AG Chipkarten
des AK Technik
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder

Anforderungen zur informationstechnischen Sicherheit bei Chipkarten

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 Krankenversichertenkarte (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.:

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 Chipkartenbasierte Dienstleistungssysteme (CDLS) genannt. Beispiele für solche Systeme sind:

Öffentliches Telefon-Kartenterminal
Funktelefon (Handy)
PC mit externem Kartenterminal oder integriertem Kartenleser
Laptop mit PCMCIA-Kartenleser
Geldausgabeautomat
Point-of-Sale-Kartenterminal (POS-Kartenterminal)
Versicherten-Kartenterminal in seiner Stand-alone-Ausführung (ohne PC-Anschluß)
Kontoauzugsdrucker
Airline-Checkin-Terminal
Customer-Service-Terminal
Fahrschein-/Parkticket-Terminal

Sicherheitsbetrachtungen zum Einsatz von Chipkarten müssen deshalb auch die Sicherheit dieser Infrastrukturen einbeziehen.

Wichtige Funktionalitäten der Chipkarten sind:

Chipkarten als Speicher von Daten, die hinsichtlich ihrer Vertraulichkeit und/oder Integrität hohen Schutzbedarf aufweisen (z. B. Kontodaten, medizinische Individualdaten, Personalausweisdaten, Führerscheindaten);
Chipkarten als Mittel zur Authentisierung 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.);

...

Chipkarten als Träger elektronischer Geldbörsen.

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 Krankenversichertenkarte 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 Betriebsmitteln (Verlust der Verfügbarkeit);
unbefugte Änderung identifizierender Angaben (Verlust der Authentität).

Diese Gefahren sind sowohl dann zu betrachten, wenn die Daten auf der Chipkarte gespeichert werden, als auch dann, wenn sie in einer externen Datenbank gespeichert werden, die durch Chipkarten erschlossen wird.

Vor der Entscheidung über den sicherheitsrelevanten Einsatz von Chipkarten-Anwendungen sollte eine projektbezogene 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 Chipkarte 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 CDLS realisiert. Datenschutzrechtliche Anforderungen erstrecken sich hier neben den CDLS auch auf die Rahmenbedingungen bei der Herstellung, bei der Initialisierung, beim Versand und bei der Ersatzbeschaffung von Chipkarten in Fällen des Verlustes oder der Zerstörung einschließlich des "Ungültigkeitsmanagements". Die Hersteller bieten Chipkarten an, deren Leistungsfähigkeit und Funktionsweise diesbezüglich zum Teil sehr unterschiedlich ist. Eine Standardisierung wäre auch aus datenschutzrechtlicher Sicht in diesem Bereich dringend zu empfehlen.

Das Sicherungskonzept für Chipkarten sollte folgende Mindestanforderungen erfüllen, wenn Schutzbedarf besteht:

1. Grundschutzmaßnahmen
   Ausstattung des Kartenkörpers mit fälschungssicheren Authentisierungsmerkmalen 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 Verschlüsselungs- und Signaturfunktionen sowie zur Generierung von Zufallszahlen.
   Sicherung der Kommunikation zwischen der Chipkarte, dem CDLS und dem ggf. im Hintergrund wirkenden System durch kryptographische Maßnahmen.
   Sicherung unterschiedlicher Chipkartenanwendungen auf einer Chipkarte durch gegenseitige Abschottung.
   Durchführung einer gegenseitigen Authentisierung von Chipkarte und CDLS 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. Zur Sicherung von Transaktionen oder zur Rekonstruktion nicht korrekt abgelaufener Transaktionen kann ein Logging vorhanden sein.
   Auslagerung von Teilen der Sicherheitsfunktionen des Betriebssystems in dynamisch bei der Initialisierung bzw. Personalisierung zuladbare Tabellen, damit der Chipkartenhersteller nicht über ein "Gesamtwissen" verfügt.

3. Grundsätzlich sollte zunächst die Möglichkeit in Betracht gezogen werden, daß

bei der Chipkartenbenutzung Anonymität gewahrt bleiben kann. Ist dies nicht möglich, 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 datenschutzrelevanter Chipkartenanwendungen 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.

9. Sicherheitsrelevante Karten (z.B. Bankkarten) sollten über den gesamten Lebenszyklus der Karte kryptographisch gesichert sein.

