bzw. Anforderungen nicht zu erreichen. Konkrete Rechtsprobleme und Risiken lassen sich nur mit einem Bezug zu bestimmten inhaltlichen und technischen Rahmenbedingungen aufzeigen. Die geplanten Gesundheits- und Patientenchipkartensysteme sind insoweit geeignete Beispiele.

Notwendig erscheint auch eine dauernde Bereitschaft, die schnell fortschreitende technologische Weiterentwicklung aufmerksam zu begleiten und bei Bedarf steuernd einzugreifen, denn die datenschutztechnischen Fragestellungen werden umso komplexer, je weiter sich die Chipkartentechnologie entwickelt.

Künftige neue Anwendungen werden sich tendenziell der Prozessorchipkartentechnologie bedienen. Prozessorchipkarten sind miniaturisierte Computer, die allerdings nicht über eigene Mensch-Maschine-Schnittstellen verfügen. Diese werden über Kartenterminals realisiert. Datenschutzrechtliche Anforderungen erstrecken sich hier neben den Kartenterminals auch auf die Rahmenbedingungen bei der Herstellung, bei der Initialisierung, beim Versand und bei der Ersatzbeschaffung in Fällen des Verlustes oder der Zerstörung einschließlich des „Ungültigkeitsmanagements“. Mehrere Hersteller bieten derartige spezielle Chipkarten bereits heute schon an. Deren Leistungsfähigkeit und Funktionsweise ist zum Teil noch sehr unterschiedlich. Eine Standardisierung wäre auch aus datenschutzrechtlicher Sicht in diesem Bereich dringend zu empfehlen.

Das Sicherungskonzept für Chipkarten sollte folgende Mindestanforderungen erfüllen:

1. Grundschutzmaßnahmen
   - Ausstattung des Kartenkörpers mit fälschungssicheren Authentifizierungsmerkmalen wie z.B. Unterschrift, Foto, Hologramme.

   - Steuerung der Zugriffs- und Nutzungsberechtigungen durch die Chipkarte selbst.

   - Realisierung aktiver und passiver Sicherheitsmechanismen gegen eine unbefugte Analyse der Chip-Inhalte sowie der chipintegrierten Sicherheitsfunktionen.

   - Benutzung allgemein anerkannter, veröffentlichter Algorithmen für Verschlüsse-

lungs- und Signaturfunktionen sowie zur Generierung von Zufallszahlen.

- Sicherung der Kommunikation zwischen der Chipkarte, dem Kartenterminal und dem ggf. im Hintergrund wirkenden System durch kryptographische Maßnahmen), wobei eine Übertragung des (geheimen) kryptographischen Schlüssels der Chipkarte zum Kommunikationsgerät ausgeschlossen sein muß bzw. im Ausnahmefall nur verschlüsselt erfolgen darf. Das Einlesen bzw. Ändern des kryptographischen Schlüssels muß durch ein Authentifikationsverfahren abgesichert sein.

- Sicherung unterschiedlicher Chipkartenanwendungen auf multifunktionalen Chipkarten durch gegenseitige Abschottung.

- Sicherung der gegenseitigen Authentifizierung von Chipkarte und KT mit dem Challenge-Response-Verfahren.

2. Erweiterte Sicherungsmaßnahmen

   - Realisierung weiterer „aktiver“ Sicherheitsfunktionen des Betriebssystems wie „Secure Messaging“, I/O-Kontrolle aller Schnittstellen, Interferenzfreiheit der einzelnen Anwendungen, Verzicht auf Trace- und Debug-Funktionen und dergleichen.

   - Auslagerung von Teilen der Sicherheitsfunktionen des Betriebssystem in dynamisch zuladbare Tabellen, damit der Chipkartenhersteller nicht über ein „Gesamtwissen“ verfügt.

3. Grundsätzlich sollte bei Chipkartenbenutzung Anonymität gewahrt bleiben. Wenn dies nicht möglich ist, sollten Wahlmöglichkeiten anonymer Alternativen geschaffen werden.

4. Der Chipkarteninhaber bzw. die Betroffenen sollten die Möglichkeit erhalten, auf neutralen, zertifizierten Systemumgebungen die Dateninhalte und Funktionalitäten ihrer Chipkarten einzusehen (Gebot der Transparenz).

5. Die gesamte Infrastruktur ist zu dokumentieren und die Produktion, die Initialisierung und der Versand der Chipkarten zu überwachen.

6. Für die gesamte Infrastruktur ist ein Mindestschutzniveau vorzuschreiben, das bei unbefugten Handlungen das Strafrecht anwendbar macht.

7. Alle Systemkomponenten sind auf der Basis der Grundsätze ordnungsgemäßer Datenverarbeitung zu evaluieren.

8. Für die Informationsstrukturen sind zu Echtheits- und Gültigkeitsüberprüfungen (z.B. Abgleich gegen Sperr- und Gültigkeitsdateien) Kontrollmöglichkeiten zu schaffen.

