

DIN EN 14890-2



ICS 35.240.15

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

Application Interface for smart cards used as Secure Signature Creation Devices –
Part 2: Additional Services;
German version EN 14890-2:2008

Interface d'application des cartes intelligentes utilisées comme dispositifs sûrs de création
de signature –
Partie 2: Services complémentaires;
Version allemande EN 14890-2:2008

Gesamtumfang 73 Seiten

Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN

Nationales Vorwort

Dieses Dokument (EN 14890-2:2008) 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 14890-2 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 14890-2 legt DIN EN 14890-1 ergänzende 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 14890-2 ersetzt das CEN Workshop Agreement CWA 14890-2:2004.

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 2: Zusätzliche Dienste**

Application Interface for smart cards used as Secure
Signature Creation Devices —
Part 2: Additional Services

Interface d'application des cartes intelligentes utilisées
comme dispositifs sûrs de création de signature —
Partie 2: Services complémentaires

Diese Europäische Norm wurde vom CEN am 5. Oktober 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	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe	6
4 Abkürzungen und Notation	7
5 Wahl zusätzlicher Dienste	8
6 Client/Server-Authentisierung	11
6.1 Allgemeines	11
6.2 Client/Server-Protokolle	11
6.3 Vor der Client/Server-Authentisierung durchzuführende Schritte	12
6.4 Paddingformat	12
6.4.1 PKCS #1 v 1-5	12
6.4.2 DSI nach PKCS #1 V2.x (PSS)	12
6.5 Client/Server-Protokoll	14
6.5.1 Allgemeines	14
6.5.2 Schritt 1 — Zertifikat lesen	15
6.5.3 Schritt 2 — Signierschlüssel für Client/Server-Authentisierung setzen	15
6.5.4 Schritt 3 — Interne Authentisierung	17
6.5.5 Ausführungsabfolge für Client/Server-Authentisierung	18
6.5.6 Befehlsdatenfeld für die Client/Server-Authentisierung	20
7 Rollenauthentisierung	20
7.1 Rollenauthentisierung der Karte	20
7.2 Rollenauthentisierung des Servers	21
7.3 Symmetrische externe Authentisierung	21
7.3.1 Protokoll	21
7.3.2 Rollenbeschreibung	24
7.4 Asymmetrische externe Authentisierung	24
7.4.1 Auf RSA beruhendes Protokoll	24
7.4.2 Rollenbeschreibung	27
8 Dechiffrierung verschlüsselter Schlüssel	27
8.1 Vor der Schlüsselentschlüsselung durchzuführende Schritte	28
8.2 Schlüsselverwaltung mit RSA	28
8.2.1 Allgemeines	28
8.2.2 OAEP-Padding	29
8.2.3 Ausführungsabfolge	29
8.3 Diffie-Hellman-Schlüsselaustausch	31
8.3.1 Allgemeines	31
8.3.2 Ausführungsabfolge	33
8.4 Algorithmusbezeichner für DECIPHER	34
9 Signaturüberprüfung	35
9.1 Ausführungsabfolge der Signaturüberprüfung	35
9.1.1 Schritt 1 — Hash empfangen	36
9.1.2 Schritt 2 — Überprüfungsschlüssel wählen	37
9.1.3 Schritt 3 — Digitale Signatur überprüfen	37
10 Zertifikate für zusätzliche Dienste	38
10.1 Dateiaufbau	39
10.2 EF.C.CH.AUT	39
10.3 EF.C.CH.KE	40
10.4 Lesen von Zertifikaten und des öffentlichen Schlüssels von CA	40

