

DIN EN 14890-1



ICS 35.240.15

**Anwendungsschnittstelle für Chipkarten, die zur Erzeugung
qualifizierter elektronischer Signaturen verwendet werden –
Teil 1: Allgemeine Dienste;
Deutsche Fassung EN 14890-1:2008**

Application Interface for smart cards used as Secure Signature Creation Devices –
Part 1: Basic services;
German version EN 14890-1:2008

Interface applicative des cartes à puces utilisées comme dispositifs de création de
signature numérique sécurisés –
Partie 1: Services de bases;
Version allemande EN 14890-1:2008

Gesamtumfang 203 Seiten

Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN

Nationales Vorwort

Dieses Dokument (EN 14890-1:2008) wurde vom Technischen Komitee CEN/TC 224 „Maschinenlesbare Karten und zugehörige Geräteschnittstellen und Verfahren“ erarbeitet, dessen Sekretariat vom AFNOR (Frankreich) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 043-01-17 AA „Karten und persönliche Identifikation“ im Normenausschuss Informationstechnik und Anwendung (NIA).

DIN EN 14890-1 ist Teil einer zweiteiligen Normenreihe zur Festlegung von Anwendungsschnittstellen für Chipkarten, die zur Erzeugung qualifizierter elektronischer Signaturen verwendet werden.

Die Normenreihe DIN EN 14890 liefert eine robuste Ausgangsbasis für die Schaffung europaweiter rechtlicher Rahmenbedingungen für elektronische Signaturen. Die Normenreihe DIN EN 14890 legt die Anforderungen an die Funktionalität und an die Sicherheit fest für Chipkarten, die gemäß der Europäischen Richtlinie 1999/93/EG als sichere Signaturerstellungseinheiten (Secure Signature Creation Device, SSCD) eingesetzt werden sollen.

DIN EN 14890 legt dabei verbindliche Basis-Anforderungen an ein SSCD fest, die der Erfüllung der allgemeinen IAS-Dienste (Identification, Authentication and Digital Signature) dienen können, wie sie von der Richtlinie 1999/93/EG gefordert werden.

DIN EN 14890-1 ersetzt das CEN Workshop Agreement CWA 14890-1:2004.

Die Teile 1 bis 4 der Vornormenreihe DIN V 66291 *Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV* sind als deutsche Beiträge zu den Europäischen Normen in DIN EN 14890-1 und DIN EN 14890-2 eingeflossen. Da die Vornormen gegenüber den Europäischen Normen zusätzliche für Implementierer nützliche Informationen nicht-normativen Charakters enthalten, wurden die Vornormen zunächst noch nicht zurückgezogen. Es gelten aber im Zweifelsfalle die Europäischen Normen.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN V 66291-1:2000-04, *Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV — Teil 1: Anwendungsschnittstelle*

DIN V 66291-2:2003-01, *Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV — Teil 2: Personalisierungs-Prozesse*

DIN V 66291-3:2003-07, *Chipkarten mit Digitaler Signatur - Anwendung/Funktion nach SigG und SigV — Teil 3: Personalisierungskommandos*

DIN V 66291-4:2002-04, *Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV — Teil 4: Grundlegende Sicherheitsdienste*

Deutsche Fassung

Anwendungsschnittstelle für Chipkarten, die zur Erzeugung
qualifizierter elektronischer Signaturen verwendet werden —
Teil 1: Allgemeine Dienste

Application Interface for smart cards used as Secure
Signature Creation Devices —
Part 1: Basic services

Interface applicative des cartes à puces utilisées comme
dispositifs de création de signature numérique sécurisés —
Partie 1: Services de bases

Diese Europäische Norm wurde vom CEN am 27. September 2008 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Management-Zentrum des CEN oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, Ungarn, dem Vereinigten Königreich und Zypern.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

Management-Zentrum: rue de Stassart, 36 B- 1050 Brüssel

Inhalt

	Seite
Vorwort	6
1 Anwendungsbereich	7
2 Normative Verweisungen	8
3 Begriffe	8
4 Symbole und Abkürzungen	11
5 Signaturanwendung	14
5.1 Anwendungsabfolge	14
5.2 Vertrauenswürdige Umgebung im Vergleich zu nicht vertrauenswürdiger Umgebung	15
5.3 Wahl der E-SIGN-Anwendung.....	16
5.3.1 Allgemeines	16
5.3.2 Ausnahmen für Secure Messaging	17
5.4 Wahl der kryptographischen Informationsanwendung	17
5.5 Gleichzeitige Nutzung von Signaturanwendungen	17
5.5.1 Allgemeines	17
5.5.2 Verfahren der Kanalwahl.....	17
5.5.3 Sicherheitsaspekte bei mehreren Kanälen	17
5.6 Wahl der Sicherheitsumgebung.....	17
5.7 Wahl des Schlüssels	18
5.8 Allgemeine Sicherheitsdienste.....	18
6 Benutzerüberprüfung	19
6.1 Allgemeines	19
6.2 Wissensbasierte Benutzerüberprüfung	19
6.2.1 Allgemeines	19
6.2.2 Explizite Benutzerüberprüfung	20
6.2.3 Passwortbezogene Parameter.....	20
6.2.4 Darstellungsformate	20
6.2.5 Wiederholungszähler	21
6.2.6 Änderung des Passworts.....	21
6.2.7 Zurücksetzen des Wiederholungszählers und Setzen eines neuen Passworts	22
6.3 Biometrische Benutzerüberprüfung	23
6.3.1 Allgemeines	23
6.3.2 Abrufen des Biometric Information Template	24
6.3.3 Durchführung der biometrischen Benutzerüberprüfung.....	25
6.3.4 Zurücksetzen des Wiederholungszählers	27
7 Digitaler Signaturdienst	27
7.1 Signaturerzeugungsalgorithmen	27
7.2 Aktivierung des digitalen Signaturdienstes.....	28
7.3 Allgemeine Aspekte.....	28
7.4 Signaturerzeugung	30
7.4.1 Kein Hashing in der Karte	30
7.4.2 Partielles Hashing	31
7.4.3 Sämtliches Hashing in der Karte.....	32
7.5 Wahl unterschiedlicher Schlüssel, Algorithmen und Eingabeformate	33
7.5.1 Wiederherstellen einer bestehenden SE	34
7.5.2 Modifizieren des HT einer aktuellen SE.....	34
7.5.3 Modifizieren des DST einer aktuellen SE	35
7.6 Zertifikate und zertifikatbezogene Informationen lesen	35
7.6.1 Zertifikatbezogene CIO lesen	36
7.6.2 Zertifikat des Unterzeichners aus der Chipkarte auslesen	36
7.6.3 Abrufen des Zertifikats des Unterzeichners aus einem Verzeichnisdienst.....	37

8	Geräteauthentisierung	37
8.1	Zertifizierungsinstanz und Zertifikate	38
8.1.1	Zertifikatketten	38
8.1.2	Verwendung von Cross-Zertifikaten	39
8.2	Authentisierungsumgebungen	40
8.2.1	SCA in vertrauenswürdiger Umgebung	40
8.2.2	SCA in nicht vertrauenswürdiger Umgebung	41
8.2.3	UmgebungsNorm	41
8.2.4	Anzeigetextmechanismus	41
8.2.5	Zusätzliche Authentisierungsumgebungen	42
8.3	Schlüsseltransport- und Schlüsselvereinbarungsmechanismus	42
8.4	Schlüsseltransportprotokoll auf der Grundlage von RSA	42
8.4.1	Authentisierungsschritte	44
8.4.2	Erstellung von Sitzungsschlüsseln	54
8.5	Geräteauthentisierung mit Schutz personenbezogener Daten	54
8.5.1	Authentisierungsschritte	55
8.6	„Modular EAC (mEAC)“-Protokoll mit Einschränkung im Hinblick auf den Schutz personenzogener Daten und mit Nichtbeweisbarkeitsmerkmal (auf der Grundlage elliptischer Kurven)	70
8.6.1	Beispiel für einen Beweisbarkeitsfall	70
8.6.2	Notation	71
8.6.3	Authentisierungsschritte	72
8.7	Asymmetrische Authentisierung — Zusammenfassung	84
8.8	Symmetrisches Authentisierungsschema	84
8.8.1	Authentisierungsschritte	84
8.8.2	Erstellung von Sitzungsschlüsseln	88
8.9	Sitzungsschlüssel aus dem Schlüsselmaterial (Key Seed) $K_{IFD/ICC}$ berechnen	89
8.9.1	TDES-Sitzungsschlüssel berechnen	89
8.9.2	AES-128-Sitzungsschlüssel für CBC-Modus und EMAC berechnen	90
8.9.3	AES-128-Sitzungsschlüssel für CBC-Modus und CMAC berechnen	90
8.10	Berechnung des Sendefolgezählers SSC	91
8.11	Postauthentisierungsphase	91
8.12	Beenden der sicheren Sitzung	91
8.12.1	Beispiel für das Beenden einer sicheren Sitzung	91
8.12.2	Regeln zum Beenden einer sicheren Sitzung	92
8.13	Lesen des Anzeigetextes	92
8.14	Aktualisieren des Anzeigetextes	94
9	Secure Messaging	95
9.1	CLA-Byte	96
9.2	TLV-Codierung der Befehls- und Antwortnachricht	96
9.3	Umgang mit Secure-Messaging-Fehlern	96
9.4	Padding zur Prüfsummenberechnung	96
9.5	Sendefolgezähler (SSC)	97
9.6	Nachrichtenaufbau von Secure-Messaging-APDU	97
9.6.1	Kryptogramme	97
9.6.2	Kryptographische Prüfsummen (CC)	100
9.6.3	Konstruktion der letzten Befehls-APDU	103
9.7	Schutz der Antwort-APDU	104
9.8	Verwendung von TDES und AES	110
9.8.1	Verschlüsselung/Entschlüsselung mit TDES/AES	110
9.8.2	CBC-Modus	111
9.8.3	Retail-MAC mit TDES	111
9.8.4	EMAC mit AES	112
9.8.5	CMAC mit AES	113
10	Schlüsselgenerierung	113
10.1	Schlüsselgenerierung und -export mittels PrK.ICC.AUT	114

10.2	Schlüsselerzeugung und -export mit dynamischem oder statischem Secure Messaging.....	114
10.3	Zertifikate schreiben.....	114
10.4	Setzen von Schlüsseln bei statischem Secure Messaging	114
11	Schlüsselbezeichner und -parameter.....	115
11.1	Schlüsselbezeichner (KID).....	115
11.2	Öffentliche Schlüsselparameter.....	115
11.3	DSA mit öffentlichen ELC-Schlüsselparametern	116
11.4	RSA-Diffie-Hellman-Schlüsselaustauschparameter	117
11.5	ELC-Schlüsselaustauschparameter	117
12	Datenstrukturen	117
12.1	CRT.....	117
12.1.1	CRT AT für die Wahl interner Authentisierungsschlüssel	118
12.1.2	CRT für die Wahl des PuK.CA _{IFD} .CS_AUT des Schnittstellengeräts	118
12.1.3	CRT für die Wahl des PuK.IFD.AUT des Schnittstellengeräts	118
12.1.4	CRT AT für die Wahl der öffentlichen DH-Schlüsselparameter	119
12.1.5	DH-Schlüsselparameter für GENERAL AUTHENTICATE.....	119
12.1.6	CRT AT zur Wahl des privaten Authentisierungsschlüssels der Chipkarte.....	119
12.1.7	CRT für die Wahl des PuK.IFD.AUT des Schnittstellengeräts	120
12.1.8	CRT für die Wahl von PrK.ICC.KA.....	120
12.2	Schlüsseltransport-Geräteauthentisierungsprotokoll	120
12.2.1	EXTERNAL AUTHENTICATE	121
12.2.2	INTERNAL AUTHENTICATE.....	121
12.3	Geräteauthentisierungsprotokoll mit Schutz personenbezogener Daten	122
12.3.1	EXTERNAL AUTHENTICATE	122
12.3.2	INTERNAL AUTHENTICATE.....	123
13	AlgID, Hash- und DSI-Formate	124
13.1	Algorithmusbezeichner und OID.....	124
13.2	Hash-Eingabeformate.....	126
13.2.1	PSO:HASH ohne Befehlsverkettung.....	127
13.2.2	PSO:HASH mit Befehlsverkettung	128
13.3	Formate von DSI (Digital Signature Input)	128
13.3.1	DSI nach ISO/IEC 14888-2 (scheme 2)	129
13.3.2	DSI nach PKCS #1 V 1.5	130
13.3.3	Digest-Info für SHA-X	131
13.3.4	DSI nach PKCS #1 V 2.x	133
13.3.5	DSA mit DH-Schlüsselparametern	134
13.3.6	Elliptic Curve Digital Signature Algorithm — ECDSA.....	134
14	CV-Zertifikate und Schlüsselverwaltung	134
14.1	Vertrauenswürdigkeit eines Zertifikats	135
14.2	Schlüsselverwaltung	135
14.3	Kartenverifizierbare Zertifikate.....	136
14.3.1	Signaturzertifikate.....	136
14.3.2	Authentisierungszertifikate	136
14.4	Verwendung des aus dem Zertifikat extrahierten öffentlichen Schlüssels	136
14.5	Gültigkeit des aus einem Zertifikat extrahierten Schlüssels	137
14.6	Aufbau des CVC.....	137
14.6.1	Nicht selbstbeschreibende Zertifikate.....	138
14.6.2	Selbstbeschreibende Zertifikate	138
14.7	Zertifikatinhalt	138
14.7.1	CPI — Zertifikatprofilbezeichner	139
14.7.2	CAR — Zertifizierungsinstanzreferenz	140
14.7.3	CHR — Zertifikatinhaberreferenz	141
14.7.4	CHA — Zertifikatinhaberberechtigung	142
14.7.5	Norm des Rollenbezeichners	143
14.7.6	CHAT — Template für Zertifikatinhaberberechtigung	146
14.7.7	OID — Objektbezeichner	146

14.7.8	CED — Gültigkeitsbeginn des Zertifikats	148
14.7.9	CXD — Ablaufdatum des Zertifikats	148
14.8	Zertifikatsignatur	149
14.8.1	Nicht selbstbeschreibende Zertifikate	149
14.8.2	Selbstbeschreibende Zertifikate	150
14.9	Codierung des Zertifikatinhalts	150
14.9.1	Nicht selbstbeschreibende Zertifikate	150
14.9.2	Selbstbeschreibende Zertifikate	151
14.9.3	Selbstbeschreibende Zertifikate für Kryptographie mit elliptischen Kurven.....	151
14.10	Schritte der CVC-Überprüfung	154
14.10.1	Erste Runde: CVC-Überprüfung von einem Root-PuK.....	155
14.10.2	Anschließende Runde(n)	156
14.11	Befehle zur Handhabung des CVC	156
14.12	C_CV.IFD.AUT (nicht selbstbeschreibend).....	156
14.13	C_CV.CA.CS_AUT (nicht selbstbeschreibend)	158
14.14	C.ICC.AUT	159
14.15	Selbstbeschreibende CV-Zertifikate (Beispiel)	159
14.15.1	Öffentlicher Schlüssel.....	160
15	Dateien.....	161
15.1	Dateiaufbau	161
15.2	Dateibezeichner	162
15.3	EF.DIR.....	163
15.4	EF.SN.ICC	163
15.5	EF.DH	164
15.6	EF.ELC	164
15.7	EF.C.ICC.AUT	165
15.8	EF.C.CA _{ICC} .CS-AUT	165
15.9	EF.C_X509.CH.DS.....	166
15.10	EF.C_X509.CA.CS (DF.ESIGN)	166
15.11	EF.DM.....	167
16	Kryptographische Informationsanwendung.....	167
16.1	Beispiel für den Aufbau der kryptographischen Informationen einer ESIGN-Anwendung.....	169
16.1.1	EF.CIAInfo	169
16.1.2	EF.AOD	170
16.1.3	EF.PrKD	173
16.1.4	EF.PuKD	175
16.1.5	EF.CD	176
16.1.6	EF.DCOD	177
Anhang A (informativ)	Geräteauthentisierung — Kryptographische Sicht	180
A.1	Algorithmen zur Authentisierung mit Schlüsselaustausch oder Schlüsselvereinbarung	180
A.2	Geräteauthentisierung mit Schlüsseltransport.....	180
A.2.1	Nach ISO/IEC 11770-3	180
A.2.2	Verwendung von min(SIG, N-SIG) für das Signatortoken	183
A.3	Geräteauthentisierung mit Schlüsselvereinbarung	184
A.3.1	Diffie-Hellman-Schlüsselaustausch	184
A.4	Geräteauthentisierung mit Schutz personenbezogener Daten	187
A.4.1	Authentizität der öffentlichen DH-Parameter.....	189
A.5	Geräteauthentisierung mit Nichtbeweisbarkeit.....	191
A.5.1	Diffie-Hellman-Schlüsselaustausch	191
A.6	Der „Grandmaster-Chess-Angriff“	193
Anhang B (informativ)	Personalisierungsszenarios	195
Anhang C (informativ)	Bildungsschema für mEAC-Objektbezeichner	197
Literaturhinweise		199

Vorwort

Dieses Dokument (EN 14890-1:2008) wurde vom Technischen Komitee CEN/TC 224 „Maschinenlesbare Karten und zugehörige Geräteschnittstellen und Verfahren“ erarbeitet, dessen Sekretariat vom AFNOR gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Juni 2009, und etwaige entgegenstehende nationale Normen müssen bis Juni 2009 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Texte dieses Dokuments Patentrechte berühren können. CEN [und/oder CENELEC] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Dieses Dokument ersetzt CWA 14890-1:2004.