III. Technische Grundlagen

III.1 Hardware der Chipkarten

Chipkarten gibt es in vielfältigen Bauformen, Funktionsweisen und Funktionsspektren.
Man unterscheidet Chipkarten hinsichtlich der

- Art der Datenübertragung bei der Interaktion mit der Außenwelt:

  ⇒ kontaktbehaftet oder
  ⇒ kontaktlos über elektromagnetische Felder (Solche kontaktlosen Karten können auch über eine Entfernung von mehreren Metern von einem KT gelesen werden);

- Art der in der Karte bereitgestellten IT-Ressourcen:

  ⇒ reinen Speicherchipkarten mit nicht flüchtigem Speicher (z.B. Identifikationskarten),
  ⇒ intelligenten Speicherchipkarten mit EPROM-Logik (z.B. Telefonkarte),
  ⇒ Prozessorchipkarten mit EEPROM, RAM, ROM und CPU
  ⇒ Prozessorchipkarten mit Coprozessoren für die Abwicklung kryptografischer Verfahren (Krypto-Coprozessor).

- Art der Anwendung:

  ⇒ elektronischer Zahlungsverkehr (Elektronische Geldbörse),
  ⇒ Wegwerfkarten (Telefonkarte),
  ⇒ wiederaufladbare Karten (z.B. Chipkarten im öffentlichen Personennahverkehr),
  ⇒ multifunktionale wiederaufladbare Chipkarten (z.B. unterschiedlicher "Geldbörsen auf einer Chipkarte)

Der Mikroprozessor einer Chipkarte leistet derzeit ca. 1 Million Befehle pro Sekunde. Direktzugriffsspeicher (RAM) erreichen eine Kapazität von 256 KB, Festwertspeicher (ROM) für das Betriebssystem erreichen derzeit eine Kapazität von 16 KB, der elektrisch löschbare, programmierbare Festwertspeicher (EEPROM) mit der Kapazität von 16 KB erlaubt die Installation einer kleinen Datenbank. Im Vergleich dazu leisten Mikroprozessoren heute üblicherweise eingesetzter PCs ca. 100 - 150 Millionen Befehle pro Sekunde und arbeiten mit RAM-Speichern von 8 - 16 MB.

III.2 Chipkarten-Betriebssysteme

Prozessorchipkarten verfügen über einen nicht überschreibbaren Speicherbereich, der keine Änderungen und somit auch keine Manipulationen an den hier abgelegten Programmen und Daten ermöglicht.

In diesem "Read-Only-Memory" (ROM) befindet sich auch das Betriebssystem der Chipkarte. Für Chipkarten-Betriebssysteme existiert die Norm ISO 7816-4, in der die Befehle solcher Systeme beschrieben werden. Die untersuchten Chipkarten-Betriebssysteme OSCAR (OKI Electric Europe GmbH), STARCOS (Giesicke & Devrient), TCOS (Deutsche Telekom AG), SCOS (Oldenbourg Datensysteme) nutzen diese Befehle in unterschiedlicher Weise. Sie ermöglichen die multifunktionale Nutzung von Chipkarten, können also mehrere unterschiedliche Anwendungen unterstützen.

Die folgende Darstellung wird exemplarisch an das verbreitete STARCOS angelehnt:

III.2.1 Filesystem

Die Dateien des Betriebssystems sind hierarchisch organisiert. Den Ursprung des Dateisystems bildet das Master File (MF), das jene Daten enthält, die von allen Anwendungen der Chipkarte gemeinsam genutzt werden sollen (z.B. Daten über den Karteninhaber, Seriennummer, Schlüssel). Es kann Dateien einer niedrigeren Hierarchiestufe enthalten wie Dedicated Files (DF) und Elementary Files (EF).

Ein DF enthält wie ein herkömmliches Verzeichnis die EFs zu einer Anwendung. Für jedes DF können separate Sicherheitsfunktionen definiert werden. Die DFs einer Chipkarte sind physikalisch und logisch voneinander getrennt, können aber auf die Daten des MF zugreifen.

EFs können im MF und in DFs angelegt sein. Es werden Internal EFs (IEF) und Working EFs (WEF) unterschieden. Die Daten eines IEF unterliegen der Zugriffskontrolle des Betriebssystems. Ein direkter Zugriff mittels des KT ist nicht möglich.

Ein IEF enthält z.B. anwendungsbezogene Paßwörter und Schlüssel. Die WEFs enthalten die Nutzdaten einer Anwendung. Die Daten können nach obligatorischer Authentifizierung unter Verwendung eines IEF unter Berücksichtigung von Sicherheitsattributen gelesen und/oder verändert werden. Es gibt unterschiedliche Dateistrukturen für EFs: Sie können Records mit fester (linear fixed) oder variabler (linear variable) Länge enthalten, können eine Ringstruktur mit fester Länge (cyclic) haben, können jedoch auch eine amorphe, d.h. vom Benutzer frei wählbare Struktur (transparent) aufweisen, auf denen auf Daten byte- oder blockweise zugegriffen werden kann.

III.2.2 Authentifizierung

Die Authentifizierungstechniken zwischen Chipkarte und KT werden in der Norm ISO/IEC 9798-2 beschrieben. Es wird dabei zwischen interner Authentifizierung, bei der sich die Chipkarte gegenüber dem KT authentisiert, externer Authentifizierung, bei der sich das KT gegenüber der Chipkarte authentifiziert, und der gegenseitigen Authentifizierung unterschieden. Die Norm ISO 7816-4 kennt nur die interne und externe Authentifizierung, in STARCOS S ist dagegen auch die gegenseitige Authentifizierung möglich.

