HANSER

Chipkarten-Anwendungen

Wolfgang Rankl

Entwurfsmuster für Einsatz und Programmierung von Chipkarten

ISBN 3-446-40403-1

Leseprobe

Kapitel 4

Muster zu Grundlagen

Noch vor den eigentlichen Spezifikationsarbeiten gilt es, bei einem Chipkarten-System eine Reihe von grundlegenden Dingen zu berücksichtigen, die noch unabhängig von Design und Implementierung sind. Diese Dinge müssen bereits in den frühen Phasen eines Projekts bedacht werden, da sie sich zu einem späteren Zeitpunkt nur noch mit überproportionalem Zusatzaufwand einbeziehen lassen. Dies sind die Gebiete Datenschutz, Exportkontrolle, Kryptoregulierung und auch die normativen Grundlagen. Beim Start eines Chipkarten-Projekts muss ferner festgelegt werden welche Form und welchen Inhalt die zu erstellenden Dokumente haben sollen. Werden alle diese Punkte frühzeitig und vollständig bedacht, so lassen sich die darauf folgenden Schritte nahtlos und ohne Komplikationen anfügen. Besonders in dieser Phase eines Projekts gilt das Allgemeingut der Informatik, dass Fehler in frühen Phasen nur noch mit unverhältnismäßig hohem Aufwand in den späteren Phasen berichtigt werden können.

4.1 Datenschutz (*data protection*)

Auf nichttechnischer Ebene und abstrakt betrachtet sind Chipkarten Träger von personenbezogenen Daten. Naturgemäß weckt dies bei den unterschiedlichsten staatlichen und nichtstaatlichen Organisationen erhebliche Begehrlichkeiten.

Die ersten Datenschutzgesetze (*data protection law*) entstanden Anfang der siebziger Jahre, so etwa der US-amerikanische Fair Credit Reporting Act (1970), das Datenschutzgesetz in Hessen (1970) und Schweden (1972). Auf eine breite Basis wurde der Datenschutz aber erst in den neunziger Jahren gestellt, als nahezu alle Industrieländer entsprechende Gesetze verabschiedet hatten.

Die Ursprünge des Datenschutzes in Deutschland gehen zu einem erheblichen Teil auf das so genannte Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 zurück, in dem das „Recht auf informationelle Selbstbestimmung“ formuliert wurde. Die Argumentation ist eine hervorragende Begründung, warum Datenschutz ein wichtiges Bürgerrecht ist: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzu-

schätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen."

Ein adäquater Schutz der persönlichen Daten sollte in einer modernen Gesellschaft eine Selbstverständlichkeit sein. Der weit verbreiteten naiven Argumentation „Ich habe doch nichts zu verbergen" kann man gut den Vergleich zum Alltag entgegenstellen, in dem Anonymität seit jeher eine Selbstverständlichkeit ist. Im IT-Leben sollte dies ebenfalls gelten.

Die rechtlichen Rahmenbedingungen werden durch eine Reihe von Gesetzen und Vorgaben wie die Richtlinien über personenbezogene Daten der Vereinten Nationen von 1990, die Empfehlungen für den Schutz des Persönlichkeitsbereichs der OECD von 1980, dem Datenschutz-Übereinkommen des Europarats von 1981 und in Deutschland das Bundesdatenschutzgesetz (BDSG) gegeben. Das sehr umfangreiche Gebiet, das mittlerweile auch ein Spezialgebiet der Rechtswissenschaften ist, wird im Folgenden auf der Grundlage genereller technischer Prinzipien mit Fokus auf Chipkarten behandelt.

Es herrscht eine erhebliche Abhängigkeit der jeweiligen Datenschutzgesetze von Kultur, Land, Politik und auch dem aktuellen Zeitgeschehen. So wurden beispielsweise nach den Terroranschlägen vom 11. September 2001 in einigen Ländern bestimmte Datenschutzmaßnahmen erheblich ausgehöhlt. Die Datenschutzgesetze bewegen sich in einem Spannungsfeld, bei dem oftmals eine Güterabwägung zwischen den Interessen der Bürger und den Interessen des Staates stattfinden muss. Der Schutz von persönlichen Daten kann deshalb auch nicht absolut sein, da es kritische Situationen gibt, in denen die Gesellschaft handlungsfähig sein muss.

Datenschutz muss sowohl durch Technik und entsprechende Gesetze realisiert werden, wobei es aber durchaus datenschutzfreundliche Technologien gibt. Ein Beispiel dafür sind Chipkarten, bei denen beispielsweise ein unberechtigter Zugriff aufgrund der dezentralen Datenspeicherung deutlich schwieriger ist als bei Daten, die auf einem zentralen Server liegen. Richtig eingesetzt, können Chipkarten die Qualität des Schutzes personenbezogener Daten stark erhöhen.

4.1.1 Begriffsbestimmung

Datenschutz ist definiert als der technische und rechtliche Schutz von einer einzelnen Person zuzuordnenden Informationen über persönliche und sachliche Verhältnisse. Man bezeichnet diese Art von Daten auch als personenbezogene Daten. Mit ihnen kann eine Person direkt oder indirekt identifiziert werden.

Die Anonymisierung ist die Veränderung von personenbezogenen Daten in einer Weise, dass es nicht mehr möglich ist, diese veränderten Daten der ursprünglichen Person zuzuordnen. Bei der Pseudonymisierung werden hingegen personenbezogene Daten in einer Weise verändert, dass diese veränderten Daten ohne Kenntnis der Zuordnungsvorschrift

nicht mehr der ursprünglichen Person zugeordnet werden können. Der Begriff Pseudonymisierung rührt daher, dass im einfachsten Fall der ursprüngliche Name durch ein eindeutiges Pseudonym ersetzt wird. In einer Zuordnungstabelle, der so genannten Zuordnungsvorschrift, wird die Verbindung zwischen Pseudonym und ursprünglichem Namen hergestellt. Eine Deanonymisierung, d. h. die Rückgängigmachung der Anonymisierung, ohne Zugriff auf die Zuordnungstabelle darf dabei nicht möglich sein.

Im Gegensatz zum Datenschutz bezeichnet die Datensicherheit den Schutz vor unberechtigten Zugriffen und Zerstörung von Daten.

4.1.2 Allgemeine Grundsätze

Die konkreten Maßnahmen für Datenschutz unterscheiden sich von Land zu Land erheblich. Für international eingesetzte Systeme kann die Findung eines in allen Einsatzländern tragfähigen Kompromisses mit großem Aufwand und unter Umständen sogar auch Funktionsbeschränkungen verbunden sein. So ist beispielsweise in Deutschland der Datenschutz nur bei natürlichen Personen (d. h. Menschen) verbindlich zu beachten, in anderen Ländern wie der Schweiz auch bei juristischen Personen (z. B. Firmen).

Im Folgenden sind die wesentlichen global anerkannten Grundsätze des Datenschutzes aufgeführt und kurz erklärt. Als Basis wurde dabei vom Recht auf informationelle Selbstbestimmung der Betroffenen ausgegangen und die Grundsätze der Erforderlichkeit, Zweckbindung und Transparenz beachtet. Dies ist konform zur Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten.[1] Weitere Hinweise finden sich im Bundesdatenschutzgesetz[2], der Internetseite des Bundesbeauftragten für den Datenschutz[3] und in dem sehr umfassenden Buch von Peter Schaar[4].

Transparenz Der Benutzer muss jederzeit Transparenz haben, was mit seinen Daten passiert, und er muss über seine Rechte informiert worden sein. Bei Lese- und Schreibvorgängen an einem Chipkarten-Terminal darf es keine verdeckten Aktionen geben, und es sollten verständliche Angaben gemacht werden, was mit den Daten gemacht wird.

Zweckbindung Die erhobenen Daten sind an einen bestimmten und rechtmäßigen Zweck gebunden und dürfen auch zu einem späteren Zeitpunkt nicht anderweitig genutzt werden.

Einwilligung Der Betroffene muss vorab mit eindeutiger und bewusster Handlung die Einwilligung zur Speicherung und Verarbeitung seiner Daten gegeben haben, sofern die Daten ihm direkt oder indirekt zugeordnet sind. Weiterhin ist es unerlässlich, dass der Betroffene über seine Rechte bezüglich des Datenschutzes unmissverständlich informiert wird.

Erforderlichkeit Die gesammelten und verarbeiteten persönlichen Daten müssen für den genannten Zweck auch tatsächlich erforderlich sein.

[1] Siehe auch [EU 95].
[2] Siehe auch [BDSG 01].
[3] Siehe auch [BfD].
[4] Siehe auch [Schaar 02].

Datenqualität Die verarbeiteten Daten müssen korrekt und auf dem aktuellen Stand sein.

Datensparsamkeit und Datenvermeidung Es dürfen nur die für den Zweck erforderlichen persönlichen Daten gesammelt und verarbeitet werden und keine zusätzlichen Informationen. Alle Daten, die die eindeutige Identifizierung einer Person ermöglichen, sollten nur so lange wie unbedingt notwendig gespeichert werden.

Auskunftsrecht Die betroffenen Personen haben das Recht, ohne unzumutbare Verzögerung oder übermäßige Kosten in angemessenen Zeitabständen und in verständlicher Form Auskunft über die verarbeiteten Daten zu bekommen. Sie haben auch das Recht auf Berichtigung oder Löschung von Daten, wenn diese nicht korrekt sind oder den einschlägigen Gesetzen widersprechen.

Nichtdiskriminierung Besonderem Schutz unterliegt die Verarbeitung von personenbezogenen Daten, die eine der folgenden Informationen enthalten oder daraus abgeleitet werden können: rassische und ethnische Herkunft, politische Meinung, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, steuerliche und soziale Verhältnisse, Dienst- und Arbeitsverhältnisse sowie Daten über Gesundheit und Sexualleben.

Verschwiegenheit Personenbezogene Daten, die für einen bestimmten Zweck gesammelt und gespeichert worden sind, dürfen nicht an Dritte weitergegeben werden.

4.1.3 Empfehlungen für Chipkarten-Systeme

Die folgenden Absätze sind eine Zusammenstellung von Vorschlägen, um heute übliche Systeme mit Chipkarten an die Grunderfordernisse des Datenschutzes anzupassen. Weitere einschlägige Hinweise für allgemeine Systeme findet man bei den Empfehlungen des Hamburgischen Datenschutzbeauftragten[1], bei Hansjürgen Garstka[2] und natürlich im IT-Grundschutzhandbuch[3].