Diese Norm stellt zusätzlich Dienste zur generischen Identifizierung, Authentisierung und Signaturerstellung (Identification, Authentication and Digital Signature, IAS) bereit und umfasst daher sämtliche zusätzlichen in CWA 14890-2 festgelegten Dienste.

Die Norm ermöglicht die Entwicklung interoperabler Karten, die von einem beliebigen Kartensektor ausgegeben werden. Sie beschreibt eine Anwendungsschnittstelle und das Verhalten von sicheren Signaturerstellungseinheiten (Secure Signature Creation Device, SSCD); eine Implementierung, z. B. in systemspezifische und interpreterbasierte Karten, sollte somit möglich sein.

Die Norm stimmt mit anderen im Rahmen der Europäischen Richtlinie 1999/93 entwickelten Europäischen Normen überein.

Diese Norm *Anwendungsschnittstelle für Chipkarten, die zur Erzeugung qualifizierter elektronischer Signaturen verwendet werden* besteht aus zwei Teilen:

- Teil 1: „Allgemeine Dienste“ beschreibt die obligatorischen Festlegungen für eine SSCD als Teil von generischen IAS-Diensten, die entsprechend den Anforderungen von Artikel 5.1 der Signaturrechtlinie zu verwenden sind;
- Teil 2: „Zusätzliche Dienste“ beschreibt die übrigen IAS-Dienste.

1 Anwendungsbereich

Teil 1 dieser Reihe legt die Anwendungsschnittstelle für Chipkarten während ihrer Verwendung zur Erzeugung gesicherter Signaturen entsprechend den Bedingungen der Europäischen Richtlinie 1999/93 über elektronische Signaturen zur Ermöglichung der Interoperabilität und Verwendung als sichere Signaturerstellungseinheiten (Secure Signature Creation Devices, SSCD) auf nationaler oder europäischer Ebene fest.

Dieses Dokument beschreibt die obligatorischen Dienste für die Verwendung von Chipkarten als SSCD auf der Grundlage von CEN CWA 14890 (alle Teile). Dazu gehören die Signierfunktion, das Speichern von Zertifikaten, die entsprechende Benutzerüberprüfung, die Einrichtung und Verwendung vertrauenswürdiger Pfade und Kanäle, Anforderungen an die Schlüsselerzeugung sowie die Zuteilung und das Format von Betriebsmitteln, die zur Ausführung dieser Funktionen erforderlich sind sowie entsprechende kryptographische Tokeninformationen.

Somit wird die Funktionalität von CWA 14890-1 in den folgenden Bereichen verbessert:

- Geräteauthentisierung mit elliptischen Kurven (Elliptic Curves, ELC) für bestehende asymmetrische Authentisierungsprotokolle (RSA Transport, Privacy Protocol);
- Verbesserung bestehender asymmetrischer Authentisierungsprotokolle aufgrund von Einschränkungen im Hinblick auf den Schutz personenbezogener Daten (Privacy) und Nichtbeweisbarkeit (Non-Traceability);
- kartenverifizierbare (Card Verifiable, CV) Zertifikatsformate (selbstbeschreibend) mit ELC für alle Arten von Authentisierungs- und Berechtigungsprotokollen;
- Tags für Secure Messaging (sichere Nachrichtenübermittlung) und Verwendung von Befehlen mit Odd-INS-Code entsprechend ISO/IEC 7816-4;
- weitere Hash-Algorithmen (SHA2-Familie) mit entsprechendem Objektbezeichner und Algorithmenreferenzen;
- Verwendung von AES in Authentisierungsprotokollen;
- Verwendung von AES für Secure Messaging.

Die folgenden Aspekte liegen außerhalb des Anwendungsbereichs dieser Norm:

- 1) die physikalischen, elektrischen und transportprotokollbezogenen Merkmale der Karte;
- 2) der externe Signaturerstellungsprozess und die Signaturumgebung;
- 3) die Elemente, die zur Überprüfung einer elektronischen Unterschrift erforderlich sind, die von einer als SSCD verwendeten Karte erzeugt wurde;
- 4) der Fehlerbehandlungsprozess.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ANMERKUNG Für zukünftige Implementierungen sind die jeweils aktuellsten Versionen der in Bezug genommenen Dokumente hinzuzuziehen; die folgende Auflistung bezieht sich auf Versionen der Dokumente, die bei Veröffentlichung dieser Norm EN 14890 galten.

EN ISO 3166-1:2006, *Codes für die Namen von Ländern und deren Untereinheiten — Teil 1: Codes für Ländernamen (ISO 3166-1:2006)*

ISO/IEC 7816-4:2005, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

ISO/IEC 7816-6, *Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange*

ISO/IEC 7816-8:2004, *Identification cards — Integrated circuit cards — Part 8: Commands for security operations*

ISO/IEC 7816-11:2004, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*

ISO/IEC 7816-15:2004, *Identification cards — Integrated circuit cards with contacts — Part 15: Cryptographic information application*

ISO/IEC 9796-2:2008, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*

ISO 11568-2:2005, *Banking — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*

ISO/IEC 14888-2:2008, *Information technology — Security techniques — Digital Signatures with appendix — Part 2: Integer factorization-based mechanisms*

ISO/IEC 15946-1, *Information Technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 1: General*

ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 7816-4:2005 und die folgenden Begriffe.

3.1

Answer-to-Reset-Datei

Elementardatei, die die Betriebsmerkmale der Karte angibt

3.2

Befehl-Antwort-Paar

Satz zweier Nachrichten: ein Befehl gefolgt von einer Antwort

3.3

Datenelement

Information, die an der Schnittstelle sichtbar ist und für die ein Name, eine Beschreibung des logischen Inhalts, ein Format und eine Codierung definiert sind

3.4

Datenobjekt

Information, die an der Schnittstelle sichtbar ist und die aus einem Tag, einer Länge und einem Wert besteht (d. h. ein Datenelement)

ANMERKUNG In dieser Norm werden Datenobjekte als BER-TLV-Datenobjekte bezeichnet.

3.5

Dateneinheit

kleinster Satz von Bits, der eindeutig referenziert werden kann

3.6

zugeordnete Datei

Datei, die Dateisteuerungsinformationen und wahlweise Speicher zur Zuteilung enthält

ANMERKUNG Eine zugeordnete Datei kann Parent von EF und/oder DF sein.

3.7

DF-Name

Byte-Strang, der eine zugeordnete Datei auf der Karte eindeutig kennzeichnet

3.8

Elementardatei

Satz von Dateneinheiten oder Datensätzen, die denselben Identifikator aufweisen

ANMERKUNG Eine Elementardatei kann nicht Parent einer anderen Datei sein.

3.9

Dateisteuerungsparameter

logische, aufbaubezogene und sicherheitsbezogene Attribute einer Datei

3.10

Identifikator

2-Byte-Binärwert zur Adressierung einer Datei

3.11

Masterdatei

obligatorisch eindeutig zugeordnete Datei, die die Wurzel des Dateiaufbaus darstellt

3.12

Nachricht

Bytestrang, der vom Schnittstellengerät zur Karte oder umgekehrt gesendet wird, ausgenommen übertragungsorientierte Zeichen nach ISO/IEC 7816-3

3.13

Parentdatei

zugeordnete Datei, die einer bestimmten Datei in der Hierarchie unmittelbar vorangeht

3.14

Passwort

Daten, die der Kartenbenutzer der Karte vorlegen muss, wenn von der Anwendung gefordert

ANMERKUNG Ein Passwort im Sinne dieser Norm ist ein Strang von Zahlen und/oder ASCII-Zeichen.

3.15

Pfad

Verkettung von Identifikatoren ohne Begrenzung

ANMERKUNG Wenn der Pfad mit dem Identifikator der Masterdatei beginnt, handelt es sich um einen absoluten Pfad.

3.16

privater Schlüssel

geheimer Teil eines asymmetrischen Schlüsselpaars, z. B. Signaturerstellungsdaten entsprechend der EG-Richtlinie über elektronische Signaturen

3.17

öffentlicher Schlüssel

öffentlicher Teil eines asymmetrischen Schlüsselpaars

3.18

Datensatz

Bytestrang, der von der Karte als Gesamtheit behandelt und durch eine Datensatznummer referenziert werden kann

3.19

Datensatznummer

laufende Nummer, die jedem Datensatz zugewiesen wird und die den Datensatz innerhalb seiner Elementardatei identifiziert

3.20

Wiederholungszähler

Zähler, der verwendet wird, um die Anzahl fehlerhafter Verwendungen eines entsprechenden (Sicherheits-)Objekts zu zählen

ANMERKUNG Wenn das Objekt (z. B. Passworteingabe) korrekt verwendet wurde (korrektes Passwort eingegeben), wird der Wiederholungszähler auf seinen Ausgangswert zurückgesetzt. Ein typischer Wert eines Wiederholungszählers ist 3.

3.21

geheimer Schlüssel

entweder ein symmetrischer Schlüssel oder ein privater Teil eines öffentlichen Schlüsselpaars

3.22

vertrauenswürdiger Kanal

Mittel, durch das eine TSF und ein vertrauenswürdiges fernes IT-Produkt mit dem erforderlichen Vertrauen kommunizieren können, um die TSP zu unterstützen

3.23

vertrauenswürdige Umgebung

Betriebsumgebung, die durch Definition ihrer physikalischen Lage, ihres physikalischen Schutzes oder ihrer physikalischen Zugriffsbedingungen oder sonstige Maßnahmen den Betrug mit den an der Kommunikationsschnittstelle sichtbaren Daten verhindert, um gegen Fälschung oder Einschleusen von Daten zu schützen

ANMERKUNG Siehe 8.2.3.

3.24

vertrauenswürdiger Pfad

Mittel, durch das ein Benutzer und eine TSF mit dem erforderlichen Vertrauen kommunizieren können, um die TSP zu unterstützen

3.25

nicht vertrauenswürdige Umgebung

Betriebsumgebung, die Fälschung und Einschleusen von an der Kommunikationsschnittstelle vorliegenden Daten zulässt

ANMERKUNG Die Entscheidung, ob eine Umgebung vertrauenswürdig ist, kann nicht immer auf Systemebene erfolgen und muss daher möglicherweise vom Karteninhaber getroffen werden.

3.26

Verwendungszähler

Zähler, der bei jeder Verwendung eines entsprechenden Objektes aktualisiert wird

ANMERKUNG Im Gegensatz zu Wiederholungszählern werden Verwendungszähler nicht auf ihren Ausgangswert zurückgesetzt, nachdem das Objekt erfolgreich verwendet wurde

4 Symbole und Abkürzungen

AES	Advanced Encryption Standard
AID	Anwendungsbezeichner (Application Identifier)
AKI	Instanzschlüsselbezeichner (Authority Key Identifier)
AKP	Asymmetrisches Schlüsselpaar (Asymmetric key pair)
APDU	Anwendungsprotokoll-Dateneinheit (Application protocol data unit)
AT	Authentisierungstemplate (Authentication Template), CRT für Authentisierung
AUT	Authentisierung (Authentication)
BCD	Binärcode für Dezimalziffern (Binary Coded Decimal)
BER	Basic Encoding Rules
C	Zertifikat (Certificate)
CA	Zertifizierungsinstanz (Certification Authority)
CAR	CA-Referenz (CA Reference)
CC	Kryptographische Prüfsumme (Cryptographic Checksum)
CG	Kryptogramm (Cryptogram)
CH	Karteninhaber (Cardholder)
CHA	Berechtigung des Zertifikatinhabers (Certificate Holder Authorization)
CHR	Zertifikatinhaberreferenz (Certificate Holder Reference)
CIA	Kryptographische Informationsanwendung (Cryptographic Information Application)
CIO	Kryptographisches Informationsobjekt (Cryptographic Information Object)
CLA	Klassenbyte (Class byte)
CPI	Zertifikatprofilbezeichner (Certificate Profile Identifier)
CRT	Control Reference Template
CS	CertSign, Zertifikat, das den öffentlichen Teil eines Signaturschlüsselpaars enthält
CV	Kartenverifizierbar (Card Verifiable)
CWA	CEN Workshop Agreement
C/S	Client/Server
D[key](msg)	Dechiffrierung (Decipherment) von <msg> mit <key>
DE	Datenelement (Data Element)
DES	Datenverschlüsselungsstandard (Data Encryption Standard)
DF	Zugeordnete Datei (Dedicated File)
DH	Diffie-Hellman
DIR	Verzeichnis (Directory)