Neben diversen Befehlen zum Lesen, Schreiben und Löschen (jeweils nach der Authentifizierung) von Files sowie zur Auswahl von zu bearbeitenden Files definiert ISO 7816-4 einige Kommandos, die für die Implementation von Sicherheitsfunktionalitäten bedeutsam sind:

- VERIFY zur Benutzerauthentifizierung mit einer PIN. Dies kann eine im MF gespeicherte globale PIN oder eine in einem IEF gespeicherte anwendungsbezogene PIN sein. Der Befehl überträgt die vom Nutzer eingegebene PIN und die Nummer der zu überprüfenden PIN an die Karte. Diese vergleicht die eingegebene PIN mit der gespeicherten. Bei Erfolg wird der Status an das KT übertragen, ansonsten ein interner Fehlversuchszähler dekrementiert. Bei Zählerstand 0 wird die PIN blockiert. Bei einigen Betriebssystemen kann die Blokkierung durch Eingabe eines Personal Unblocking Key (PUK) aufgehoben werden, der ebenfalls durch einen Fehlerzähler geschützt werden kann und im gleichen IEF gespeichert sein muß wie die PIN.

- INTERNAL AUTHENTICATE löst eine interne Authentifizierung aus. Dazu erhält die Chipkarte aus dem KT den Schlüsselbezeichner des ausgewählten IEF und Authentifizierungsdaten (Zufallszahlen). Die Chipkarte verschlüsselt dann die Zufallszahlen mit dem Schlüssel des ausgewählten IEF und sendet das Chiffrat an das KT zurück. Dieses entschlüsselt und prüft die Übereinstimmung der Zufallszahlen.

- EXTERNAL AUTHENTICATE löst die externe Authentifizierung aus. Dazu fordert das KT mit dem Befehl GET CHALLENGE eine Zufallszahl von der Chipkarte ab, verschlüsselt diese und sendet das Ergebnis zusammen mit der Nummer des zu verwendenden Schlüssels an die Karte zurück. Dann entschlüsselt die Karte die Zufallszahl mit dem Schlüssel der angegebenen Schlüsselnummer. Bei Übereinstimmung wird das KT als authentisch anerkannt.

III.3 Kartenterminals

Wie in der Einleitung kurz dargestellt, sind Chipkarten nicht als isolierte Träger von Risiken zu betrachten, wenn es um Fragen ihrer IT-Sicherheit geht. Aufwendige sicherheitstechnische Maßnahmen an und in der Chipkarte können durch unsichere Systemumgebungen bei der weiteren Verwendung der Daten konterkariert werden.

Wenn zum Beispiel das System eines zugriffsberechtigten Arztes) nicht den erforderlichen Schutz bietet, können die Schutzmaßnahmen der Karte umgangen werden. Der Schutz der Chip-

karte gegen unbefugte Manipulationen ist weitgehend wertlos, wenn beim elektronischen Zahlungsverkehr das Kartenterminal leicht manipuliert werden kann.

Hier sollen jedoch nur für solche Komponenten Sicherheitsbetrachtungen angestellt werden, die chipkartenspezifisch sind. Solange die Chipkarten keine eigenen Mensch-Maschine-Schnittstellen enthalten, sind für die Erschließung der Chipkarteninhalte und -funktionen Systeme notwendig, mit denen die Chipkarten gelesen und beschrieben werden können, die hier sog. Kartenterminals (KT). Auch wenn es einmal möglich sein wird, direkt mit der Chipkarte zu kommunizieren, z.B. über Sensorfelder, werden KTs kaum entbehrlich sein, denn sie stellen zumindest die Schnittstelle zu jenen Nutzern dar, die mit dem Inhaber der Karte nicht identisch sind. KTs können eigene Verarbeitungskapazitäten bieten und auch die Verbindung zu anderen Systemteilen herstellen.

Bisher sind für alle Chipkarten-Anwendungen (Telefonkarten, Krankenversicherungskarten, Sicherungskarten für Mobiltelefone usw.) spezielle KTs entwickelt und eingesetzt worden. Soweit erkennbar werden universell einsetzbare KTs bisher nicht auf dem Markt angeboten. Der derzeitige Stand der Technik wird faktisch durch die Spezifikationen für multifunktionale KTs definiert, die im Zusammenhang mit der Planung und der versuchsweisen Einführung von Gesundheitskarten von der Arbeitsgemeinschaft "Karten im Gesundheitswesen" und der Gesellschaft für Mathematik und Datenverarbeitung (GMD) beschrieben worden sind.

Diesen Spezifikationen liegt folgende Konzeption zugrunde:

- Die Kartenterminals sind transparent für jeden Dialog zwischen einem Anwendungsprogramm und einer Chipkarte, sofern dieser Dialog über eine genormte Schnittstelle geführt wird. Damit ist ihre Anwendung außerhalb des Gesundheitswesens ***möglich***.

- Allerdings ist die Option, ein universell einsetzbares KT zu schaffen, aus pragmatischen Erwägungen heraus relativiert worden. Von den nach ISO 7816-3 zulässigen Optionen für die Übertragungsparameter wird nur ein Teil unterstützt. Dies entspricht der Politik des Kreditkartensektors, die zulässigen Lösungen enger zu fassen als das Spektrum der Optionen. Es finden ferner nur die Protokolle Anwendung, die schon bei der Krankenversicherungskarte zugelassen waren. Damit wurden allerdings die wichtigsten marktgängigen Lösungen erfaßt.

