

	Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV Teil 1: Anwendungsschnittstelle	Vornorm DIN V 66291-1

ICS 35.240.15

Chipcards with digital signatur application/function according to SigG and SigV –
Part 1: Application interface

Cartes à circuit intégré avec application/fonction signature digitale selon SigG et SigV –
Partie 1: Interface de l'application

Eine Vornorm ist das Ergebnis einer Normungsarbeit, das wegen bestimmter Vorbehalte zum Inhalt oder wegen des gegenüber einer Norm abweichenden Aufstellungsverfahrens vom DIN noch nicht als Norm herausgegeben wird. Zur vorliegenden Vornorm ist kein Entwurf veröffentlicht worden.

Vorwort

DIN V 66291-1 wurde vom Arbeitsausschuß Identifikationskarten im Normenausschuß Informationstechnik (NI) erarbeitet. Sie beschreibt die Schnittstelle zur Chipkarte für Chipkarten mit Digitaler Signatur-Anwendung/Funktion gemäß SigG.

Am 22.07.1997 wurde vom Deutschen Bundestag als Artikel 3 des Informations- und Kommunikationsdienstes-Gesetzes (IuKDG) das Gesetz zur digitalen Signatur (SigG) verabschiedet, am 22.10.1997 wurde dieses Gesetz um die Verordnung zur digitalen Signatur (Signaturverordnung - SigV) ergänzt. DIN V 66291-1 stellt die Umsetzung der gesetzlichen Rahmenbedingungen auf der Spezifikations-Ebene der Signatur-Chipkarte dar. Die Kommandos und Datenelemente, die im Rahmen der Signatur-Anwendung/Funktion verwendet werden, basieren ausschließlich auf den Internationalen Normen der Reihe ISO/IEC 7816 (insbesondere ISO/IEC 7816-4 "Interindustry commands for interchange", ISO/IEC 7816-5 "Numbering system and registration procedure for application identifiers", ISO/IEC 7816-6 "Interindustry data elements", ISO/IEC 7816-8 "Security related interindustry commands" und ISO/IEC 7816-9 "Additional commands and security attributes").

Die Spezifikation berücksichtigt alle Signatur-Algorithmen und Hash-Funktionen, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für digitale Signaturen zugelassen und im Bundesanzeiger veröffentlicht wurden. Als Benutzer-Authentisierungs-Funktion wurde das bisher übliche wissensbasierte Verfahren (PIN-Mechanismus) vorgesehen. Koexistent kann jedoch auch ein biometrisches Benutzer-Authentisierungsverfahren eingesetzt werden, falls der Abgleich zwischen den Referenzdaten und den Verifikationsdaten in der Karte erfolgt und die Mechanismenstärke "hoch" gegeben ist.

Von besonderer Bedeutung sind auch die Sicherheitsmechanismen, die für die Nutzung von Signatur-Chipkarten nach SigG/SigV an Geschäftsterminals vorgesehen sind: hier werden "Card Verifiable Certificates" in Verbindung mit "Public Key"-basierten Authentisierungsverfahren eingesetzt, wobei Bestandteil der Authentisierungsprozedur auch die Vereinbarung von "Secure Messaging"-Schlüsseln ist. Diese werden dazu genutzt, um die Kommandos und Antworten mit einer kryptografischen Prüfsumme absichern und Daten, falls nötig, als Kryptogramm übertragen zu können.

Das "Public Key"-basierte Authentisierungsverfahren mit den "Card Verifiable Certificates" wird auch bei den Personalisierungsmodellen verwendet, die in DIN V 66291-2 (Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV – Teil 2: Personalisierungsabläufe; in Vorbereitung) beschrieben werden wird. Hierbei spielt auch die Schlüsselgenerierungsfunktion auf der Signatur-Chipkarte eine große Rolle, so daß das Signatur-Schlüsselpaar auf der Chipkarte erzeugt werden kann.

Fortsetzung Seite 2 bis 71

Normenausschuß Informationstechnik (NI) im DIN Deutsches Institut für Normung e.V.

INHALT

	Seite
1 Anwendungsbereich.....	3
2 Normative Verweisungen.....	3
3 Definitionen, Abkürzungen und Notationen.....	4
4 Technische Charakteristiken	6
5 Answer-to-Reset	6
6 Protocol Parameter Selection.....	6
7 Übertragungs-Protokolle.....	6
8 Ablaufdiagramm und Einbettung der SigG-Funktion.....	7
9 Zertifizierungsstellen und Zertifikate.....	9
10 Datei-Struktur und Datenobjekte.....	10
11 Chipkarten-Eröffnung.....	13
12 Anwendungs-Eröffnung.....	14
13 Authentisierung des Karteninhabers.....	15
14 Berechnen einer digitalen Signatur.....	17
15 Lesen von Zertifikaten und Zertifikats-Prüfchlüsseln (PK.CAs).....	20
16 Verifizieren einer digitalen Signatur.....	20
17 Signatur-Protokollierung.....	22
18 Interaktion mit Geschäftsterminals.....	23
19 MF-Selektion.....	28
20 Nutzung der Signatur-Funktion simultan zu anderen Anwendungen.....	28
21 GET RESPONSE	29
22 CLA-Byte und Status Bytes.....	29
Anhang A (normativ): DS-Formate	30
Anhang B (normativ): Authentisierungs-Zertifikate	36
Anhang C (normativ): SigG Files	45
Anhang D (normativ): Geräte-Authentisierung, Session-Key-Vereinbarung und Secure.....	
Messaging	48
Anhang E (normativ): Object Identifier	59
Anhang F (normativ): SSD Templates	62
Anhang G (informativ): Nutzung der Security Service Descriptors.....	66
Anhang H (informativ): ATR-Codierung	68
Literaturhinweise.....	71

1 Anwendungsbereich

Diese Vornorm beschreibt die Schnittstelle zur Chipkarte (IFD/ICC-Schnittstelle) für Chipkarten mit Digitaler Signatur-Anwendung/Funktion gemäß SigG. Die Vornorm berücksichtigt

- SigG
- SigV
- die Technik-Anforderungen aus den Maßnahmenkatalogen nach § 16 (6) SigV (insbesondere das Kapitel "Chipkarte als Signaturkomponente", ...) und
- relevante internationale Normen für Chipkarten (insbesondere ISO/IEC 7816).

Alle definierten Codierungen (Kommandos/Datenstrukturen) basieren auf ISO/IEC 7816 (Teile 4, 5, 6 und 8). Bei Anwendungen mit anderen Kommando-Codierungen sind die funktionalen Abläufe und Sicherheitsvorgaben sinngemäß umzusetzen.

2 Normative Verweisungen

Diese Vornorm enthält durch datierte oder undatierte Verweisungen Festlegungen aus anderen Publikationen. Diese normativen Verweisungen sind an den jeweiligen Stellen im Text zitiert, und die Publikationen sind nachstehend aufgeführt. Bei datierten Verweisungen gehören spätere Änderungen oder Überarbeitungen dieser Publikationen nur zu dieser Vornorm, falls sie durch Änderung oder Überarbeitung eingearbeitet sind. Bei undatierten Verweisungen gilt die letzte Ausgabe der in Bezug genommenen Publikation.

Gesetz zur digitalen Signatur (Signaturgesetz – SigG) vom 22.07.1997 (BGBl. I S. 1870, 1872), verkündet als Artikel 3 des "Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste" (Informations- und Kommunikationsdienste-Gesetz – IuKDG)

Verordnung zur digitalen Signatur (Signaturverordnung – SigV), 22.10.1997 (BGBl. I S. 2498)

Schnittstellenspezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV (SigI),
Abschnitt A1: Zertifikate, Version 4.0

DIN EN ISO 3166:1997
Codes für die Namen von Ländern und deren Untereinheiten – Teil 1: Codes für Ländernamen (ISO 3166-1:1997)

DIN EN ISO 11568-2:1996
Bankwesen – Schlüsselverwaltung (Einzelhandel) –
Teil 2: Schlüsselverwaltungstechniken für symmetrische Verschlüsselungen (ISO 11568-2:1994);
Englische Fassung EN ISO 11568-2:1996

DIN V ENV 1375-1:1995
Identifikationskartensysteme – Zusätzliche Formate von branchenübergreifenden Chipkarten – Teil 1: Kartengröße ID-000 und physikalische Eigenschaften;
Deutsche Fassung ENV 1375-1:1994

ISO/IEC DIS 11770:1998-08
Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques

ISO/IEC 7810:1995
Identification cards – Physical characteristics

ISO/IEC CD 7812-1:1999
Identification cards – Identification of issuers – Part 1: Numbering system

ISO/IEC CD 7812-2:1999
Identification cards – Identification of issuers – Part 2: Application and registration procedures

ISO/IEC DIS 7816-2:1996
Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of contacts

ISO/IEC 7816-3:1997
Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols

ISO/IEC 7816-4:1995
Information technology – Identification cards – Integrated circuit(s) cards with contacts –

Part 4: Interindustry commands for interchange
Part 4/AM1: Impact of secure messaging on the
structures of APDU messages

ISO/IEC 7816-5:1994
Information technology – Identification cards –
Integrated circuit(s) cards with contacts –
Part 5: Numbering system and registration
procedure for application identifiers

ISO/IEC 7816-6:1996
Information technology – Identification cards –
Integrated circuit(s) cards with contacts –
Part 6: Interindustry data elements
AM1: IC manufacturer registration