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 (bestimmte kontaktlose Karten können auch über eine Entfernung von mehreren Metern von einem CDLS gelesen werden);

- Art der in der Karte bereitgestellten IT-Ressourcen:

reine Speicherchipkarten mit nicht flüchtigem Speicher (z.B. Identifikationskarten),
intelligente Speicherchipkarten mit EPROM (z.B. Telefonkarte) oder EEPROM (z.B. Krankenversichertenkarten
Prozessorchipkarten mit EEPROM, RAM, ROM und CPU
Prozessorchipkarten mit Coprozessor 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. unterschiedliche "Geldbörsen auf einer Chipkarte)
Berechtigungskarten (z.B. Mobiltelefone, Betriebsausweise)

Der Mikroprozessor einer Chipkarte leistet derzeit ca. 1 Million Befehle pro Sekunde. Direktzugriffsspeicher (RAM) erreichen eine Kapazität von 512 Byte, 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 - 32 MB.

III.2 Chipkarten-Betriebssysteme

Prozessorchipkarten verfügen über einen nicht überschreibbaren Speicherbereich, der keine Änderungen und somit auch keine Manipulationen ermöglicht.

In diesem "Read-Only-Memory" (ROM) befindet sich das Betriebssystem einer Chipkarte. Für Chipkarten-Betriebssysteme existiert u.a. die Normen aus der Serie ISO/IEC 7816, in der die Befehle solcher Systeme beschrieben werden. Die Chipkarten-Betriebssysteme nutzen diese Befehle in unterschiedlicher Weise, d.h. nicht jedes Betriebssystem unterstützt jedes Kommando oder jede Option eines Kommandos. Auch weisen fast alle Chipkarten-Betriebssysteme zusätzliche herstellerspezifische Kommandos auf. Die Chipkarten-Betriebssysteme ermöglichen die multifunktionale Nutzung von Chipkarten, können also mehrere unterschiedliche Anwendungen unterstützen.

Die folgende Darstellung wird an den internationalen Standard angelehnt:

III.2.1 Filesystem

Die Dateien des Betriebssystems sind hierarchisch organisiert. Den Ursprung des Dateisystems bildet das Master File (MF). Auf der MF-Ebene können Daten vorhanden sein, die von allen Anwendungen der Chipkarte gemeinsam genutzt werden (z.B. Daten über den Karteninhaber, Seriennummer, Schlüssel). Sie sind in der Regel in Elementary Files (EF) abgelegt.

Daneben gibt es auch sog. Dedicated Files (DF), die mit ihren untergeordneten EFs und ihren Funktionen die Anwendungen in einer Karte repräsentieren. Für jedes DF können separate Sicherheitsfunktionen definiert werden. Die DFs einer Chipkarte sind physikalisch und logisch voneinander getrennt, können aber auf die Daten auf der MF-Ebene zugreifen.

EFs können dem Betriebssystem zugeordnet sein und damit Daten enthalten, die das Betriebssystem nutzt, z.B. anwendungsbezogene Paßwörter, Schlüssel und andere Zugriffsattribute zu Nutzdaten. Ein direkter Zugriff mittels des CDLS ist nicht

möglich.

Sie können aber auch die Nutzdaten einer Anwendung enthalten, die ggfs. erst nach einer Authentisierung 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 Authentisierung

Die Authentisierungstechniken zwischen Chipkarte und einer externen Einheit werden in der Norm ISO/IEC 9798-2 beschrieben. Es wird dabei zwischen interner Authentisierung, bei der sich die Chipkarte gegenüber der externen Einheit authentisiert und externer Authentisierung, bei der sich die externe Einheit gegenüber der Chipkarte authentisiert unterschieden. Die gegenseitige Authentisierung ist in Vorbereitung.

Neben diversen Befehlen zum Lesen, Schreiben und Löschen (jeweils nach der Authentisierung) 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 Benutzerauthentisierung mit einer PIN. Dies kann eine auf MF-Ebene gespeicherte globale PIN oder eine DF-spezifische anwendungsbezogene PIN sein. Der Befehl überträgt die vom Nutzer eingegebene PIN und - falls erforderlich - die Nummer der zu überprüfenden PIN an die Karte. Diese vergleicht die eingegebene PIN mit dem gespeicherten Referenzwert. Ein Erfolg wird durch Senden des Status "OK" angezeigt, ansonsten ein interner Fehlversuchszähler dekrementiert und als Status "nicht OK" übertragen. Bei Zählerstand 0 wird die Anwendung der Applikation, die die PIN benutzt, blockiert. Bei einigen Betriebssystemen kann die Blockierung durch Eingabe eines Personal Unblocking Key (PUK) aufgehoben werden, der ebenfalls durch einen Fehlerzähler geschützt ist.

INTERNAL AUTHENTICATE löst eine interne Authentisierung aus. Dazu erhält die Chipkarte den Schlüsselbezeichner des ausgewählten EF und Authentisierungsdaten (Zufallszahl). Die Chipkarte verschlüsselt dann die Zufallszahlen mit dem Schlüssel des ausgewählten EF und sendet das Chiffrat zurück. Die prüfende Einheit (z.B. das CDLS oder eine Patientenkarte) entschlüsselt und prüft die Übereinstimmung der Zufallszahlen.