- Es können anwendungsspezifische Funktionen im Kartenterminal realisiert werden, die dann nicht dem Anwendungsprogramm überlassen werden, solange nicht andere Vorkehrungen zum Schutz der Karte vor unbefugten oder durch Fehlfunktionen ausgelösten schreibenden Zugriffen getroffen sind. So ist z.B. ein Modul zur Verarbeitung der Versichertenkarte gem. § 291 SGB V für Gesundheitskarten-Terminal spezifiziert worden.

- Es können je nach Anwendung weitere anwendungsspezifische Module definiert werden, die periphere Geräte steuern. So wurde für die Gesundheitschipkarten ein Modul definiert, das einen Drucker steuert, damit Ärzte ohne IT-Einsatz die Kartensysteme zumindest für die Übertragung des Inhalts der Versichertenkarte auf die Belege der vertragsärztlichen Versorgung nutzen können. Das Druckmodul mit der parallelen Schnittstelle ist optional zu realisieren.

- Eine Download-Funktion zum Herunterladen von Programmen erlaubt Anpassungen der Versichertenkarten-Anwendung an die Rechtsentwicklung und schafft die Möglichkeit, für bestimmte neue Kartenanwendungen anwendungsspezifische Funktionen softwareseitig zu realisieren.

- Damit können dem KT neben der Lese- und Schreibfunktion weitere Aufgaben zugewiesen werden, etwa Sicherheitsfunktionen wie Authentifizierung, Zugriffsauthorisierung und Verschlüsselung.

- Die Spezifikation gilt für kontaktbehaftete Chipkarten nach ISO 7816 in 5-Volt-Technologie. Kontaktlose Chipkarten und kontaktbehaftete Chipkarten in 3-Volt-Technologie sollen einbezogen werden, wenn die Normung Klarheit geschaffen hat. Das gleiche gilt für eine Erweiterung von Standards für die Nutzung der Kontakte und für höhere als derzeit spezifizierte Übertragungsraten.

- Das Anwendungssystem in einem PC wird auf eine anwendungsunabhängige Schnittstelle für die Integration der Chipkartentechnik aufgesetzt.

- KTs als separate Endgeräte können zusätzlich mit folgenden Optionen ausgestattet sein:

  * Display und Tastatur,
  * zweite Kontaktiereinheit für eine Chipkarte im Normalformat gem. ISO-IEC 7816-2

oder im Plug-in-Format.

IV. Sicherheitstechnische Gestaltungsspielräume

Für die Entwicklung sicherer Chipkartenanwendungen gibt es eine Vielzahl von Ansatzpunkten, die je nach den in einer anwendungsspezifischen Sicherheitspolitik definierten Anforderungen zur Verbesserung der Sicherheit mit gewissen Spielräumen ausgenutzt werden können. In diesem abschließenden Kapitel geht es einerseits darum, diese sicherheitstechnischen Gestaltungsspielräume darzustellen und andererseits die Empfehlungen der Datenschutzbeauftragten zur Ausschöpfung dieser Spielräume hervorzuheben.

IV.1. Allgemeine Anforderungen

Wie bereits einleitend dargestellt sind Chipkarten als miniaturisierte Computer anzusehen, die (noch) nicht über eigene Mensch-Maschine-Schnittstellen verfügen. Daraus ergeben sich folgende Konsequenzen:

- Chipkarten sind leicht transportable Rechner. Die besonderen Bedrohungen der IT-Sicherheit, die z.B. bei anderen transportablen Rechnern (Laptops, Notebooks,...) berücksichtigten werden müssen, existieren in ähnlicher Weise auch für Chipkarten.

- Die Interaktion zwischen Mensch und Chipkarte bedarf zwischengeschalteter technischer Systeme (KT), die ebenfalls besonders zu sichern sind. Eine Chipkarte bildet zusammen mit dem KT ein vollständiges Rechnersystem mit Ein- und Ausgabekomponente. Die Evaluation der richtigen Funktionsweise setzt voraus, daß dabei alle Systemkomponenten einbezogen sind.

- Noch zu geringe Speicher- und Prozessorkapazitäten bilden Schranken für Sicherheitsfunktionen. Die technische Entwicklung dürfte diese Engpässe bald beseitigen. Heutige Betrachtungen müssen sie jedoch noch berücksichtigen.

Allgemein sind an die Sicherheitsfunktionen folgende Anforderungen zu stellen:

- Zugriffs- und Nutzungsberechtigungen sollten soweit möglich von der Chipkarte selbst geprüft und gesteuert werden.

- In Anwendungen sollten sich alle beteiligten Rechner (incl. Chipkarten) gegenseitig authentifizieren. Die Authentifizierung des Benutzers hat gegenüber der Chipkarte zu erfolgen, wobei für die Zukunft angestrebt werden sollte, daß dies möglichst ohne zwischengeschaltete Systeme erfolgen kann. Dies würde eine autonome Stromversorgung der Chipkarte und geeignete Mensch-Maschine-Schnittstellen voraussetzen (z.B. Sensorfelder für biometrische Merkmale).