ISO/IEC FDIS 7816-8:1998
Information technology – Identification cards –
Integrated circuit(s) cards with contacts –
Part 8: Security related interindustry commands

ISO/IEC CD 7816-9.2:1998
Information technology – Identification cards –
Integrated circuit(s) cards with contacts –
Part 9: Additional interindustry commands and
security attributes

ISO/IEC 8824:1995
Information technology – Abstract Syntax
Notation One (ASN.1): Specification of basic
notation

ISO/IEC 8825-1:1995
Information technology – ASN.1 encoding rules:
Specification of Basic Encoding Rules (BER),
Canonical Encoding Rules (CER) and
Distinguished Encoding Rules (DER)

ISO DIS 9564-1:1998
Banking – Personal identification number
management and security –
Part 1: PIN protection principles and techniques
(Revision of ISO 9564-1:1991)

ISO 9564-2:1991
Banking – Personal identification number
management and security –
Part 2: Approved algorithm(s) for PIN
encipherment

ISO/IEC 9594-8:1995
Information technology – Open Systems
Interconnection – The directory: Authentication
framework

ISO/IEC 9796-2:1997
Information technology – Security techniques –
Digital signature schemes giving message
recovery –
Part 2: Mechanisms using a hash-function

ISO/IEC 10118:1997
Information technology – Security techniques –
Hash functions –
Part 3: Dedicated hash functions

PKCS #1: RSA Encryption Standard
Version 1.5, Nov. 1993

ITU-T X.509 Information technology – Open
Systems Interconnection – The Directory:
Authentication framework

3 Definitionen, Abkürzungen und Notationen

3.1 Definitionen

Digitale Signatur-Anwendung (SigG-
Anwendung): Anwendung mit SigG-AID und
digitaler Signatur-Funktion sowie ggf. Zusatz-
Funktionen.

Digitale Signatur-Funktion (SigG-Funktion):
Bezeichnung für alle nach SigG, SigV und den
relevanten Maßnahmenkatalogen geforderten
Funktionen wie Entity-Authentisierung, Benutzer-
Authentisierung, digitale Signatur-Erzeugung
und Objekt-Bereitstellung (Zertifikate, PK der ZS
etc.).

Verification data: Daten zur wissensbasierten
und/oder biometrischen Benutzer-
Authentisierung (PIN, Paßwort, Fingerabdruck
etc.).

3.2 Abkürzungen

AID	Application Identifier
AKI	Authority Key Identifier
AT	CRT for Authentication
ATR	Answer-to-Reset
B	Byte
BCD	Binary Coded Digit
BER	Basic Encoding Rules
C	Certificate
CA	Certification Authority

CAR	CA Reference
CC	Cryptographic Checksum
CG	Cryptogram
CH	Cardholder
CHA	Certificate Holder Authorisation
CHN	Cardholder Name
CHR	Certificate Holder Reference
CRT	Control Reference Template
CPI	Certificate Profile Identifier
CS	CertSign
CV	Card Verifiable
D()	Decipherment of
DE	Data Element
DF	Dedicated File
DIR	Directory
DO	Data Object
DS	Digital Signature
DSI	Digital Signature Input
DST	CRT for Digital Signature
E()	Encipherment of
EF	Elementary File
FCI	File Control Information
FID	File Identifier
h()	hash value of
HB	Historical Bytes
ICC	Integrated Circuit(s) Card
ICCSN	ICC Serial Number
IFD	Interface Device
IFSC	Information Field Size Card
IFSD	Information Field Size Device
IIN	Issuer Identification Number
KID	Key Identifier
MF	Master File
MII	Major Industry Identifier
MSE	MANAGE SECURITY ENVIRONMENT
NAD	Node Address
OID	Object Identifier
PCA	Policy Certification Authority
PK	Public Key
PKCS	Public Key Cryptography Standards
PI	Padding Indicator
PIN	Personal Identification Number
PPS	Protocol Parameter Selection
PRND	Padding Random Number
PROV	Provider
PSO	PERFORM SECURITY OPERATION
PV	Plain Value
PW	Password
RC	Retry Counter
RCA	RootCA
RD	Reference Data
RegTP	Regulierungsbehörde Telekom u. Post
RFU	Reserved for Future Use
SE	Security Environment
SIG()	Signature of

SigG	Signatur-Gesetz
SigV	Signatur-Verordnung
SM	Secure Messaging
SSD	Security Service Descriptor
SK	Secret Key
SM	Secure Messaging
SN	Serial Number
SSC	Send Sequence Counter
TLV	Tag, Length, Value
VD	Verification Data
VR	Verification Requirement
ZS	Zertifizierungsstelle

Die Abkürzung ICC wird sowohl für kontaktbasierte als auch für kontaktlose Chipkarten verwendet.

3.3 Notationen

Für die Kennzeichnung von Schlüsseln und Zertifikaten wird folgende Notation (vereinfachte Backus-Naur-Notation) verwendet:

<object descriptor> ::= <key descriptor> |
<certificate descriptor>

<key descriptor> ::=
<key>.<keyholder>.<usage>

<key> ::= <secret key> | <public key>
<secret key> ::= SK
<public key> ::= PK

<keyholder> ::= <cardholder> |
<certification authority> | <integrated
circuit(s) card> | <interface device>
<cardholder> ::= CH
<certification authority> ::= CA | RCA
<integrated circuit(s) card> ::= ICC
<interface device> ::= IFD

<usage> ::= <digital signature> |
<authentication> | <CertSign>
<digital signature> ::= DS
<authentication> ::= AUT
<CertSign> ::= CS

<certificate descriptor> ::=
<certificate>.<certholder>.<usage>
<certificate> ::= C

<certholder> ::= <cardholder> |
<certification authority> | <integrated
circuit(s) card> | <interface device>

Für die Darstellung von Sequenzen von Daten wird folgende Notation verwendet:

|| = Concatenation of data

4 Technische Charakteristiken

Chipkarten mit SigG-Anwendung sind Chipkarten mit der Fähigkeit zur Ausführung von PK-Verfahren (z.B. RSA).
Bei kontaktlosen Chipkarten sind die entsprechenden Normen bez. Energie- und Datenübertragung zu beachten.
Bei kontaktbasierten Chipkarten sollen die Dimensionen und die Lage der Kontakte ISO/IEC 7816-2-konform sein. Das Format soll entweder ID-1 (Normal-Format, siehe ISO/IEC 7810) oder ID-000 (Plug-in-Card-Format, siehe DIN V ENV 1375-1) entsprechen (siehe Bild 1).
Die Daten sollen mit 'Direct Convention' übertragen werden. Programmierspannung Vpp wird vom IFD nicht unterstützt und soll von den Chipkarten nicht angefordert werden.

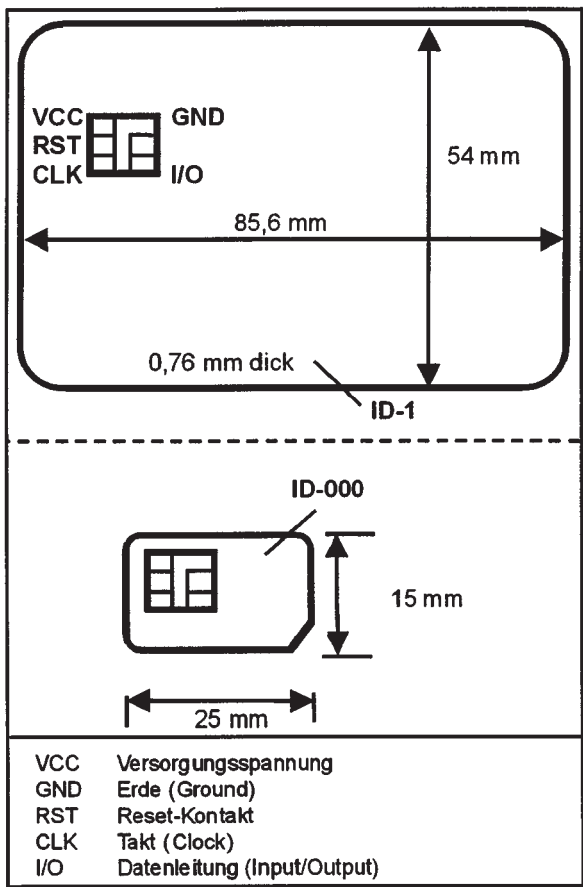


Bild 1: Chipkarten-Formate

5 Answer-to-Reset

5.1 Global Interface Characters

Der Aufbau des ATR für kontaktbasierte Chipkarten ist im informativen Anhang H beschrieben.

5.2 Historical Bytes

Die Historical Bytes (HB) enthalten entsprechend ISO/IEC 7816-4 Datenobjekte wie

- Category Indicator
- Pre-issuing Data Object
- Card Profile Data Object
- Card Life Cycle
- Status Bytes.

Die Codierung ist in Anhang H beschrieben.

6 Protocol Parameter Selection

Protocol Parameter Selection (PPS) entsprechend ISO/IEC 7816-3 ist von denjenigen Chipkarten zu unterstützen, die den 'negotiable mode' anzeigen und mit einer anderen als der voreingestellten Fi/Di-Kombination (Fi = clock rate conversion factor, Di = bit rate conversion factor) zur Erzielung einer höheren Übertragungsrate arbeiten können.