EXTERNAL AUTHENTICATE löst die externe Authentisierung aus. Dazu wird mit dem Befehl GET CHALLENGE eine Zufallszahl von der Chipkarte gefordert, die an die zu authentisierende Instanz übergeben wird. Diese verschlüsselt sie 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 die zu authentisierende Instanz als authentisch anerkannt.

...

Weitere Sicherheitsfunktionen werden derzeit in ISO 7816-8 spezifiziert. Von besonderer Bedeutung ist hierbei das Kommando PERFORM SECURITY OPERATION, mit dem folgende Sicherheitsoperationen ausgeführt werden können:

COMPUTE DIGITAL SIGNATURE
VERIFY DIGITAL SIGNATURE
VERIFY CERTIFICATE
HASH
COMPUTE CRYPTOGRAPHIC CHECKSUM
VERIFY CRYPTOGRAPHIC CHECKSUM
ENCIPHER
DECIPHER.

In ISO 7816-7 sind außerdem spezielle Sicherheitsfunktionen beschrieben, die sich auf Chipkarten mit einer sog. SCQL-Datenbank (Structured Card Query Language) beziehen.

III.3 Chipkartenbasierte Dienstleistungssysteme (CDLS)

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 Chipkarte gegen unbefugte Manipulationen ist weitgehend wertlos, wenn beim elektronischen Zahlungsverkehr das POS-Terminal leicht manipuliert werden kann. Jedoch sieht ISO/IEC 7816 Schutzmechanismen vor, die bei richtiger Anwendung mit vertretbarem Aufwand nicht umgangen werden können.

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. Auch wenn es einmal möglich sein wird, direkt mit der Chipkarte zu kommunizieren, z.B. über Sensorfelder, werden CDLS kaum entbehrlich sein, denn sie stellen zumindest die Schnittstelle zu jenen Nutzern dar, die mit dem Inhaber der Karte nicht identisch sind. CDLS können eigene Verarbeitungskapazitäten bieten und auch die Verbindung zu anderen Systemteilen herstellen.

Bisher sind für alle Chipkarten-Anwendungen (Telefonkarten, Krankenversichertenkarten, Sicherungskarten für Mobiltelefone usw.) spezielle CDLS entwickelt und eingesetzt worden. Soweit erkennbar, werden universell einsetzbare CDLS bisher nicht auf dem Markt angeboten. Im Gesundheitswesen werden derzeit CDLS eingesetzt, deren Verwendung auf die Kommunikation mit der Krankenversicherungskarte eingeschränkt wurde. Da sich weitergehende Anwendungen abzeichnen, wurde eine Spezifikatione für multifunktionale CDLS angefertigt, die von einem Arbeitskreis der Arbeitsgemeinschaft "Karten im Gesundheitswesen" und der Gesellschaft für Mathematik und Datenverarbeitung

(GMD) herausgegeben worden ist.

Dieser Spezifikation liegt folgende Konzeption zugrunde:

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

Allerdings ist die Option, ein universell einsetzbares CDLS zu schaffen, aus pragmatischen Erwägungen heraus relativiert worden. Von den nach ISO 7816-3 zulässigen Optionen für die Übertragungsparameter wird nur ein Teil als obligatorisch gefordert. Dies entspricht der Politik des Kreditkartensektors, die zulässigen Lösungen enger zu fassen als das Spektrum der Optionen. Der Spezifikation entsprechende CDLS können sowohl mit synchronen Chipkarten wie die Krankenversicherungskarte als auch mit Prozessor-Chipkarten kommunizieren, die ein standardisiertes Übertragungsprotokoll unterstützen.

Es können anwendungsspezifische Funktionen im CDLS 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 erlaubt die Behebung von Softwarefehlern und ggf. im gewissen Umfang einen Upgrade von Leistungen.
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.
CDLS als separate Endgeräte können zusätzlich mit folgenden Optionen ausgestattet sein:

Display und/oder Tastatur,
mehrere Kontaktiereinheiten 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 (CDLS), die ebenfalls besonders zu sichern sind. Eine Chipkarte bildet zusammen mit dem CDLS ein vollständiges Rechnersystem mit Ein- und Ausgabekomponente. Die Evaluation der richtigen Funktionsweise setzt voraus, daß dabei alle Systemkomponenten einbezogen sind.
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 in sicherer Umgebung oder 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,
die Produktion und das Laden von Software,
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)
aufgebrachtes 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 auf äußere Eingriffe passend reagieren und ggfs. den Chip zerstören.