- Es muß grundsätzlich ein Mindestschutz vorhanden sein, mit dem die in § 202a Abs. 1 StGB geforderte „besondere Sicherung gegen unberechtigten Zugang“ realisiert wird, um bei unbefugter Nutzung einer Chipkarte das Strafrecht anwendbar zu machen.

IV.2. Hardwarebezogene Maßnahmen zur IT-Sicherheit bei Chipkarten

IV.2.1 Herstellung, Initialisierung und Versand von Chipkarten

Sicherheitserwägungen greifen bereits bei der Herstellung, Initialisierung und dem Versand von Chipkarten. Dabei müssen

- die Produktion der Prozessoren und Chipkarten,

- das Erzeugen der Schlüssel

- das Laden der Schlüssel in die Sicherheitsmodule (Internal Elemetary Files),

- das Laden von Hersteller- und Transportschlüssel für die spätere Initialisierung und

- der Versand der Chipkarten und Transportschlüssel an den Empfänger

durch entsprechende technische und organisatorische Maßnahmen abgesichert werden.

IV.2.2 Sicherheitsmerkmale des Kartenkörpers

Zur Unterstützung der Authentifizierung des Karteninhabers gegenüber der Chipkarte und damit des Nachweises, daß die Chipkarte

- zur jeweiligen Anwendung gehört und
- die die Karte vorlegende Person die Karte rechtmäßig nutzt,

sollte der Kartenkörper mit Sicherheitsmerkmalen ausgestattet sein, die der Sensibilität angemessen sind:

- Aufdruck
- Hologramm
- Unterschrift des Besitzers (nur bei nicht anonymen Anwendungen)
- Foto des Besitzers (nur bei nicht anonymen Anwendungen)
- Echtheitsmerkmal
- Multiple Laser Image (durch Lasergravur auf der Chipkarte aufgebrachte hologrammähnliches Kippbild mit kartenindividuellen Informationen).

Dabei ist allerdings zu berücksichtigen, daß es Sicherheitsmerkmale gibt, die z.B. bei anonymen Chipkartenanwendungen (z.B. anonyme Zahlungsverfahren) die Anonymität aufheben würden und daher dabei nicht verwendet werden können

IV.2.3 Sicherheitsmechanismen der Chip-Hardware

Sicherheitsmechanismen der Chip-Hardware richten sich vor allem gegen die Analyse der Chip-Inhalte und -Sicherheitssysteme mit Hilfe von Spezialgeräten, z.B. durch Abtragen dünner

Chipschichten. Dabei kann unterschieden werden zwischen passiven Mechanismen, bei denen eine bestimmte Bauweise des Chips die Schutzfunktionen ergibt, und aktiven Mechanismen, die äußere Eingriffe erkennen und ggfs. den Chip außer Funktion setzen.

Passive Mechanismen:

- Es gibt von außen keine direkte Verbindung zu den Funktionseinheiten. Ein Testmodus, der eventuell später nicht mehr erlaubte Zugriffe auf den Speicher ermöglicht, muß irreversibel auf den Benutzermodus geschaltet werden können.

- Interne Busse werden nicht nach außen geführt.

- Der Datenfluß auf den Bussen wird mit Scrambling geschützt.

- Der ROM befindet sich in den unteren Halbleiterschichten, um eine optische Analyse zu verhindern.

- Gegen das Abtasten von Ladungspotentialen erfolgt über den RAM-Bereichen eine Metallisierung.

- Die Chipnummern werden eindeutig vergeben (werden u.U. von den Anwendungen benötigt).

Aktive Mechanismen:

- Es wird eine Passivierungsschicht aufgebracht, deren Entfernen einen Interrupt auslöst, der die Ausführung der Software unterbindet, sowie Schlüssel und andere sicherheitsrelevante Daten löscht.

- Es erfolgt eine Spannungsüberwachung. Wenn der Spannungswert den zulässigen Bereich überschreitet, wird die weitere Ausführung von Prozessorbefehlen unterbunden. Damit werden Angriffe erschwert, mit denen die Abarbeitung einzelner Befehle analysiert werden soll.

- Den gleichen Zweck verfolgt die Taktüberwachung.

- Es erfolgt eine Power-On-Erkennung, um bei Reset einen definierten Zustand herzustellen.

- Es werden Sensoren für Licht und Temperatur angebracht. Wenn zulässige Werte (etwa durch Einwirkung von Analysesystemen) überschritten werden, werden sensible Speicherbereiche gelöscht.

IV.3. Softwarebezogene Maßnahmen zur IT-Sicherheit bei Chipkarten

IV.3.1 Basisalgorithmen für Schutzfunktionen der Software

Die Schutzfunktionen der Chipkarten-Software basieren auf den bekannten und teilweise standardisierten Algorithmen zur Verschlüsselung, Signatur und Generierung von Zufallszahlen.

Dazu gehören symmetrische Verschlüsselungsalgorithmen wie DES, Triple-DES, IDEA und SC85 und asymmetrische Verfahren wie RSA, Signieralgorithmen wie DSS und RSA mit MD5, Einwegfunktionen zur Berechnung des MAC und für das Hashing wie SHA und MD5 sowie Zufallszahlengeneratoren.