7 Übertragungs-Protokolle

7.1 Allgemeine Aspekte

Eine kontaktbasierte Chipkarte soll das asynchrone half-duplex Character Transmission Protocol T = 0 und/oder das asynchrone half-duplex Block Transmission Protocol T = 1 unterstützen.

7.2 Übertragungs-Protokoll T = 0

Die Implementation soll den Konventionen in ISO/IEC 7816-3 entsprechen.

7.3 Übertragungs-Protokoll T = 1

Die Implementation soll den Konventionen in ISO/IEC 7816-3 entsprechen.

Folgende Vereinfachungen sind für Karten erlaubt:

- NAD Byte: nicht ausgewertet (NAD sollte von IFD und Chipkarte auf '00' gesetzt werden)
- S-Block ABORT: nicht benutzt
- S-Block VPP state error: nicht benutzt

Die Information Field Size Card (IFSC) soll im ATR angezeigt werden (Character TA3, empfohlener Wert: mindestens '80' = 128 Bytes).

Die Information Field Size Device (IFSD) soll vom IFD direkt nach dem ATR angezeigt werden, d.h. das IFD soll unmittelbar nach dem ATR den S-Block IFS Request senden, der von der Chipkarte mit dem S-Block IFS Response zu beantworten ist. Der empfohlene Wert für IFSD ist 254 Bytes.

8 Ablaufdiagramm und Einbettung der SigG-Funktion

Bild 2 zeigt das logische Ablaufdiagramm für eine Chipkarte mit SigG-Anwendung. In diesem Ablaufdiagramm gibt es nach Anwendungseröffnung 2 parallele Zweige, die den Einsatz der Chipkarte an unterschiedlichen Terminals zeigen:

- privates oder firmeneigenes Benutzerterminal
- Geschäftsterminal.

Die Chipkarte kann zunächst nicht erkennen, in welcher Einsatzumgebung sie verwendet wird. Ein Geschäftsterminal (d.h. ein Terminal, das geschäftsmäßig Dritten zur Nutzung angeboten wird) muß jedoch den Authentisierungszeitweig durchlaufen. Das Sicherheitsmodul des Geschäftsterminals, das z.B. eine Plug-in-Karte beinhalten kann, darf jedoch eine Authentisierung nur zulassen, wenn der Sicherheitszustand des Geschäftsterminals unverändert gegeben ist.

Während der Authentisierung werden Session Keys zur Absicherung der weiteren Kommunikation mit Secure Messaging ausgehandelt (siehe Anhang D). Damit der Benutzer sicher sein kann, daß dies auch tatsächlich stattfindet, wird eine kartenspezifische Display-Info aus der Chipkarte gelesen, die dem Benutzer angezeigt werden muß. Diese Display-Info wird von der Chipkarte

nur nach erfolgreich abgewickelter gegenseitiger Authentisierung zum Lesen freigegeben.

Der Karteninhaber muß dann entweder durch eine wissensbasierte Identifikation (PIN- oder Paßwort-Eingabe) und/oder durch eine biometrische Identifikation nachweisen, daß er der rechtmäßige Benutzer der betreffenden Chipkarte ist. Das wissensbasierte und das biometrische Benutzer-Authentisierungsverfahren können koexistent in der Chipkarte realisiert sein.

Chipkarten können je nach Konfigurierung bei der Personalisierung bzw. der Fähigkeit des jeweiligen Betriebssystems im Bezug auf die Benutzer-Authentisierung zwei Verhaltensweisen zeigen:

1. Die Karte verlangt vor jeder Ausführung der Digitalen Signatur eine Benutzer-Authentisierung.
2. Die Karte verlangt nur eine einmalige Benutzer-Authentisierung, d.h. aus der Sicht der Chipkarte können dann im Prinzip beliebig viele Signaturen nacheinander angefertigt werden.

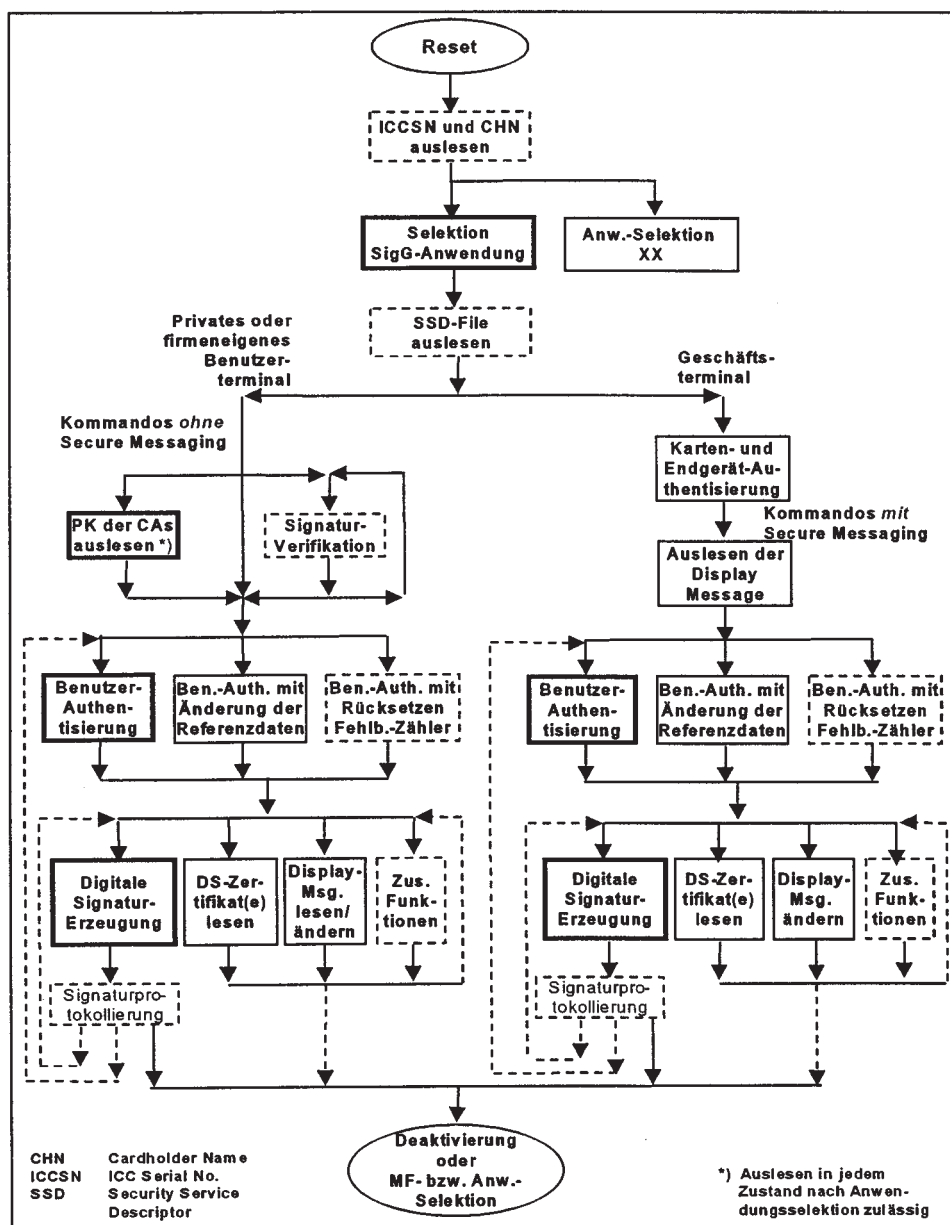


Bild 2: Ablaufdiagramm für Chipkarten mit SigG-Anwendung

Wünschenswert ist auch die Unterstützung eines Zählers, der nach einer konfigurierbaren Anzahl von Signaturen abläuft und dabei den Sicherheitsstatus zurücksetzt. Vor einer weiteren Signatur ist dann eine erfolgreiche Benutzer-Authentisierung erforderlich.

Im SSD-File kann die PIN usage policy angezeigt werden (DO '5F2F').

Bei der zweiten Variante kann jedoch in Anwendungs-Umgebungen, wo

- vor jeder digitalen Signatur oder
- vor einer digitalen Signatur nach n digitalen Signaturen oder
- vor einer digitalen Signatur nach Ablauf einer definierbaren Zeitspanne x nach der letzten digitalen Signatur

erneut die Benutzer-Authentisierung durchlaufen werden soll, vom Karteninhaber über eine entsprechende Bedienerführung oder durch Konfigurierung des Anwendungssystems die Einstellung der gewünschten Variante veranlaßt werden (Schutz vor unbefugter Änderung erforderlich). Aus Systemsicht bedeutet dies, daß sofort nach Eintreten des entsprechenden Ereignisses (Signatur erzeugt, n Signaturen erzeugt oder Zeit abgelaufen) das Anwendungssystem entweder

- ein Reset zur Chipkarte oder
- einen Rücksprung zum übergeordneten DF (d.h. in der Regel zum MF) durch Selektion des übergeordneten DF

veranlaßt, so daß bei erneutem Signierwunsch des Benutzers eine erneute Anwendungsselektion erfolgt und anschließend wieder die Benutzer-Authentisierung angefordert wird.

Die digitale Signatur-Funktion (SigG-Funktion, siehe Definition in 3.1) kann auch im Rahmen einer anderen Anwendung auftreten, wie Bild 3 zeigt.