DO	Datenobjekt (Data Object)
DS	Digitale Signatur (Digital Signature)
DSA	Digitaler Signaturalgorithmus (Digital Signature Algorithm)
DSI	Digitale Signatureingabe (Digital Signature Input)
DST	Template für digitale Signatur (Digital Signature Template), CRT für DS
E[key](msg)	Chiffrierung (Encipherment) von <msg> mit <key>
ECC	Europäische Bürgerkarte (European Citizen Card)
EDFB	Encrypted Data Formatted Block
EF	Elementardatei (Elementary File)
ELC	Kryptographie mit elliptischen Kurven (Elliptic Curve Cryptography)
FCI	Dateisteuerungsinformation (File Control Information)
FID	Identifikator (File Identifier)
h(msg)	Hash-Code von <msg>
HT	CRT für Hash-Code
ICC	Karte mit integrierten Schaltkreisen, Chipkarte (Integrated Circuit(s) Card)
ID	Bezeichner (Identifier)
IFD	Schnittstellengerät (Interface Device)
INS	Befehlsbyte (Instruction byte)
KE	Schlüsselchiffrierung (Key Encipherment)
KID	Schlüsselbezeichner (Key Identifier)
MAC[key](msg)	Nachrichtenauthentisierungscode (Message Authentication Code) von <msg>, erstellt mit <key>
MF	Masterdatei (Master File)
MSE	MANAGE SECURITY ENVIRONMENT
OID	Objektbezeichner (Object Identifier)
PI	Padding-Indikator (Padding Indicator)
PIN	Persönliche Identifikationsnummer (Personal Identification Number)
PKCS	Standards zur Verschlüsselung mit öffentlichem Schlüssel (Public Key Cryptography Standards)
PKI	Public-Key-Infrastruktur (Public Key Infrastructure)
PrK	Privater Schlüssel (Private Key)
PRND	Zufallspaddingzahl (Padding Random Number)
PSO	PERFORM SECURITY OPERATION
PSS	Probabilistisches Signatursystem (Probabilistic Signature Scheme)
PuK	Öffentlicher Schlüssel (Public Key)
P1-P2	Parameterbytes (Parameter bytes)
RC	Wiederholungszähler (Retry Counter)
RCA	RootCA
RD	Referenzdaten (Reference Data)
RFU	Für zukünftige Verwendung reserviert (Reserved for Future Use)

RID	Registrierter Bezeichner des Anwendungsanbieters (Registered application provider identifier)
RND	Zufallszahl (Random number)
RSA	Signatur-Algorithmus nach Rivest, Shamir, Adleman
SCA	Signaturerstellungsanwendung (Signature-Creation Application)
SE	Sicherheitsumgebung (Security Environment)
SHA	Sicherer Hash-Algorithmus (Secure Hash Algorithm)
SIG()	Signatur von
SK	Geheimer Schlüssel (Secret Key)
SM	Sichere Nachrichtenübermittlung (Secure Messaging)
SN	Laufende Nummer (Serial Number)
SSC	Sendefolgezähler (Send Sequence Counter)
SSCD	Sichere Signaturerstellungseinheit (Secure Signature Creation Device)
SW1-SW2	Statusbytes (Status bytes)
TDES	Triple-DES
TOE	Evaluierungsvorgabe (Target of evaluation)
TLV	Tag, Länge, Wert (Tag, Length, Value)
TSF	TOE-Sicherheitsfunktionen
TSP	TOE-Sicherheitsrichtlinien

5 Signaturanwendung

5.1 Anwendungsabfolge

Die folgenden Schaubilder veranschaulichen eine typische Anwendungsabfolge nach CWA 14170 [3].

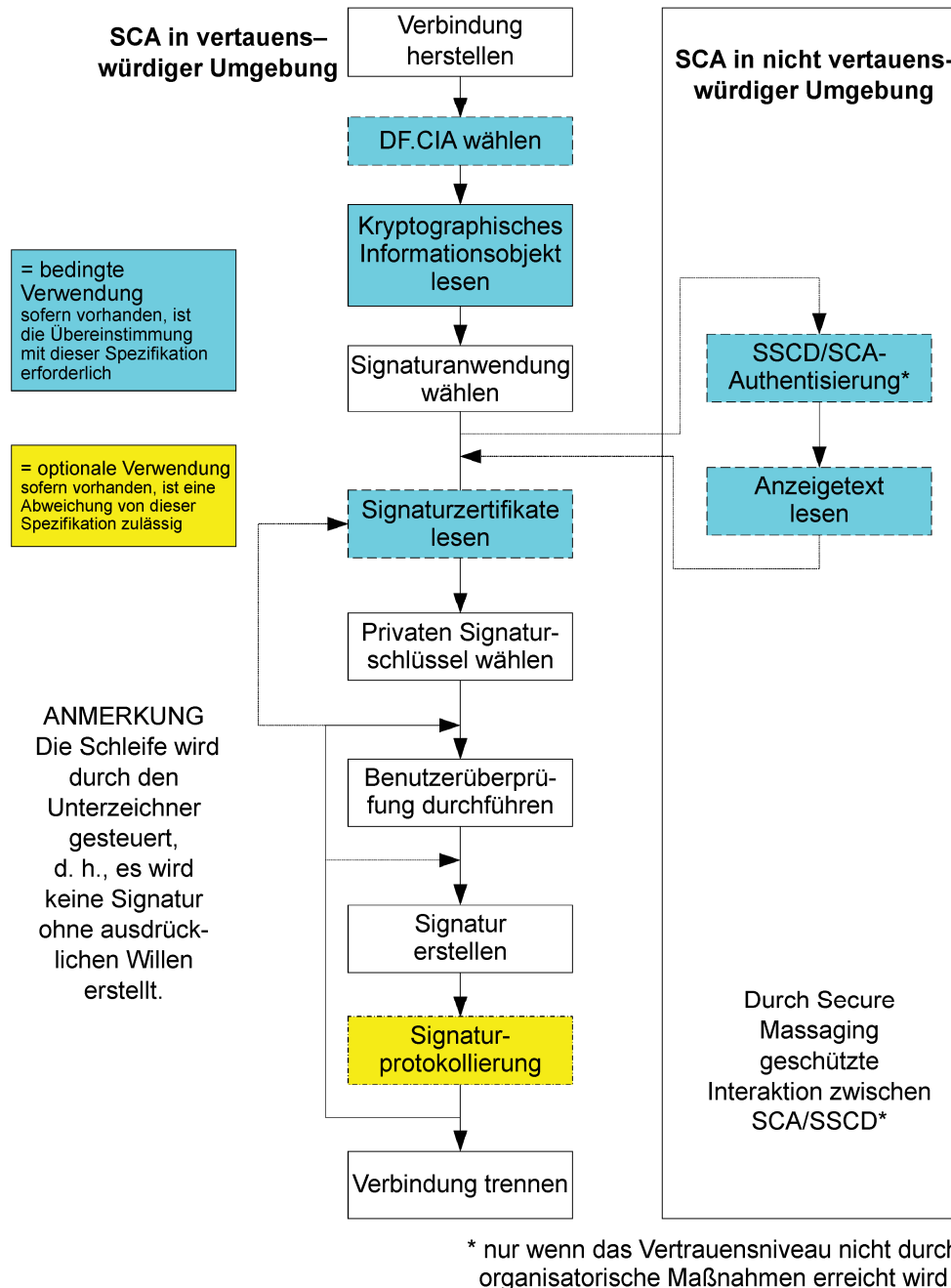


Bild 1 — Interaktionsfolgen zwischen SCA und SSCD in Übereinstimmung mit der EG-Richtlinie

ANMERKUNG Die Geräteauthentisierung kann alternativ vor der Wahl der Signaturanwendung erfolgen.



Das folgende Szenario zeigt die typische Befehlsabfolge beim Starten einer Anwendung.

5.3 Wahl der ESIGN-Anwendung

5.3.1 Allgemeines

Eine ESIGN-Anwendung wird von deren Anwendungsbezeichner (AID) gewählt [32]. Der RID wird von der ISO-Registrierungsstelle registriert und weist den folgenden Wert auf:

A0 00 00 01 67.

Der gesamte AID weist den folgenden Wert auf:

AID = A0 00 00 01 67 || "ESIGN" = A0 00 00 01 67 45 53 49 47 4E

Dabei ist

Category = 'A.....' (international)

PIX = 'ESIGN' = 5 Bytes

Tabelle 1 — SELECT-ESIGN-Anwendung — Befehls-APDU

Befehls-parameter	Bedeutung
CLA INS	nach ISO/IEC 7816-4 'A4' — SELECT
P1 P2	'04' nach DF-Namen wählen '00' oder '02' FCI-Information zurücksenden (siehe Bemerkung unten)
Lc-Feld	Länge des Befehlsdatenfeldes
Datenfeld	AID.ESIGN — Anwendungsbezeichner
Le-Feld	'xx' erwartete Länge der Antwort

Zur Beschreibung des SELECT-Befehls, siehe ISO/IEC 7816-4:2005, 7.1.1.

Bemerkungen:

P2 Es ist der jeweiligen Anwendung überlassen, andere festgelegte Werte aus ISO/IEC 7816-4 zu verwenden; die vorliegende Europäische Norm schreibt den Abruf der Dateisteuerungsinformationen nicht obligatorisch vor. JAVA-Karten erfordern jedoch P2 = '00' oder P2 = '02'.

Datenfeld Enthält den AID.ESIGN, wie oben beschrieben.

Tabelle 2 — SELECT-ESIGN-Anwendung — Antwort-APDU

Antwort-parameter	Bedeutung
Datenfeld	Daten nach P2. Eine FCI muss mindestens das DO '84' enthalten (DF-Name)
SW1-SW2	siehe ISO/IEC 7816-4

5.3.2 Ausnahmen für Secure Messaging

Im Fall einer Karte ohne eine MF muss der Befehl SELECT nach AID einer Anwendung vom Datenendgerät stets in Klartext ausgegeben werden, selbst wenn eine Secure-Messaging-Sitzung gerade aktiv ist. Bei derartigen Karten darf dieser Befehl SELECT nach AID in Klartext die (ggf. aktive) aktuelle Secure-Messaging-Sitzung nicht unterbrechen. Bei derartigen Karten ist dieses Verhalten erforderlich, um die Zuweisung einer Applet-Instanz zu einer Anwendung auf einer Java-Karte zu ermöglichen. Siehe 8.12.

5.4 Wahl der kryptographischen Informationsanwendung

Nach ISO/IEC 7816-15 weist die zu der ESIGN-Anwendung gehörende kryptographische Informationsanwendung (CIA) den folgenden AID auf:

AID.CIA_ESIGN = 'E8 28 BD 08 0F A0 00 00 01 67 || "ESIGN" (15 Byte)

Die Wahl der DF.CIA(ESIGN) erfolgt wie oben gezeigt mit einem DF-Namen.

5.5 Gleichzeitige Nutzung von Signaturanwendungen

5.5.1 Allgemeines

Die gleichzeitige Nutzung von Signaturanwendungen kann unter Verwendung der Mechanismen von logischen Kanälen nach ISO/IEC 7816-4 erreicht werden.

5.5.2 Verfahren der Kanalwahl

Der Mechanismus für die Wahl des Kanals ist freigestellt.

Ein Kanal kann wie folgt gewählt werden:

- implizit mit CLA-Byte des SELECT-Befehls;
- explizit mit dem Befehl MANAGE CHANNEL.

Beide Verfahren sind in ISO/IEC 7816-4 beschrieben und werden in der vorliegenden Europäischen Norm nicht erläutert.

5.5.3 Sicherheitsaspekte bei mehreren Kanälen

Um auf die Betriebsmittel der Chipkarte von einem anderen Kanal aus zuzugreifen, muss das 'shareable'-Bit (Bit für gemeinsame Nutzung) in der FCI der Anwendungs-DF gesetzt werden.

Jeder Aufruf einer ESIGN-Anwendung besitzt ihren eigenen Sicherheitsstatus.

5.6 Wahl der Sicherheitsumgebung

Eine Signaturkarte kann mehr als einen Authentisierungs- oder Signaturschlüssel und ein oder mehrere Benutzerreferenzdaten enthalten. In diesem Fall muss der FID die entsprechenden Schlüssel, die bei Authentisierungs- oder Signaturvorgängen und/oder der Benutzerüberprüfung beteiligt sein sollen, wählen (z. B. PIN, Passwort oder biometrische Daten). Der Befehl MANAGE SECURITY ENVIRONMENT (SET) (siehe ISO/IEC 7816-4:2005, 7.5.11) wird verwendet, um die bei dem nächsten Vorgang gewünschten Schlüssel festzulegen.

Eine Wahl der Sicherheitsumgebung mittels eines Befehls MSE:RESTORE ist bei folgenden Vorgängen anwendbar:

- Benutzerüberprüfung (PIN, Passwort oder biometrische Daten);
- Signaturerstellung nach Abschnitt 7;
- Geräteauthentisierung nach Abschnitt 8;
- Schlüsselerzeugung nach Abschnitt 10;
- Überprüfung von kartenverifizierbaren Zertifikaten nach Abschnitt 14;
- Authentisierungsdienste nach Abschnitt 6 von EN 14890-2:2008;
- Authentisierungsdienste nach Abschnitt 7 von EN 14890-2:2008;
- Schlüsseldechiffrierung nach Abschnitt 8 von EN 14890-2:2008;
- Signaturüberprüfung nach Abschnitt 9 von EN 14890-2:2008.

Die eigentliche Anwendung des Befehls MANAGE SECURITY ENVIRONMENT ist in den entsprechenden Abschnitten erläutert.

5.7 Wahl des Schlüssels

Die Wahl von Schlüsseln erfolgt mit dem Befehl MSE:SET, sofern nicht anders angegeben (z. B. in den Parametern des Befehls-Headers). Ein entsprechender Schlüsselbezeichner wird vorgelegt und in der Chipkarte gespeichert, um den mit dem (den) nächsten Befehl(en) zu verwendenden Schlüssel festzulegen. Die Wahl des Schlüssels muss vor einer Sicherheitsoperation erfolgen, sofern der Schlüssel nicht bereits zuvor gewählt wurde.

Ein Schlüsselbezeichner ist üblicherweise eine durch ein oder mehrere Bytes dargestellte Zahl, die einen nicht genormten anwendungs- oder betriebssystemspezifischen Wert beschreibt. Der FID kann die Verknüpfung zwischen einem Zertifikat und einem entsprechenden KeyID von den DF.CIA-Anwendungsdaten nach Abschnitt 16 abrufen.

5.8 Allgemeine Sicherheitsdienste

Ein allgemeiner Sicherheitsdienst ist im Gegensatz zu einem erweiterten Sicherheitsdienst ein Satz von SSCD-Funktionen, die der Signaturerzeugung, Überprüfung, Authentisierung oder Schlüsselchiffrierung/-dechiffrierung dienen.

Ein erweiterter Sicherheitsdienst umfasst die Installation von Daten und Schlüsseln, Lebenszyklusmanagement und sonstige Funktionen, die über den in der EU-Richtlinie [1] beschriebenen Anwendungsbereich hinausgehen.

In den beiden Teilen des vorliegenden Dokuments sind die folgenden allgemeinen Sicherheitsdienste festgelegt.

- **Benutzerüberprüfungsdienst**, siehe Abschnitt 6;
- **Schlüsselerzeugung**, siehe Abschnitt 10;
- **Geräteauthentisierungsdienst**, einschließlich Secure Messaging, siehe Abschnitt 8;

- **digitaler Signatordienst** für die fortgeschrittenen elektronischen Signatordienste des Karteninhabers, siehe Abschnitt 7;
- **Authentisierungsdienst**, der für bestimmte Authentisierungsprozeduren erforderlich ist, siehe Abschnitt 6 von EN 14890-2:2008;
- **Dechiffrierdienst für verschlüsselte Schlüssel**, siehe Abschnitt 8 von EN 14890-2:2008;
- **Signaturüberprüfungsdienst**, siehe Abschnitt 9 von EN 14890-2:2008.

6 Benutzerüberprüfung

6.1 Allgemeines

Die Benutzerüberprüfung ist Teil der in Bild 2 beschriebenen Anwendungsabfolge.

Es stehen drei allgemeine Verfahren der Benutzerüberprüfung zur Verfügung:

- wissensbasierte Benutzerüberprüfung (z. B. Passwort);
- biometrische Benutzerüberprüfung.