IV.3.2 Schutzfunktionalitäten und -mechanismen des Betriebssystems

Zunächst sollte sichergestellt sein, daß sich nicht alle Teile des Betriebssystems im ROM befinden, damit der Chiphersteller nicht über das ganze Wissen über die Sicherung der Chipkarte verfügt. Wesentliche Teile des Betriebssystems können bei der späteren Initialisierung über entsprechend authentisierte KTs dynamisch aus Tabellen geladen werden.

Darüberhinaus sollte das Betriebssystem in folgender Weise Sicherheit "erzeugen":

a) Die Identifizierung und Authentifizierung des Benutzers erfolgt mittels PIN und PUK oder mit biometrischen Verfahren.

Üblicherweise erfolgt die Prüfung einer PIN. Zwar können die normale Forderungen zur Paßwortverwaltung bei Rechnern nicht voll auf Chipkarten übertragen werden, jedoch sollte die PIN-Länge je nach Sensibilität mindestens 4 oder mehr Stellen betragen, die Anzahl der Fehlversuche begrenzt sein, die Möglichkeit bestehen, die PIN zu ändern und eine Freischaltung der Karte auch mittels Personal Unblocking Key (PUK) in Abhängigkeit von der Anwendung ermöglicht werden.

Biometrische Verfahren erfassen Fingerabdrücke, Augenhintergründe, Handgeometrien, Sprachmerkmale oder Unterschriftsdynamiken, verformeln sie und übertragen das Ergebnis zur Überprüfung auf die Chipkarte.

b) Es erfolgt eine Zugriffskontrolle mit einer Rechteverwaltung, wobei die Zugriffsrechte an die einzelnen Dateien geknüpft werden. Den Dateien sind Sicherheitsattribute zugeordnet, mit denen festgelegt wird, ob die Dateien (Daten) gelesen, kopiert, beschrieben, gelöscht, gesperrt oder freigegeben werden dürfen.

c) Wenn anderen Personen als dem Karteninhaber Zugriffsmöglichkeiten auf die Chipkarte gewährt werden sollen, erfolgt dies im Rahmen einer Programm-Programm-Kommunikation mit einem anderen Rechner oder einer anderen Karte (z.B. mit einer Professional Card). Der Rechner bzw. die andere Karte muß authentifiziert werden.

Die Rechnerauthentifizierung wird meist nach einem auf DES basierenden Challenge-Response-Verfahren vorgenommen.

Nach dem gleichen Schema verläuft die gegenseitige Authentifizierung von Chipkarte und Professional Card. Beide Benutzer müssen ihre Chipkarte aktivieren. Dann erfolgt die Authentifizierung zwischen den beiden Karten, wobei das KT die Daten transparent weiterleitet.

d) Zum Schutz gegen Ausforschung und Manipulation erfolgt eine sichere Datenübertragung zwischen Chipkarte und KT ("Secure Messaging").

e) Im gesicherten Zusammenwirken mit Kryptoterminals werden Signier- und Verschlüsselungsfunktionen bereitgestellt.

Solche Verfahren werden von verschiedenen Herstellern angeboten. Es gibt auf dem Markt Kryptoprozessoren, in die die meisten gängigen Verschlüsselungs- und Hash-Algorithmen implementiert werden können.

Auf Hybridkarten können die Daten auf der optischen Fläche verschlüsselt abgelegt werden. Die Entschlüsselung kann so durch den Prozessor erfolgen, daß eine Speicherung von Schlüsseln außerhalb der Chipkarte unnötig ist.

f) Das Betriebssystem führt eine I/O-Kontrolle aller Schnittstellen gegen unerlaubte Zugriffe durch.

g) Die Interferenzfreiheit der einzelnen Anwendungen wird gewährleistet, d.h. eine gegenseitige unerwünschte Beeinflussung der Anwendungen wird ausgeschlossen.

h) Trace- und Debugfunktionen sind nicht verfügbar.

i) Beim Initialisieren des Betriebssystems werden RAM und EEPROM geprüft.

j) Fehleingaben werden abgefangen.

k) Der Befehlsumfang wird auf die notwendigen Befehle reduziert. Funktionalitäten, die nicht zugelassen werden sollen, werden vom Betriebssystem unterbunden.

l) Die Dateiorganisation, Header und Speicherbereiche im EEPROM werden durch Prüfsummen abgesichert.

m) Das Betriebssystem sieht die Möglichkeit vor, die Chipkarte durch Löschung zu deaktivieren (etwa nach Ablauf einer Gültigkeitsdauer), jedoch verhindert es die mißbräuchliche Deaktivierung.

IV.3.3 Die Sicherheit der Anwendung

Die Betrachtung der Sicherheit bei der Anwendung von Chipkarten setzt die ganzheitliche Betrachtung der Kommunikation zwischen Chipkarten, KT und im Hintergrund wirkenden Systemen voraus. Die Kommunikation zwischen den einzelnen Systemen und Systembestandteilen ist ebenfalls mit kryptographischen Methoden zu sichern:

- Zur Unterstützung der Sicherheit der Kommunikation dienen Funktionen des Chipkarten-Betriebssystems zur gegenseitigen Authentifizierung von Chipkarten und Rechnern, zur sicheren Datenübertragung und zum Signieren und Verschlüsseln (siehe IV.3.2. c), d)).