Innerhalb der Signatur-Anwendung können zusätzliche Funktionen wie z.B. Dokumentenverschlüsselung auftreten.

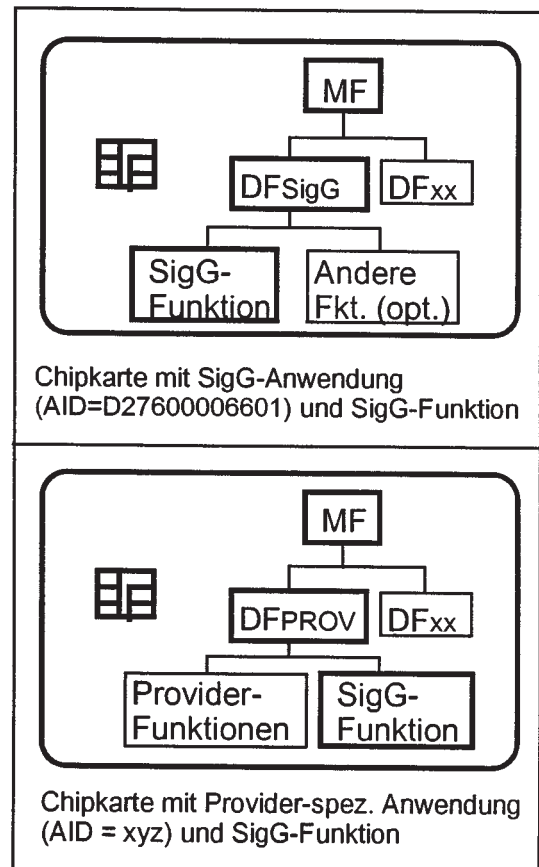


Bild 3: Anwendungen mit SigG-Funktion

9 Zertifizierungsstellen und Zertifikate

Die Regulierungsbehörde RegTP übt die Rolle der Haupt-Zertifizierungsstelle (RootCA) aus und erstellt Zertifikate für die nachgeordneten Zertifizierungsstellen. Diese wiederum erstellen die Zertifikate für die Benutzer mit SigG-Chipkarten (siehe Bild 4).

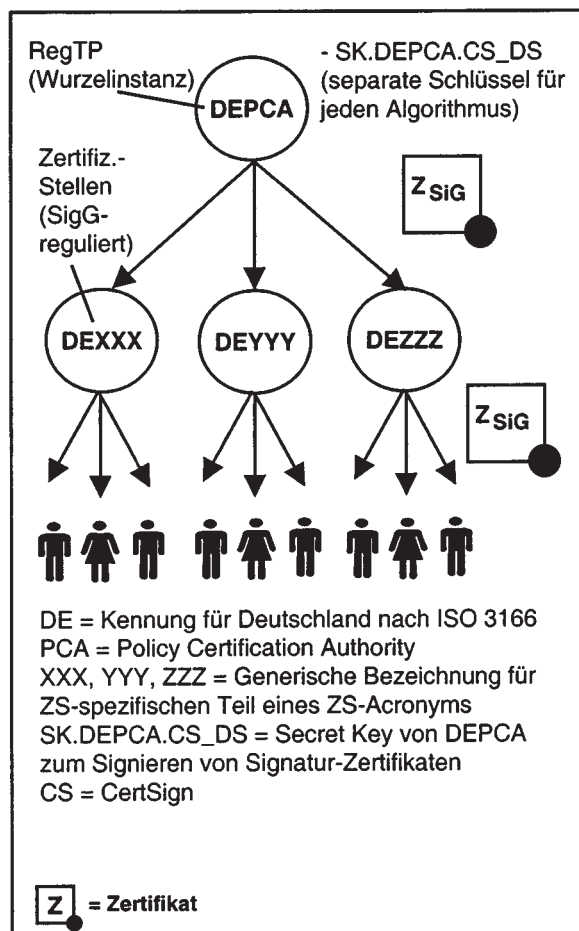


Bild 4: Zertifizierungsstellen und Zertifikate für SigG-Zertifikate

Für die Nutzung von SigG-Chipkarten an Geschäftsterminals ist eine gegenseitige Authentisierung von Chipkarte und Geschäftsterminal erforderlich. Da hierfür ebenfalls PK-Verfahren eingesetzt werden sollen, sind ICC- und IFD-Authentisierungs-Zertifikate erforderlich. Für Signatur und Authentisierung werden separate Schlüsselpaare eingesetzt. Träger des ICC-Authentisierungs-Zertifikats ist die Chipkarte, Träger des IFD-Authentisierungs-Zertifikats ist eine Plug-in-Karte als Beispiel für die Realisierung eines Endgeräte-Sicherheitsmoduls (siehe Bild 5).

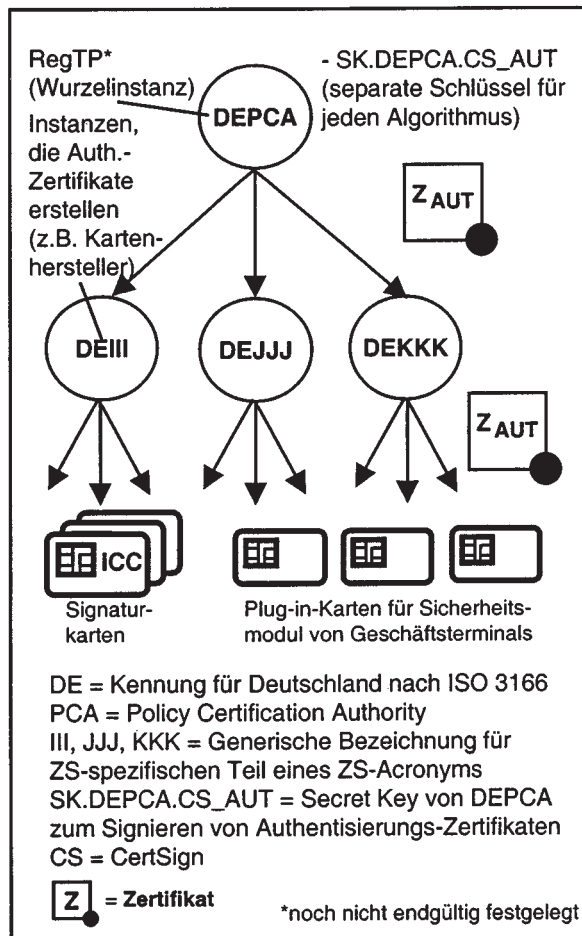


Bild 5: Zertifizierungsstellen und Zertifikate für ICC- und IFD-Authentisierungs-Zertifikate

10 Datei-Struktur und Datenobjekte

10.1 Datei-Struktur

Die File-Organisation in der Chipkarte soll mit ISO/IEC 7816-4 kompatibel sein. Die Datei-Struktur der Chipkarte zeigt Bild 6. Die Kenndaten der einzelnen Files sind im Anhang C beschrieben.

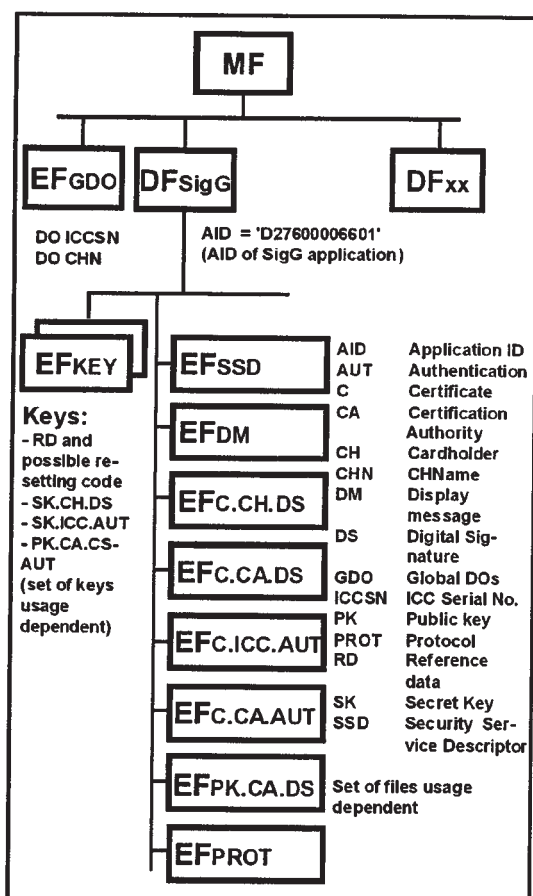


Bild 6: Datei-Struktur einer Chipkarte mit SigG-Anwendung

Unterstützt eine Chipkarte mehrere Signatur-Algorithmen (z.B. RSA und DSA oder mehrere Signatur-Formate (z.B. RSA entsprechend ISO/IEC 9796-2 oder PKCS #1)), dann sind die jeweiligen Teilnehmer-Zertifikate in separaten Files abgelegt (siehe Anhang C). Die SigG-Anwendung (DFSigG) trägt einen ISO/IEC 7816-5-konformen Application Identifier (AID), dessen Aufbau und Codierung Bild 7 zeigt.