Es sind bestimmte lokale Überprüfungsdaten anzuwenden, die dazu bestimmt sind, die Verwendung des privaten Schlüssels zur Signaturerzeugung zu schützen. Wenn auf der Karte mehrere private Schlüssel zur Signaturerzeugung vorhanden sind, kann deren Verwendung wahlweise durch unterschiedliche Überprüfungsdaten geschützt werden.

Zum Schutz der Client/Server-Authentisierungsfunktion und der Schlüsseldechiffrierungsfunktion sind separate (je nach Sicherheitsrichtlinien globale oder lokale) Überprüfungsdaten zu verwenden.

In jedem dieser Fälle sind Änderungen der Überprüfungsdaten vorbehalten.

Zum Verwalten des Überprüfungsprozesses werden nach ISO/IEC 7816-4 die folgenden Befehle verwendet:

- VERIFY (Überprüfen);
- CHANGE REFERENCE DATA (Referenzdaten ändern);
- RESET RETRY COUNTER (Wiederholungszähler zurücksetzen).

Unabhängig von der Verwendung dieser Befehle ist jederzeit sicherzustellen, dass die Verwendung des Signaturschlüssels durch vorherige Benutzerüberprüfung geschützt ist.

ANMERKUNG Wenn wissensbasierte oder biometrische Benutzerüberprüfung Teil einer Common-Criteria-Bewertung ist, muss eine Strength-of-Funktion-Analyse (SOF-Analyse) durchgeführt werden. Die Bewertung eines wissensbasierten Mechanismus ist eine relativ einfache und hinreichend etablierte Wahrscheinlichkeitsanalyse. Bei biometrischen Authentisierungsmechanismen ist die SOF-Analyse komplexer, da z. B. für den Nachweis, dass eine beanspruchte False Acceptance Rate (FAR) eingehalten wird, eine umfassende Datenbank mit Fingerabdrücken erforderlich sein kann.

6.2 Wissensbasierte Benutzerüberprüfung

6.2.1 Allgemeines

Die wissensbasierte Benutzerüberprüfung erfordert die Eingabe eines Passwortes durch den Benutzer. Die eigentliche Überprüfung erfolgt mit dem Befehl VERIFY.

6.2.2 Explizite Benutzerüberprüfung

Bei europäischen Anwendungen sind Passwörter häufig auf Zahlen beschränkt. Daher werden sie auch als PIN bezeichnet. Zu weiteren Informationen, siehe 6.2.3.

Ausführungsabfolge 1 von 1

Tabelle 3 — VERIFY — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'20' VERIFY
P1	'00'
P2	<keyref> Passwortreferenz
Lc-Feld	Länge des Befehlsdatenfeldes
Datenfeld	<verification data>

Zu Aufbau und Codierung des Befehls VERIFY, siehe ISO/IEC 7816-4:2005, 7.5.6.

Tabelle 4 — VERIFY— Antwort-APDU

Antwortparameter	Bedeutung
Datenfeld	nicht vorhanden
SW1-SW2	siehe ISO/IEC 7816-4

6.2.3 Passwortbezogene Parameter

Passwortreferenzwert (beschrieben als Schlüsselbezeichner KID)

Der Parameter P2 codiert den Referenzwert des Passworts.

Diese Norm legt die folgenden KID fest:

KID = '8x' Schlüsselreferenz zu lokalen Referenzdaten zum Schutz der Verwendung eines privaten Signaturschlüssels (min. 6 Ziffern oder Zeichen); der Wert des KID und der Zweck des Signaturpassworts sind in den kryptographischen Informationsobjekten anzugeben.

Andere Passwörter können ebenfalls vom Typ „lokal“ sein.

KID = '0x' Schlüsselreferenz zu globalen Referenzdaten; der Wert des KID und der Zweck des Passworts sind in den kryptographischen Informationsobjekten anzugeben.

ANMERKUNG Um das Nebeneinander von EMV-Anwendungen und E-SIGN-Anwendungen auf derselben Chipkarte zu ermöglichen, sollten zur Unterscheidung von Schlüsseln nur die drei niedrigstwertigen Bits verwendet werden. Siehe EMV 2000, Integrated Circuit Card Specification for Payment Systems Book 3, „Application Specification Version 4.1“, Mai 2004 [11].

6.2.4 Darstellungsformate

Das Datenfeld codiert die Überprüfungsdaten in einem der folgenden Formate.

Das Passwort lautet '12345'

BCD-Codierung	<table><tr><td>12</td><td>34</td><td>5F</td></tr></table>	12	34	5F						
12	34	5F								
ASCII-Codierung	<table><tr><td>31</td><td>32</td><td>33</td><td>34</td><td>35</td></tr></table>	31	32	33	34	35				
31	32	33	34	35						
UTF8	<table><tr><td>31</td><td>32</td><td>33</td><td>34</td><td>35</td></tr></table>	31	32	33	34	35	bestimmte (z. B. sprach-spezifische) Zeichen unterscheiden sich von der ASCII-Codierung			
31	32	33	34	35						
Half-Nibble-BCD	<table><tr><td>F1</td><td>F2</td><td>F3</td><td>F4</td><td>F5</td></tr></table>	F1	F2	F3	F4	F5				
F1	F2	F3	F4	F5						
PIN in Format 2 PIN Block (siehe ISO 9564-1)	<table><tr><td>25</td><td>12</td><td>34</td><td>5F</td><td>FF</td><td>FF</td><td>FF</td><td>FF</td></tr></table>	25	12	34	5F	FF	FF	FF	FF	
25	12	34	5F	FF	FF	FF	FF			

Bild 3 — Beispiel für die Codierung von '12345' in unterschiedlichen Darstellungsformaten

Bild 3 zeigt die Codierung bei Verwendung der unterschiedlichen Darstellungsformate. Das tatsächliche Darstellungsformat kann aus in DF.CIA vorliegenden Informationen abgerufen werden (siehe Abschnitt 16), sofern es nicht implizit bekannt ist.

Passwörter, die die Verwendung von Signaturschlüsseln schützen, müssen mindestens 6 Ziffern oder Zeichen aufweisen. Alle übrigen Passwörter müssen mindestens 5 Ziffern oder Zeichen aufweisen.

ANMERKUNG Die Festlegungen stimmen mit entsprechenden Schutzprofilen überein, z. B. CEN CWA 14169 [2].

6.2.5 Wiederholungszähler

Um umfassende Suchangriffe zu vermeiden, muss das Passwort durch einen entsprechenden Wiederholungszähler geschützt sein.

Um einen umfassenden Suchangriff auf das Passwort unter einem bekannten Rücksetzcode zu vermeiden, sollte der Rücksetzcode durch einen entsprechenden Verwendungszähler mit einer Verwendungszählergrenze mit einem niedrigen Wert (üblicherweise $U = 3$) geschützt sein.

Nach erfolgreicher Vorlage wird der entsprechende Wiederholungszähler automatisch auf seinen Ausgangswert (üblicherweise $N = 3$) zurückgesetzt.

Zur Definition der Zählerarten, siehe Abschnitt 3.

6.2.6 Änderung des Passworts

Der Befehl CHANGE REFERENCE DATA zum Ändern des globalen Passworts kann vom Karteninhaber zu jedem beliebigen Zeitpunkt verwendet werden.

Die Änderung des DF-spezifischen (lokalen) Passworts kann nur nach Wahl der entsprechenden DF erfolgen.

Ausführungsabfolge 1 von 1

Tabelle 5 — Änderung des Passworts — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'24' CHANGE REFERENCE DATA
P1	'00' kein Algorithmus festgelegt
P2	['0x' '8x'] KID des referenzierten Passworts
Lc-Feld	Länge des Befehlsdatenfeldes
Datenfeld	<password> <new password>

Zur Beschreibung des Befehls, siehe ISO/IEC 7816-4:2005, 7.5.6.

Die Länge der vorhandenen Referenzdaten ist der Karte bekannt, daher ist weder ein Begrenzer noch Padding zum Auffüllen fester Formate erforderlich. Die Länge des neuen Passworts berechnet sich daher wie folgt: $L_{\text{neu}} = L_c - L_{\text{alt}}$.

Tabelle 6 — Änderung des Passworts — Antwort-APDU

Antwortparameter	Bedeutung
Datenfeld	nicht vorhanden
SW1-SW2	siehe ISO/IEC 7816-4

6.2.7 Zurücksetzen des Wiederholungszählers und Setzen eines neuen Passworts

Nach N (wobei N durch die Anwendung festgelegt ist) aufeinander folgenden falschen Eingaben des Passworts wird das Passwort gesperrt und lässt keine weitere Nutzung der geschützten Funktionen zu.

Mit dem Befehl RESET RETRY COUNTER nach ISO/IEC 7816-4 kann der Karteninhaber das Zurücksetzen des Wiederholungszählers RC auf seinen Ausgangswert N einleiten. Der Rücksetzcode muss eine Länge von mindestens 6 Ziffern¹⁾ aufweisen.

Es ist auch möglich, mit dem Befehl RESET RC ein neues Passwort zu definieren.

Das Zurücksetzen des DF-spezifischen (lokalen) Wiederholungszählers kann nur nach Wahl der entsprechenden DF erfolgen.

1) „Ziffer“ kann auch ein Zeichen als Teil eines Passworts sein.

Tabelle 7 — RESET RETRY COUNTER — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'2C' RESET RETRY COUNTER
P1	['00' .. '03']
P2	['0x' '8x'] KID des referenzierten Passworts
Lc-Feld	Länge des Befehlsdatenfeldes
Datenfeld	siehe unten

Zur Codierung des Befehls RESET RETRY COUNTER, siehe ISO/IEC 7816-4:2005, 7.5.10.

Der Inhalt des Datenfeldes hängt von dem Wert von P1 ab. Der Befehl RESET RETRY COUNTER darf den Sicherheitsstatus nicht ändern, d. h. zur Verwendung des Signaturerstellungsschlüssels ist der Befehl VERIFY dennoch erforderlich.

P1 = '00' Rücksetzcode, auf den ohne Begrenzung neue Referenzdaten folgen

P1 = '01' Rücksetzcode

P1 = '02' neue Referenzdaten

P1 = '03' Datenfeld nicht vorhanden

Tabelle 8 — Passwort ändern — Antwort-APDU

Antwortparameter	Bedeutung
Datenfeld	nicht vorhanden
SW1-SW2	siehe ISO/IEC 7816-4

Nach erfolgreicher Eingabe des Rücksetzcodes wird der Wiederholungszähler des referenzierten Passworts automatisch auf seinen Ausgangswert zurückgesetzt (üblicherweise $N = 3$).

6.3 Biometrische Benutzerüberprüfung

6.3.1 Allgemeines

Die Unterstützung einer biometrischen Benutzerüberprüfung (On-Card-Matching) ist freigestellt.

Es stehen zwei allgemeine Verfahren zur biometrischen Benutzerüberprüfung zur Verfügung:

- der Sensor befindet sich außerhalb der Karte (off-card), d. h., die Daten zur biometrischen Überprüfung werden vom Schnittstellengerät an die Karte gesendet;
- der Sensor befindet sich auf der Karte (on-card), sodass keine Notwendigkeit besteht, die Daten zur biometrischen Überprüfung von dem Schnittstellengerät an die Karte zu senden.

Wird eine biometrische Benutzerüberprüfung unterstützt und befindet sich der Sensor außerhalb der Karte, ist der Finger Minutiae Matcher (Einrichtung zum Abgleich von Fingerminutien) nach ISO/IEC 19794-2 zu verwenden. Das durch den CBEFF-Formattyp '0005' bezeichnete kompakte Fingerminutienformat ist als Codierungsformat für Fingerabdruckmerkmale (Minutien) anzuwenden.

Die Chipkarte muss dem Schnittstellengerät Informationen zu dem unterstützten Dienst zur biometrischen Überprüfung bereitstellen, und zwar unter Verwendung eines Biometric Information Template (Vorlage für biometrische Informationen, BIT) nach ISO/IEC 7816-11, das wie in Tabelle 14 dargestellt, zu codieren ist. Das BIT darf kein Datenobjekt für eine durch Tag '82' referenzierte Minutenreihenfolge enthalten, d. h., die Karte darf sich nicht auf eine durch das Schnittstellengerät vorgenommene Ordnung verlassen.

6.3.2 Abrufen des Biometric Information Template

Vor der Überprüfung benötigt die SCA möglicherweise folgende Informationen:

- AlgID des Abgleichsalgorithmus und Schlüsselreferenz der biometrischen Referenzdaten;
- Biometriotyp (z. B. Fingerabdruck);
- Biometriotypinstanz (z. B. linker Zeigefinger registriert);
- Formatinhaber der biometrischen Daten;
- Formattyp der biometrischen Daten;
- On-/Off-Card-Sensor.

Diese Informationen können der DF.CIA-Beschreibung entnommen werden (siehe Abschnitt 16).

Alternativ können diese Informationen in dem Biometric Information Template (BIT) bereitgestellt werden, siehe ISO/IEC 7816-11. Das BIT kann in dem DF.CIA vorliegen oder mit dem Befehl GET DATA abgerufen werden.

Der Registrierungsprozess für Fingerabdrücke liegt außerhalb des Anwendungsbereichs der vorliegenden Norm.

Tabelle 9 — Biometric Information Template(s) abrufen — Befehls-APDU (optional)

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'CA' GET DATA
P1-P2	'7F60' Beispiel: Biometric Information Template
Le-Feld	'00'

Zur Codierung des Befehls GET DATA, siehe ISO/IEC 7816-4:2005, 7.4.2.

Tabelle 10 — Biometric Information Template(s) abrufen — Antwort-APDU (optional)

Antwortparameter	Bedeutung
Datenfeld	BIT (Wertefeld des/der Biometric Information Template(s))
SW1-SW2	siehe ISO/IEC 7816-4

Zum Format des Biometric Information Template, siehe 6.3.3.2.

6.3.3 Durchführung der biometrischen Benutzerüberprüfung

6.3.3.1 Allgemeines

Es sind zwei Situationen zu unterscheiden:

- der Sensor befindet sich **außerhalb** der Karte (**Off-Card-Sensor**);
- der Sensor befindet sich **auf** der Karte (**On-Card-Sensor**).

Beindet sich der Sensor außerhalb der Karte, ist beim Ausführen von Befehlen zur biometrischen Benutzerüberprüfung Secure Messaging (siehe 9.6) erforderlich.

6.3.3.2 Off-Card-Sensor

Der Sensor befindet sich nicht auf der Chipkarte, d. h., die erfassten biometrischen Daten müssen zum On-Card-Matching an die Chipkarte gesendet werden.

Mit dem Befehl GET DATA nach 6.3.2 ruft das Schnittstellengerät das Biometric Information Template ab. Das entsprechende Pfadattribut in der kryptographischen Informationsanwendung bezeichnet die zugeordnete Datei, die vor diesem GET-DATA-Befehl zu wählen ist.

Zum Verarbeiten der entsprechend dem biometrischen Template aufgebauten biometrischen Daten verwendet das Schnittstellengerät dann einen VERIFY-Befehl.

Tabelle 11 — Biometrische Benutzerüberprüfung — Befehls-APDU (Biometrische Überprüfung)

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'21' VERIFY
P1	'00'
P2	'xx' Referenzdaten-Kennzeichner
Lc-Feld	Länge des Befehlsdatenfeldes
Datenfeld	<biometric data template>, siehe Tabelle 13

Zu Aufbau und Inhalt der APDU, siehe ISO/IEC 7816-4:2005, 7.5.6.