- Gegen die unberechtigte Nutzung der Daten auf der Chipkarte muß eine Zugriffskontrolle erfolgen, die auf einer sicheren Identifikation und Authentifizierung der Benutzer beruht (siehe IV.3.2 a), b)).

Darüber hinaus sind die folgenden für die Sicherheit der Anwendung bedeutsamen Maßnahmen zu berücksichtigen:

- Den Dateien auf der Chipkarte sind Befehle zuzuordnen, die mit ihnen ausgeführt werden können. Die Ausführung anderer Befehle ist zu unterbinden.

- Zugriffe auf geschützte Datenbereiche und Veränderungen der Daten sollten protokolliert werden - vorzugsweise auf der Chipkarte. Die Anwendung muß die Auswertung der Protokolldaten unterstützen.

- Bedarfsweise sollten Überprüfungen durch Abgleich mit Hintergrundsystemen erfolgen, z.B. die Erkennung gesperrter Karten durch Abgleich mit Sperrdateien, Feststellung von Betragslimits im chipkartengestützten Zahlungsverkehr.

- Die eindeutige Nummer des Chips kann zu Echtheitsprüfungen herangezogen werden.

Bei den letzten beiden Spiegelstrichen muß allerdings berücksichtigt werden, daß mit solchen Maßnahmen bei anonymen Systemen unter Umständen die Anonymität gefährdet sein kann. Es kann nicht immer ausgeschlossen werden, daß anonyme Chipkarten einzelnen Nutzern zugeordnet werden, wenn die Identifizierung der Karte möglich ist.

IV.4. Risiken und Anforderungen bei Kartenterminals (KT)

Zwar bilden - wie oben festgestellt - Chipkarten und KTs erst zusammen ein vollwertiges Rechensystem, jedoch befinden sich beide Komponenten in der Regel in unterschiedlicher Verfügungsgewalt, die Karte in der des Inhabers und das KT in der von Anwendern. Denkbar ist auch, daß bei Inhabern und Anwendern unterschiedliche Vorstellungen und Interessen mit der Nutzung verbunden werden.

Wesentliche Teile der unabdingbaren Sicherheitsmechanismen der Karte können daher konterkariert werden, indem die Steuerungssoftware des KT verändert oder die Hardware des KT manipuliert wird. Eine Zertifizierung von KTs kann sich daher nur auf unveränderliche Teile beziehen.

Wenn eine Chipkarte in ein KT eingeführt wird, gibt der Inhaber die Verfügungsgewalt über die Software auf der Karte und die ihn betreffenden Datenbestände auf. Eine unbefugte Veränderung der Software muß daher technisch verhindert werden.

Allerdings sind die Datenbestände grundsätzlich variabel. Sie können daher benutzt werden, über das KT Daten abzulegen, die für den Karteninhaber verdeckt sind und nur mit bestimmten Codes gelesen werden können (verdeckte Kanäle). Dies eröffnet Möglichkeiten für unbefugtes oder gar kriminelles Handeln.

Der Karteninhaber sollte daher nicht nur die Möglichkeit haben, sich den Inhalt der gespeicherten Daten anzeigen zu lassen, sondern die tatsächlichen Funktionen z.B. auf neutralen KTs testen können. Wegen der u.U. unterschiedlichen Interessenlagen (z.B. in wirtschaftlichen Beziehungen) ist die Prüfung der korrekten Funktion der Software sowie umgekehrt des Ausschlusses ungewollter Funktionen im realisierbaren Rahmen zu ermöglichen.

Manipulationen an der Hardware und der Eingabesteuerungssoftware der KTs können auch dazu führen, daß die geheimen oder unverfälschbaren Authentifizierungsmerkmale (PIN, biometrische Merkmale), die bei der Authentifizierung des Kartenbesitzers in das KT übertragen werden und so Dritten bekannt werden.

Es sind daher folgende Sicherheitsanforderungen an KTs zu stellen:

- Die KTs müssen über mechanisch gesicherte Gehäuse verfügen, damit eine Hardware-Manipulation verhindert oder erschwert wird.

- Sicherheitsmodule, die die für die vertrauliche Kommunikation mit Chipkarten und die gegenseitigen Authentifizierungen erforderlichen Hauptschlüssel enthalten, sind mechanisch (zum Beispiel durch Vergießung in Epoxidharz) und elektrisch gegen vielfältige Angriffsformen besonders abzusichern. Jeder Angriff auf das Sicherheitsmodul muß zum Löschen aller Schlüssel im Sicherheitsmodul führen. Dies setzt auch voraus, daß das Sicherheitsmodul weitgehend von der Stromversorgung des KT autark sein muß.

- Die KTs müssen alle Sicherheitsmerkmale des Kartenkörpers prüfen können, müssen demzufolge also über alle entsprechenden Sensoren verfügen (siehe IV.2.2).

- Sofern die Kommunikation zwischen Chipkarte und KT nicht durch kryptographische Verfahren gegen Abhören und Manipulation gesichert wird, ist das Abhören der Kommunikation durch mechanische Maßnahmen (sog. Shutter zum Abschneiden aller manipulativ mit der Karte in das KT eingebrachten Drähte) zu verhindern.