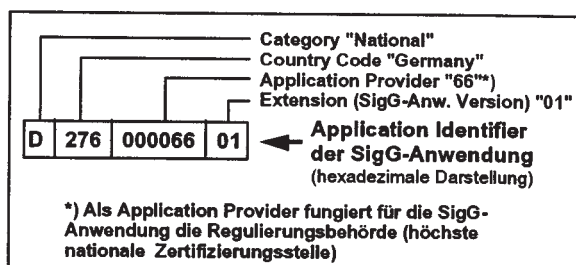


Bild 7: AID der SigG-Anwendung

10.2 EF.GDO

In dem EF.GDO sollen das DO „ICC Serial Number (ICCSN)“ (tag '5A', siehe Bild 8) und das DO „Cardholder Name“ (tag '5F20', Inhalt wie auf Kartenvorderseite) abgelegt sein.

Die ICCSN besteht aus der Kartenherausgeberkennung gefolgt von einer Serien-Nummer und einem Prüfbyte entsprechend der Luhn-Formel (siehe ISO/IEC CD 7812-1). Die ICCSN ist eine eindeutige Chipkarten-Kennung und kann z.B. für Chipkarten-Sperrlisten verwendet werden. Der genaue Aufbau der ICCSN kann ggf. anwendungsspezifisch variieren.

Bild 8 und Bild 9 zeigen mögliche Varianten, wobei die Nutzung der Variante nach Bild 9 empfohlen wird.

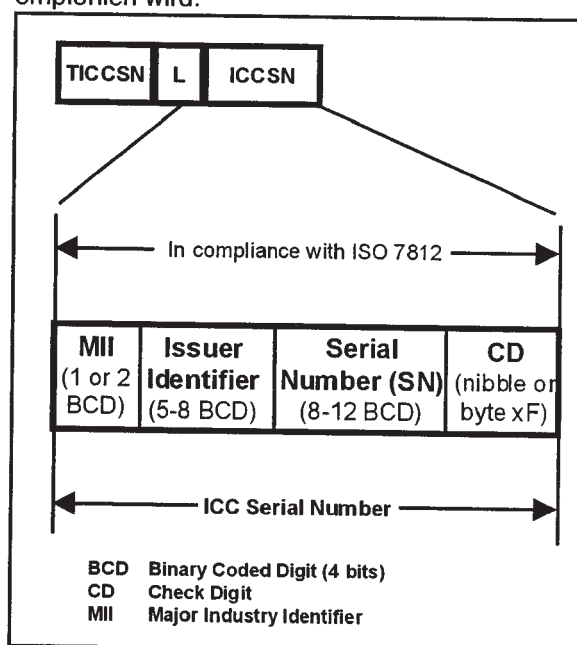


Bild 8: ICCSN (ISO/IEC 7812-orientiert)

Issuer Identification No.	Serial No.
'D2 76 nn nn nn' (5 Bytes, n = BCD)	'xx .. xx' (8 Bytes, e.g. chip serial no.)

Bild 9: ICCSN (ISO/IEC 7816-5/6-orientiert mit Category D und Country Code)

ANMERKUNG: Für die Vergabe einer IIN entsprechend Bild 9 ist die CCG in Köln als beim DIN akkreditierte Instanz zuständig. (CCG - Centrale für Coorganisation GmbH, Maarweg 133, D - 50825 Köln)

Das DO CHN enthält den Cardholder Name in der Form, wie er auf dem Cover einer ID-1-Chipkarte steht. Als Codierungsschema für CHN ist ASCII zu verwenden.

Die globalen Datenobjekte sollen mit SELECT FILE und READ BINARY ausgelesen werden können, wobei das Vorhandensein des DO CHN in Chipkarten mit dem Format ID-1 optional, für Chipkarten mit dem Format ID-000 aber mandatory ist.

10.3 EF.KEY

Die für die SigG-Anwendung benötigten Schlüssel/Referenzdaten gliedern sich in 3 Gruppen:

1. Referenzdaten für Benutzer-Authentisierung

- Referenzdaten für die wissensbasierte Benutzer-Authentisierung (PIN bzw. Paßwort, Resetting Code)
- Ggf. Referenzdaten für biometrische Benutzer-Authentisierung (Biometrische Daten, Resetting Code)

2. Geheime Schlüssel

- SK.CH.DS für die digitale Signatur-Funktion (ggf. mehrere Secret Keys)
- SK.ICC.AUT der Chipkarte für Authentisierung

3. Öffentliche Schlüssel

- PK.CA.AUT für Terminal-Authentisierung (ggf. mehrere Public Keys, falls erforderlich)
- Ggf. ein oder mehrere PK.IFD.AUT

Der Aufbau und die Art der Nutzung von Key Files ist betriebssystemspezifisch.

Geheime Schlüssel und Referenzdaten dürfen nicht auslesbar sein. Installierte geheime Schlüssel dürfen nicht verändert werden können. Auch der Resetting Code darf nach Installation nicht mehr änderbar sein. Darüber hinaus muß sichergestellt werden, daß die jeweiligen Schlüssel nur für den jeweiligen Dienst verwendet werden (z.B. ein Signatur-Schlüssel darf nur zur Erzeugung der digitalen Signatur verwendet werden).

Öffentliche Schlüssel werden in der Regel in einem separaten PK-Key-File abgelegt. PKs werden entweder bei der Karten-

Personalisierung eingetragen oder durch das Betriebssystem als Teiloperation von VERIFY CERTIFICATE (z.B. Eintragung eines PK.IFD.AUT).

Als Key Reference wird bei Referenzdaten und geheimen Schlüsseln eine KID verwendet, die in der Regel 1 Byte lang ist. Bei PK.CA.AUT-Schlüsseln dient die Kennung der Zertifizierungsstelle als Schlüssel-Identifizier. Bei PK.IFD.AUT-Schlüsseln dient die IFD-Kennung als Schlüssel-Identifizier. PKs sind schreibgeschützte Objekte.

10.4 EF.SSD

Der EF.SSD stellt für das Terminal Informationen zur Ansteuerung der SigG-Funktion bereit, die zulässige Ablaufvarianten darstellen. Hierzu gehören:

- Anzeige der Algorithmen, die von der Chipkarte bei der externen Authentisierung (Endgeräte-Authentisierung) verwendet werden können.
- Anzeige, wie die Chipkarte die digitale Signatur erzeugt (z.B. Hash-Funktion verfügbar, verschiedene DSI-Formate).
- Anzeige, ob auch Signaturen verifiziert werden können.
- Anzeige, ob zur Benutzer-Authentisierung nur das wissensbasierte Identifikationsverfahren (PIN/Paßwort-Verfahren) oder zusätzlich auch ein biometrisches Identifikationsverfahren zur Verfügung steht. Für das wissensbasierte Identifikationsverfahren kann angezeigt werden, ob die Chipkarte das PIN-Format "Format 2 PIN-Block" zusätzlich oder alternativ verwendet.

Die verfügbaren Sicherheitsfunktionen werden mit Hilfe von Security Service Descriptoren beschrieben. Im EF.SSD sind daher SSD-Templates zu finden oder ein Security Service Profile Identifier.

Aufbau und Inhalt des EF.SSD sind in Anhang F dargestellt.

10.5 EF.DM

In der Datei EF.DM steht die Display Message. Sie soll aus 8 Buchstaben in ASCII-Codierung bestehen und aussprechbar sein, damit der

Karteninhaber sie bei Anzeige leichter wiedererkennen kann.

10.6 EF.C.CH.DS

In der Datei EF.C.CH.DS wird das 'Signatur'-Zertifikat des Karten-Inhabers abgelegt. Der Aufbau eines DS-Zertifikats ist in Sigl (Signatur-Interoperabilitätsspezifikation) beschrieben. Besitzt der Karten-Inhaber mehrere Signatur-Zertifikate, dann sind diese in separaten Files abgelegt.

10.7 EF.C.CA.DS

In der Datei EF.C.CA.DS wird das 'Signatur'-Zertifikat der Zertifizierungsstelle abgelegt, die das Signatur-Zertifikat C.CH.DS des Karten-Inhabers erzeugt hat. Das 'Signatur'-Zertifikat C.CA.DS wurde von der höchsten Zertifizierungsstelle (RegTP) erzeugt.

10.8 EF.C.ICC.AUT

In der Datei EF.C.ICC.AUT wird das 'Authentication'-Zertifikat C.ICC.AUT abgelegt (Aufbau: siehe Anhang B).

10.9 EF.C.CA.AUT

In der Datei EF.C.CA.AUT wird das 'Authentication'-Zertifikat C.CA.AUT der Zertifizierungsstelle abgelegt (Aufbau: siehe Anhang B).

10.10 EF.PK.CA.DS

In der Datei EF.PK.CA.DS werden Public Keys von Zertifizierungsstellen gespeichert, die als "Sicherheitsanker" von der Software bei der Verifikation von Zertifikaten verwendet werden. Der Inhalt von EF.PK.CA.DS ist in Anhang A beschrieben.

10.11 EF.PROT

Die optionale Datei EF.PROT mit zyklischer Datei-Struktur dient der Protokollierung von

Signaturen. Sie ist als Hilfsmittel für den Benutzer, jedoch nicht im Sinne einer juristischen Beweissicherung zu sehen. Ein Record-Inhalt (Signaturprotokolleintrag) besteht aus

- Datum (12 Bytes, JJJJMMTHHMM),
- Terminalkennung (18 Bytes, z.B. ICCSN.IFD in printable form),
- Dokumenten-Kennung (20 Bytes) und
- Signaturzähler (3 Bytes, Ziffern).

Als Codierungsschema ist ASCII zu verwenden.