Tabelle 12 — Biometrische Benutzerüberprüfung 2 von 2 — Antwort-APDU

Antwortparameter	Bedeutung
Datenfeld	nicht vorhanden
SW1-SW2	siehe ISO/IEC 7816-4

6.3.3.3 Biometrische Templates

Tabelle 13 — Biometric Data Template

Tag	Länge	Wert		
'7F 2E'	variabel	Biometric Data Template		
		Tag	Länge	
		'81'	variabel	biometrische Daten mit genormtem Format (einfache Codierung)

Tabelle 14 — Biometric Information Template

Tag	Länge	Wert					Vorhanden- sein			
‘7F 60’	variabel	Biometric Information Template (BIT)								
		Tag	Länge	Wert						
		‘83’	‘01’	Referenzdaten-Kennzeichner				obligatorisch		
		‘A1’	variabel	Biometric Header Template (BHT) entsprechend CBEFF					obligatorisch	
				Tag	Länge	Wert				
				‘81’	‘01’	‘08’ (Fingerabdruck)			obligatorisch	
				‘82’	‘01’	biometrischer Untertyp (siehe ISO/IEC 7816-11:2004, Tabelle C.3)			obligatorisch	
				‘87’	‘02’	‘0101’ (ISO/IEC JTC 1)			obligatorisch	
				‘88’	‘02’	‘00 05’			obligatorisch	
				‘B1’	variabel	Parameter für den Algorithmus zum biometrischen Abgleich				optional
						Tag	Länge	Wert		
		‘81’	‘02’			Mindestanzahl erforderlicher Minuten (1 Byte, Binärcodierung) Höchstanzahl akzeptierter Minuten (1 Byte, Binärcodierung)				

6.3.3.4 On-Card-Sensor

Zur On-Card-Überprüfung wählt der Befehl VERIFY durch P2 die biometrische Datenreferenz.

Ausführungsabfolge

Tabelle 15 — Biometrische Überprüfung — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'21' VERIFY
P1	'00' kein Algorithmus festgelegt
P2	['0x' '8'x] KID des referenzierten Passworts bzw. der biometrischen Datenreferenz
Lc-Feld	Länge des Befehlsdatenfeldes
Datenfeld	'5F2E' '00' '4D' '00' leeres Überprüfungs-DO und DO der erweiterten Header-Liste

Zur Beschreibung des Befehls, siehe ISO/IEC 7816-4:2005, 7.5.6.

Die Länge der bestehenden Referenzdaten ist der Karte bekannt, sodass weder ein Begrenzer noch Padding zum Auffüllen fester Formate notwendig ist.

Tabelle 16 — Biometrische Überprüfung — Antwort-APDU

Antwortparameter	Bedeutung
Datenfeld	nicht vorhanden
SW1-SW2	siehe ISO/IEC 7816-4

Zu Aufbau und Inhalt der APDU, siehe ISO/IEC 7816-4:2005, 7.5.6.

6.3.4 Zurücksetzen des Wiederholungszählers

Zum Zurücksetzen des Wiederholungszählers, siehe 6.2.6.

Im Hinblick auf biometrische Referenzdaten sind in diesem Dokument nur die Varianten des Befehls RESET RETRY COUNTER festgelegt, die P1 = '01' und P1 = '03' verwenden. Die Verwendung der Befehlsvarianten mit P1 = '00' und P1 = '02' liegt außerhalb des Anwendungsbereichs dieses Dokuments, da der Registrierungsprozess nicht in diesem Dokument definiert ist.

7 Digitaler Signaturdienst

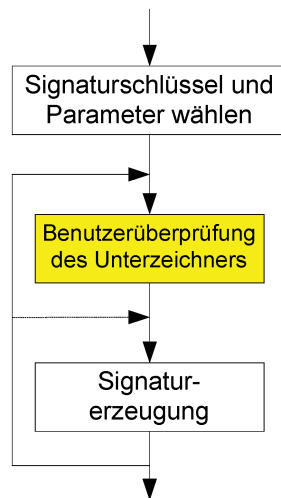
Dieser Abschnitt behandelt „qualifizierte elektronische Signaturen“ entsprechend der EG-Richtlinie 1999/EG, Artikel 5.1 [1].

7.1 Signaturerzeugungsalgorithmen

Zur Signaturerzeugung sind Algorithmen nach den aktuellen europäischen und nationalen Algorithmenkatalogen anzuwenden. Beispiele für bestehende Dokumente sind in [4], [5], [6], [7] und [8] angegeben.

7.2 Aktivierung des digitalen Signaturdienstes

Um den digitalen Signaturdienst zu aktivieren, muss vor der Signaturerzeugung die Benutzerüberprüfung erfolgen.



Anmerkung Der Kreis wird durch den Unterzeichner gesteuert, d. h., es wird keine Signatur ohne den ausdrücklichen Willen erstellt.

Bild 4 — Benutzerüberprüfung des Unterzeichners

Ein Überblick über den Signaturerzeugungsablauf ist in Bild 1 dargestellt.

Eine wissensbasierte Interaktion drückt stets den ausdrücklichen Willen des Karteninhabers, ein Dokument zu signieren, aus, wogegen eine biometrische Identifizierung nicht notwendigerweise die Absicht des Signierens ausdrückt. Daher ist die wissensbasierte Benutzerüberprüfung ein obligatorisches Merkmal, sofern der Anspruch dieser Norm nicht durch eine bestimmte Norm in einem entsprechenden Schutzprofil ersetzt wird.

Zur Beschreibung der Benutzerüberprüfung, siehe Abschnitt 6.

7.3 Allgemeine Aspekte

Der Prozess der Erzeugung einer digitalen Signatur besteht aus mehreren Schritten. Einige dieser Schritte erfolgen außerhalb der Chipkarte, einige innerhalb der Chipkarte, und einige können sowohl auf als auch außerhalb der Karte ausgeführt werden.

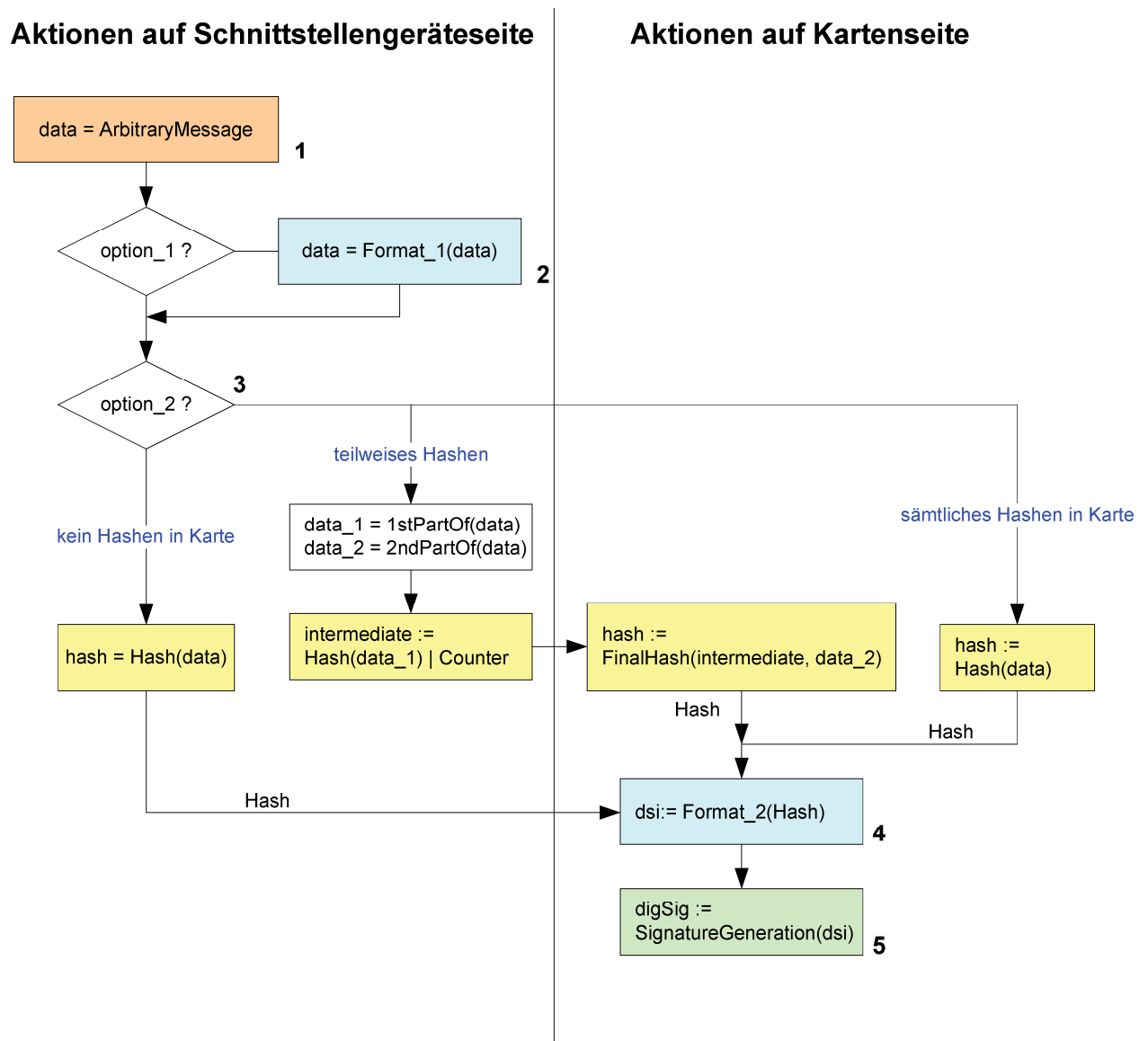


Bild 5 — Darstellung des Datenstroms für den Signaturerzeugungsprozess (RSA-Beispiel)

Bild 5 zeigt ein Beispiel der Alternativen bei der Verarbeitung eines Hash. Die Zahlen 1 bis 5 bezeichnen die unten beschriebenen Schritte. Der intermediäre Hash-Code ist der Digest der vorherigen Hash-Runde, gefolgt von dem Big-Endian-Bit-Count. Es werden nur vollständig gehashte Blöcke gesendet, daher ist die Länge von *data_1* (beim partiellen Hashen) stets ein Vielfaches der Digest-Größe, bezogen auf den angewendeten Algorithmus.

Grundsätzlich funktioniert der Signaturerzeugungsprozess wie folgt:

- 1) Der Signaturerzeugungsprozess beginnt mit einer arbiträren Nachricht.
- 2) Wahlweise ist die Ursprungsnachricht auf eine anwendungsspezifische Art und Weise formatiert. Üblicherweise werden der arbiträren Nachricht neben dem eigentlichen zu signierenden Dokument Signaturnattribute und sonstige Formatinformationen hinzugefügt. Der Prozess des Vorformatierens der zu hashenden Daten wird als **Format_1**-Mechanismus ausgedrückt. Die Norm des optionalen Format-Mechanismus **Format_1** liegt außerhalb des Anwendungsbereichs dieses Dokuments.

- 3) Die Daten sind zu hashen, indem eine Hash-Funktion aus der Liste der anwendbaren Hash-Funktionen angewendet wird. Der Hash-Code kann als eine komprimierte Version des Textes angesehen werden. In Abhängigkeit von *option_2* erfolgt das Hashen entweder:
- vollständig außerhalb der Chipkarte;
 - zum Teil außerhalb und zum Teil innerhalb der Chipkarte, die Daten werden somit in zwei Teile aufgeteilt;
 - vollständig innerhalb der Chipkarte, je nach Kartenfunktionalität und Softwareorganisation.
- 4) Je nach Signaturalgorithmus ist der *Hash-Code* durch einen Format-Mechanismus **Format_2** zu formatieren. Dabei handelt es sich üblicherweise um einen in 13.3 beschriebenen *Padding-Mechanismus*. Das Ergebnis dieser Formatierung ist ein *Digital Signature Input (dsi)*. Es wurden verschiedene Format-Mechanismen definiert; einige dieser Mechanismen sind als „schwach“ bewertet und sollten nicht verwendet werden. In den Algorithmenkatalogen sind diese Aspekte behandelt und Formatierungsschemata vorgeschlagen, die bis zu einem bestimmten Datum zugelassen sind.
- 5) Die endgültige *dsi* (Digital Signature Input) ist der durch den Signaturalgorithmus umzuwandelnde Strang. Das Ergebnis ist die digitale Signatur DS[<key>](*dsi*).

7.4 Signaturerzeugung

Je nachdem, welcher Datenpfad in Bild 5 verwendet wird, können aus Chipkartensicht folgende Fälle unterschieden werden.

7.4.1 Kein Hashing in der Karte

Die zu signierenden Daten werden vollständig außerhalb der Chipkarte gehasht. Je nach Algorithmus wird der *Hash-Code* durch den Befehl PSO:COMPUTE DIGITAL SIGNATURE an die Chipkarte übertragen und von dieser signiert.

Ausführungsabfolge 1 von 1

Tabelle 17 — Signaturberechnung (kein Hashing in Karte) — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'2A' PERFORM SECURITY OPERATION
P1	'9E' COMPUTE DIGITAL SIGNATURE
P2	'9A' 'data to be signed'
Lc-Feld	Länge des Befehlsdatenfeldes
Datenfeld	zu signierende Daten
Le-Feld	'00'

Zu Aufbau und Inhalt der APDU, siehe ISO/IEC 7816-8:2004, 5.8.

Das Antwortdatenfeld enthält die *Klartextsignatur* ohne weitere TLV-Codierung.

Tabelle 18 — Signaturberechnung (kein Hashing in Karte) — Antwort-APDU

Antwortparameter	Bedeutung
Datenfeld	Klartextsignatur ohne weitere TLV-Codierung
SW1-SW2	siehe ISO/IEC 7816-4

7.4.2 Partielles Hashing

Der erste Teil der zu signierenden Daten wird außerhalb der Chipkarte gehasht. Der intermediäre Hash-Code wird durch den Befehl PSO:HASH zusammen mit dem verbleibenden Teil der Daten an die Chipkarte übertragen. Anschließend wird die Signatur durch den Befehl PSO:COMPUTE DIGITAL SIGNATURE erzeugt.

Ausführungsabfolge 1 von 2

Tabelle 19 — Signaturberechnung 1 von 2 (intermediären Hash-Code übertragen) — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'2A' PERFORM SECURITY OPERATION
P1	'90' Hash
P2	'A0' Eingabe-Template für Hash-Berechnung
Lc-Feld	Länge des Befehlsdatenfeldes
Datenfeld	'90' L ₉₀ <intermediate hash-code followed by big endian bit counter> '80' L ₈₀ <data to be hashed>

Zu Aufbau und Inhalt der APDU, siehe ISO/IEC 7816-8:2004, 5.8.

Zum Inhalt des Befehlsdatenfeldes oder Datenobjekts 'A0', siehe 13.2.

Das Antwortdatenfeld ist nicht vorhanden.

Tabelle 20 — PSO Hash — Antwort

Antwortparameter	Bedeutung
Datenfeld	nicht vorhanden
SW1-SW2	siehe ISO/IEC 7816-4

Ausführungsabfolge 2 von 2

Der zweite Befehl führt eine digitale Signatur an dem gehashten Wert aus.

Tabelle 21 — Signaturberechnung 2 von 2 (Signatur berechnen) — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'2A' PERFORM SECURITY OPERATION
P1	'9E' COMPUTE DIGITAL SIGNATURE
P2	'9A' zu signierende Daten
Le-Feld	'xx'

Zu Aufbau und Inhalt der APDU, siehe ISO/IEC 7816-8:2004, 5.8.