Die bisherigen Spezifikationen für die KTs lassen nicht erkennen, daß Maßnahmen gegen Penetrationsversuche aus der IT-Umgebung der Chipkartenanwendung im KT ergriffen werden können. Es fehlt daher an einem schlüssigen Sicherheitskonzept für das Zusammenspiel zwischen dem Betriebssystem und den Applikationen der (übergeordneten) IT-Umgebung und dem Betriebssystem und den Applikationen des Systems Chipkarte/KT.

Abkürzungsverzeichnis

CPU	Central Processing Unit (Zentraleinheit)
DDS	Signieralgorithmus
DES	Symmetrischer Verschlüsselungsalgorithmus (Data Encryption Standard)
DF	Dedicated File
EEPROM	Electrically Erasable Programmable Read Only Memory (elektrisch löschbarer, programmierbarer Festwertspeicher)
EF	Elementary File
EPROM	Erasable Programmable Read Only Memory (löschbarer, programmierbarer Festwertspeicher)
GMD	Gesellschaft für Mathematik und Datenverarbeitung
IDEA	Symmetrischer Verschlüsselungsalgorithmus
IEC	International Electrotechnical Commission
IEF	Internal Elementary File
ISO	International Standardisation Organisation
IT	Informationstechnik
KB	Kilobyte
KT	Kartenterminal
KVK	Krankenversicherungskarte
MAC	Message Authentification Code
MB	Megabyte
MD 5	Hash-Algorithmus
MF	Masterfile
OSCAR	Chipkartenbetriebssystem der Fa. OKI Electric Europe GmbH
PC	Personal Computer
PIN	Persönliche Identifikations-Nummer
PUK	Personal Unblocking Key
RAM	Random Access Memory (Direktzugriffsspeicher)
ROM	Read Only Memory (Festwertspeicher)
RSA	Asymmetrischer Verschlüsselungsalgorithmus (Rivest-Shamir-Adleman)
SC 85	Symmetrischer Verschlüsselungsalgorithmus
SCOS	Chipkartenbetriebssystem der Fa. Oldenbourg Datensysteme GmbH
SGB V	Sozialgesetzbuch V (Gesetzliche Krankenversicherung)
SHA	Hash-Algorithmus
STARCOS	Chipkartenbetriebssystem der Fa. Giesicke & Devrient AG

TCOS	Chipkartenbetriebssystem der Fa. Deutsche Telekom AG	WEF	Working Elementary File

Literaturangaben

Das Papier basiert in wesentlichen Teilen auf dem Buch

Rankl, W.; Effing, W.: Handbuch der Chipkarten, Aufbau - Funktionsweise - Einsatz, München, Wien: Carl Hanser-Verlag, 1995

Ferner wurden verwendet:

Giesicke & Devirent GmbH (Hrsg.): Referenz-Handbuch STARCOS S 1.1, Jan. 1995

Krummeck, G.; König, R.: Chipkarten im Gesundheitswesen - Technikfolgen-Abschätzung zur Sicherheit in der Informationstechnik, BSI-Schriftenreihe zur Informationstechnik, 1994

Zur ergänzenden Lektüre wird empfohlen:

Aberer, Karl: ISO/IEC 7816-8 SCQL-Database: Technik- und Mutzungsmöglichkeiten, in: Struif, B. (Hrsg.): Tagungsband des 6. GMD-Smart Card Workshops, GMD, 1996

Bachmeier, Roland: Chipkarten und Datenschutz, in: Struif, B. (Hrsg.): Tagungsband des 5. GMD-Smart Card Workshops, GMD, 1995

Ferreira, Malzahn, Quisquater, Wille: A High Performance Third Generation Crypto Card, in: Glade, Reimer, Struiff: Digitale Signatur und sicherheitssensitive Anwendungen, Vieweg

Fumy: Authentifizierung und Schlüsselmanagement, in: Struif, B. (Hrsg.): Tagungsband des 5. GMD-Smart Card Workshops, GMD, 1995

Hamann, Hirsch: Chipkarten-IC´s - die richtige Lösung für sicherheitssensitive Anwendungen, in: Glade, Reimer, Struif: Digitale Signatur und sicherheitssensitive Anwendungen, Vieweg

Horster, Lender: Hybride Opto-Chip-Karten, in: Struif, B. (Hrsg.): Tagungsband des 5. GMD-Smart Card Workshops, 1995

Kruse, Peuckert: Chipkarte und Sicherheit; DuD 3/95, S. 142 ff

Kruse: Sicherheitszertifikate für Chipkarten; DuD 9/95, S. 537 ff

Normann, Ute: Telefonkarten-Chip und Sicherheit, in Struif, B. (Hrsg.): Tagungsband des 6. GMD-Smart Card Workshops, GMD, 1996

SmartsCards - eine neue Dimension in der Informationstechnik, Der GMD-Spiegel 1/92, GMD, 1992

Struif, B.: Chipkarten - State of the Art, Tutorium „Verläßliche Informationssysteme“, anläßlich der Fachtagung VIS 1991

Struif, B.: Neue Smart Card-Features aus Normensicht, in: Struif, B. (Hrsg.): Tagungsband des 6. GMD-Smart Card Workshops, 1996

Weikmann: Die neue Generation von Chipkarten-Mikrocontrollern, in: Glade, Reimer, Struiff: Digitale Signatur und sicherheitssensitive Anwendungen, Vieweg