11	APDU-Datenstrukturen	40
11.1	Algorithmusbezeichner.....	41
11.1.1	AlgID für Client/Server-Authentisierung	41
11.1.2	AlgID für DECIPHER.....	41
11.2	CRT	41
11.2.1	CRT DST zur Wahl des privaten Client/Server-Authentisierungsschlüssels der Chipkarte	42
11.2.2	CRT AT zur Wahl des privaten Client/Server-Authentisierungsschlüssels der Chipkarte	42
11.2.3	CRT CT zur Wahl des privaten Schlüssels der Chipkarte.....	42
11.2.4	CRT CT zur Wahl des DH-Verschlüsselungsschlüssels der Chipkarte.....	43
11.2.5	CRT DST zur Wahl des öffentlichen Schlüssels des Schnittstellengeräts (Signaturüberprüfung)	43
Anhang A (normativ) Templates für Sicherheitsdienstdeskriptoren		44
A.1	Einleitung	44
A.2	Prinzip der Sicherheitsdienstdeskriptoren	44
A.3	SSD-Datenobjekte	45
A.3.1	DO Erweiterte Headerliste, Tag '4D'	45
A.3.2	DO Befehlssatzmapping (Instruction set mapping, ISM), Tag '80'	45
A.3.3	DO Auszuführender Befehl (Command to perform CTP), Tag '52' (siehe ISO/IEC 7816-6)	45
A.3.4	DO Algorithmus-Objektbezeichner (Object identifier, OID), Tag '06' (siehe ISO/IEC 7816-6).....	45
A.3.5	DO Algorithmusreferenz, Tag '81'	46
A.3.6	DO Schlüsselreferenz, Tag '82'	46
A.3.7	DO FID Schlüsselreferenz, Tag '83'	46
A.3.8	DO Schlüsselgruppe, Tag '84'	46
A.3.9	DO FID Basiszertifikatdatei, Tag '85'	46
A.3.10	DO FID Datei mit beigefügtem Zertifikat, Tag '86'	46
A.3.11	DO Zertifikatreferenz, Tag '87'	46
A.3.12	DO Zertifikatkennzeichner, Tag '88'	46
A.3.13	DO FID für Datei mit öffentlichem Schlüssel der Zertifizierungsinstanz PK(CA), Tag '89'	46
A.3.14	DO PIN-Verwendungsregeln, Tag '5F2F' (siehe ISO/IEC 7816-6).....	47
A.3.15	DO PIN-Referenz, Tag '8A'	47
A.3.16	DO Anwendungsbezeichner (Application identifier, AID), Tag '4F' (siehe ISO/IEC 7816-6)	47
A.3.17	DO CLA-Codierung, Tag '8B'	47
A.3.18	DO Statusinformation (SW1-SW2), Tag '42' siehe (ISO/IEC 7816-6).....	47
A.3.19	DO Frei verfügbare Daten, Tag '53' (siehe ISO/IEC 7816-6)	48
A.3.20	DO SE-Nummer, Tag '8C'	48
A.3.21	DO SSD-Profilbezeichner, Tag '8D'.....	48
A.3.22	DO FID Mapping, Tag '8E'	48
A.4	Ort der SSD-Templates	48
A.5	Beispiele für SSD-Templates	48
Anhang B (informativ) Schlüssel- und Signaturformate für elliptische Kurven über Primkörpern		
	GF(p)	50
B.1	Allgemeines	50
B.2	Parameter elliptischer Kurven	50
B.3	Öffentlicher Schlüsselpunkt.....	51
B.4	Signaturformat ECDSA	51
Anhang C (informativ) Sicherheitsumgebungen		52
C.1	Einleitung	52
C.2	Definition von CRT (Beispiele).....	53
C.2.1	Allgemeines	53
C.2.2	CRT für Authentisierung (AT)	54
C.2.3	CRT für kryptographische Prüfsumme (CCT)	55
C.2.4	CRT für digitale Signatur (DST)	56
C.2.5	CRT für Vertraulichkeit (CT)	57

	Seite
C.3 Sicherheitsumgebungen (Beispiel).....	58
C.3.1 Allgemeines.....	58
C.3.2 Sicherheitsumgebung #10	58
C.3.3 Sicherheitsumgebung #11	58
C.4 Codierung von Zugriffsbedingungen (Beispiel)	59
C.4.1 Allgemeines	59
C.4.2 Zugriffsbedingungen	60
C.4.3 Zugriffsregelreferenzen.....	60
C.4.4 Zugriffsbedingungen für EF.ARR.....	61
C.4.5 EF.ARR-Datensätze	62
Anhang D (informativ) Aspekte der Interoperabilität.....	64
D.1 Allgemeines.....	64
D.2 Wahl der Geräteauthentisierung	64
D.2.1 Allgemeines.....	64
D.2.2 Signaturgenerierungsablauf mit möglichen Verarbeitungsoptionen.....	65
D.3 Wahl des Benutzerüberprüfungsverfahrens.....	66
Anhang E (informativ) Beispiel für DF.CIA	67
Literaturhinweise	71

Vorwort

Dieses Dokument (EN 14890-2:2008) wurde vom Technischen Komitee CEN/TC 224 „Maschinenlesbare Karten und zugehörige Geräteschnittstellen“ 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 Mai 2009, und etwaige entgegenstehende nationale Normen müssen bis Mai 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 14890-2:2004.

Diese Europäische Norm soll die stabile Implementierung des europäischen rechtlichen Rahmens für elektronische Signaturen unterstützen, indem sie Teil 1 und Teil 2 von CEN CWA 14890 einbindet und die funktions- und sicherheitsbezogenen Anforderungen an eine Chipkarte zur Verwendung als sichere Signaturerstellungseinheit entsprechend den Bedingungen der Europäischen Richtlinie 1999/93 über elektronische Signaturen definiert, nach denen eine mit der Norm übereinstimmende Karte in der Lage sein muss, eine "qualifizierte elektronische Signatur" zu erzeugen, die Artikel 5.1 der Signaturrechtlinie erfüllt und daher als zu handschriftlichen Signaturen äquivalent betrachtet werden kann.

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 systemspezifischen und interpreterbasierten Karten sollte somit möglich sein.

Diese Europäische Norm *Anwendungsstellen 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 [1] zu verwenden sind;
- Teil 2: „Zusätzliche Dienste“ beschreibt die übrigen IAS-Dienste.

Entsprechend der CEN/CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn, Vereinigtes Königreich und Zypern.