Das Antwortdatenfeld enthält die Klartextsignatur ohne weitere TLV-Codierung.

Tabelle 22 — PSO:COMPUTE DIGITAL SIGNATURE — Antwort

Antwortparameter	Bedeutung
Datenfeld	Klartextsignatur
SW1-SW2	siehe ISO/IEC 7816-4

7.4.3 Sämtliches Hashing in der Karte

Die zu signierenden Daten werden in der Chipkarte gehasht. Dies erfolgt durch den Befehl PSO:HASH. Schließlich wird die Signatur durch den Befehl PSO:COMPUTE DIGITAL SIGNATURE erzeugt.

Ausführungsabfolge 1 von 2

Tabelle 23 — Signaturberechnung 1 von 2 (sämtliches Hashing in Chipkarte) — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'2A' PSO:HASH
P1	'90' Hash-Vorgang
P2	'80' Klarwert
Lc-Feld	'xx'
Datenfeld	zu hashende Klartextdaten

Zu Aufbau und Inhalt der APDU, siehe ISO/IEC 7816-8:2004, 5.8.

Das Antwortdatenfeld ist nicht vorhanden.

Tabelle 24 — Signaturberechnung 1 von 2 (sämtliches Hashing in Chipkarte) — Antwort-APDU

Antwortparameter	Bedeutung
Datenfeld	nicht vorhanden
SW1-SW2	siehe ISO/IEC 7816-4

Ausführungsabfolge 2 von 2

Im zweiten Schritt wird die digitale Signatur berechnet.

Tabelle 25 — Signaturberechnung 2 von 2 (Signatur berechnen) — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'2A' PERFORM SECURITY OPERATION
P1	'9E' COMPUTE DIGITAL SIGNATURE
P2	'9A' zu signierende Daten
Le-Feld	'00'

Zu Aufbau und Inhalt der APDU, siehe ISO/IEC 7816-8:2004, 5.8.

Das Antwortdatenfeld enthält die Klarsignatur ohne weitere TLV-Codierung.

Tabelle 26 — PSO COMPUTE DIGITAL SIGNATURE — Antwort

Antwortparameter	Bedeutung
Datenfeld	Klarsignatur
SW1-SW2	siehe ISO/IEC 7816-4
^a Im Falle eines ECDSA wird die digitale Signatur nach ISO/IEC 15946-1 berechnet; zum Format, siehe 5.3.	

7.5 Wahl unterschiedlicher Schlüssel, Algorithmen und Eingabeformate

Wenn die Karte mehr als einen Schlüssel unterstützt und eine implizite Wahl nicht zur Verfügung steht, ist der private Signaturschlüssel zu wählen.

Unterstützt die Karte verschiedene digitale Signaturalgorithmen oder unterschiedliche DSI-Formate (siehe Abschnitt 13), muss der Algorithmus bzw. das DSI-Format wählbar sein. Es ist jedoch möglich, dass z. B. ein Algorithmus implizit festgelegt ist, wenn ein Schlüssel gewählt wird.

Weiterhin ist es möglich, dass ein Algorithmus, ein Schlüssel oder ein Signatureingabeformat weder implizit bekannt noch eindeutig festgelegt ist.

In sämtlichen der oben genannten Fälle ist der geeignete Parameter explizit mit dem Befehl MANAGE SECURITY ENVIRONMENT nach ISO/IEC 7816-4:2005, 7.5.11 zu wählen.

Dies kann erreicht werden durch:

- Wiederherstellen einer bestehenden Sicherheitsumgebung SE (siehe 7.5.1);
- Modifizieren eines KeyID/[AlgID] in einem Template (siehe 7.5.3).

7.5.1 Wiederherstellen einer bestehenden SE

Ausführungsabfolge 1 von 1

Tabelle 27 — MANAGE SECURITY ENVIRONMENT — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'22' MANAGE SECURITY ENVIRONMENT
P1	'F3' RESTORE
P2	SE# Nummer der Sicherheitsumgebung

Zu Aufbau und Inhalt der APDU, siehe ISO/IEC 7816-4:2005, 7.5.11.

Das Antwortdatenfeld ist nicht vorhanden.

Tabelle 28 — MANAGE SECURITY ENVIRONMENT — Antwort

Antwortparameter	Bedeutung
Datenfeld	nicht vorhanden
SW1-SW2	siehe ISO/IEC 7816-4

ANMERKUNG Die tatsächliche SE# ist in Teil 2 dieser Norm beschrieben.

7.5.2 Modifizieren des HT einer aktuellen SE

Wenn ein Hash-Algorithmus der Chipkarte nicht implizit bekannt ist, ist dieser mit dem Befehl MANAGE SECURITY ENVIRONMENT zu wählen.

Ausführungsabfolge 1 von 1

Tabelle 29 — Hash-Template setzen — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'22' MANAGE SECURITY ENVIRONMENT
P1	'41' SET (Hash-Template nach p2)
P2	'AA' CRT für HT (Hash-Template)
Lc-Feld	'xx' Länge der folgenden Daten
Datenfeld	'80' L ₈₀ yy AlgId

Zu Aufbau und Inhalt der APDU, siehe ISO/IEC 7816-4:2005, 7.5.11.

Das Antwortdatenfeld ist nicht vorhanden.

Tabelle 30 — Hash-Template setzen — Antwort

Antwortparameter	Bedeutung
Datenfeld	nicht vorhanden
SW1-SW2	siehe ISO/IEC 7816-4

7.5.3 Modifizieren des DST einer aktuellen SE

Wenn ein Signierschlüssel der Chipkarte nicht implizit bekannt ist, ist dieser mit dem Befehl **MANAGE SECURITY ENVIRONMENT** zu wählen. Wahlweise kann ein Algorithmusbezeichner zu Verfügung gestellt werden, um Variationen des Algorithmus festzulegen (z. B. für Padding-Formate).

Ausführungsabfolge 1 von 1

Tabelle 31 — Wahl des Signaturschlüssels — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'22' MANAGE SECURITY ENVIRONMENT
P1	'41' SET für Signaturerstellung
P2	'B6' CRT für DST
Lc-Feld	'xx' Länge der folgenden Daten
Datenfeld	'84' L ₈₄ xx ['80' L ₈₀ yy] Key Id [AlgId]

Zu Aufbau und Inhalt der APDU, siehe ISO/IEC 7816-4:2005, 7.5.11.

Zum Algorithmusbezeichner, siehe Tabelle 143.

Das Antwortdatenfeld ist nicht vorhanden.

Tabelle 32 — Wahl des Signaturschlüssels — Antwort

Antwortparameter	Bedeutung
Datenfeld	nicht vorhanden
SW1-SW2	siehe ISO/IEC 7816-4

7.6 Zertifikate und zertifikatbezogene Informationen lesen

Ist in der Karte mehr als ein Signaturschlüssel vorhanden, muss der Benutzer möglicherweise den Signaturschlüssel für eine bestimmte Signaturerstellung wählen. In den Benutzerzertifikaten sind Felder vorhanden, in denen angegeben ist, ob es sich um ein privates oder geschäftliches Zertifikat handelt. Daher ist es ratsam, dass der Benutzer diese Felder auswertet, um das geeignete Zertifikat und den zugehörigen privaten Schlüssel zu wählen. In den CIO ist eine Verknüpfung zwischen einem Zertifikat und dem zugehörigen privaten Schlüssel enthalten sowie eine Angabe dazu, wo die Zertifikate zu finden sind (in der Karte oder auf einem Server); im letztgenannten Fall stellt die Karte eine URL und wahlweise eine laufende Nummer des Zertifikats bereit.

7.6.1 Zertifikatbezogene CIO lesen

Zertifikatbezogene CIO geben an, welche Zertifikate in der Chipkarte vorliegen oder auf einem Server zu finden sind und welcher private Schlüssel dem in dem Zertifikat vorhandenen öffentlichen Schlüssel entspricht (siehe Abschnitt 16).

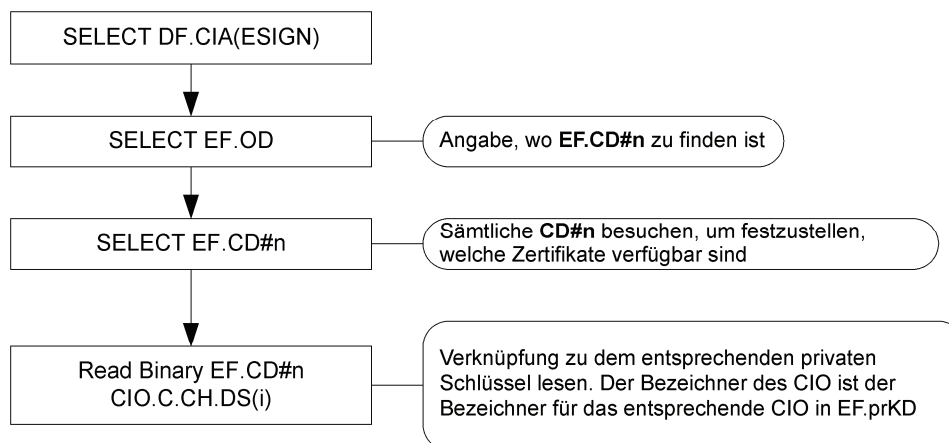


Bild 6 — Lesen von zertifikatbezogenen Informationen (Zertifikat liegt in der Chipkarte vor)

Die zertifikatbezogenen Informationen enthalten den Bezeichner für das entsprechende CIO in EF.PrKD, das den KeyID des betreffenden privaten Schlüssels enthält.

7.6.2 Zertifikat des Unterzeichners aus der Chipkarte auslesen

Sofern vorhanden, kann (können) die entsprechende(n) Zertifikatdatei(en) aus der Chipkarte ausgelesen werden. Zuvor muss die entsprechende Datei gewählt werden. Der Ort (z. B. Pfad oder (kurzer) FileID) ist in dem entsprechenden CIO in EF.CD#n angegeben.

Zertifikatbezogene Informationen sind in EF.C.CH.DS(i) gespeichert. Nach der Wahl von EF.C.CH.DS(i) entsprechend den in dem CIO.C.CH.DS(i) vorgefundenen Informationen können entweder das Zertifikat oder damit zusammenhängende Informationen aus der EF.C.CH.DS(i) ausgelesen werden.

Der tatsächliche für EF.C.CH.DS(i) zu erwartende Inhalt ist in DF.CIA beschrieben. Wenn keine andere Beschreibung zur Verfügung steht, dann enthält EF.C.CH.DS(i) das Zertifikat.

Ausführungsabfolge 1 von 1

Tabelle 33 — Zertifikat des Unterzeichners lesen — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'B0' READ BINARY
P1-P2	'xxxx' Offset
Le-Feld	'00' sämtliche Daten lesen

Das Antwortdatenfeld codiert den Dateninhalt von EF.C.CH.DS(i).

Tabelle 34 — Zertifikat des Unterzeichners lesen — Antwort-APDU

Antwortparameter	Bedeutung
Datenfeld	data.EF.C.CH.DS(i)
SW1-SW2	siehe ISO/IEC 7816-4

Die Befehls- und die Antwort-APDU sind in ISO/IEC 7816-4:2005, 7.2.3 beschrieben.

Der Aufbau und die Codierung von EF.C.CH.DS(i) ist üblicherweise ein X.509-Zertifikatformat, könnte jedoch auch ein anderes Format sein. Das tatsächliche Format ist anwendungsspezifisch und liegt außerhalb des Anwendungsbereichs dieser Norm.

ANMERKUNG Wenn die erwartete Länge die Länge des APDU-Antwortdatenfeldes überschreitet, muss READ BINARY möglicherweise mehrmals mit einem geeigneten Offset aufgerufen werden.

7.6.3 Abrufen des Zertifikats des Unterzeichners aus einem Verzeichnisdienst

Um das Zertifikat des Unterzeichners durch einen Verzeichnisdienst abzurufen, muss der Karteninhaber das Zertifikat eindeutig identifizieren. Diese Referenzwertinformationen können durch Auslesen des entsprechenden CIO.C.CH.DS aus der DF.CIA(ESIGN) nach Bild 6 abgerufen werden.

Nach ISO/IEC 7816-15:2004, 8.7.2 „X.509 certificate attributes“, enthält das entsprechende Datenobjekt CIO.C.CH.DS folgende Felder:

```
X509CertificateAttributes ::= SEQUENCE
{
  value ObjectValue { Certificate },
  subject Name OPTIONAL,
  issuer [0] Name OPTIONAL,
  serialNumber CertificateSerialNumber OPTIONAL,
  ... -- Für künftige Erweiterungen
}
```

Dabei gilt folgende Interpretation der Komponenten:

X509CertificateAttributes.value: Der Wert muss ein *referenzierter Wert* sein, der entweder eine Datei bezeichnet, die ein DER-codiertes Zertifikat an dem gegebenen Ort enthält, oder eine URL, die auf einen Ort verweist, an dem das Zertifikat vorzufinden ist [27].

8 Geräteauthentisierung

Dieser Abschnitt betrifft die Annahme/das Modell, dass eine Geräteauthentisierung durchgeführt wurde (werden muss). Jegliche Aussagen in diesem Abschnitt unterliegen dieser Annahme. Eine Norm für den Bedarf einer Geräteauthentisierung ist in 8.2 angegeben.

Die Geräteauthentisierung erfordert obligatorische Schritte, um eine sichere Authentisierung bereitzustellen. Eine Geräteauthentisierung erfolgt gegenseitig und kombiniert zwei Mechanismen:

- eine Chipkarte überprüft die externe Welt und wird von dieser ebenfalls überprüft;
- die Geräte handeln oder tauschen Informationen aus, um gemeinsame Sitzungsschlüssel (Session Keys) für anschließende Vorgänge zu erstellen.

Nach dem Aushandeln der symmetrischen Schlüssel wird eine sichere Sitzung eingerichtet. Eine sichere Sitzung ist ein kryptographischer Schutz der Nachrichten durch beide Seiten. Der kryptographische Schutz

kann eine kryptographische Prüfsumme an einem Klartext oder ein verschlüsselter Nachrichtentext sein. Siehe Abschnitt 9.

Aus Gründen der Leistungsfähigkeit sind die für diese sichere Nachrichtenübermittlung verwendeten Schlüssel symmetrische Schlüssel. Daher beschreibt dieses Dokument lediglich die Einrichtung symmetrischer Sitzungsschlüssel und behandelt nicht die Möglichkeit asymmetrischer Sitzungsschlüssel.

Nachdem die Sitzungsschlüssel eingerichtet wurden, steht ein vertrauenswürdiger Kanal zum Schutz oder Verbergen der über die Schnittstelle gesendeten Informationen zur Verfügung. Die Anwendung von Secure Messaging (SM) ist für **jeden anschließenden Vorgang obligatorisch**, um die Bereitstellung eines vollkommen vertrauenswürdigen Kanals sicherzustellen. Zu Ausnahmen, siehe 5.3.2. Die Bedingungen zum Beenden einer Secure-Messaging-Sitzung sind in 8.12 angegeben.

In diesem Dokument sind folgende Mechanismen zur Geräteauthentisierung beschrieben:

- Mechanismus für asymmetrischen Sitzungsschlüsseltransport auf der Grundlage von RSA;
- Mechanismus für asymmetrische Sitzungsschlüsselvereinbarung mit Schutz personenbezogener Daten;
- Mechanismus für asymmetrische Sitzungsschlüsselvereinbarung mit Nichtbeweisbarkeit und Schutz personenbezogener Daten auf der Grundlage von ELC;
- symmetrischer Authentisierungsmechanismus, um ein gegenseitiges Authentisierungsprotokoll zwischen Schnittstellengerät und Chipkarte auszuführen.