Grundsätzlich sollten bei Chipkarten-Systemen immer so weit wie möglich datenschutzfreundliche Techniken Anwendung finden. Das typische Beispiel dazu ist die anzustrebende dezentrale Datenhaltung in Chipkarten unter der Kontrolle des Betroffenen anstelle einer missbrauchsanfälligen Datenhaltung auf zentralen Servern. Des Weiteren muss dem Betroffenen eindeutig klar sein, wer welche Daten zu welchem Zweck über ihn verarbeitet.

Man sollte auch nicht dem weithin verbreiteten Irrglauben anhängen, dass bestimmte persönliche Daten ohnehin nur Bagatelldaten sind und deshalb die Datenschutzbestimmungen nicht beachtet werden müssen. Personenbezogene Daten unterliegen in aller Regel dem Datenschutz und sind dementsprechend zu verarbeiten.

Idealerweise berücksichtigt auch die Dokumentation des Systems und der Chipkarten-Anwendung bereits die Aspekte des Datenschutzes, sodass entsprechende Kontrollen problemlos durchführtbar sind. Das Recht auf informationelle Selbstbestimmung bedeutet auch, dass der Betroffene der Erfassung, Verarbeitung und Nutzung seiner persönlichen

[1] Siehe auch [Datenschutz 96].
[2] Siehe auch [Garstka 03].
[3] Siehe auch [IT-Grundschutzhandbuch 04].

Daten durch Dritte zustimmen kann. Dies ist der übliche Ansatz, um persönliche Daten in einem System verwenden zu dürfen.

Berücksichtigung beim Systemdesign Die Aspekte des Datenschutzes müssen bereits bei Beginn eines Chipkartenprojekts beim Systemdesign berücksichtigt werden. Datenschutz verhält sich in dieser Hinsicht analog den Eigenschaften Qualität und Sicherheit, da Maßnahmen für den Datenschutz mit vertretbarem Aufwand nicht mehr nachträglich eingebaut werden können. Dies betrifft sowohl das gesamte Chipkarten-System wie auch das Betriebssystem und die eigentliche Anwendung auf der Chipkarte. Idealerweise bezieht man bereits ab Projektanfang einen Experten für Datenschutz in die Entscheidungen ein. Günstig ist es auch, dass nach Abschluss der Systemarchitektur die Einhaltung der Datenschutzgrundsätze durch eine externe und unabhängige Kontrollinstanz mit einem Datenschutzaudit bestätigt wird. Damit können bereits in einem relativ frühen Projektstadium spätere Änderungen aufgrund von nicht eingehaltenen Datenschutzbestimmungen mit hoher Wahrscheinlichkeit vermieden werden.

Transparenz Die Transparenz eines Chipkarten-Systems gegenüber dem Benutzer ist ein wichtiger Punkt. Es darf keinesfalls sein, dass Daten versteckt erhoben, gelesen oder gespeichert werden. Wichtig ist eine Anzeige am Terminal, anhand der der Benutzer eindeutig informiert wird, ob ein Zugriff auf die Chipkarte stattfindet. Insbesondere bei kontaktlosen Chipkarten ist dies für den Benutzer oftmals die einzige Möglichkeit, überhaupt herauszufinden, ob ein Terminal mit der Chipkarte kommuniziert.

Hinsichtlich der Transparenz ist es von Bedeutung, dass der Benutzer bei der Ausgabe der Chipkarte vollständige Informationen darüber enthält, was darauf gespeichert ist. Diese Daten befinden sich oftmals individuell ausgedruckt auf dem Anschreiben, das der entsprechenden Karte beiliegt. Dies ist eine Maßnahme, die zwischen Kartenherausgeber und Benutzer Vertrauen schafft, da genau erkennbar ist, welche Daten gespeichert sind. Im Bereich der Krankenversichertenkarten ist dies in der Regel sehr gut geregelt. Ein Negativbeispiel geben hier immer wieder manche GSM-Netzbetreiber ab, die über die Luftschnittstelle im Hintergrund und ohne Information des Benutzers ihre Servicetelefonnummern auf der SIM ändern. Dies mag zwar für viele Kunden nützlich sein, da er damit beispielsweise immer die aktuelle Rufnummer der Auskunft auf seiner SIM gespeichert hat, doch hinterlässt es auch ein gewisses Unbehagen.

Berücksichtigung der Zweckbindung Die erhobenen und gespeicherten persönlichen Daten sind immer an einen bestimmten Zweck gebunden und dürfen nicht anderweitig verwendet werden. Diese Zweckbindung der Daten bedeutet auch, dass die beliebte Idee, die Krankenversicherungskarte als kostenlose ID-Karte für Firmen zu verwenden, den Datenschutzgesetzen völlig widerspricht. Die Daten der Krankenversicherungskarte sind strikt an den Zweck der Krankenversichung gebunden.

Datensparsamkeit und -vermeidung Grundsätzlich sollten bei einem Chipkarten-System nur personenbezogene Daten erhoben und gespeichert werden, die auch unmittelbar zum Systembetrieb notwendig sind. Vor allem in Protokolldateien dürfen nur so wenig Datenspuren wie unbedingt notwendig hinterlassen werden. Auch sollten alle personenbezogenen Daten, die nicht mehr erforderlich sind, unverzüglich physikalisch gelöscht werden. In manchen Fällen kann es auch nützlich sein, für bestimmte Daten eine Höchst-

speicherfrist festzulegen und die Daten danach physikalisch zu löschen. Dies ist auf einer Chipkarte technisch nicht einfach, da dort intern kein authentisches Datum und Zeit vorhanden sind. Die Höchstspeicherfrist kann jedoch beispielsweise auch von einem Transaktionszähler abhängig sein, sodass die Chipkarte autark und automatisch die Löschung der betreffenden Daten bei einem bestimmten Zählerstand durchführen kann.

Datenzugriff Es sollte nicht möglich sein, datenschutzrechtlich relevante Daten frei aus der Chipkarte zu lesen. So können etwa frei lesbare Protokolldateien auf einer Börsenkarte sehr gut zur Erstellung von Nutzungsprofilen verwendet werden. Um Missbrauch zu verhindern, wird der Lesezugriff nur erlaubt, wenn vorher eine erfolgreiche PIN-Prüfung durchgeführt wurde. Grundsätzlich sollte auch sichergestellt sein, dass keine Daten, die für andere bestimmt sind, gelesen, verändert oder gelöscht werden. Dies ist bei den heutigen frei programmierbaren Multifunktionsterminals jedoch schwierig sicherzustellen. Der beste Schutz ist immer noch, dass die Chipkarten-Anwendung so gestaltet ist, dass jeglicher unautorisierte Zugriff auf personenbezogene Daten verhindert wird.

Im GSM-Mobilfunksystem gibt es bei der SIM zum Thema des rollenspezifischen Datenzugriffs einen ausgeklügelten, aber trotzdem ziemlich unkomplizierten Mechanismus. Dieser besteht im Wesentlichen aus zwei voneinander unabhängigen PINs, wobei PIN 1 die des Benutzers ist und PIN 2 dem Besitzer des Mobiltelefons zugeordnet ist. Mit der PIN 1 kann der Benutzer zwar telefonieren, aber aufgrund der Dateizugriffsbedingungen nicht auf die Daten des Besitzers zugreifen. Nach Eingabe von PIN 2 darf der Besitzer alle Daten lesen und schreiben. Damit ist es möglich, dass der Besitzer sein Mobiltelefon verleiht, ohne dass der Benutzer beispielsweise die zuletzt gewählten Nummern des Besitzers lesen kann. Leider wird dieser Mechanismus in der Praxis aus Bequemlichkeitsgründen selten eingesetzt.

Löschen von Daten Müssen Daten auf der Chipkarte gelöscht werden, so ist grundsätzlich dem physikalischen Löschen der Vorzug zu geben, da beim logischen Löschen die betreffenden Daten rekonstruiert werden können.

Dieses Prinzip lässt sich anhand der SIMs im Mobilfunksystem GSM gut verdeutlichen. Wird auf der SIM eine Kurzrufnummer (ADN – *abbreviated dialing number*) gelöscht, so muss der ganze betreffende Record im EF_{ADN} mit 'FF' überschrieben werden – der Record wird also physikalisch gelöscht. Damit ist es nicht mehr möglich, die Kurzrufnummer nach dem Löschen zu lesen. Bei den Kurznachrichten (SMS – *short message service*) hingegen reicht es nach der GSM-Spezifikation TS 51.011 aus, das erste Byte des Records im EF_{SMS} mit '00' zu überschreiben. Dies ist das Statusbyte, das angibt, ob die folgenden Daten gültig oder ungültig sind. Dieses logische Löschen der Daten führt dazu, dass die Kurznachricht nach wie vor im EF_{SMS} gespeichert ist und mit einem READ RECORD-Kommando gelesen werden kann. Der Grund für diesen aus Datenschutzsicht bedenklichen Löschvorgang liegt in dem schnelleren logischen Löschvorgang, da nur ein einziges Byte geändert werden muss und nicht der ganze Record wie beim physikalischen Löschen.

Zentrale Speicherung von Daten Eine zentrale Speicherung von personenbezogenen Daten ist grundsätzlich problematisch, da alle Zugriffe außerhalb der Kontrolle des Benutzers sind und je nach Zugriffsberechtigung beliebige Instanzen die Daten lesen oder

ändern können. Wenn möglich, sollte man deshalb eine zentrale Speicherung vermeiden, da sie *per se* keine datenschutzfreundliche Technologie darstellt und missbrauchsanfällig ist.

Allerdings sprechen oftmals starke Gründe für die zentrale Speicherung, da so bei Verlust oder Defekt der Karte eine Neuausstellung einfach durchführbar ist. Außerdem ist die Realisierung von Online-Abfragen der Daten durch den Benutzer ohne Komplikationen möglich. Viele weit verbreitete Bonuspunktesysteme arbeiten nach diesem Prinzip, dabei wird zur Benutzeridentifizierung oftmals nur eine Magnetstreifenkarte oder eine Karte mit Barkode benutzt. Gleichwohl sind beispielsweise Klebemarken, Stempelkarten oder Speicherung auf anonymen Chipkarten datenschutzrechtlich deutlich unbedenklicher als für den Benutzer völlig intransparente zentrale Datenbanken.

Abschottung von Anwendungen Es ist für moderne Chipkarten-Betriebssysteme eine Selbstverständlichkeit, dass sie nebeneinander existierende Anwendungen vollständig voneinander abschotten, sodass von einer Anwendung aus nicht auf die Daten einer anderen zugegriffen werden kann. Allerdings gibt es durchaus Möglichkeiten und auch sinnvolle Einsatzzwecke, um die Abschottung unbewusst oder bewusst wieder auszuhebeln. Es darf jedoch keinesfalls möglich sein, dass von einer Anwendung unautorisiert auf datenschutzrelevante Daten einer anderen Anwendung zugegriffen werden kann.