11 Chipkarten-Eröffnung

11.1 Kommando-Sequenzen

Nach Einführung der Chipkarte muß zunächst ein Reset ausgeführt werden. Konditional (siehe 10.2) sind nach dem Reset dann die globalen Datenobjekte ICCSN und CHN auszulesen.

ICC Commands	Bedeutung
Hardware reset 	Cold reset und Answer-to-Reset mit Anzeige der Anwendungs-Selektions-Methode
SELECT FILE <EF.GDO> 	EF.GDO selektieren
READ BINARY 	DO ICC Serial No. und DO CardholderName lesen

Bild 10: Chipkarten-Eröffnung

11.2 Lesen der globalen Datenobjekte

Zum Lesen der globalen Datenobjekte werden die ISO/IEC 7816-4-Kommandos SELECT FILE und READ BINARY verwendet.

Tabelle 1: SELECT FILE Command zum Selektieren des GDO-File

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'A4' = SELECT FILE
P1	'02' = EF file selection
P2	'0C' = No FCI to be returned
Lc	'02' = Length of subsequent data field
Data field	FID of GDO file, see annex C
Le	Empty

Tabelle 2: SELECT FILE Response

Data field	Empty
SW1-SW2	'9000' or specific status bytes

Tabelle 3: READ BINARY Command zum Lesen der Global Data Objects

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'B0' = READ BINARY
P1	'00'
P2	'00'
Lc	Empty
Data field	Empty
Le	'00' = Read until end-of-file

Tabelle 4: READ BINARY Response

Data field	DO ICCSN DO CHN
SW1-SW2	'9000' or specific status bytes

12 Anwendungs-Eröffnung

12.1 Kommando-Sequenzen

Die Anwendungs-Eröffnung besteht aus der Anwendungsselektion und ggf. dem Auslesen des SSD-Files.

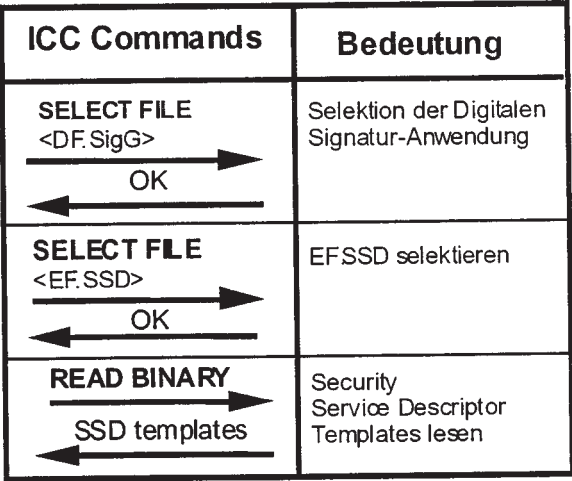


Bild 11: Kommandos bei der Anwendungs-Eröffnung

12.2 Anwendungs-Selektion

Zur Anwendungs-Selektion wird das ISO/IEC 7816-4-Kommando SELECT FILE mit Angabe des 'Application Identifier' verwendet (direkte Anwendungs-Selektion).

Tabelle 5: SELECT FILE Command zur Anwendungs-Selektion mit AID

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'A4' = SELECT FILE
P1	'04' = DF selection by AID
P2	'0C' = No FCI to be returned
Lc	'06' = Length of subsequent data field
Data field	'D27600006601' = AID der SigG-Anwendung
Le	Empty

Tabelle 6: SELECT FILE Response

Data field	Empty
SW1-SW2	'9000' or specific status bytes

12.3 Lesen der SSD-Templates

Zum Lesen des Security-Service-Descriptor-File sind folgende Kommandos nötig:

Tabelle 7: SELECT FILE Command zum Selektieren des SSD-File

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'A4' = SELECT FILE
P1	'02' = EF file selection
P2	'0C' = No FCI to be returned
Lc	'02' = Length of subsequent data field
Data field	FID of SSD file, see annex C
Le	Empty

Tabelle 8: SELECT FILE Response

Data field	Empty
SW1-SW2	'9000' or specific status bytes

Tabelle 9: READ BINARY Command zum Lesen der SSD-Templates

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'B0' = READ BINARY
P1	'00'
P2	'00'
Lc	Empty
Data field	Empty
Le	'00' = Read until end-of-file

Tabelle 10: READ BINARY Response

Data field	SSD templates
SW1-SW2	'9000' or specific status bytes

13 Authentisierung des Karteninhabers

13.1 Kommando-Übersicht

Die Benutzer-Authentisierungs-Kommandos VERIFY, CHANGE REFERENCE DATA und RESET RETRY COUNTER (siehe Bild 12) haben unterschiedliche Funktionalität und sind unabhängig voneinander benutzbar.

ICC Commands	Bedeutung
VERIFY <verification data> 	Prüfung der Echtheit des Benutzers
CHANGE RD <old RD new RD> 	Änderung der Reference Data
RESET RC <resetting code new RD> 	Rücksetzen des Fehlbedienungs Zählers und Setzen neuer Reference Data

Bild 12: Benutzer-Authentisierungs-Kommandos

Werden die Kommandos zur Benutzer-Authentisierung von einem Geschäftsterminal gesendet, dann ist das jeweilige Kommando-Datenfeld als Kryptogramm zu übertragen und das Kommando mit einer kryptografischen Prüfsumme zu versehen (siehe Anhang D).

13.2 Benutzer-Authentisierung

Zur Benutzer-Authentisierung wird das ISO/IEC 7816-4-Kommando VERIFY verwendet. Der Initialwert des Fehlbedienungs Zählers (Retry Counter) beträgt 3 für PIN/PW-Präsentation. Bei biometrischen Verfahren ist der Initialwert in Abhängigkeit von dem jeweiligen Verfahren festzulegen.

Die Art und Weise der Speicherung der Referenzdaten in der Chipkarte (z.B. Speicherung nicht in Klartextform) ist nicht Gegenstand dieser Vornorm.

Tabelle 11: VERIFY Command

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'20' = VERIFY
P1	'00'
P2	'81' = PIN/PW reference '91' = Biometrical data reference
Lc	'xx' = Length of subsequent data field
Data field	If P2 = '81': PIN or PW (min. 6, max. 8 ASCII characters) If P2 = '91': Biometrical verification data
Le	Empty

Weitere PIN-Formate können Verwendung finden, wie

P2 = '80': PIN im Format 2 PIN-Block (siehe ISO 9564-1).

Solche Zusatzformate können im SSD-File angezeigt werden.

Tabelle 12: VERIFY Response

Data field	Empty
SW1-SW2	'9000' or specific status bytes

Folgende speziellen Status Bytes sind von besonderer Bedeutung:

- '9000': Benutzer-Authentisierung erfolgreich
- '6300': Warnung – Verifikation nicht erfolgreich (keine weitere Information)
- '6983': Authentisierungs-Verfahren blockiert (diese Status-Meldung soll gesandt werden, wenn der Wiederholungszähler den Wert 0 hat)
- '63CX': Warnung – Verifikation nicht erfolgreich ('X' gibt die Anzahl der erlaubten Wiederholungen an)

13.3 Änderung der Referenzdaten

13.3.1 Wissensbasierte Benutzer-Authentisierung

Die Änderung der Referenzdaten (PIN- bzw. Paßwort-Änderung) erfolgt mit dem ISO/IEC 7816-8-Kommando CHANGE REFERENCE DATA. Das Kommando ist in jedem Zustand nach Anwendungsselektion erlaubt.

Tabelle 13: CHANGE REFERENCE DATA Command

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'24' = CHANGE REFERENCE DATA
P1	'00' = Exchange reference data
P2	'81' = PIN/PW reference
Lc	Length of subsequent data field
Data field	Existing reference data (6 to 8 bytes) followed by new reference data (6 to 8 bytes, ASCII coding)
Le	Empty

Die Länge der alten Reference Data ist der Chipkarte bekannt, so daß weder Delimiter noch Padding zum Auffüllen nötig sind. Haben die bisherigen Referenzdaten eine Länge von 6 Bytes und die neuen eine Länge von 7 Bytes, dann hat das Lc-Feld den Wert '0D' (= 13).

Wird beim VERIFY-Kommando das Format 2 PIN-Block benutzt (siehe 13.2), so ist dieses auch hier mit P2 = '80' zu verwenden.

Tabelle 14: CHANGE REFERENCE DATA Response

Data field	Empty
SW1-SW2	'9000' or specific status bytes

13.3.2 Biometrische Benutzer-Authentisierung

Die Änderung biometrischer Referenzdaten, sofern dies für das betreffende Verfahren sinnvoll und möglich ist (z.B. beim Fingerprint-Verfahren), erfolgt mit dem ISO/IEC 7816-8-Kommando CHANGE REFERENCE DATA. Das Kommando ist nur nach erfolgreicher Benutzer-Authentisierung erlaubt, da hier nur die neuen Referenzdaten übergeben werden.