Die Darstellung der asymmetrischen Schemata erfolgt stufenweise, um die Sicherheitsmerkmale mit der erforderlichen Komplexität der Authentisierungsprotokolle zu behandeln.

ANMERKUNG 1 Authentisierung erfordert im Allgemeinen die Verarbeitung einer definierten Reihenfolge von Schritten. Wird gegen diese Reihenfolge verstoßen, kann dies dazu führen, dass der Vorgang durch die Chipkarte abgebrochen wird. Der Mechanismus zur Steuerung der ordnungsgemäßen Reihenfolge der Ausführungsschritte liegt außerhalb des Anwendungsbereichs dieser Norm.

ANMERKUNG 2 Das Schnittstellengerät stellt üblicherweise jede beliebige externe Schnittstelle bereit, die nicht besonders festgelegt ist.

8.1 Zertifizierungsinstanz und Zertifikate

8.1.1 Zertifikatketten

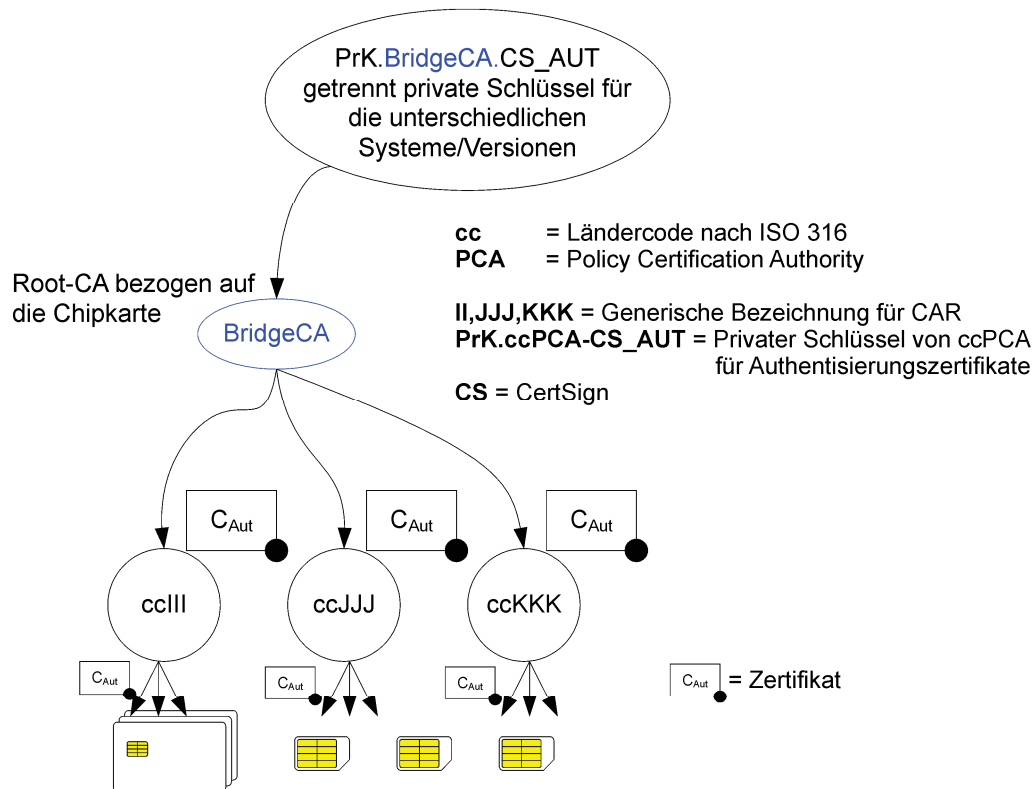
Eine asymmetrische Authentisierung erfordert die Vorlage von öffentlichen Schlüsseln in Zertifikaten. Möglicherweise ist eine Kette von Zertifikaten vorzulegen. Um den „Vertrauensbeginn“ festzulegen, muss das erste an die Chipkarte gesendete Zertifikat stets mit einem öffentlichen Schlüssel überprüfbar sein, der bereits in der Karte vorhanden ist. Der allgemeinste derartige Schlüssel kann ein öffentlicher Root-CA-Schlüssel sein. Jedes Zertifikat führt einen weiteren öffentlichen Schlüssel ein, während das vorgelegte Zertifikat stets mit einem der Chipkarte bekannten Schlüssel signiert wird.

Ein von einem Abkömmling von Root A signiertes Zertifikat, das einen öffentlichen Schlüssel transportiert, der ein Abkömmling von Root B ist, wird als Cross-Zertifikat bezeichnet (siehe 8.1.2). Die Verwendung von Cross-Zertifikaten ermöglicht die Verwendung der Chipkarte in unterschiedlichen Anwendungsumgebungen. Cross-Zertifikate sind auch im Hinblick auf Fragen zum Ablauf von Zertifikaten erforderlich.

Steht ein Root-Zertifikat zur Verfügung, so stellt die Root-CA Zertifikate für die untergeordneten CA zur Verfügung, oder es werden Cross-Zertifikate verwendet, um den (die) öffentlichen Schlüssel zu transportieren.

Untergeordnete CA stellen Zertifikate für Benutzer mit der entsprechenden E-Sign-Anwendung aus.

Die Karte ist der Träger des Chipkarten-Authentisierungszertifikats; Träger des Authentisierungszertifikats für das Schnittstellengerät könnte eine Steckkarte als Ausführungsbeispiel eines Authentisierungsmoduls in der SCA sein (siehe Bild 7).



Das vorstehende Beispiel wiederholt sich für jeden in der Karte vorhandenen RCA-Schlüssel.

8.1.2 Verwendung von Cross-Zertifikaten

Eine typische Verwendung von Cross-Zertifikaten ist die Verknüpfung einer bestehenden Zertifikatkette mit der bestehenden Freigabe eines öffentlichen Schlüssels.

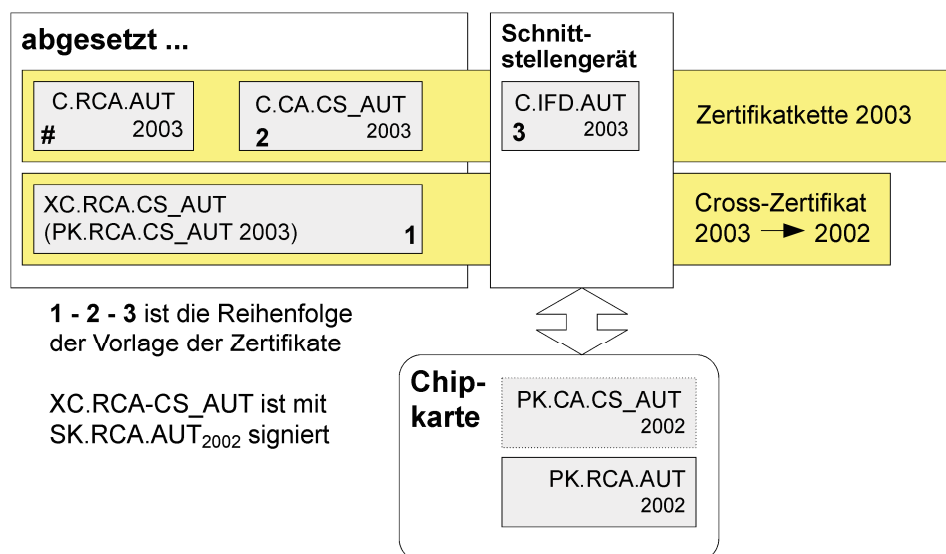


Bild 8 — Verwendung von Cross-Zertifikaten für unterschiedliche Schlüsselversionen

Das vorstehende Beispiel zeigt den an der Chipkarte verfügbaren PK.CA.CS_AUT(2002). Dieser Schlüssel wurde im Jahr 2002 auf die Karte gespielt, 2003 wurde jedoch der Root-Schlüssel geändert, und es wurde eine andere Schlüsselkette

PK.RCA.AUT(2003) → C.CA.CS_AUT(2003) → C.IFD.AUT(2003)

bei der Erzeugung des Zertifikats C.IFD.AUT(2003) des Schnittstellengeräts verwendet.

Um die Authentisierung des Schnittstellengeräts zu erlauben, muss die Chipkarte in dem oben stehenden Beispiel möglicherweise zunächst ein Cross-Zertifikat XC.RCA.CS_AUT(2003) empfangen. Dieses Zertifikat ist mit dem PrK.RCA.AUT(2002) signiert, transportiert jedoch den PuK.RCA.AUT(2003).

Nach Überprüfung des Cross-Zertifikats XC.RCA.CS_AUT(2003) kann die Chipkarte nun die Zertifikate der 2003er-Kette bis zum C.IFD.AUT empfangen, das den zur Authentisierung erforderlichen endgültigen öffentlichen Schlüssel trägt.

Die Chipkarte erkennt nicht, ob ein eintreffendes Zertifikat ein Cross-Zertifikat oder Teil einer Zertifikatkette ist. Wenn sie das eintreffende Zertifikat mit einem bestehenden öffentlichen Schlüssel überprüfen kann, akzeptiert sie den transportierten öffentlichen Schlüssel und kann diesen für die nächste Instanz der Kette verwenden. Der „Vertrauensbeginn“ wird stets mit dem ersten Zertifikat eingerichtet, das mit einem in der Chipkarte verfügbaren öffentlichen Schlüssel überprüft wird.

Beim Überprüfen eines Zertifikats muss der Überprüfende die korrekte Rolle des Unterzeichners überprüfen. Nur den Rollen, denen das Signieren von Zertifikaten erlaubt ist, darf die Vorlage einer Zertifikatkette gestattet werden. Die Rolle eines Zertifikats ist in 14 festgelegt.

8.2 Authentisierungsumgebungen

In [3] werden im Hinblick auf Signaturerstellungsanwendungen (SCA) zwei Umgebungen unterschieden.

8.2.1 SCA in vertrauenswürdiger Umgebung

Die Umgebung wird vom Benutzer als vertrauenswürdig eingestuft. Eine Geräteauthentisierung ist nicht erforderlich, da dem Karteninhaber die vertrauenswürdige Umgebung, in der er die Karte einsetzt, bekannt ist.

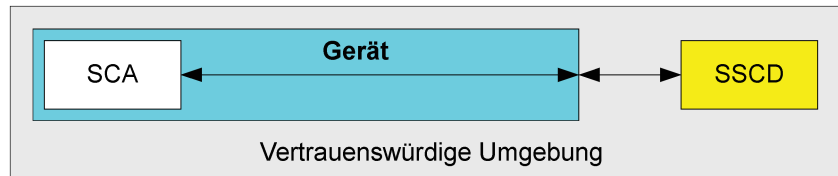


Bild 9 — Vertrauenswürdige Umgebung

In dieser Umgebung ist die im verbleibenden Abschnitt beschriebene Geräteauthentisierung freigestellt.

8.2.2 SCA in nicht vertrauenswürdiger Umgebung

Eine Geräteauthentisierung ist vorzunehmen, wenn der Betriebsumgebung der Karte nicht vollständig vertraut werden kann. Dies kann der Fall sein bei öffentlichen Signaturgeräten oder sonstigen Geräten, die keinen vertrauenswürdigen Kanal bereitstellen können.

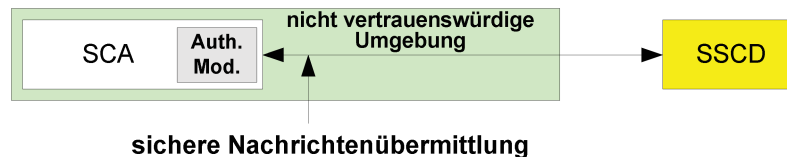


Bild 10 — Kommunikation in nicht vertrauenswürdige Umgebung

Die Geräteauthentisierung erfolgt gegenseitig. Die Chipkarte muss das Schnittstellengerät authentisieren und umgekehrt. Die Reihenfolge der Authentisierung kann jedoch je nach angewendetem Schema unterschiedlich sein.

Nach einer erfolgreichen Geräteauthentisierung stehen auf beiden Seiten Sitzungsschlüssel zur Verfügung, die in aufeinander folgenden Sendungen zu verwenden sind. Die entsprechende sichere Nachrichtenübermittlung erfolgt in Übereinstimmung mit ISO/IEC 7816-4 und ist in Abschnitt 9 beschrieben.

Beispiele für eine nicht vertrauenswürdige Umgebung sind:

- SCA und SSCD befinden sich nicht am gleichen Ort, d. h., die Karte ist abgesetzt;
- Verwendung von biometrischen Daten, wenn sich der Sensor außerhalb der Karte befindet;
- Verwendung kontaktloser Karten.

8.2.3 UmgebungsNorm

Ob eine Umgebung vertrauenswürdige ist oder nicht, kann von dem Schnittstellengerät nicht im Vorfeld beurteilt werden. Daher muss es dem Karteninhaber überlassen bleiben, ob er der Anwendungsumgebung vertrauen kann oder nicht. Die Einleitung einer Geräteauthentisierung in der Anwendungsumgebung liegt außerhalb des Anwendungsbereichs dieser Norm.

8.2.4 Anzeigetextmechanismus

Für den Fall, dass der Karteninhaber eine Geräteauthentisierung eingeleitet hat, schlägt diese Norm einen Mechanismus für einen Anzeigetext (Display Message) vor, um zu überprüfen, ob die Geräteauthentisierung erfolgreich durchgeführt wurde. In diesem Fall muss nach einer erfolgreichen Geräteauthentisierung ein Anzeigetext auf die erfolgreiche Geräteauthentisierung hinweisen, um den Benutzer über das Vorhandensein eines vertrauenswürdigen Kanals in Kenntnis zu setzen. Die Anwendung des Anzeigetexts ist in 8.13 beschrieben.

8.2.5 Zusätzliche Authentisierungsumgebungen

Eine Geräteauthentisierung kann außerdem angewendet werden bzw. erforderlich sein im Fall der Personalisierung mehrerer Instanzen (was jedoch nicht im Anwendungsbereich dieser Norm liegt).

8.3 Schlüsseltransport- und Schlüsselvereinbarungsmechanismus

Schlüsseltransport ist der Prozess des Übertragens eines von einer Instanz (oder einem Trusted Center, also einer vertrauenswürdigen Stelle) gewählten geheimen Schlüssels an eine andere Instanz, wobei geeigneterweise ein Schutz durch asymmetrische Verfahren zur Anwendung kommt. Der Schlüsseltransport erfordert die Verschlüsselung des Schlüsselteils; dies erfolgt üblicherweise mit dem öffentlichen Schlüssel der Gegenseite. In diesem Fall wird zur Einrichtung der sicheren Nachrichtenübermittlung ein Schlüsseltransport in beide Richtungen genutzt, um einen gemeinsamen Schlüssel in dem Schnittstellengerät und der Chipkarte zu erhalten.

Schlüsselvereinbarung ist der Prozess des Einrichtens eines gemeinsam genutzten geheimen Schlüssels zwischen zwei Instanzen A und B, und zwar so, dass keine der beiden Instanzen den Wert des gemeinsam genutzten geheimen Schlüssels vorhersagen kann. Schlüsselvereinbarungsmechanismen dürfen in die Geräteauthentisierung integriert werden.

Im Zusammenhang mit der Einrichtung von Sitzungsschlüsseln bedeutet „implizite Schlüsselaauthentisierung“, dass nach Ausführung des Mechanismus nur eine bezeichnete Instanz den korrekten, gemeinsam genutzten geheimen Schlüssel besitzen kann.