Anonymität und Pseudonymität Wo und wann es möglich ist, sollten nur anonymisierte Daten benutzt werden. Eine Deanonymisierung darf dabei nicht möglich sein. Für die statistische Systemüberwachung reicht dies in den meisten Fällen völlig aus. Falls eine Anonymität in besonderen Fällen nicht möglich ist, sollten zumindest Pseudonyme benutzt werden.

Anonyme Chipkarten-Systeme wie beispielsweise vorbezahlte anonyme Chipkarten (Prepaid-Karten) sind datenschutzrechtlich deshalb immer deutlich einfacher zu betreiben als personenbezogene Systeme. Ein Beispiel für Pseudonymisierung kommt aus dem GSM Mobilfunksystem. Dort ist die IMSI (*international mobile subscriber identity*) eine international eindeutige Kennung für die Teilnehmeridentität. Im Normalbetrieb wird jedoch nicht die IMSI benutzt, sondern die TMSI (*temporary mobile subscriber identity*), welche ein Pseudonym ist, da sie nicht im gesamten Mobilfunksystem eindeutig ist. Die TMSI reicht aber im Regelfall zur Authentisierung des Teilnehmers aus.[1] Dies zeigt, dass man durchaus nicht immer die Teilnehmeridentität verwenden muss, sondern es ausreichen kann, im System mit einem Pseudonym zu arbeiten.

4.1.4 Zusammenfassung

Die Datenschutzgesetze greifen dann, wenn personenbezogene Daten gespeichert oder verarbeitet werden. Sofern es sich um Daten handelt, die nicht eindeutig einer einzelnen Person zugeordnet werden können, müssen die Aspekte des Datenschutzes nicht berücksichtigt werden. Ist der Datenschutz hingegen zu berücksichtigen und die Speicherung bzw. Verarbeitung nicht durch ein Gesetz explizit erlaubt, so muss der Betroffene über die verarbeiteten Daten und den Zweck informiert werden. Die wohl wirksamste Maßnahme

[1] Siehe auch [Rankl 02].

für einen weithin akzeptablen Datenschutz ist schlichtweg der weitgehende Verzicht auf die Sammlung und Verarbeitung personenbezogener Daten.

Ein großes gesellschaftliches Problem beim heutigen Datenschutz ist das mangelnde Bewusstsein vieler Menschen, dass sie selbst bestimmen können, was andere mit sie betreffenden Informationen machen. Die Änderung dieses Verständnisses wird sich über eine lange Zeitspanne erstrecken, doch sollten heutige Systeme bereits vorausschauend ein adäquates Datenschutzniveau anstreben, denn jeder Betreiber eines Systems muss sich immer vor Augen führen, dass alle Personen das Recht auf Schutz der sie betreffenden personenbezogenen Daten haben.

4.2 Exportkontrolle

Die meisten Güter dürfen ohne Einschränkungen in andere Ländern exportiert werden. Für bestimmte Kategorien von Gütern gibt es jedoch aufgrund einer Reihe von internationalen und nationalen Gesetzen und Vereinbarungen Ausfuhrbeschränkungen oder -verbote.

Auf internationaler Ebene ist das Wassenaar-Arrangement[1] von 1996 die Referenz für die Ausfuhrkontrolle von Rüstungsgütern und Gütern mit doppeltem Verwendungszweck. Dies schließt auch Produkte ein, die Kryptografie verwenden. Die Details dazu finden sich in der Wassenaar Arrangement Kontrolliste[2].

Nicht zu vernachlässigen sind im internationalen Handel die Exportbeschränkungen der USA, die zwar formal keine internationale Gültigkeit haben, weltweit jedoch durchaus unter Androhung oder Einsatz von Sanktionen durchgesetzt werden.

In Europa regelt neben den länderspezifischen Gesetzen auch eine spezielle Verordnung des Rates[3] den Export. Die meisten Länder haben ähnliche Gesetze und Einschränkungen und zum Teil drakonische Strafen für einen unerlaubten Export. So ist in Deutschland nach § 34 Abs. 5 AWG bereits der Versuch einer Straftat strafbar, und nach § 34 Abs. 4 und 6 AWG beträgt die Mindeststrafe zwei Jahre. Der Import von ausfuhrbeschränkten Gütern ist wissenswerterweise beinahe überall erlaubt.

In Deutschland ist die rechtliche Grundlage für Ausfuhrbeschränkungen oder -verbote das Außenwirtschaftsgesetz (AWG)[4] und die Außenwirtschaftsverordnung (AWV)[5]. Die Details dazu legt die Ausfuhrliste[6] des Bundesministeriums für Wirtschaft und Arbeit fest, die regelmäßig aktualisiert wird. Sie kann abhängig von der aktuellen politischen Lage durchaus auch kurzfristig angepasst werden. Diese Ausfuhrliste ist die eigentliche Grundlage für die Exportkontrolle.

Neben dieser Exportregulierung kann für ein bestimmtes Land und für bestimmte Güter auch noch ein generelles Ausfuhrverbot (Embargo) ausgesprochen werden. Damit dürfen die im Embargo genannten Güter in dieses Land grundsätzlich nicht mehr ausgeführt werden.

[1] Siehe auch [WA].
[2] Siehe auch [WAL].
[3] Siehe auch [EGV 00].
[4] Siehe auch [AWG 04].
[5] Siehe auch [AWV 04].
[6] Siehe auch [AL 04].

Der Beschränkung oder dem Verbot des Exports unterliegende Güter gehören in den militärischen, kerntechnischen, chemischen oder biologischen Bereich, aber auch in den Bereich der Informationstechnik. Dazu gehören auch Geräte für leistungsfähige Ver- und Entschlüsselung. Dies sind beispielsweise Chipkarten oder Sicherheitsmodule. Die Beschränkungen betreffen im Übrigen nicht nur den Export von Gütern, sondern auch den Wissenstransfer in die betreffenden Länder.

In diesem Zusammenhang ist auch zu beachten, dass manche Güter einen doppelten Verwendungszweck haben können. Man nennt sie auch „dual-use-Güter“. Es sind Güter, die sowohl für zivile und auch für militärische Zwecke eingesetzt werden können. Chipkarten können je nach Funktionsumfang also durchaus dual-use-Güter sein.

Die Exportrestriktionen greifen auch bei wesentlichen Einzelteilen eines Gesamtsystems, die als solche nicht genehmigungspflichtig sind. Man kann die Exportbeschränkungen also nicht umgehen, indem man ein genehmigungspflichtiges Gerät in viele nicht genehmigungspflichtige Teile aufteilt und diese dann einzeln exportiert.

Ähnlich verhält es sich damit, ein exportbeschränktes Gut zuerst in ein Zwischenland zu senden, in dem keine Exportbeschränkung für dieses Gut besteht, und von da aus weiter in das eigentliche Zielland zu exportieren. Eine solche Umgehung der Exportbeschränkungen ist selbstverständlich verboten. Dies wird rechtlich durch eine Endverbleibserklärung (*end use certificate*) unterbunden, in der der Empfänger des ersten Landes bestätigen muss, dass er das Gut nicht weiter exportiert.

In Deutschland ist das Bundesamt für Wirschaft und Ausfuhrkontrolle[1] (BAFA) die für die Ausfuhrkontrolle zuständige Behörde. Muss also ein der Ausfuhrgenehmigungspflicht unterliegendes Gut exportiert werden, so ist vorab beim BAFA ein entsprechender Antrag zu stellen. Wird diesem Antrag stattgegeben, dann erst darf das Gut exportiert werden. Die Exporterlaubnis hängt von verschiedenen Rahmenbedingungen ab. Die wichtigsten Punkte sind natürlich die Funktion des Gutes und das Land, in das exportiert werden soll.

Nach Abschnitt „5A002“ der deutschen Ausfuhrliste sind Systeme, Geräte, Module und integrierte Schaltungen für den Bereich Informationssicherheit mit Verwendung von Kryptotechnik prinzipiell ausfuhrgenehmigungspflichtig. Abschnitt „5B002“ beschränkt weiterhin auch die Ausfuhr von Einrichtungen zur Herstellung von Gütern, die unter Abschnitt „5A002“ genannt sind. Für die Praxis sind vor allem die Ausnahmen von der Genehmigungspflicht von Bedeutung. Ausgenommen von der Genehmigungspflicht sind nämlich Geräte, die lediglich Authentisierung und digitale Signatur unterstützen und auch symmetrische Kryptoalgorithmen mit einer Schlüssellänge von kleiner als 56 Bit.

Asymmetrische Kryptoalgorithmen, wie RSA, deren Sicherheit auf der Faktorisierung von ganzen Zahlen kleiner sind als 2^{512} beruhen, sind ebenfalls ausgenommen. Dies gilt auch für asymmetrische Kryptoalgorithmen, beruhend auf dem diskreten Logarithmusproblem (z. B. Elliptische Kurven) mit einer Ordnung kleiner als 2^{112}. Diese Liste ließe sich noch weiter fortsetzen.

Es sei hier jedoch auf die aktuelle Ausfuhrliste[2] hingewiesen, die vom Web-Server des BAFA kostenlos bezogen werden kann. Personenbezogene Mikroprozessorkarten für Mobilfunk, Rundfunk, Pay-TV, Digital Rights Management, Kopierschutz und für Zahlungs-

[1] Siehe auch [BAFA].
[2] Siehe auch [AL 04].

verkehr fallen explizit nicht unter Abschnitt „5A002“ und dürfen deshalb ohne besondere Genehmigung exportiert werden.

Eine im Mobiltelefon befindliche SIM oder eine elektronische Geldbörse in Kartenform darf also problemlos außer Landes gebracht werden. Eine Chipkarte ist jedoch exportbeschränkt, wenn ihre Funktion die Ver- und Entschlüsselung von Daten mit einem AES Kryptoalgorithmus mit 128 Bit Schlüssellänge ist. Dies gilt auch für frei programmierbare Chipkarten, die einen uneingeschränkten Zugriff auf Ver- und Entschlüsselungsfunktionen mit entsprechend großer Schlüssellänge zulassen.

4.3 Kryptoregulierung

Als die Kryptologie mit Beginn der siebziger Jahre zu einer öffentlichen Wissenschaft geworden war und viele der Kryptoalgorithmen und Kryptoprotokolle publiziert und allgemein verfügbar waren, kam es in den neunziger Jahren in den westlichen Industrieländern zu einer intensiven politischen Diskussion ob man die Benutzung starker Kryptografie einschränken sollte. Als starke Kryptografie werden alle Kryptoalgorithmen bezeichnet, die von staatlichen Stellen nicht gebrochen werden können.