Tabelle 15: CHANGE RD Command

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'24' = CHANGE REFERENCE DATA
P1	'01' = Change reference data
P2	'91' = Biometrical data reference
Lc	Length of subsequent data field
Data field	New reference data
Le	Empty

Tabelle 16: CHANGE RD Response

Data field	Empty
SW1-SW2	'9000' or specific status bytes

13.4 Rücksetzen des Fehlbedienungszählers und Setzen neuer Referenzdaten

Für den Fall, daß nach dreimaliger aufeinanderfolgender Falscheingabe der Verifikations-Daten die Nutzung der SigG-

Funktion blockiert ist, soll mit Hilfe des ISO/IEC 7816-8-Kommandos RESET RETRY COUNTER der Fehlbedienungs-zähler auf seinen Initialwert gesetzt und damit die Nutzung der SigG-Funktion wieder freigeschaltet werden können. Hierbei ist der Resetting Code einzugeben (8 Ziffern, Initialwert des Fehlbedienungs-zählers für den Resetting Code ist 3).

Bei wissensbasierter Benutzer-Authentisierung kann auch eine neue PIN bzw. ein neues Paßwort gesetzt werden (P1 = '00').

Bei biometrischer Benutzer-Authentisierung wird nur die Unterstützung von P1 = '01' empfohlen.

Die Unterstützung dieses Kommandos ist optional.

Tabelle 17: RESET RETRY COUNTER Command

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'2C' = RESET RETRY COUNTER
P1	'00' = Reset retry counter and set new reference data '01' = Reset retry counter
P2	'81' = PIN/PW reference '91' = Biometrical data reference
Lc	Length of subsequent data field
Data field	- if P1 = '00': Resetting code (8 bytes) followed by new reference data (6 to 8 bytes, ASCII coding) - if P1 = '01': Resetting code (8 bytes)
Le	Empty

Wird beim VERIFY-Kommando das Format 2 PIN Block benutzt (siehe 13.2), so ist dieses auch hier mit P2 = '80' zu verwenden.

Tabelle 18: RESET RETRY COUNTER Response

Data field	Empty
SW1-SW2	'9000' or specific status bytes

14 Berechnen einer digitalen Signatur

14.1 Signatur-Prozess und Kommando-Übersicht

Bild 13 zeigt den generellen Ablauf eines digitalen Signatur-Prozesses. Die Funktion 'Format Mechanisms' ist leer für Algorithmen, die unmittelbar den Hash-Wert zur Signatur-Produktion verwenden (z.B. DSA).

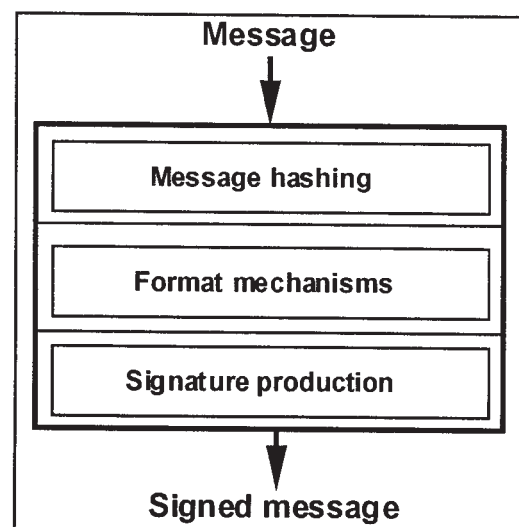


Bild 13: Signatur-Prozess

Beim Ablauf der digitalen Signatur-Funktion kann es Alternativen geben:

Fall 1: Ablauf ohne Hash-Funktion in der Chipkarte

Fall 2: Ablauf mit Hash-Funktion (letzte Runde in der Chipkarte)

Fall 3: Ablauf mit Hash-Funktion (komplettes Hashen in der Chipkarte)

ICC Commands	Bedeutung
PSO: COMPUTE DS <hash value or digestinfo> 	Berechnen einer Digitalen Signatur (Vorgang kann wiederholt werden)

Bild 14: Signatur-Ablauf ohne Hashen in der Karte

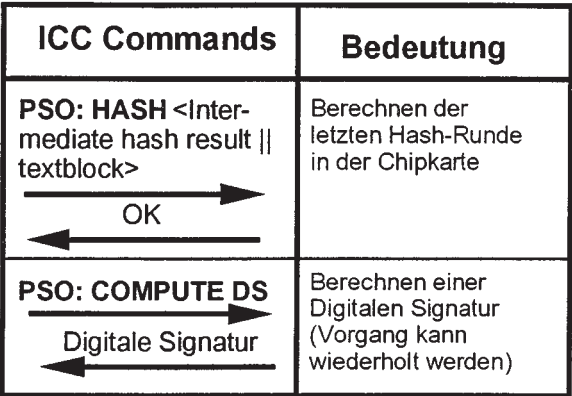


Bild 15: Signatur-Ablauf mit Hashen in der Karte (letzte Runde)

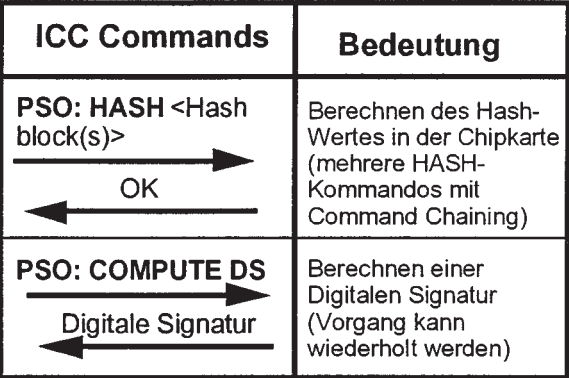


Bild 16: Signatur-Ablauf mit Hashen in der Karte (komplettes Hashen)

14.2 Chipkarten ohne Hash-Funktion

Das Kommando zur Berechnung der digitalen Signatur entsprechend ISO/IEC 7816-8 zeigt die nachfolgende Tabelle. Hierbei wird der Hash-Wert (oder ggf. die DigestInfo) im Datenfeld des Kommandos übergeben. Signatur-Schlüssel sowie Signatur-Algorithmus und damit verbunden das Signatur-Format (siehe Anhang A) sind entweder

- voreingestellt und damit implizit selektiert oder
- müssen explizit mit dem **MANAGE SECURITY ENVIRONMENT**-Kommando (siehe 16.3) eingestellt werden.

Welcher Algorithmus und welches DSI-Format voreingestellt sind, kann dem SSD-File entnommen werden.

Tabelle 19: PSO: COMPUTE DS Command

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'2A' = PERFORM SECURITY OPERATION: COMPUTE DIG. SIGNATURE
P1	'9E' (= return digital signature)
P2	'9A' (= data field contains data to be integrated in the DSI)
Lc	Length of subsequent data field
Data field	Data to be integrated in the DSI: hash value or digestinfo (the length of the data field shall not exceed 40 % of the length of the modulus in case of RSA)
Le	'00' or length of expected dig. signature

Tabelle 20: PSO: COMPUTE DS Response

Data field	Digital signature
SW1-SW2	'9000' or specific status bytes

14.2.1 Chipkarten mit Hash-Funktion

a) Hashen der letzten Runde(n) vor Signieren

Chipkarten, die über eine Hash-Funktion verfügen und die letzte(n) Runde(n) des Hashens Chipkarten-intern ausführen, erwarten zunächst das ISO/IEC 7816-8-Kommando **PSO: HASH**.

Das Kommando kann auch dazu benutzt werden, den kompletten Hash-Wert der Karte zu übergeben.

Tabelle 21: PSO: HASH Command

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'2A' = PERFORM SECURITY OPERATION: HASH
P1	'90' (= compute hash value)
P2	'A0' (= data field contains DOs relevant for hashing)
Lc	Length of subsequent data field
Data field	- If data shall be hashed: '90' - L - Intermediate hash result (see annex A) '80' - L - Data to be hashed - If the final hash value shall be transmitted: '90' - L - Hash value
Le	Empty

Tabelle 22: PSO: HASH Response

Data field	Empty
SW1-SW2	'9000' or specific status bytes

Anschließend wird das Kommando PSO: COMPUTE DIGITAL SIGNATURE gesendet.

Tabelle 23: PSO: COMPUTE DS Command

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'2A' = PERFORM SECURITY OPERATION: COMPUTE DIG. SIGNATURE
P1	'9E' (= return digital signature)
P2	'9A' (=data field contains data to be signed or integrated in the DSI)
Lc	Empty
Data field	Empty (i.e. DSI already present in the card)
Le	'00' or length of expected digital signature

Tabelle 24: PSO: COMPUTE DS Response

Data field	Digital signature
SW1-SW2	'9000' or specific status bytes

b) Komplettes Hashen in der Chipkarte

Chipkarten, die über eine Hash-Funktion verfügen und ein komplettes Hashen Chipkarten-intern ausführen, erwarten zunächst das ISO/IEC 7816-8-Kommando PSO: HASH. Hierbei kann Command-Chaining (siehe ISO/IEC 7816-8) erforderlich sein.

Tabelle 25: PSO: HASH Command

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'2A' = PERFORM SECURITY OPERATION: HASH
P1	'90' (= compute hash value)
P2	'80' (= data field contains data to be hashed)
Lc	Length of subsequent data field
Data field	Data to be hashed (one or more blocks)
Le	Empty

ANMERKUNG: Der letzte übertragene Block ist kleiner oder gleich der normalen Blocklänge. Das Padding des Hash-Inputs wird von der Karte durchgeführt.

Tabelle 26: PSO: HASH Response

Data field	Empty
SW1-SW2	'9000' or specific status bytes

Anschließend wird das Kommando PSO: COMPUTE DS gesendet (siehe Tabellen 23 und 24).

