

# DIN EN 14890-1:2009-03 (D)

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

---

Inhalt	Seite
Vorwort .....	6
1 Anwendungsbereich .....	7
2 Normative Verweisungen .....	8
3 Begriffe .....	8
4 Symbole und Abkürzungen .....	11
5 Signaturanwendung .....	16
5.1 Anwendungsabfolge .....	16
5.2 Vertrauenswürdige Umgebung im Vergleich zu nicht vertrauenswürdiger Umgebung .....	17
5.3 Wahl der E-SIGN-Anwendung .....	18
5.3.1 Allgemeines .....	18
5.3.2 Ausnahmen für Secure Messaging .....	19
5.4 Wahl der kryptographischen Informationsanwendung .....	19
5.5 Gleichzeitige Nutzung von Signaturanwendungen .....	19
5.5.1 Allgemeines .....	19
5.5.2 Verfahren der Kanalwahl .....	19
5.5.3 Sicherheitsaspekte bei mehreren Kanälen .....	19
5.6 Wahl der Sicherheitsumgebung .....	19
5.7 Wahl des Schlüssels .....	20
5.8 Allgemeine Sicherheitsdienste .....	20
6 Benutzerüberprüfung .....	21
6.1 Allgemeines .....	21
6.2 Wissensbasierte Benutzerüberprüfung .....	21
6.2.1 Allgemeines .....	21
6.2.2 Explizite Benutzerüberprüfung .....	22
6.2.3 Passwortbezogene Parameter .....	22
6.2.4 Darstellungsformate .....	22
6.2.5 Wiederholungszähler .....	23
6.2.6 Änderung des Passworts .....	23
6.2.7 Zurücksetzen des Wiederholungszählers und Setzen eines neuen Passworts .....	24
6.3 Biometrische Benutzerüberprüfung .....	25
6.3.1 Allgemeines .....	25
6.3.2 Abrufen des Biometric Information Template .....	26
6.3.3 Durchführung der biometrischen Benutzerüberprüfung .....	27
6.3.4 Zurücksetzen des Wiederholungszählers .....	29
7 Digitaler Signaturdienst .....	29
7.1 Signaturerzeugungsalgorithmen .....	29
7.2 Aktivierung des digitalen Signaturdienstes .....	30
7.3 Allgemeine Aspekte .....	30
7.4 Signaturerzeugung .....	32
7.4.1 Kein Hashing in der Karte .....	32
7.4.2 Partielles Hashing .....	33
7.4.3 Sämtliches Hashing in der Karte .....	34
7.5 Wahl unterschiedlicher Schlüssel, Algorithmen und Eingabeformate .....	35
7.5.1 Wiederherstellen einer bestehenden SE .....	36
7.5.2 Modifizieren des HT einer aktuellen SE .....	36
7.5.3 Modifizieren des DST einer aktuellen SE .....	37
7.6 Zertifikate und zertifikatbezogene Informationen lesen .....	37
7.6.1 Zertifikatbezogene CIO lesen .....	38