Es gab Überlegungen, vorzuschreiben, dass bei der Benutzung von starken Kryptoalgorithmen grundsätzlich die Schlüssel bei einer staatlichen Stelle hinterlegt werden müssen (*key escrow*). Alternativ dazu wurde ein besonderer kryptografischer Algorithmus (DSS – *digital signature standard*) entwickelt, der nur für Signaturen und nicht zur Verschlüsselung geeignet war. Weiterhin wurde versucht, besondere Hardwarebausteine (Clipper Chip, Capstone Chip) mit dazugehöriger Schlüsselhinterlegung bei staatlichen Stellen in unterschiedlichsten Geräten zu etablieren. Es wurde auch angestrebt, bei verschiedener Kryptosoftware zusätzliche Mechanismen zur Schlüsselrückgewinnung (*key recovery*) einzuführen. Ein Beispiel dazu ist der ADK (*additional decryption key*) bei PGP, der Firmen die Möglichkeit eröffnet, auf PGP-verschlüsselte Dokumente ihrer Mitarbeiter zuzugreifen. Systeme, die auf IBE (*identity based encryption*) aufbauen, besitzen im Übrigen systemimmanent eine Instanz, die alle geheimen Schlüssel der Benutzer kennt. Ein anderer Beschränkungsansatz im Zug der staatlichen Reglementierung von Kryptografie war, nur die Benutzung von bestimmten Kryptoalgorithmen zu erlauben, die dann bei Bedarf mit einem für staatliche Stellen überschaubaren Aufwand gebrochen werden können.

Die Befürworter einer Regulierung von Kryptotechnik führen als Hauptargument ins Feld, dass es in bestimmten Fällen staatlichen Stellen möglich sein muss, die Kommunikation von Personen abzuhören. Die Gründe der Gegner einer Kryptoregulierung sind vielschichtiger. So argumentieren sie, dass starke Kryptografie notwendig ist, um in öffentlichen Netzen überhaupt verlässliche und im Zweifelsfalle einer gerichtlichen Überprüfung standhaltende Geschäftsprozesse durchführen zu können. Zudem würden sich Kriminelle durch Verbote ohnehin nicht davon abhalten lassen, die bekannten und frei verfügbaren starken Kryptoverfahren für ihre Kommunikation einzusetzen. Das ist in der Praxis zudem schwierig nachzuweisen, da man beispielsweise Nachrichten zuerst mit einem starken Verfahren und dann mit dem erlaubten schwachen Verfahren verschlüsseln könnte (Überverschlüsselung) oder stark verschlüsselt Nachrichten mittels Steganografie in eine unauffällige Nachricht einbetten kann.

Die Konsequenz aus Vorangehendem wäre, dass staatliche Stellen vor allem die Kommunikation der unbescholtenen Bürger abhören könnten. Ein weiteres Argument ist, dass die Verfahren zur Schlüsselhinterlegung und Schlüsselrückgewinnung durchaus Ansatzpunkte aufweisen, mit denen Dritte gegebenenfalls unerlaubt die geheimen Schlüssel ermitteln könnten. Einen guten Überblick zu dem Thema gibt der Report von Hal Abelson et al. [1]

Die Diskussion führte Ende der neunziger Jahre dazu, dass in Deutschland auf eine gesetzliche Regelung zur Einschränkung von Kryptografie verzichtet wurde. Dies entspricht der Lage in den meisten westlichen Industrieländern. Allerdings gibt es durchaus einige Ausnahmen[2] dazu. In Frankreich war die Verschlüsselung in den Jahren 1990 bis 1996 per Gesetz vollständig verboten. Diese harte Regulierung wurde 1996 etwas entschärft. So dürfen nunmehr Verschlüsselungsverfahren benutzt werden, es muss jedoch staatlichen Stellen möglich sein, bei Bedarf die Nachrichten zu entschlüsseln. In Rußland ist es nach wie vor grundsätzlich verboten, Nachrichten ohne eine entsprechende Lizenz zu verschlüsseln. In den USA dürfen innerhalb des Landes beliebige Kryptoalgorithmen benutzt werden, bei einer Kommunikation in andere Länder jedoch kann es beim Einsatz von starker Kryptografie zu rechtlichen Problemen kommen.

Es ist aber durchaus vorstellbar, wenn auch momentan nicht sehr wahrscheinlich, dass die aktuelle liberale Kryptopolitik unter bestimmten Umständen revidiert wird. Es dürfen heute ohne Beschränkungen alle Kryptoalgorithmen verwendet werden, und es gibt keinen Zwang, (geheime) Hintertüren für Sicherheitsbehörden in Systemen mit starker Kryptografie einzubauen, was der Zuverlässigkeit und dem Vertrauen in entsprechende Systeme erheblich zugute kommt. Für eine aktuelle Chipkarten-Anwendung bedeutet dies, dass man die technisch am besten geeigneten Verfahren benutzen kann. Dabei ist es sicherlich nicht notwendig, immer die kryptografisch stärksten Algorithmen zu benutzen, da diese mehr Rechenzeit und größere Schlüssel benötigen. Es sollten jedoch auch keine zu schwachen Verfahren eingesetzt werden, damit Dritte keine Ansatzpunkte für Angriffe haben.

Der allgemein anerkannte Kriterienkatalog[3] der Regulierungsbehörde für Telekommunikation und Post[4] (Reg TP) lässt sich ganz gut als Ausgangpunkt für eigene Entscheidungen nutzen. Dort werden beispielsweise die Hash-Algorithmen RIPEMD-160 und SHA-256 als für den Einsatz bis Ende 2010 geeignet aufgeführt. Beim RSA-Algorithmus gilt als Empfehlung für die Schlüssellänge 2 048 Bit, sofern ein langfristig akzeptables Sicherheitsniveau angestrebt wird.

4.4 Normen

Eine wichtige Eigenschaft von Chipkarten ist ihre weite Kompatibilität zu den unterschiedlichsten informationstechnischen Infrastrukturen. Dies wird vor allem durch eine große Zahl von den staatlichen Normungsinstanzen herausgegebenen Normen und von nichtstaatlichen Instanzen publizierten (Industrie-) Standards erreicht, an denen sich Kartenhersteller, Betriebssystem- und Anwendungsentwickler orientieren.

[1] Siehe auch [Abelson 97].
[2] Siehe auch [Crypto 02].
[3] Siehe auch [Kriterien 05].
[4] Siehe auch [Reg TP].

Die weltweit und für alle Chipkarten-Anwendungen gültigen ISO/IEC-Normen haben bei vielen technischen Punkten einen sehr allgemeinen Charakter. Deshalb werden sie in der Regel als normatives Rahmenwerk angesehen, und aufbauend auf ihnen legen dann weitere Normen und Standards die Details für bestimmte Anwendungszwecke fest. Dies sind dann wiederum die eigentlichen Vorgaben für die Spezifikationen, [1] die dann eindeutig die eigentliche Implementierung festlegen.

Die Verfügbarkeit von Normen und Standards hat sich in den letzten Jahren deutlich gewandelt. Mittlerweile ist es üblich geworden, dass viele Standards kostenlos im Internet publiziert werden, und selbst langjährig etablierte Normungsinstanzen wie ETSI [2] bieten alle GSM- und UMTS-Normen der Öffentlichkeit frei zum Herunterladen via World Wide Web an. Die weltweit gültigen ISO/IEC-Normen sind leider nicht frei erhältlich und müssen bei Bedarf zu relativ hohen Preisen gekauft werden.

4.4.1 Normen zum Kartenkörper

Die generellen physischen Eigenschaften einer Karte werden in der ISO/IEC 7810 beschrieben. Darauf aufbauend, existiert eine Reihe von Normen, wie TS 102 221 und EMV Book 1, die in den einleitenden Abschnitten Konkretisierungen und Ausführungsformen der ISO/IEC enthalten.

4.4.2 Normen zum Betriebssystem

Die wichtigste Normenreihe zu Chipkarten-Betriebssystemen ist die ISO/IEC 7816, welche die wesentlichen informationstechnischen Gesichtspunkte einer Chipkarte beschreibt. Im Teil 3 sind dabei die fundamentalen Parameter der Datenübertragung (ATR, PPS, T=0, T=1) spezifiziert. Das USB-Protokoll für Chipkarten hingegen befindet sich im Teil 12, und die Festlegung der kontaktlosen Datenübertragung für Proximity-Karten ist in der aus vier Teilen bestehenden Norm ISO/IEC 14 443 beschrieben.

Der Teil 4 der ISO/IEC 7816 enthält eine Beschreibung des Dateisystems inklusive Dateiarten (MF, DF, EF)[3], Dateistrukturen (transparent, linear, linear variabel, zyklisch, TLV-kodiert)[4] und Selektionsmöglichkeiten[5]. In dieser Norm sind auch die wesentlichen Mechanismen von der gesicherten Datenübertragung [6] (*secure messaging*) festgelegt. Hinsichtlich der grundlegenden Chipkarten-Kommandos [7] ist ebenfalls Teil 4 der ISO/IEC 7816 die wichtigste Referenz. Die administrativen Kommandos sind in ISO/IEC 7816-9 und die Kommandos für kryptografische Operationen in ISO/IEC 7816-8 beschrieben.

Bezüglich des ausführbaren Programmkodes hat sich Java auf Chipkarten durchgesetzt, und die betreffenden Spezifikationen[8] der Firma Sun sind die wichtigsten Grundlagen

[1] Siehe auch Abschnitt 4.5 „Dokumente für Chipkarten-Systeme“ auf Seite 50.
[2] Siehe auch [ETSI].
[3] Siehe auch Abschnitt 2.1.1 „Dateitypen“ auf Seite 12.
[4] Siehe auch Abschnitt 2.1.3 „Dateistrukturen“ auf Seite 13.
[5] Siehe auch Abschnitt 2.1.5 „Dateiselektion“ auf Seite 15.
[6] Siehe auch Abschnitt 2.3.4 „Sicherung der Datenübertragung“ auf Seite 27.
[7] Siehe auch Abschnitt 2.2 „Kommandos“ auf Seite 19.
[8] Siehe auch [JCVMS 03], [JCRES 03], [JCAPI 03] und [JCAPN 03].

dafür. Zum Laden und Verwalten dieser programmkodebasierten Anwendungen gibt es ebenfalls einen weithin akzeptierten Standard. Es ist dies die Open Platform-Spezifikation des Global Platform Gremiums[1].