14.3 Selektion eines Security Environment

Unterstützt eine Chipkarte mehr als einen Signatur-Algorithmus (z.B. RSA und DSA) oder im Rahmen eines Signatur-Algorithmus mehrere Signatur-Formate, dann kann mit dem MSE-Kommando das entsprechende Security Environment eingestellt werden. SE Nr.1 gilt als voreingestellt. Welche SEs die betreffende Chipkarte unterstützt, zeigt sie im SSD-File an (siehe Anhang F und Anhang G). Alternativ kann z.B. auch eine Alg.-ID mit der SET-Option des MSE-Kommandos gesetzt werden (siehe Anhang F).

Tabelle 27: MANAGE SECURITY ENVIRONMENT Command

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'22' = MANAGE SECURITY ENVIRONMENT
P1	'F3' (= RESTORE)
P2	'xx' (= SE number)
Lc	Empty
Data field	Empty
Le	Empty

Tabelle 28: MANAGE SECURITY ENVIRONMENT Response

Data field	Empty
SW1-SW2	'9000' or specific status bytes

15 Lesen von Zertifikaten und Zertifikats-Prüfchlüsseln (PK.CAs)

15.1 Kommando-Sequenzen

Zum Lesen eines Zertifikats bzw. von Zertifikatsschlüsseln sind folgende Kommandos nötig:

ICC Commands	Bedeutung
SELECT FILE <EF.C.CH.DS> 	EF.C.CH.DS selektieren
READ BINARY  Certificate C.CH.DS	Zertifikat C.CH.DS lesen
SELECT FILE <EF.PK.CA.DS> 	EF.PK.CA.DS selektieren
READ BINARY  PK.CA.DS-Info	PK.CA.DS-Info lesen

Bild 17: Kommandos zum Auslesen von Zertifikaten und Public Keys

15.2 Selektieren und Lesen der Daten-Files

Tabelle 29: SELECT FILE Command zum Selektieren eines Zertifikats- oder PK-File

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'A4' = SELECT FILE
P1	'02' = EF file selection
P2	'0C' = no FCI to return
Lc	'02' = Length of subsequent data field
Data field	FID of respective certificate file or public key file (see Annex C)
Le	Empty

Tabelle 30: SELECT FILE Response

Data field	Empty
SW1-SW2	'9000' or specific status bytes

Tabelle 31: READ BINARY Command zum Lesen des Zertifikats

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'B0' = READ BINARY
P1, P2	'0000' or offset
Lc	Empty
Data field	Empty
Le	'xx' = Length of data to be read ('00' = Read until end-of-file)

Tabelle 32: READ BINARY Response

Data field	Certificate
SW1-SW2	'9000' or specific status bytes

Die Public Keys der Zertifizierungsstellen sind mit den gleichen Kommandos auszulesen, doch ist als FID das Dateikennzeichen von EF.PK.CA.DS anzugeben.

16 Verifizieren einer digitalen Signatur

16.1 Kommando-Übersicht

Zum Verifizieren von digitalen Signaturen (diese Funktion ist optional) werden folgende Datenelemente benötigt:

- Hash-Wert
- Public Key des Signierenden
- Digital Signature

Da Chipkarten heutiger Technologie keine X.509-Zertifikate auswerten können, macht diese Funktion derzeit nur dann Sinn, wenn der PK des Signierenden bereits in der Chipkarte vorhanden ist (diese Situation ist in der Regel nicht gegeben).

Bei der digitalen Signatur muß die Chipkarte bei reversiblen Signatur-Algorithmen das DSI-Format kennen, um den Hash-Wert auffinden zu können.

Zur Abwicklung einer Signatur-Prüfung wird eine Kommandofolge benötigt, wie sie Bild 18 zeigt.

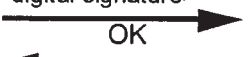
ICC Commands	Bedeutung
PSO: HASH <hash related data> 	Übergeben des Hash-Wertes bzw. Hashen der letzten Runde
MSE SET<key ref> 	Setzen der Key Reference von PK.USER.DS
VERIFY SIGNATURE <digital signature> 	Prüfung der Signatur

Bild 18: Kommandos zur Signaturprüfung

16.2 Übergabe des Hash-Wertes

Zur Übergabe des Hash-Wertes wird das PSO: HASH-Kommando verwendet.

Tabelle 33: PSO: HASH Command

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'2A' = PERFORM SECURITY OPERATION: HASH
P1	'90' (= compute hash value)
P2	'A0' (= data field contains DOs relevant for hashing)
Lc	Length of subsequent data field
Data field	- If data shall be hashed: '90' - L - Intermediate hash result (see annex A) '80' - L - Data to be hashed - If the final hash value shall be transmitted: '90' - L - Hash value
Le	Empty

Tabelle 34: PSO: HASH Response

Data field	Empty
SW1-SW2	'9000' or specific status bytes

16.3 Selektieren des Signatur-Prüfsschlüssels

Vor dem PSO: VERIFY SIGNATURE-Kommando ist mit dem MSE-Kommando der PK des Signierenden zu selektieren.

Tabelle 35: MANAGE SECURITY ENVIRONMENT Command

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'22' = MANAGE SECURITY ENVIRONMENT
P1	'81' (= SET for verification)
P2	'B6' (= DST)
Lc	'xx' = Length of subsequent data field
Data field	'83 0x xx ... xx' (DO KeyRef of the user's PK, tag '83')
Le	Empty

Tabelle 36: MANAGE SECURITY ENVIRONMENT Response

Data field	Empty
SW1-SW2	'9000' (= PK set) or '6xxx' (= PK not available or other error condition)

ANMERKUNG: Wird das MSE-Kommando zum Selektieren eines Signaturschlüssels verwendet, dann ist P1 = '41' (= SET for computation), P2 = 'B6' (= DST) und im Datenfeld die Schlüsselreferenz im DO mit Tag '84' anzugeben.

16.4 Signatur-Verifikation

Dann folgt das Kommando PSO: VERIFY DS:

Tabelle 37: PSO: VERIFY DS Command

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'2A' = PERFORM SECURITY OPERATION: VERIFY DIGITAL SIGNATURE
P1	'00'
P2	'A8' (= data field contains DOs relevant for verification)
Lc	'xx' = Length of subsequent data field
Data field	'9E' - L - Digital signature (DSI format to be detected by the card)
Le	Empty

Tabelle 38: PSO: VERIFY DIGITAL SIGNATURE Response

Data field	Empty
SW1-SW2	'9000' or specific status bytes

17 Signatur-Protokollierung

17.1 Kommando-Sequenzen

Ziel der Signatur-Protokollierung ist das Schreiben eines Kennsatzes (Protokoll-Record) zu jeder ausgeführten Signatur.

Anzustreben ist hierbei, daß von der Chipkarte

- der aktuelle Signaturzählerstand (durch die Chipkarte zu inkrementieren),
- der signierte Hash-Wert,
- die Zeitangabe und
- ggf. die Terminerkennung

in einen zyklischen File eingetragen wird, wobei diese Information noch durch Freitextdaten wie z.B. die Kennung des signierten Dokumentes von außen ergänzt werden können muß. Diese Freitextdaten könnten z.B. im PSO: COMPUTE DS-Kommando in dem "Plain Value"-DO übergeben werden. Diese Leistungen stehen jedoch noch nicht zur Verfügung. Falls in der Chipkarte die Signatur-Protokollierungs-Datei vorhanden ist, wird daher der in 10.11 spezifizierte Kennsatz komplett außerhalb der Chipkarte zusammengestellt und dann in die Protokoll-Datei eingetragen.

Zuvor ist jedoch der letzte Protokolleintrag zu lesen, um diesem den aktuellen Signaturzählerstand entnehmen zu können. Bild 19 zeigt die Kommando-Sequenz zur Signatur-Protokollierung.

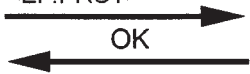
ICC Commands	Bedeutung
SELECT FILE <EF.PROT> 	Protokoll-Datei selektieren
READ RECORD 	Lesen eines Datensatzes
APPEND RECORD <Protocol data> 	Schreiben eines neuen Datensatzes

Bild 19: Kommandos zur Signatur-Protokollierung

17.2 Selektieren der Protokoll-Datei

Als erster Arbeitsschritt ist die Datei EF.PROT zu selektieren.

Tabelle 39: SELECT FILE Command zum Selektieren der Protokoll-Datei

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'A4' = SELECT FILE
P1	'02' = EF file selection
P2	'0C' = No FCI to be returned
Lc	'02' = Length of data field
Data field	FID of EF.PROT, see annex C
Le	Empty

Tabelle 40: SELECT FILE Response

Data field	Empty
SW1-SW2	'9000' or specific status bytes

17.3 Lesen und Schreiben eines Protokoll-Records

Zum Lesen des letzten Protokolleintrags ist folgendes Kommando zu verwenden:

Tabelle 41: READ RECORD Command zum Lesen eines Protokoll-Records

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'B2' = READ RECORD
P1	'01' = Record no. 1 (last written record)
P2	'04' = Read record P1
Lc	Empty
Data field	Empty
Le	'xx' = Length of record

Tabelle 42: READ RECORD Response

Data field	Protocol data
SW1-SW2	'9000' or specific status bytes

Weitere Protokoll-Records können durch Hochschalten der Record-Nummer in P1 gelesen werden.

Zum Schreiben eines Protokoll-Records ist folgendes Kommando zu verwenden: