

# DIN EN 14890-2:2009-03 (D)

Anwendungsschnittstelle für Chipkarten, die zur Erzeugung qualifizierter elektronischer Signaturen verwendet werden - Teil 2: Zusätzliche Dienste; Deutsche Fassung EN 14890-2:2008

---

Inhalt	Seite
Vorwort .....	7
1 Anwendungsbereich .....	9
2 Normative Verweisungen .....	9
3 Begriffe .....	9
4 Abkürzungen und Notation .....	10
5 Wahl zusätzlicher Dienste .....	11
6 Client/Server-Authentisierung .....	15
6.1 Allgemeines .....	15
6.2 Client/Server-Protokolle.....	15
6.3 Vor der Client/Server-Authentisierung durchzuführende Schritte.....	16
6.4 Paddingformat .....	16
6.4.1 PKCS #1 v 1-5 .....	16
6.4.2 DSI nach PKCS #1 V2.x (PSS) .....	17
6.5 Client/Server-Protokoll.....	20
6.5.1 Allgemeines .....	20
6.5.2 Schritt 1 — Zertifikat lesen .....	20
6.5.3 Schritt 2 — Signierschlüssel für Client/Server-Authentisierung setzen .....	21
6.5.4 Schritt 3 — Interne Authentisierung.....	22
6.5.5 Ausführungsabfolge für Client/Server-Authentisierung .....	24
6.5.6 Befehlsdatenfeld für die Client/Server-Authentisierung .....	25
7 Rollenauthentisierung.....	26
7.1 Rollenauthentisierung der Karte.....	26
7.2 Rollenauthentisierung des Servers .....	26
7.3 Symmetrische externe Authentisierung .....	27
7.3.1 Protokoll .....	27
7.3.2 Rollenbeschreibung .....	29
7.4 Asymmetrische externe Authentisierung .....	29
7.4.1 Auf RSA beruhendes Protokoll.....	29
7.4.2 Rollenbeschreibung .....	32
8 Dechiffrierung verschlüsselter Schlüssel.....	32
8.1 Vor der Schlüsselentschlüsselung durchzuführende Schritte .....	34
8.2 Schlüsselverwaltung mit RSA.....	34
8.2.1 Allgemeines .....	34
8.2.2 OAEP-Padding .....	35
8.2.3 Ausführungsabfolge .....	36
8.3 Diffie-Hellman-Schlüsselaustausch .....	38
8.3.1 Allgemeines .....	38
8.3.2 Ausführungsabfolge .....	41
8.4 Algorithmusbezeichner für DECIPHER .....	42
9 Signaturüberprüfung.....	43
9.1 Ausführungsabfolge der Signaturüberprüfung .....	43
9.1.1 Schritt 1 — Hash empfangen .....	44
9.1.2 Schritt 2 — Überprüfungsschlüssel wählen .....	45
9.1.3 Schritt 3 — Digitale Signatur überprüfen.....	45