4.4.3 Normen zu Daten und zur Datenstrukturierung

Die bei Chipkarten-Systemen häufig verwendete Strukturierung von Daten nach ASN.1 ist in den beiden umfangreichen Normen ISO/IEC 8824 und ISO/IEC 8825 festgelegt. Hinsichtlich Zertifikaten von Public-Key-Infrastrukturen ist die ITU-Norm X.509 die wichtigste Referenz. Anwendungsübergreifende Datenelemente und deren TLV-konforme Bezeichnungen sind in der ISO/IEC 7816-6 beschrieben.

4.4.4 Normen zur Rechneranbindung

Die softwaretechnische Anbindung von Chipkarten-Terminals an Rechner ist in der PC/SC-Spezifikation geregelt. Sie legt eine Schnittstelle zwischen Chipkarte und PC-Programmen fest. Beim Einsatz von Java als Programmiersprache können darauf aufbauend oder parallel dazu die Mechanismen aus der OCF-Spezifikation herangezogen werden.

4.4.5 Normen zu Anwendungen

Da es mit den auf dem Markt befindlichen mächtigen Chipkarten-Betriebssystemen relativ einfach ist, eigene Anwendungen mit und ohne Programmkode zu entwickeln, sollte je nach Anwendungstyp auf die folgenden Normen Rücksicht genommen werden. Dies ist auch insbesondere deshalb angeraten, da manche Fehler eines unerfahrenen Anwendungsentwicklers durch die Einhaltung der Normen und Standards erst gar nicht auftreten können.

Signaturanwendungen Es gibt mittlerweile eine große Bandbreite von unterschiedlichsten Signaturkarten. Diese müssen jedoch in die verschiedensten übergeordneten Systeme eingebunden werden, um die Signaturfunktionen brauchbar nutzen zu können. Auf seiten der Chipkarte ist die ISO/IEC 7816-15 die wichtigste Grundlage, die Norm stammt vom PKCS #15 Standard der Firma RSA ab. Die aus zwei Teilen bestehende europäische CEN-Normenreihe 14 890 regelt die wesentlichen Gesichtspunkte der Gestaltung einer Signaturkarte.

Zahlungsverkehrsanwendungen Anwendungen im Zahlungsverkehr basieren oftmals auf nationalen Spezifikationen und sind meist für die typischen Zahlungsweisen und die Zahlungsverkehrsinfrastruktur eines bestimmten Landes maßgeschneidert. Eines der bekanntesten Beispiele dafür ist die deutsche Geldkarte, die hinsichtlich der im Feld befindlichen Chipkarten weltweit die größte Zahlungsverkehrsanwendung ist. Allerdings ist die Spezifikation nicht öffentlich, und die Karten werden vor allem in Deutschland eingesetzt. Die wichtigsten weltweit benutzten Spezifikationen für Debit- und Kreditkarten sind die

[1] Siehe auch Abschnitt 2.4.4 „Anwendungsverwaltung“ auf Seite 29.

vier Bände der EMV-Spezifikation[1]. Elektronische Geldbörsen als einzelne Anwendung auf einer Chipkarte oder auch als eine Anwendung auf einer Multiapplikationskarte sind in der EN 1546 in nahezu der gesamten vorstellbaren Variationsbreite beschrieben. Diese Norm ist auch der Ausgangspunkt beinahe aller in Betrieb befindlichen elektronischen Geldbörsen.

Telekommunikationsanwendungen Das GSM-Mobilfunksystem ist die weltweit größte Anwendung für Chipkarten. Bei GSM ist vor allem die Norm TS 51.011 ausschlaggebend – sie spezifiziert die SIM (*subscriber identity module*), das Übertragungsprotokoll, das Dateisystem und die Kommandos. Das Rahmenwerk „SIM Application Toolkit“ für kartenseitige Zusatzanwendungen ist in der Norm TS 51.014 festgelegt.

Für die Chipkarte des UMTS-Systems wurden die Normen zur SIM erheblich umstrukturiert und erweitert. Es wurde eine Plattform, die UICC (*universal integrated chip card*) definiert, auf der dann alle weiteren Anwendungen aufbauen. Die wichtigste Anwendung ist dabei zweifelsfrei die Telekommunikationsanwendung für die USIM (*universal subscriber identity module*). Dabei sind neben einigen anderen die folgenden Normen wichtig: TS 102 221 für die UICC-Plattform, TS 31.102 für die USIM-Anwendung und TS 102 222 für die administrativen Kommandos. Diese sind der unerlässliche Kern für alle Chipkarten in der Telekommunikation.

An den GSM- und UMTS-Normen orientieren sich auch alle anderen Mobilfunksysteme wie das CDMA- oder TETRA-System. Allerdings sind Chipkarten dort meist nur optional vorgesehen.

Identifikationsanwendungen Die weltweit gültige Grundlage für maschinenlesbare Reisedokumente, d. h. typische ID-Karten, wird von der ICAO in dem Dokument Doc 9303-3 gesetzt. Alle weiteren Details bei staatlichen ID-Anwendungen werden in der Regel durch landesspezifische Normen oder auch Gesetze abgedeckt.

4.5 Dokumente für Chipkarten-Systeme

Zur Beschreibung von Chipkarten-Systemen sind eine Reihe von Dokumenten notwendig. Der Umfang hängt dabei stark vom jeweiligen Projekt ab. Für eine große nationale Zahlungsverkehrsanwendung wie beispielsweise die Geldkarte in Deutschland, bei der auch noch ein eigenes Betriebssystem (SECCOS) definiert ist, haben die Spezifikationen im direkten Umfeld der Chipkarte einen Umfang von mehr als 1 450 Seiten. [2]

Zur Orientierung seien im Folgenden noch einige Angaben über die Spezifikationsgröße von verbreiteten Chipkarten aufgeführt. Die Kernspezifikation für die SIM – die Chipkarte im GSM-Mobilfunksystem – hat einen Umfang von 180 Seiten (3GPP TS 51.011 V4.1.0). Bei der deutschen Gesundheitskarte hat die auf Anforderungsniveau gehaltene Spezifikati-

[1] Siehe auch [EMV Book 1], [EMV Book 2], [EMV Book 3] und [EMV Book 4].

[2] Dabei wurden folgende Schnittstellenspezifikationen für die ZKA-Chipkarte betrachtet: Applikation elektronische Geldbörse (Geldkarte): 92 Seiten, Applikation electronic cash: 43 Seiten, EMV-Kommandos: 198 Seiten, Zusatzanwendung Applikation Marktplatz: 39 Seiten, Zusatzanwendung Applikation Elektronischer Fahrschein: 38 Seiten, Signatur-Anwendung: 304 Seiten, Secure Chip Card Operating System (SECCOS): 659 Seiten und Konzept zur Personalisierung von ZKA-Chipkarten mit dem Betriebssystem SECCOS: 77 Seiten).

on für die Betriebssystemplattform ca. 30 Seiten und die eigentliche Anwendungsspezifikation ca. 80 Seiten. Die Spezifikation von ICAO für maschinenlesbare Reisedokumente [1] hat einen Umfang von ca. 141 Seiten. Bei Kreditkarten mit Chip nach EMV-Spezifikation umfasst das applikationsunabhängige Grundlagendokument [2] 110 Seiten und die eigentliche Beschreibung der Anwendung [3] 164 Seiten.

Bei weniger komplexen Anwendungen und bei Verwendung eines der üblichen Chipkarten-Betriebssysteme reduziert sich der Spezifikationsumfang natürlich erheblich. Soll etwa die Gleitzeiterfassung oder die Zugangskontrolle einer mittelgroßen Firma mit Chipkarten durchgeführt werden, so kann die Chipkarten-Anwendung durchaus in einer Spezifikation mit 20 bis 30 Seiten Umfang vollständig beschrieben werden. Dies ist deshalb möglich, weil auf separate Grundlagendokumente verwiesen werden kann, wie beispielsweise auf die Beschreibung der Übertragungsprotokolle oder die Spezifikation des benutzten Chipkarten-Betriebssystems.

Die Dokumente bei einem Chipkarten-System folgen üblicherweise einer klaren Hierarchie. Das Lastenheft (*user requirements specification*) enthält auf der höchsten Abstraktionsebene Ausgangssituation und Anforderungen an das System. Diese Anforderungen sind unabhängig von der Implementierung und geben eine Aussage, „was“ gemacht werden soll. Üblicherweise wird das Lastenheft vom Auftraggeber erstellt und ist auch die Grundlage für Aufwandsabschätzung und Angebot.

In der nächst niedrigen Abstraktionsebene befindet sich das Pflichtenheft (*answer to user requirements specification*). Es beschreibt aus Sicht des Auftragnehmers, „wie“ die Anforderungen des Lastenhefts gelöst werden. Dabei ist der Abstraktionsgrad noch so hoch, dass es von einem technisch nicht ganz so versierten Auftragnehmer verstanden werden kann.

Spezifikationen liegen in der Abstraktionsebene direkt über dem Quellkode und haben den Zweck, technische Teile des Chipkarten-Systems eindeutig und nicht auslegungsfähig zu beschreiben.[4]

Alle Konjunktive wie „könnte, sollte, müsste“ oder Satzkonstruktionen wie „wäre empfehlenswert, ist in Betracht zu ziehen“ und Ähnliches dürfen in Spezifikationen nicht benutzt werden. Dies würde dazu führen, dass die Entwickler keine eindeutigen Vorgaben haben und dann je nach Lage der Dinge bewusst oder unbewusst eine der möglichen Varianten wählen. Das Entwicklungsteam einer weiteren Komponente entscheidet sich im ungünstigsten Fall für den anderen möglichen Weg, und in der Integrationsphase stellen dann die Beteiligten fest, dass beispielsweise Chipkarte und Terminal bei bestimmten Funktionen nicht miteinander arbeiten.

An dieser Stelle sei eine Anmerkung hinsichtlich des schriftstellerischen Ehrgeizes bei vielen Spezifikationserstellern gemacht. Eine Spezifikation soll nicht zeigen, dass der Autor großes Wissen über ein bestimmtes Thema hat, sondern dass er es versteht, in klaren, einfachen Worten und unmissverständlich einen technischen Sachverhalt zu beschreiben.

[1] Siehe auch [ICAO 9303].
[2] Siehe auch [EMV Book 1].
[3] Siehe auch [EMV Book 3].
[4] Die einzelnen Vorgehensschritte von der Anforderung bis zur vollständigen Spezifikation können hier aus Platzgründen leider nicht detailliert beschrieben werden. Eine sehr umfangreiche und genaue Erläuterung findet sich im V-Modell [V-Modell XT].

Es gibt Spezifikationen, in denen seitenlang der Kryptoalgorithmus DES im Detail erklärt wird. Dies ist schlichtweg unnötiger Aufwand und eventuell sogar missverständlich (da unter Umständen der Implementierer annimmt, es sei eine DES-Variante) und lenkt von den essenziellen Inhalten ab. In so einem Fall reicht es z. B. völlig aus, einen „SPA/DPA resistenten und rauschfreien DES mit einer Ausführungszeit von kleiner als 2 ms pro 8 Byte Block“ zu fordern, anstelle seitenlange Abhandlungen zu erstellen.