7.6.2	Zertifikat des Unterzeichners aus der Chipkarte auslesen .....	38
7.6.3	Abrufen des Zertifikats des Unterzeichners aus einem Verzeichnisdienst.....	39
8	Geräteauthentisierung .....	39
8.1	Zertifizierungsinstanz und Zertifikate.....	40
8.1.1	Zertifikatketten .....	40
8.1.2	Verwendung von Cross-Zertifikaten.....	41
8.2	Authentisierungsumgebungen.....	42
8.2.1	SCA in vertrauenswürdiger Umgebung .....	42
8.2.2	SCA in nicht vertrauenswürdiger Umgebung.....	43
8.2.3	UmgebungsNorm.....	43
8.2.4	Anzeigetextmechanismus.....	43
8.2.5	Zusätzliche Authentisierungsumgebungen.....	44
8.3	Schlüsseltransport- und Schlüsselvereinbarungsmechanismus .....	44
8.4	Schlüsseltransportprotokoll auf der Grundlage von RSA.....	44
8.4.1	Authentisierungsschritte .....	46
8.4.2	Erstellung von Sitzungsschlüsseln .....	56
8.5	Geräteauthentisierung mit Schutz personenbezogener Daten.....	56
8.5.1	Authentisierungsschritte .....	57
8.6	„Modular EAC (mEAC)“-Protokoll mit Einschränkung im Hinblick auf den Schutz personenzbezogener Daten und mit Nichtbeweisbarkeitsmerkmal (auf der Grundlage elliptischer Kurven).....	72
8.6.1	Beispiel für einen Beweisbarkeitsfall .....	72
8.6.2	Notation .....	73
8.6.3	Authentisierungsschritte .....	74
8.7	Asymmetrische Authentisierung — Zusammenfassung.....	86
8.8	Symmetrisches Authentisierungsschema .....	86
8.8.1	Authentisierungsschritte .....	86
8.8.2	Erstellung von Sitzungsschlüsseln .....	90
8.9	Sitzungsschlüssel aus dem Schlüsselmaterial (Key Seed) $K_{IFD/ICC}$ berechnen.....	91
8.9.1	TDES-Sitzungsschlüssel berechnen .....	91
8.9.2	AES-128-Sitzungsschlüssel für CBC-Modus und EMAC berechnen .....	92
8.9.3	AES-128-Sitzungsschlüssel für CBC-Modus und CMAC berechnen .....	92
8.10	Berechnung des Sendefolgezählers SSC .....	93
8.11	Postauthentisierungsphase.....	93
8.12	Beenden der sicheren Sitzung .....	93
8.12.1	Beispiel für das Beenden einer sicheren Sitzung .....	93
8.12.2	Regeln zum Beenden einer sicheren Sitzung.....	94
8.13	Lesen des Anzeigetextes .....	94
8.14	Aktualisieren des Anzeigetextes.....	96
9	Secure Messaging .....	97
9.1	CLA-Byte.....	98
9.2	TLV-Codierung der Befehls- und Antwortnachricht .....	98
9.3	Umgang mit Secure-Messaging-Fehlern.....	98
9.4	Padding zur Prüfsummenberechnung .....	98
9.5	Sendefolgezähler (SSC) .....	99
9.6	Nachrichtenaufbau von Secure-Messaging-APDU .....	99
9.6.1	Kryptogramme .....	99
9.6.2	Kryptographische Prüfsummen (CC) .....	102
9.6.3	Konstruktion der letzten Befehls-APDU.....	105
9.7	Schutz der Antwort-APDU .....	106
9.8	Verwendung von TDES und AES .....	112
9.8.1	Verschlüsselung/Entschlüsselung mit TDES/AES.....	112
9.8.2	CBC-Modus .....	113
9.8.3	Retail-MAC mit TDES.....	113
9.8.4	EMAC mit AES.....	114
9.8.5	CMAC mit AES .....	115
10	Schlüsselgenerierung .....	115
10.1	Schlüsselgenerierung und -export mittels PrK.ICC.AUT .....	116

10.2	Schlüsselerzeugung und -export mit dynamischem oder statischem Secure Messaging .....	116
10.3	Zertifikate schreiben .....	116
10.4	Setzen von Schlüsseln bei statischem Secure Messaging.....	116
11	Schlüsselbezeichner und -parameter.....	117
11.1	Schlüsselbezeichner (KID) .....	117
11.2	Öffentliche Schlüsselparameter .....	117
11.3	DSA mit öffentlichen ELC-Schlüsselparametern .....	118
11.4	RSA-Diffie-Hellman-Schlüsselaustauschparameter .....	119
11.5	ELC-Schlüsselaustauschparameter .....	119
12	Datenstrukturen.....	119
12.1	CRT .....	119
12.1.1	CRT AT für die Wahl interner Authentisierungsschlüssel .....	120
12.1.2	CRT für die Wahl des PuK.CA <sub>IFD</sub> .CS_AUT des Schnittstellengeräts.....	120
12.1.3	CRT für die Wahl des PuK.IFD.AUT des Schnittstellengeräts .....	120
12.1.4	CRT AT für die Wahl der öffentlichen DH-Schlüsselparameter.....	121
12.1.5	DH-Schlüsselparameter für GENERAL AUTHENTICATE .....	121
12.1.6	CRT AT zur Wahl des privaten Authentisierungsschlüssels der Chipkarte .....	121
12.1.7	CRT für die Wahl des PuK.IFD.AUT des Schnittstellengeräts .....	122
12.1.8	CRT für die Wahl von PrK.ICC.KA .....	122
12.2	Schlüsseltransport-Geräteauthentisierungsprotokoll.....	122
12.2.1	EXTERNAL AUTHENTICATE .....	123
12.2.2	INTERNAL AUTHENTICATE .....	123
12.3	Geräteauthentisierungsprotokoll mit Schutz personenbezogener Daten.....	124
12.3.1	EXTERNAL AUTHENTICATE .....	124
12.3.2	INTERNAL AUTHENTICATE .....	125
13	AlgID, Hash- und DSI-Formate .....	126
13.1	Algorithmusbezeichner und OID .....	126
13.2	Hash-Eingabeformate .....	128
13.2.1	PSO:HASH ohne Befehlsverkettung .....	129
13.2.2	PSO:HASH mit Befehlsverkettung.....	130
13.3	Formate von DSI (Digital Signature Input).....	130
13.3.1	DSI nach ISO/IEC 14888-2 (scheme 2).....	131
13.3.2	DSI nach PKCS #1 V 1.5.....	132
13.3.3	Digest-Info für SHA-X.....	133
13.3.4	DSI nach PKCS #1 V 2.x.....	135
13.3.5	DSA mit DH-Schlüsselparametern.....	136
13.3.6	Elliptic Curve Digital Signature Algorithm — ECDSA .....	136
14	CV-Zertifikate und Schlüsselverwaltung.....	136
14.1	Vertrauenswürdigkeit eines Zertifikats .....	137
14.2	Schlüsselverwaltung.....	137
14.3	Kartenverifizierbare Zertifikate .....	138
14.3.1	Signaturzertifikate .....	138
14.3.2	Authentisierungszertifikate .....	138
14.4	Verwendung des aus dem Zertifikat extrahierten öffentlichen Schlüssels.....	138
14.5	Gültigkeit des aus einem Zertifikat extrahierten Schlüssels .....	139
14.6	Aufbau des CVC .....	139
14.6.1	Nicht selbstbeschreibende Zertifikate .....	140
14.6.2	Selbstbeschreibende Zertifikate .....	140
14.7	Zertifikatinhalt.....	140
14.7.1	CPI — Zertifikatprofilbezeichner.....	141
14.7.2	CAR — Zertifizierungsinstanzreferenz.....	142
14.7.3	CHR — Zertifikatinhaberreferenz.....	143
14.7.4	CHA — Zertifikatinhaberberechtigung .....	144
14.7.5	Norm des Rollenbezeichners .....	145
14.7.6	CHAT — Template für Zertifikatinhaberberechtigung .....	148
14.7.7	OID — Objektbezeichner .....	148
14.7.8	CED — Gültigkeitsbeginn des Zertifikats .....	150
14.7.9	CXD — Ablaufdatum des Zertifikats.....	150
14.8	Zertifikatsignatur .....	151
14.8.1	Nicht selbstbeschreibende Zertifikate .....	151

14.8.2	Selbstbeschreibende Zertifikate .....	152
14.9	Codierung des Zertifikatinhalts .....	152
14.9.1	Nicht selbstbeschreibende Zertifikate .....	152
14.9.2	Selbstbeschreibende Zertifikate .....	153
14.9.3	Selbstbeschreibende Zertifikate für Kryptographie mit elliptischen Kurven .....	153
14.10	Schritte der CVC-Überprüfung .....	156
14.10.1	Erste Runde: CVC-Überprüfung von einem Root-PuK .....	157
14.10.2	Anschließende Runde(n) .....	158
14.11	Befehle zur Handhabung des CVC .....	158
14.12	C_CV.IFD.AUT (nicht selbstbeschreibend) .....	158
14.13	C_CV.CA.CS_AUT (nicht selbstbeschreibend) .....	160
14.14	C.ICC.AUT .....	161
14.15	Selbstbeschreibende CV-Zertifikate (Beispiel) .....	161
14.15.1	Öffentlicher Schlüssel .....	162
15	Dateien .....	163
15.1	Dateiaufbau .....	163
15.2	Dateibezeichner .....	164
15.3	EF.DIR .....	165
15.4	EF.SN.ICC .....	165
15.5	EF.DH .....	166
15.6	EF.ELC .....	166
15.7	EF.C.ICC.AUT .....	167
15.8	EF.C.CA <sub>ICC</sub> .CS-AUT .....	167
15.9	EF.C_X509.CH.DS .....	168
15.10	EF.C_X509.CA.CS (DF.ESIGN) .....	168
15.11	EF.DM .....	169
16	Kryptographische Informationsanwendung .....	169
16.1	Beispiel für den Aufbau der kryptographischen Informationen einer ESIGN-Anwendung .....	171
16.1.1	EF.CIAInfo .....	171
16.1.2	EF.AOD .....	173
16.1.3	EF.PrKD .....	175
16.1.4	EF.PuKD .....	177
16.1.5	EF.CD .....	178
16.1.6	EF.DCOD .....	179
<b>Anhang A (informativ) Geräteauthentisierung — Kryptographische Sicht .....</b>		<b>182</b>
A.1	Algorithmen zur Authentisierung mit Schlüsselaustausch oder Schlüsselvereinbarung .....	182
A.2	Geräteauthentisierung mit Schlüsseltransport .....	182
A.2.1	Nach ISO/IEC 11770-3 .....	182
A.2.2	Verwendung von min(SIG, N-SIG) für das Signatortoken .....	185
A.3	Geräteauthentisierung mit Schlüsselvereinbarung .....	186
A.3.1	Diffie-Hellman-Schlüsselaustausch .....	186
A.4	Geräteauthentisierung mit Schutz personenbezogener Daten .....	189
A.4.1	Authentizität der öffentlichen DH-Parameter .....	191
A.5	Geräteauthentisierung mit Nichtbeweisbarkeit .....	193
A.5.1	Diffie-Hellman-Schlüsselaustausch .....	193
A.6	Der „Grandmaster-Chess-Angriff“ .....	195
<b>Anhang B (informativ) Personalisierungsszenarios .....</b>		<b>197</b>
<b>Anhang C (informativ) Bildungsschema für mEAC-Objektbezeichner .....</b>		<b>199</b>
<b>Literaturhinweise .....</b>		<b>201</b>