10	Zertifikate für zusätzliche Dienste.....	46
10.1	Dateiaufbau .....	48
10.2	EF.C.CH.AUT .....	48
10.3	EF.C.CH.KE.....	48
10.4	Lesen von Zertifikaten und des öffentlichen Schlüssels von CA.....	49
11	APDU-Datenstrukturen.....	49
11.1	Algorithmusbezeichner .....	49
11.1.1	AlgID für Client/Server-Authentisierung .....	49
11.1.2	AlgID für DECIPHER .....	49
11.2	CRT.....	50
11.2.1	CRT DST zur Wahl des privaten Client/Server-Authentisierungsschlüssels der Chipkarte.....	50
11.2.2	CRT AT zur Wahl des privaten Client/Server-Authentisierungsschlüssels der Chipkarte .....	50
11.2.3	CRT CT zur Wahl des privaten Schlüssels der Chipkarte .....	51
11.2.4	CRT CT zur Wahl des DH-Verschlüsselungsschlüssels der Chipkarte .....	51
11.2.5	CRT DST zur Wahl des öffentlichen Schlüssels des Schnittstellengeräts (Signaturüberprüfung) .....	51
<b>Anhang A (normativ) Templates für Sicherheitsdienstdeskriptoren.....</b>		<b>53</b>
A.1	Einleitung.....	53
A.2	Prinzip der Sicherheitsdienstdeskriptoren .....	53
A.3	SSD-Datenobjekte.....	54
A.3.1	DO Erweiterte Headerliste, Tag '4D' .....	54
A.3.2	DO Befehlssatzmapping (Instruction set mapping, ISM), Tag '80' .....	54
A.3.3	DO Auszuführender Befehl (Command to perform CTP), Tag '52' (siehe ISO/IEC 7816-6).....	54
A.3.4	DO Algorithmus-Objektbezeichner (Object identifier, OID), Tag '06' (siehe ISO/IEC 7816-6) .....	54
A.3.5	DO Algorithmusreferenz, Tag '81' .....	55
A.3.6	DO Schlüsselreferenz, Tag '82' .....	55
A.3.7	DO FID Schlüsselreferenz, Tag '83' .....	55
A.3.8	DO Schlüsselgruppe, Tag '84' .....	55
A.3.9	DO FID Basiszertifikatdatei, Tag '85'.....	55
A.3.10	DO FID Datei mit beigefügtem Zertifikat, Tag '86' .....	55
A.3.11	DO Zertifikatreferenz, Tag '87' .....	55
A.3.12	DO Zertifikatkennzeichner, Tag '88' .....	55
A.3.13	DO FID für Datei mit öffentlichem Schlüssel der Zertifizierungsinstanz PK(CA), Tag '89' .....	55
A.3.14	DO PIN-Verwendungsregeln, Tag '5F2F' (siehe ISO/IEC 7816-6).....	56
A.3.15	DO PIN-Referenz, Tag '8A' .....	56
A.3.16	DO Anwendungsbezeichner (Application identifier, AID), Tag '4F' (siehe ISO/IEC 7816-6).....	56
A.3.17	DO CLA-Codierung, Tag '8B' .....	56
A.3.18	DO Statusinformation (SW1-SW2), Tag '42' siehe (ISO/IEC 7816-6).....	56
A.3.19	DO Frei verfügbare Daten, Tag '53' (siehe ISO/IEC 7816-6).....	57
A.3.20	DO SE-Nummer, Tag '8C' .....	57
A.3.21	DO SSD-Profilbezeichner, Tag '8D' .....	57
A.3.22	DO FID Mapping, Tag '8E' .....	57
A.4	Ort der SSD-Templates .....	57
A.5	Beispiele für SSD-Templates .....	57
<b>Anhang B (informativ) Schlüssel- und Signaturformate für elliptische Kurven über Primkörpern</b>		
	GF(p) .....	59
B.1	Allgemeines .....	59
B.2	Parameter elliptischer Kurven.....	59
B.3	Öffentlicher Schlüsselpunkt .....	60
B.4	Signaturformat ECDSA .....	60
<b>Anhang C (informativ) Sicherheitsumgebungen.....</b>		<b>61</b>
C.1	Einleitung.....	61
C.2	Definition von CRT (Beispiele) .....	63
C.2.1	Allgemeines .....	63
C.2.2	CRT für Authentisierung (AT).....	64
C.2.3	CRT für kryptographische Prüfsumme (CCT).....	65
C.2.4	CRT für digitale Signatur (DST).....	66
C.2.5	CRT für Vertraulichkeit (CT) .....	67

	Seite
<b>C.3</b>	<b>Sicherheitsumgebungen (Beispiel) ..... 68</b>
<b>C.3.1</b>	<b>Allgemeines ..... 68</b>
<b>C.3.2</b>	<b>Sicherheitsumgebung #10 ..... 68</b>
<b>C.3.3</b>	<b>Sicherheitsumgebung #11 ..... 68</b>
<b>C.4</b>	<b>Codierung von Zugriffsbedingungen (Beispiel)..... 69</b>
<b>C.4.1</b>	<b>Allgemeines ..... 69</b>
<b>C.4.2</b>	<b>Zugriffsbedingungen..... 69</b>
<b>C.4.3</b>	<b>Zugriffsregelreferenzen ..... 70</b>
<b>C.4.4</b>	<b>Zugriffsbedingungen für EF.ARR ..... 71</b>
<b>C.4.5</b>	<b>EF.ARR-Datensätze ..... 71</b>
<b>Anhang D (informativ)</b>	<b>Aspekte der Interoperabilität ..... 74</b>
<b>D.1</b>	<b>Allgemeines ..... 74</b>
<b>D.2</b>	<b>Wahl der Geräteauthentisierung..... 74</b>
<b>D.2.1</b>	<b>Allgemeines ..... 74</b>
<b>D.2.2</b>	<b>Signaturgenerierungsablauf mit möglichen Verarbeitungsoptionen ..... 75</b>
<b>D.3</b>	<b>Wahl des Benutzerüberprüfungsverfahrens ..... 76</b>
<b>Anhang E (informativ)</b>	<b>Beispiel für DF.CIA ..... 77</b>
<b>Literaturhinweise</b>	<b>..... 81</b>