In der Praxis kommt es manchmal bei kleineren Projekten, oder wenn auf Auftraggeberseite eine hohe Sachkenntnis vorliegt, dazu, dass Pflichtenheft und Spezifikation zu einem Dokument zusammengefasst werden.

Im Folgenden ist anhand eines einfachen Beispiels die Hierarchie von der eigentlichen Anforderung bis zur Spezifikation dargestellt: Eine typische Anforderung wäre, dass das Hintergrundsystem die Echtheit einer Chipkarte feststellen kann. Davon ausgehend, ist nun im Pflichtenheft beschrieben, dass zur Feststellung der Echtheit der Chipkarte eine auf dem AES basierende Challenge-Response-Authentisierung eingesetzt wird. Auf der Grundlage des Pflichtenhefts wird dann die eigentliche Spezifikation erstellt. Dort ist dann konkret festgelegt, dass die Authentisierung der Chipkarte durch das Hintergrundsystem, das in der ISO/IEC 7816-4 spezifizierte Kommando INTERNAL AUTHENTICATE mit dem Kryptoalgorithmus AES und 256 Bit langen kartenindividuellen Schlüsseln, benutzt wird.

4.5.1 Aufteilung der Spezifikationen

Die Dokumente für ein Chipkarten-System lassen sich in beinahe allen Fällen folgendermaßen einteilen: Spezifikationen für das gesamte System, Hintergrundsystem, Chipkarten und Terminals. Je nach konkreter Systemgestaltung können der Umfang der einzelnen Dokumente und auch der Schwerpunkt der Spezifikationen erheblich differieren.

4.5.1.1 Systemspezifikationen

Alle übergeordneten Aspekte eines Chipkarten-Systems beschreiben die Systemspezifikation. Sie betreffen den Betrieb und die Zusammenarbeit der einzelnen Komponenten.

Systemüberblick (*system overview*) Dies ist der generelle Überblick über das gesamte System, die Chipkarten sind dabei nur ein kleiner Teil. Im Systemüberblick sind die Zusammenhänge zwischen den Komponenten erläutert und die grundlegenden Eigenschaften der Komponenten beschrieben. Man kann dieses Dokument auch als Zusammenfassung für den „eiligen Leser“ auffassen.

Sicherheitsarchitektur (*security architecture*) Dies ist die Spezifikation zur Beschreibung von Schlüsselhierarchien, Schlüsselerzeugung, Schlüsselableitungen, Schlüsselreferenzierung, Schlüsseltausch, eingesetzten Kryptoalgorithmen (Verschlüsselung, Signierung, Hash, Zufallszahlengenerator) und benutzten kryptografischen Protokollen. Es enthält bisweilen auch Sicherheitsanforderungen und Maßnahmen gegen potenzielle Angriffe. Dieses Dokument ist oftmals vertraulich und nur Personen zugänglich, die es zwingend für ihre Tätigkeit benötigen.

Datenverzeichnis (*data dictionary*) Diese Aufstellung, manchmal auch Datenbeschreibungsverzeichnis genannt, enthält alle im System benutzten Daten mit der dazugehörigen Kodierung.[1]

4.5.1.2 Spezifikationen für das Hintergrundsystem

Die Spezifikationen für das Hintergrundsystem beschreiben alle den Chipkarten-Terminals übergeordneten Funktionen. Dies umfasst Systembetrieb, Systemüberwachung, Kartenmanagement, Abrechnung und auch Schnittstellen zu anderen Systemen. Die dazugehörigen Dokumente können sich bei einfachen Anwendungen auf wenige Seiten beschränken, allerdings bei hochkomplexen Systemen, wie beispielsweise dem GSM-Mobilfunksystem, durchaus auch mehrere tausend Seiten einnehmen.

4.5.1.3 Chipkartenspezifikationen

Die Spezifikationen für die Chipkarten umfassen die Dokumente für den Kartenkörper, das Betriebssystem, die Anwendungen in Bezug auf Benutzer, Sonderanwendungen sowie die Personalisierung. Abschnitt 4.5.2 „Elemente einer typischen Kartenspezifikation“ auf Seite 54 enthält eine detaillierte Aufstellung über die informationstechnischen Belange, die bei kleinen und mittleren Anwendungen die zentralen Dokumente sind.

Kartenkörper (*card body*) Der Kartenkörper ist meist nicht nur der bloße Träger für das Chipmodul, sondern auch Gestaltungselement und Werbemittel. Dies führt dazu, dass die Vorgaben für aufwändige Farbdrucke, Durchsichtselemente, Hologramme und Ähnliches vorhanden sein müssen. Viele Kartenelemente wie Unterschriftsstreifen, Magnetstreifen, Hochprägung und Chipmodul sind hinsichtlich Position und Größe in den einschlägigen Normen wie ISO/IEC 7810, ISO/IEC 7811 und ISO/IEC 7813[2] festgelegt.[3] Es ist wichtig, diese Normen einzuhalten, da es sonst durchaus Probleme geben kann, wenn die Chipkarte in ein Terminal gesteckt wird.

Chipkarten-Betriebssystem (*smart card operating system*) Hier ist das Betriebssystem mit seinen Übertragungsprotokollen, Dateiverwaltung, Kommandos und Zustandsautomaten spezifiziert. Sofern nachladbarer Programmkode unterstützt wird, enthält die Spezifikation auch noch die Beschreibung der unterstützen Software-Schnittstellen und des Mechanismus zum Laden von Programmkode.

Hauptanwendung (*main application*) Diese Spezifikation legt die auf dem Chipkarten-Betriebssystem aufbauende wichtigste Anwendung für den Endanwender mit ihren Daten, Kommandos und Abläufen fest.

Zusatzanwendungen (*additional application*) Anwendungen, die neben der Hauptanwendung auf der Chipkarte untergebracht werden können, sind jeweils in separaten Dokumenten spezifiziert.

---

[1] Siehe auch Abschnitt 5.1 „Daten“ auf Seite 63.
[2] Siehe auch [ISO/IEC 7810], [ISO/IEC 7811-1], [ISO/IEC 7811-2] und [ISO/IEC 7813].
[3] Siehe auch Abschnitt 1.3 „Kartenelemente“ auf Seite 3.

Anwendung als Sicherheitsmodul (*hardware security module – HSM*) Werden Chipkarten in bestimmten Geräten, wie z. B. Terminals als Sicherheitsmodul, eingesetzt, so ist die dazugehörige Applikation in dieser Spezifikation beschrieben.

Personalisierung (*personalisation*) Die Initialisierung und Personalisierung[1] erfordert besondere Kommandos und Abläufe, die im normalen Betrieb deaktiviert sind und nur in einem bestimmten Abschnitt des Lebenszyklus verwendet werden können. Dies ist der Grund, dass oftmals die Dokumente zur informationstechnischen Kartenfertigung vom Rest der Kartenspezifikationen getrennt werden.

Migrationskonzept (*migration concept*) Dieses nur vereinzelt erstellte Dokument enthält die genaue Vorgehensweise beim Übergang von einer ursprünglichen Kartengeneration auf eine neue Kartengeneration mit veränderter technischer Ausstattung.[2] Dabei müssen vom Hintergrundsystem, über die Personalisierung bis hin zu den Terminals die entsprechenden Anpassungen berücksichtigt werden. Der Zweck ist, sicherzustellen, dass in der Übergangszeit beide Kartengenerationen voll funktionsfähig sind.

4.5.1.4 Terminalspezifikationen

Der Umfang der Spezifikation der eingesetzten Terminals hängt stark von der Art des Systems ab. Bei Zahlungsverkehrssystemen gibt es beispielsweise unterschiedliche Spezifikationen zu Händler-, Automaten-, Lade-, Sonderfunktions-, Verwaltungs- und Taschenterminals. Bei einfacheren Systemen existiert oft nur die eine Art von Terminal, mit dem der Kartenbenutzer seine Transaktionen durchführt. Manchmal gibt es noch spezielle Verwaltungsterminals zur Änderung von Daten auf der Chipkarte durch autorisierte Personen.

4.5.2 Elemente einer typischen Kartenspezifikation

Moderne Spezifikation im Chipkarten-Bereich trennen mehr oder minder vollständig Chipkarte, Chipkarten-Betriebssystem und Chipkarten-Anwendung. Dies hat gerade für große komplexe Systeme den Vorteil, dass man die grundlegenden Teile nur einmal beschreiben muss und die unterschiedlichen Anwendungsspezifikationen dann nur noch darauf referieren. In den folgenden Beispielen für Spezifikationen ist dies berücksichtigt. Es ist jedoch bei kleineren Anwendungen durchaus üblich, anstelle von drei separierten Dokumenten ein zusammengefasstes Dokument mit drei Hauptabschnitten zu erstellen.

4.5.2.1 Allgemeine Abschnitte

Die allgemeinen Abschitte sollten Bestandteil jeder Spezifikation sein und dienen dem Leser zur Orientierung und als Einführung in die jeweilige Spezifikation.

Einleitung (*introduction*) Eine Einleitung sollte Teil aller Spezifikationen sein und den Zweck (*scope)* der jeweiligen Spezifikation enthalten. Ein Abschnitt über die benutzten Abkürzungen (*abbreviations*) und Notationen (*notations*) sollte ebenfalls Bestandteil der

[1] Siehe auch Abschnitt 7.1 „Initialisierung und Personalisierung“ auf Seite 143.
[2] Siehe auch Abschnitt 7.2 „Migration“ auf Seite 147.

Einleitung sein. Eine Aufstellung der direkt referierten Normen (*normative references*), eine Bibliografie (*bibliography*) und die Definition (*definitions*) der wichtigsten verwendeten Begriffe ergänzen diesen Teil des Dokuments.

Änderungshistorie (*change history*) Sobald Spezifikationen an einem erweiterten Kreis verteilt worden sind, wird es zwingend notwendig, alle neu hinzugekommenen Änderungen zu dokumentieren. Im einfachsten Fall wird am Schluss der Spezifikation ein entsprechender Absatz aufgenommen, der die wichtigsten Änderungen mit Datum enthält. In vielen Fällen ist es jedoch stark angeraten, beim Übergang von einer Version zur nächsten zusätzlich am Seitenrand Änderungsmarkierungen anzubringen. Bei umfangreichen Dokumenten ist dies der einfachste und zuverlässigste Weg, um dem Leser Änderungen nachvollziehbar anzuzeigen.

Anhang (*annex*) Im Anhang einer Spezifikation sind oftmals Beispiele für die im Hauptteil beschriebenen Sachverhalte aufgezeigt. Gerade bei komplizierten Kodierungen von Daten, verschachtelten ASN.1-strukturierten Datenobjekten oder Zertifikaten sind diese Beispiele sehr wertvoll und teilweise für das Verständnis unabdingbar. Um die üblichen Anwendungsfälle (*use case*) leichter zu durchschauen, enthalten manche Spezifikationen auch noch detaillierte Beschreibungen von typischen Kommandosequenzen. Diese sollten im Übrigen immer in die dazugehörigen Tests der Anwendung einfließen. Da im Bereich der Informationstechnik das Patent(un)wesen immer mehr Einzug hält, ist es angebracht, eine Aufstellung der Patente (IPR – *intellectual property rights*) einzufügen, die die Spezifikation tangieren.

Grundsätzlich ist der Anhang immer ein Sammelbecken für wichtige Informationen, die nicht in den Hauptteil der Spezifikation passen, aber trotzdem nicht unerwähnt bleiben sollen.

4.5.2.2 Chipkarte

Im Abschnitt der Spezifikation über die Chipkarte sind alle mechanischen und elektrischen Rahmenparameter festgelegt. Die informationstechnischen Aspekte werden erst in den späteren Abschnitten behandelt. Verwendet man also für seine Anwendung eine bereits vorhandene Chipkarte, so ist dieser Abschnitt nicht notwendig.

Mechanische Eigenschaften (*physical characteristics*) Im Abschnitt über die mechanischen Eigenschaften sind die physischen Aspekte von Kartenkörper und Chip beschrieben. Der wichtigste Punkt dabei ist die Größe der Karte, im Normalfall ist dies das ID-1-Format.[1] Der ebenfalls aufzuführende Temperaturbereich (*temperature range*) ist ein weiterer wichtiger Parameter, da von ihm abhängt, welche Kunststoffe für den Kartenkörper verwendet werden können.

Die Spezifikation der Kontakte (*contacts*) als elektrische Schnittstelle zum Mikrocontroller ist ebenfalls Bestandteil der mechanischen Eigenschaften. Dazu gehören Größe (*dimension*) und Ort (*location*) der Kontakte sowie der maximal zulässige Kontaktierungsdruck (*contact pressure*). Ergänzt wird dies durch die Festlegung der benutzten Kontakte (*active contacts*).

[1] Siehe auch Abschnitt 1.2 „Kartenformate“ auf Seite 2.

Elektrische Eigenschaften (*electrical characteristics*) In diesem Abschnitt werden als wesentlicher Teil die elektrischen Eigenschaften der üblichen Kontakte Versorgungsspannung (Vcc), Masse (GND), Datenübertragung (I/O), Takt (CLK) und Reset (RST) beschrieben.

Teil des Dokuments ist auch die Festlegung des maximal vom Mikrocontroller zu verbrauchten Stroms in Abhängigkeit der Versorgungsspannung, was insbesondere für den Einsatz an mobilen Terminals eine kritische Kenngröße ist. Bei der Taktversorgung ist die minimal und maximal zulässige Taktfrequenz ein wesentliches Kriterium sowie die Festlegung, ob ein Anhalten des Taktes (*clock stop*) erlaubt ist. Ein weiterer Punkt ist die Aktivierungs- (*activation sequence*) und Deaktivierungssequenz (*deactivation sequence*) des Mikrocontrollers.

Da die elektrischen Eigenschaften der üblichen Chipkarten-Mikrocontroller normalerweise auf die ISO/IEC 7816-3 oder ETSI TS 102 221 ausgerichtet sind, referiert man bei Anwendungen mit kleineren und mittleren Stückzahlen in aller Regel auf diese Normen.

4.5.2.3 Chipkarten-Betriebssystem (*smart card operating system*)

Die Spezifikation eines Chipkarten-Betriebssystems ist in der Regel ein Dokument, das das Verhalten auf der Schnittstelle zwischen Chipkarte und Terminal beschreibt. Die eigentliche Implementierung des Betriebssystems ist dabei nicht festgelegt. Der Grund dafür ist schlichtweg, dass eine Schnittstellenbeschreibung deutlich weniger komplex ist als die vollständige Spezifikation eines ganzen Betriebssystems.

Datenübertragung (*data transmission*) Die Festlegung der Datenübertragung ist im Allgemeinen sehr umfangreich. Sie kann jedoch stark reduziert werden, wenn auf eine entsprechende Spezifikation referiert wird. Kritisch sind hier allerdings Referenzen auf allzu generische Normen, wie die ISO/IEC 7816-3, da diese eine so große Vielzahl von Optionen bietet, die von keinem Chipkarten-Betriebssystem vollständig unterstützt wird.

Das Dokument beginnt stets mit der Beschreibung des ATR[1] (*answer to reset*) mit seinen Datenelementen sowie dem PPS[2] (*protocol parameter selection*) zur optionalen Umschaltung der Übertragungsprotokolle.

Bei einer neuen Anwendung reicht es aus, wenn eines der beiden Übertragungsprotokolle (*transmission protocols*) T=0[3] oder T=1[4] ausgewählt wird. Dem moderneren blockorientierten T=1 Protokoll sollte dabei der Vorzug gegenüber dem älteren zeichenorientierten T=0 Protokoll gegeben werden. Die Unterstützung beider Protokolle ist in der Praxis nur aus Kompatibilitätsgründen notwendig. Hinsichtlich der Übertragungsprotokolle sollten noch die Referenz auf die entsprechende Norm aufgeführt sein und gegebenenfalls die Einschränkungen, wenn nicht alle Funktionen des Protokolls unterstützt werden.

Es gibt neuere Chipkarten, die auch das USB-Protokoll in den Geschwindigkeitsklassen low speed (1,5 MBit/s) und full speed (12 MBit/s) unterstützen. Teilweise kann das USB-Protokoll parallel zu T=0 oder T=1 benutzt werden. In den Spezifikationen für das Be-

[1] Siehe auch Abschnitt 2.3.1 „Answer to Reset (ATR)“ auf Seite 24.
[2] Siehe auch Abschnitt 2.3.2 „Protocol Parameter Selection (PPS)“ auf Seite 24.
[3] Siehe auch Abschnitt 2.3.3.1 „Kontaktbehaftetes Übertragungsprotokoll T=0“ auf Seite 26.
[4] Siehe auch Abschnitt 2.3.3.2 „Kontaktbehaftetes Übertragungsprotokoll T=1“ auf Seite 26.

triebssystem ist dies jeweils im Detail zu beschreiben. Da USB für Chipkarten bisher verhältnismäßig selten ist, sollten die betreffenden Dokumente entsprechend ausführlich sein und alle Eigenschaften des USB Protokolls festlegen.

Kommandos (*commands*) Die Definition der Kommandos beschränkt sich normalerweise auf die Eingabe- und Ausgabedaten sowie eine textuelle Darstellung der eigentlichen Funktion. Für beinahe alle Spezifikationen ist dieser Detaillierungsgrad ausreichend. Allerdings ist damit im Falle von multiplen Fehlern bei den Eingangsdaten die Reihenfolge der Returnkodes nicht festgelegt. Dies spielt in der Praxis selten eine Rolle, da bei einem unerwarteten Returnkode die Terminals üblicherweise die Transaktion abbrechen. Ist es notwendig, die exakte Reihenfolge der Abfragen und Returnkodes festzulegen, dann muss die Funktion des Kommandos in Pseudokode beschrieben werden.

Tabelle 4.1 Die Tabelle zeigt eine etablierte Beschreibungsform eines Chipkarten-Kommandos anhand des Kommandos READ BINARY.

Datenelement	**Länge**	**Inhalt**	**Beschreibung**
CLA	1 Byte	'00'	Class-Byte nach ISO/IEC 7816-4 ohne Benutzung von Secure Messaging
INS	1 Byte	'B0'	Instruction-Byte nach ISO/IEC 7816-4 für READ BINARY
P1	1 Byte	...	Parameter 1 P1.b8 = 0: Lese Daten aus der aktuell selektierten Datei mit Offset; Offset = (P1.b7 ... P1.b1 ‖ P2) P1.b8 = 1: Lese Daten nach impliziter Dateiselektion durch Short-FID mit Offset; P1 = (100 ‖ Short-FID); Short-FID = (P1.b5 ... P1.b1); Offset = P2
P2	1 Byte	...	siehe Beschreibung von P1
L_e	1 Byte	...	erwartete Länge $L_e = 0$: Lese alle Daten bis zum Ende der Datei $L_e > 0$: L_e ist die Anzahl der zu lesenden Daten

Tabelle 4.2 Die Tabelle zeigt eine etablierte Beschreibungsform für die Antwort auf ein Chipkarten-Kommando anhand des Kommandos READ BINARY.

Datenelement	**Länge**	**Inhalt**	**Beschreibung**
DATA	n Byte	...	aus der Datei gelesene Daten mit der Länge n $L_e = 0$: n = Länge der Datei $L_e > 0$: n = L_e
SW1	1 Byte	'90'	Statuswort 1 und 2 im Gutfall
SW2	1 Byte	'00'	siehe Beschreibung von SW1

Die Tabelle 4.1 auf der vorherigen Seite zeigt die übliche Darstellung eines Kommandos an eine Chipkarte, während die Tabelle 4.2 auf der vorherigen Seite und Tabelle 4.3 die dazugehörige Antwort mit den möglichen Returnkodes präsentieren.

Tabelle 4.3 Die Tabelle zeigt eine etablierte Beschreibungsform für die Returnkodes eines Chipkarten-Kommandos anhand des Kommandos READ BINARY.

SW1	**SW2**	**Bedeutung (**alle Returnkodes nach ISO/IEC 7816-4)
'62'	'81'	Die zurückgegebenen Daten können fehlerhaft sein.
'62'	'82'	Es konnten weniger als L_e Bytes zurückgegeben werden, weil das Dateiende vorher erreicht wurde.
'65'	'81'	Es ist ein Speicherfehler aufgetreten.
'67'	'00'	Die Längenangabe L_e ist falsch.
'69'	'81'	Das Kommando ist inkompatibel zur Dateistruktur.
'69'	'82'	Der erforderliche Sicherheitszustand für den lesenden Zugriff ist nicht erfüllt.
'69'	'86'	Das Kommando ist nicht erlaubt, weil keine Datei selektiert ist.

4.5.2.4 Anwendung (*application*)

Eine Anwendung auf einer Chipkarte besteht im Wesentlichen aus mehreren Dateien oder Datenobjekten sowie Kommandos, die diese Daten benutzen. Es ist notwendig, alle diese Elemente exakt zu spezifizieren, sodass die Anwendung auf einer Chipkarte implementiert werden kann.

Datenelemente (*data elements*) Die gebräuchlichste Form der Verwaltung von Datenelementen ist ein Datenverzeichnis (*data dictionary*), idealerweise in Form einer Datenbank. Bei kleineren Anwendungen kann darauf verzichtet werden, doch ist es auch dort als globale Referenz für Daten in der Regel ziemlich nützlich. Aufbauend darauf, können dann die Dateien und Datenobjekte festgelegt werden. In Abschnitt 5.1 „Daten“ auf Seite 63 ist die Struktur eines Datenverzeichnisses inklusive einiger Beispiele detailliert erläutert.

Dateien und Datenobjekte (*files and data objects*) Die Dateien und Datenobjekte setzen sich aus Datenelementen zusammen. In der Spezifikation der Anwendung wird die Zuordnung der Datenelemente zu den Dateien bzw. Datenobjekten festgelegt.

Sofern es sich um Dateien handelt, ist die Position im Dateibaum der Chipkarte zu vereinbaren, und für alle Datendateien (EFs – *elementary files*) müssen die dazugehörigen Dateinamen FIDs (*file identifier*), SFI (*short file identifier*) und die entsprechenden Dateistrukturen mit ihren Größenparametern festgelegt sein. Die Verzeichnisdateien (DFs – *dedicated files*) benötigen zur Identifizierung einen DF Namen, der einen AID (*application identifier*) enthalten kann. Wichtig ist auch, dass die Zugriffsbedingungen auf die Datendateien festgelegt sind. Die Tabelle 5.5 auf Seite 72 zeigt als Beispiel eine Protokolldatei mit allen dazugehörigen Eigenschaften.

Datenobjekte in einer Chipkarte lassen sich anhand von festzulegenden Tags (Kennzeichen) identifizieren. Unter Umständen sind die Tags auch in ein Template eingebunden, das vom Chipkarten-Betriebssystem verwaltet wird. Zur sicheren Referenzierung müssen

die Datenobjekte üblicherweise noch einem DF zugeordnet werden, und es ist auch erforderlich, jeweils die notwendigen Zugriffsrechte festzulegen.

Kommandos (*commands*) Die für eine Anwendung benötigten Kommandos können entweder aus den vorgegebenen Kommandos des Chipkarten-Betriebssystems ausgewählt werden oder auch als nachladbarer ausführbarer Programmkode in der Chipkarte realisiert sein. Sofern die Kommandos des Betriebssystems benutzt werden, reicht in der Spezifikation ein Verweis auf die entsprechenden Dokumente. Spezialkommandos, verwirklicht durch applikationsspezifischen Programmkode, müssen detailliert und eindeutig beschrieben sein, sodass sie korrekt implementiert werden können. Es ist sinnvoll, sich bei der Beschreibung an den Spezifikationen für Chipkarten-Betriebssysteme zu orientieren, wie in Abschnitt 4.5.2.3 „Kommandos (*commands*)“ auf Seite 57 aufgezeigt.

Sofern Mechanismen für Secure Messaging[1] und logische Kanäle[2] (*logical channels*) verwendet werden, ist es notwendig, diese auch zu spezifizieren.

Anwendungsprotokoll (*application protocol*) Im Anwendungsprotokoll sind anhand der typischen Szenarien die dafür vorgesehenen Kommando-Sequenzen beschrieben. Ein Beispiel dafür ist die Aufeinanderfolge aller notwendigen Kommandos für eine vollständige Authentisierung zwischen Chipkarte und Terminal. Die verbreitetsten Szenarien sind dabei Anwendungsselektion, Identifikation von Personen, Authentisierung von Geräten, Lesen und Schreiben von bestimmten Daten, Sperren und Entsperren von Dateien, Erzeugen und Löschen von Dateien und Anwendungen, Nachladen von Programmen und Signieren und Verifizieren von Daten.

4.5.3 Verteilung der Dokumente

Es ist ein unumstrittenes Prinzip von Sicherheitssystemen, dass die Sicherheit nur von der Geheimhaltung der benutzten Schlüssel abhängen darf. Dies wird auch Kerckhoffs-Prinzip genannt. Die Konsequenz daraus ist, dass bei einem entsprechenden System bis auf die geheimen Schlüssel alles veröffentlicht werden darf, ohne das System damit zu kompromittieren. Viele große Chipkarten-Systeme entsprechen diesem Prinzip in weiten Teilen, etwa das GSM-/UMTS-Mobilfunknetz, Debit-/Kreditkarten nach EMV-Standard und auch die nationale deutsche Zahlungsverkehrskarte Geldkarte.

Trotzdem sollte bedacht werden, dass man durch die Veröffentlichung aller Dokumente eines Systems potentziellen Angreifern viele Informationen zur Verfügung stellt, die sich diese sonst mit erheblichen Aufwand erarbeiten müssten. In der Praxis wird deshalb oft eine Mischform zwischen Veröffentlichung und Geheimhaltung gewählt. Ein Großteil der Spezifikationen ist öffentlich und kann damit auch von Experten ohne Rücksicht auf Vertraulichkeit kommentiert werden, ein kleinerer, aber sicherheitstechnisch wichtiger Teil ist vertraulich. So werden beispielsweise von vielen GSM-Netzbetreibern die verwendeten Kryptoalgorithmen geheim gehalten. Diese Kryptoalgorithmen wurden allerdings vor dem Einsatz von unterschiedlichen Fachleuten auf ihre Stärke hin im Detail analysiert.

[1] Siehe auch Abschnitt 2.3.4 „Sicherung der Datenübertragung“ auf Seite 27.
[2] Siehe auch Abschnitt 2.3.5 „Logische Kanäle“ auf Seite 27.

Eine entsprechende persönliche Vertraulichkeitsvereinbarung sichert ab, dass keinerlei Informationen über das Ergebnis der Untersuchung an die Öffentlichkeit gelangen.

Wichtig ist, dass diese Vorgehensweise nur dazu benutzt wird, bei einem Angreifer zusätzlichen Aufwand zu erzeugen, und nicht etwa, um Sicherheitsschwächen des Systems zu kaschieren. Es gibt eine große Menge an Beispielen, die eindringlich zeigen, dass eine geheime Spezifikation keinesfalls vor der Entdeckung von Sicherheitsschwächen bei breit eingesetzten Systemen schützt.

So wurden jahrelang im Zahlungsverkehrssystem der französischen Yescard Schlüsseln von zu kurzer Länge verwendet, was es einem ambitionierten Angreifer im Jahr 2000 leicht machte, das ganze System auszuhebeln.[1] Ganz ähnlich hat es sich mit der RFID-gestützten Wegfahrsperre für KFZs von Texas Instruments verhalten, die von vielen Autoherstellern benutzt wird. Aufgrund einer zu kurzen Schlüssellänge konnte das System 2005 gebrochen werden.[2] Die Spezifikationen beider Systeme waren vertraulich, was den Angreifern einen erheblichen Mehraufwand bescherte, aber die Sicherheit des Systems letzten Endes nicht gewährleisten konnte.

4.5.4 Versionsnummerierung von Dokumenten

Die Nummerierung von Versionen eines Dokuments erscheint auf den ersten Blick ziemlich einfach: Man verwende eine ganze Zahl und erhöhe diese von Version zu Version um eins. Geschickterweise ergänzt man diese Versionsnummer noch um eine Datumsangabe, um eine einfache zeitliche Zuordnung zu ermöglichen. Der Startwert ist typischerweise eins, wobei manchmal eine Null zur Symbolisierung von frühen unstabilen Versionen benutzt wird. Dieses Schema eignet sich gut für Dokumente, die keinen allzu häufigen Änderungen unterliegen. Ist dies aber der Fall, so erreicht man ziemlich schnell hohe Versionsnummern, unabhängig davon, ob die Änderung nur eine Rechtschreibkorrektur war oder das halbe Dokument umgeschrieben wurde.

Bei ETSI hat man bei den Telekommunikationsnormen für GSM seit längerer Zeit eine Nummerierung eingeführt, die auf drei durch Punkte getrennten unabhängigen Stellen beruht. Die erste Stelle wird erhöht, wenn große inhaltliche Änderungen in das Dokument eingeflossen sind. Bei kleineren Erweiterungen, Klarstellungen, technischen Korrekturen und Ergänzungen wird die mittlere Stelle hochgezählt. Änderungen am Layout, Rechtschreibkorrekturen und ähnliche Verbesserungen, die den technischen Inhalt nicht beeinflussen, führen zu einer Erhöhung der letzten Stelle. Dies gibt dem Leser schnell eine Übersicht zu den Modifikationen an dem Dokument.

Wird beispielsweise bei einem Dokument die Versionsnummer von 5.3.1 auf 5.3.2 erhöht, so erkennt man sofort, dass es keine inhaltlichen Änderungen gab. Im Gegensatz dazu wurden an einem Dokument, dessen Versionsnummer statt 5.3.1 nun 6.0.0 lautet, größere inhaltliche Änderungen durchgeführt. Dieses Schema ist sehr gut für Dokumente geeignet, die sich laufend weiterentwickeln.

Leider hat man bei der Spezifikationserstellung für UMTS im Rahmen des 3GPP-Projekts diese Nummerierung nicht mehr konsequent durchgehalten, sondern Ende der neunziger

[1] Siehe auch [CLUSIF 02].
[2] Siehe auch [Bono 05]

Jahre einen Bezug auf die Jahreszahl mit eingebracht und anschließend das über mehr als zehn Jahre etablierte Nummernschema der Spezifikationen komplett umsortiert.

Nummerierungsschemata wie bei dem Satzprogramm TEX, dessen Versionsnummer gegen die Zahl π strebt, sollte man vermeiden, da sie zu unübersichtlich werden. Auch die dreistellige Nummerierung des Linux-Kernels, bei dem eine ungerade mittlere Stelle (z. B. 2.3.1) angibt, dass es sich um eine Entwicklerversion handelt und eine gerade mittlere Stelle (z. B. 2.4.1) eine stabile Version kennzeichnet, ist wenig geeignet. Ähnliches gilt in der Regel für alle Vertriebs- und Marketing-getriebenen Versionsnummern, die man meist immer nur kurze Zeit durchhält und recht schnell einem neuen Überraschungseffekt opfert.

Es ist empfehlenswert, bei selten geänderten Dokumente eine einzige Stelle und für häufig überarbeitete Dokumente drei separierte Stellen analog zum ETSI Schema zu benutzen. Eine Datumsangabe sollte ebenfalls vorhanden sein, um den zeitlichen Bezug leicht fassbar zu machen.