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 eine Metallisierung des gesamten Chips.

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 über- oder unterschreitet, wird die weitere Ausführung von Prozessorbefehlen unterbunden.
Den gleichen Zweck verfolgt die Taktüberwachung. Es werden damit Angriffe erschwert, mit denen die Abarbeitung einzelner Befehle analysiert werden soll.
Es erfolgt eine Power-On-Erkennung, um bei Reset einen definierten Zustand herzustellen.

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 CDLS dynamisch aus Tabellen geladen werden.

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

a) Die Identifizierung und Authentifizierung des Benutzers erfolgt mittels PIN 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 CDLS die Daten transparent weiterleitet.

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

e) Auf Opto-Hybridkarten können die Daten auf der optischen Fläche verschlüsselt abgelegt werden. Die Entschlüsselung kann mit Hilfe des Prozessors erfolgen, der die Schlüssel verwaltet.

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, CDLS 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 schützt vor der Erstellung von Dubletten.

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 chipkartenbasierten Dienstleistungssystemen (CDLS)

Zwar bilden - wie oben festgestellt - Chipkarten und CDLS erst zusammen ein vollwertiges Rechensystem, jedoch befinden sich beide Komponenten in der Regel in unterschiedlicher Verfügungsgewalt, die Karte in der des Inhabers und das CDLS 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 CDLS verändert oder die Hardware des CDLS manipuliert wird. Eine Zertifizierung von CDLS kann sich daher nur auf unveränderliche Teile beziehen.

Wenn eine Chipkarte in ein CDLS 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 CDLS 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 CDLS testen zu 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 CDLS können auch dazu führen, daß die geheimen oder unverfälschbaren Authentifizierungsmerkmale (PIN, biometrische Merkmale) bei der Authentifizierung des Kartenbesitzers in das CDLS übertragen und so Dritten bekannt werden.

Es sind daher folgende Sicherheitsanforderungen an CDLS zu stellen:

Die CDLS müssen über mechanisch gesicherte Gehäuse verfügen, damit eine Hardware-Manipulation verhindert oder erschwert bzw. erkennbar 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 CDLS autark sein muß.
Die CDLS müssen alle automatisch prüfbaren Sicherheitsmerkmale des Kartenkörpers prüfen können, müssen demzufolge also über die entsprechenden Sensoren verfügen (siehe IV.2.2).
Sofern die Kommunikation zwischen Chipkarte und CDLS 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 CDLS eingebrachten Drähte) zu verhindern.

Als besonders angriffsgefährdet sind CDLS vom Typ "PC mit Kartenterminal" anzusehen, sofern sie nicht in manipulationsgeschützten Umgebungen eingesetzt werden. Erhöhte Schutzfunktionen werden hier als notwendig angesehen. Die bisherigen Spezifikationen für die CDLS lassen nicht erkennen, daß Maßnahmen gegen Penetrationsversuche aus der IT-Umgebung der Chipkartenanwendung im CDLS 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/CDLS.

Abkürzungsverzeichnis

CDLS	Chipkartenbasiertes Dienstleistungssystem
CPU	Central Processing Unit (Zentraleinheit)
DDS	Signieralgorithmus
DES	Symmetrischer Verschlüs- selungsalgorithmus (Data Encryption Standard)
DF	Dedicated File
DSS	Signieralgorithmus (Digital Signature Standard)
EEPROM	Electrically Erasable Programmable Read Only Memory (elektrisch löschbarer, programmierbarer Festwertspeicher)
EF	Elementary File
EPROM	Erasable Programmable Read Only Memory (löschbarer, programmier- barer Festwertspeicher)
IDEA	Symmetrischer Verschlüs- selungsalgorithmus
IEC	International Electrotechni- cal Commission
ISO	International Standardisation Organisation
IT	Informationstechnik
KB	Kilobyte
KT	Kartenterminal
KVK	Krankenversicherungskarte
MAC	Message Authentification Code
MB	Megabyte
MF	Masterfile
PC	Personal Computer
PIN	Persönliche Identifikations Nummer
PUK	Personal Unblocking Key
RAM	Random Access Memory (Direktzugriffsspeicher)
RipeMD160	Hash-Algorithmus
ROM	Read Only Memory (Festwertspeicher)
RSA	Asymmetrischer Verschlüsselungsalgorithmus (Rivest-Shamir-Adleman)
SC 85	Symmetrischer Verschlüsselungsalgorithmus
SGB V	Sozialgesetzbuch V (Gesetzliche Krankenversicherung)
SHA	Hash-Algorithmus

Zuletzt geändert:
am 16.02.97