Diese Norm beschreibt die folgenden Protokolle:

- 8.4 „Schlüsseltransportprotokoll auf der Grundlage von RSA“;
- 8.5 „Geräteauthentisierung mit Schutz personenbezogener Daten“;
- 8.6 „Modular EAC (mEAC)“-Protokoll mit Einschränkung im Hinblick auf den Schutz personenbezogener Daten und mit Nichtbeweisbarkeitsmerkmal (auf der Grundlage elliptischer Kurven)
- 8.8 „Symmetrisches Authentisierungsschema“.

8.4 Schlüsseltransportprotokoll auf der Grundlage von RSA

Das Schlüsseltransportprotokoll stellt die Authentisierungsschritte für eine Zweifaktorenauthentisierung bereit. Das Protokoll wird bereits vor der Veröffentlichung von EN 14890-1 verwendet und in Normen zitiert; es wird für Implementierungen empfohlen, die eine Kompatibilität mit Systemen der externen Welt erfordern, welche dieses Schlüsseltransportprotokoll nutzen.

Es können drei Hauptphasen unterschieden werden:

- i) Austausch öffentlicher Schlüssel zwischen Chipkarte und Schnittstellengerät;
- ii) interne Authentisierung der Chipkarte;
- iii) externe Authentisierung des Schnittstellengeräts.

Die interne Authentisierung wird zuerst verarbeitet. Daher ist dieses Protokoll für Situationen vorteilhaft, in denen die Chipkarte vor dem Schnittstellengerät authentisiert werden sollte.

Die folgende Tabelle zeigt die Geräteauthentisierung mit Schlüsseltransport. Die Informationen in den Feldern sind vereinfacht dargestellt. Eine ausführliche Beschreibung der Codierung ist im Anschluss angegeben.

Tabelle 35 — Referenzgeräteauthentisierung mit Schlüsseltransport

Stufe	Schritt	Schnittstellengerät	Übertragung	Chipkarte
1	A	Wenn PuK.CA_{IFD}.CS_AUT in der Chipkarte verfügbar ist, mit Schritt D fortfahren.		
	B	PuK.RCA.AUT wählen und/oder überprüfen	→ ←	Schlüssel wählen und/oder überprüfen. Antwort OK.
	C	PSO:Verify Certificate C_CV.CA.CS_AUT	→ ←	Zertifikat überprüfen. PuK.CA _{IFD} .CS_AUT speichern. Antwort OK.
	D	PuK.CA _{IFD} .CS_AUT wählen und/oderüberprüfen	→ ←	Schlüssel wählen und/oderüberprüfen. Antwort OK.
	E	PSO:Verify Certificate C_CV.IFD.AUT	→ ←	Zertifikat überprüfen. PuK.IFD.AUT speichern. Antwort OK.
Der öffentliche Schlüssel des Schnittstellengeräts ist der Chipkarte nun bekannt und ist vertrauenswürdig.				
2	F	Wenn PuK.CA_{ICC}.CS_AUT in dem Schnittstellengerät vorliegt, mit Schritt H fortfahren.		
	G	READ BINARY von Datei EF.C.CA _{ICC} .CS_AUT ^a	→ ←	Dateien aus festgelegter Datei auslesen. C.CA.AUT liegt in Antwort-APDU vor.
	H	READ BINARY von Datei EF.C.ICC.AUT C.ICC.AUT überprüfen und PuK.ICC.AUT temporär speichern	→ ←	Dateien aus festgelegter Datei auslesen. C.ICC.AUT liegt in Antwort-APDU vor.
Der öffentliche Schlüssel der Chipkarte ist dem Schnittstellengerät nun bekannt und ist vertrauenswürdig				
3	I	MSE:SET KeyId(PrK.ICC.AUT) für Authentisierung ^b	→ ←	PrK der ESIGN-Anwendung wählen. Antwort OK.
		MSE:SET KeyId(PuK.IFD.AUT) für Verschlüsselung	→ ←	Antwort OK.
	J	INTERNAL AUTHENTICATE (C) Dabei ist C = RND.IFD SN.IFD Mit PrK.IFD.AUT entschlüsseln und Antwort der Chipkarte mit PuK.ICC.AUT überprüfen.	→ ←	ESIGN-Anwendung berechnet: SIG = DS[PrK.ICC.AUT] (... K _{ICC} h(... K _{ICC} C) ...)) E[PuK.IFD](min(SIG, N.ICC — SIG) C stammt aus dem Befehl Internal Authenticate

Tabelle 35 (fortgesetzt)

Stufe	Schritt	Schnittstellengerät	Übertragung	Chipkarte
Das Schnittstellengerät hat die Karte nun authentisiert.				
4	K	GET CHALLENGE	→ ←	RND.ICC
	L	EXTERNAL AUTHENTICATE IFD berechnet: SIG = DS[PrK.IFD.AUT] (... K_{IFD} $h(\dots K_{\text{IFD}} \mathbf{S})$...) E[PuK.ICC.AUT] (min(SIG, N.IFD — SIG)) mit $\mathbf{S} = \text{RND.ICC} \text{SN.ICC}$ SN.ICC wurde in dem Zertifikat von Schritt H empfangen.	→ → ←	Überprüfen, ob sich K_{IFD} von K_{ICC} unterscheidet. Signatur überprüfen. OK!
Die Zweizeigeauthentisierung ist nun abgeschlossen. Schlüsselableitung nach 8.4.2.				
^a Dieser Schritt ist nur erforderlich, wenn das Schnittstellengerät nicht den öffentlichen Schlüssel der CA besitzt. ^b Beide MSE-Befehle in diesem Schritt dürfen mit einem MSE-Befehl realisiert werden, der ein CRT mit beiden Schlüsselreferenzen sendet.				

8.4.1 Authentisierungsschritte

Folgende Schritte sind für die Authentisierung mit Schlüsseltransport von wesentlicher Bedeutung. Die angegebene Referenz schützt die Identität des Schnittstellengeräts, während zunächst die Chipkarte authentisiert wird.

8.4.1.1 Schritt A — Mit Authentisierung fortfahren (bedingt)

Wenn die PuK.CA_{IFD}.CS_AUT in der Chipkarte verfügbar ist, ist eine Ausführung der Schritte B bis C nicht erforderlich.

8.4.1.2 Schritt B — Wahl des Überprüfungsschlüssels PuK.RCA.AUT (bedingt)

Ist PuK.CA_{IFD}.CS_AUT nicht in der Chipkarte verfügbar, muss der Chipkarte eine Kette von (Cross-)Zertifikaten vorgelegt werden, um die Gültigkeit jedes Zertifikats zu bestätigen. Die Kette von Zertifikaten endet bei jedem Schlüssel, der in der Chipkarte verfügbar ist. Der letzte mögliche in der Chipkarte verfügbare Schlüssel ist der öffentliche Schlüssel der Root-CA mit der Bezeichnung PuK.RCA.AUT. Die Schritte B und C sind wiederholt auszuführen, bis der korrekte PuK.RCA.AUT in der Chipkarte verfügbar ist. Dieser Prozess wird als mehrstufige Überprüfung bezeichnet.

Die mehrstufige Überprüfung ist genau dann notwendig, wenn (a) die CA nicht die Root-CA ist (wenn es sich um die Root-CA handelt, ist der Schlüssel notwendigerweise in der Karte vorhanden) und (b) der entsprechende öffentliche Schlüssel der CA nicht in der Karte vorhanden ist.

Ausführungsabfolge

Tabelle 36 — Wahl des Root-Schlüssels — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'22' MANAGE SECURITY ENVIRONMENT
P1	'81' SET für Signaturüberprüfung
P2	'B6' CRT für DST
Lc-Feld	'xx'
Datenfeld	'80' L ₈₀ AlgId '83' L ₈₃ CRT(PuK.RCA.AUT <or other key in chain>)

Zu Aufbau und Inhalt der APDU, siehe ISO/IEC 7816-4:2005, 7.5.11.

Der Aufbau und die Codierung der Schlüsselreferenzdaten sind in 12.1.2 festgelegt.

Das Antwortdatenfeld bleibt leer.

Tabelle 37 — Wahl des Root-Schlüssels — Antwort

Antwortparameter	Bedeutung
Datenfeld	leer
SW1-SW2	siehe ISO/IEC 7816-4

8.4.1.3 Schritt C — Zertifikat C_CV.CA.CS_AUT überprüfen (bedingt)

Bei der mehrstufigen Überprüfung wird das Zertifikat des öffentlichen Schlüssels C_CV.CA.CS_AUT einer CA mit dem Befehl VERIFY CERTIFICATE an die Karte gesendet. Die Chipkarte überprüft dieses Zertifikat mit dem im vorangegangenen Schritt gewählten Schlüssel. Schlägt die Überprüfung fehl, antwortet die Chipkarte mit einer entsprechenden Rückmeldung. Bei Erfolg speichert die Chipkarte den in dem Zertifikat enthaltenen PuK und erlaubt ein weiteres Importieren von Zertifikaten.

Die Rolle des Zertifikats muss mit seinem Unterzeichner übereinstimmen. Die Wahl von PuK.RCA kann stets zur Überprüfung eines verketteten Zertifikats akzeptiert werden. Jeder weitere Schlüssel, der mit Zertifikat importiert wurde, darf nur angewendet werden, wenn die Rolle seines Zertifikats mit dem Zweck der Überprüfung des nächsten eintreffenden Zertifikats übereinstimmt.

Ausführungsabfolge

Tabelle 38 — CA-Zertifikatüberprüfung — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'2A' PERFORM SECURITY OPERATION
P1	'00' Antwortdatenfeld nicht vorhanden
P2	'AE' VERIFY CERTIFICATE
Lc-Feld	'xx'
Datenfeld	C_CV.CA.CS_AUT relevante Datenfelder des Zertifikats

Zu Aufbau und Inhalt der APDU, siehe ISO/IEC 7816-8:2004, 5.8.

Der Aufbau des Zertifikats ist in 14.15 festgelegt. Das Senden des Zertifikats erfolgt jedoch ohne den Tag '7F21' entsprechend den Beispielen in ISO/IEC 7816-8:2004, A.3. Es werden nur die relevanten Datenobjekte aus dem Wertefeld des in 14.14 beschriebenen Zertifikats gesendet. Diese Datenobjekte dürfen mit Befehlsverkettung gesendet werden.

Das Antwortdatenfeld bleibt leer.

Tabelle 39 — CA-Zertifikatüberprüfung — Antwort

Antwortparameter	Bedeutung
Datenfeld	leer
SW1-SW2	siehe ISO/IEC 7816-4

Die Chipkarte muss Beweise dafür überprüfen, dass die Rolle für den PuK des Schnittstellengeräts entweder dem Signieren eines weiteren (anschließend gesendeten) Zertifikats oder dem Authentisierungsmechanismus entspricht. Die Rolle (siehe Abschnitt 14) ist Teil des Zertifikats, wenn die PuK importiert wird. Die Rolle des zuletzt mit VERIFY CERTIFICATE importierten PuK ist in der Chipkarte bis zur Ausführung des Befehls EXTERNAL AUTHENTICATE zum Zweck der Überprüfung zu speichern.

8.4.1.4 Schritt D — Wahl des Überprüfungsschlüssels PuK.CA_{IFD}.AUT

Ausführungsabfolge

Tabelle 40 — Schlüsselreferenz für Zertifikatüberprüfung wählen — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'22' MANAGE SECURITY ENVIRONMENT
P1	'81' SET für Überprüfung
P2	'B6' DST
Lc-Feld	'xx'
Datenfeld	'80' L ₈₀ AlgId '83' L ₈₃ CRT(PuK.CA _{IFD} .CS_AUT)

Zu Aufbau und Inhalt der APDU, siehe ISO/IEC 7816-4:2005, 7.5.11.

Der Aufbau und die Codierung der Schlüsselreferenzdaten sind in 12.1.2 festgelegt.

Das Antwortdatenfeld bleibt leer.

Tabelle 41 — Schlüsselreferenz für Zertifikatüberprüfung wählen — Antwort

Antwortparameter	Bedeutung
Datenfeld	leer
SW1-SW2	siehe ISO/IEC 7816-4

8.4.1.5 Schritt E — Zertifikat C_{CV}.IFD.AUT überprüfen

Das Schnittstellengerät sendet zusammen mit dem Befehl VERIFY CERTIFICATE ein kartenverifizierbares (card verifiable, CV) Zertifikat C_{CV}.IFD.AUT. Die Chipkarte überprüft das Zertifikat unter Verwendung des öffentlichen Schlüssels PuK.CA_{IFD}.CS_AUT der Zertifizierungsinstanz CA.

Das Zertifikat enthält den PuK_{IFD}.AUT des Schnittstellengeräts, der von der Chipkarte temporär gespeichert wird.

Ausführungsabfolge

Tabelle 42 — Überprüfung des Zertifikats des Schnittstellengeräts — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'2A' PERFORM SECURITY OPERATION
P1	'00' Antwortdatenfeld nicht vorhanden
P2	'AE' VERIFY CERTIFICATE
Lc-Feld	'xx'
Datenfeld	C_CV.IFD.AUT Authentisierungszertifikat des Schnittstellengeräts

Zu Aufbau und Inhalt der APDU, siehe ISO/IEC 7816-8:2004, 5.8.

Der Aufbau des Zertifikats ist in 14.14 festgelegt. Das Senden des Zertifikats erfolgt jedoch ohne den Tag '7F21' entsprechend den Beispielen in ISO/IEC 7816-8, A.3. Es werden nur die relevanten Datenobjekte aus dem Wertefeld des in 14.14 beschriebenen Zertifikats gesendet. Diese Datenobjekte dürfen mit Befehlsverkettung gesendet werden.

Das Antwortdatenfeld bleibt leer.

Tabelle 43 — Überprüfung des Zertifikats des Schnittstellengeräts — Antwort

Antwortparameter	Bedeutung
Datenfeld	leer
SW1-SW2	siehe ISO/IEC 7816-4

Zur Verwendung in anschließenden Authentisierungsschritten speichert die Chipkarte den Schlüssel zusammen mit Identifikationsdaten zum Erkennen des Schlüssels, wenn dies in einer MSE:SET-APDU festgelegt ist, an einem temporären Ort. Die CHA ist zu speichern, um die Rolle des Schlüssels zur weiteren Verwendung zu identifizieren. Siehe 14.

Die Ausführungsabfolge des Befehls VERIFY CERTIFICATE ist in 14.12 dargestellt.

Nach Schritt E ist der öffentliche Authentisierungsschlüssel PuK.IFD.AUT des Schnittstellengeräts vertrauenswürdig.

8.4.1.6 Schritt F — Lesen von Kettenzertifikaten überspringen

Wenn der öffentliche Schlüssel PuK.CA_{ICC}.CS_AUT in dem Schnittstellengerät verfügbar ist oder anders als durch Auslesen aus der Chipkarte erhalten werden kann, kann Schritt G übersprungen werden.

8.4.1.7 Schritt G — C.CA_{ICC}.AUT lesen (bedingt)

Das Schnittstellengerät erhält PuK.CA_{ICC}.CS_AUT durch Auslesen von C.CA_{ICC}.CS_AUT aus einer Datei EF.C.CA_{ICC}.AUT in der Chipkarte. Anschließend überprüft es das Zertifikat C.CA_{ICC}.CS_AUT und extrahiert und speichert den öffentlichen Schlüssel PuK.CA_{ICC}.CS_AUT temporär zur Verwendung in Schritt H.