1 Anwendungsbereich

Teil 2 dieser Reihe enthält zusätzlich zu den bereits in Teil 1 beschriebenen Diensten Dienste zur Identifizierung, Authentisierung und Signaturerstellung (IAS), um die Interoperabilität und Verwendung von IAS auf nationaler bzw. europäischer Ebene zu ermöglichen.

Dieser Teil beschreibt zusätzliche Funktionen zur Unterstützung von Diensten zur generischen Identifizierung, Authentisierung und Signaturerstellung (IAS). Er enthält die Funktionen von CEN CWA 14890, Teil 2. Dazu gehören Schlüsseldechiffrierung und Client/Server-Authentisierung (wobei der Client der Karteninhaber ist), Signaturüberprüfung sowie zugehörige kryptographische Tokeninformationen.

Darüber hinaus weist das vorliegende Dokument in folgenden Bereichen Ergänzungen auf:

- Protokolle für Client/Server-Authentisierung (C/S-Authentisierung) mit ELC und deren Beschreibung in DF.CIA;
- Identitätsverwaltung auf der Grundlage der C/S-Authentisierung;
- Beschreibung von Kartenfähigkeit und Anwendungsfähigkeit.

Folgende Aspekte liegen außerhalb des Anwendungsbereichs dieser Norm:

- 1) die physikalischen, elektrischen und transportprotokollbezogenen Merkmale der Karte;
- 2) der Prozess der Fehlerhandhabung.

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).

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

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

ISO/IEC 7816-9:2004, *Identification cards — Integrated circuit cards — Part 9: Commands for card management*

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

ISO/IEC 15946, *Information Technology — Security techniques — Cryptographic techniques based on elliptic curves*

3 Begriffe

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

3.1

externe C/S-Authentisierung

Authentisierung des Servers durch den Client. Der Client gilt als eine Kombination aus dem PC und der Chipkarte. Diese externe Authentisierung liegt außerhalb des Anwendungsbereichs dieser Norm.

3.2

interne C/S-Authentisierung

Authentisierung des Clients durch den Server. Der Client gilt als eine Kombination aus dem PC und der Chipkarte

3.3

Schnittstellengerät, IFD

Gerät oder Instanz, das/die zur externen Welt (außerhalb der Chipkarte) gehört

3.4

gesicherter Kanal

Kommunikationsverbindung zwischen der Chipkarte und einem Sicherheitsmodul (möglicherweise ebenfalls eine Chipkarte), die Authentizität und/oder Integrität und/oder Geheimhaltung bereitstellt

4 Abkürzungen und Notation

Die Abkürzungen und die Notation entsprechen den Angaben in [1].

APDU	Anwendungsprotokoll-Dateneinheit (Application protocol data unit)
ARR	Protokoll für Zugriffsregeln (Access Rule Record)
AT	CRT für die Authentisierung
C/S	Client/Server
CA	Zertifizierungsinstanz (Certification Authority)
CC	Kryptographische Prüfsumme (Cryptographic Checksum)
CCT	Template für kryptographische Prüfsumme (Cryptographic checksum template)
CIA	Kryptographische Informationsanwendung (Cryptographic Information Application)
CMS	Kartenverwaltungssystem (Card Management System)
CRT	Control Reference Template
CT	Geheimhaltungstemplate
D[key](msg)	Dechiffrierung (Decipherment) von <msg> mit <key>
DES-3	Datenverschlüsselungsstandard (Data Encryption Standard, Triple DES)
DF	Zugeordnete Datei (Dedicated File)
DH	Diffie-Hellman
DO	Datenobjekt (Data Object)
DS	Digitale Signatur (Digital Signature)
DSI	Digitale Signatureingabe (Digital Signature Input)
DST	CRT für Digitale Signatur
E[key](msg)	Chiffrierung (Encipherment) von <msg> mit <key>
EF	Elementardatei (Elementary File)
FCI	Dateisteuerungsinformation (File Control Information)
FCP	Dateisteuerungsparameter (File Control Parameters)
H_<id>	Hash-Funktion unter Verwendung von <id>-Algorithmus
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)
KEI	Eingabeformat für Schlüsselchiffrierung (Key Encipherment Input Format)
KID	Schlüsselbezeichner (Key Identifier)
MD5	Nachrichtendigest 5 [Message Digest 5 (Hash-Algorithmus)]
MF	Masterdatei (Master File)
OAEP	Optimales asymmetrisches Verschlüsselungspadding (Optimal Asymmetric Encryption Padding)
P1-P2	Parameterbytes (Parameter bytes)
PI	Padding-Indikator (Padding Indicator)
PKCS	Standards zur Verschlüsselung mit öffentlichem Schlüssel (Public Key Cryptography Standards)
PKI	Public-Key-Infrastruktur (Public Key Infrastructure)
PrK	Privater Schlüssel (Private Key)
PSO	PERFORM SECURITY OPERATION
PSS	Probabilistisches Signatursystem (Probabilistic Signature Scheme)
PuK	Öffentlicher Schlüssel (Public Key)
RCA	RootCA
RFU	Für zukünftige Verwendung reserviert (Reserved for Future Use)
RND	Zufallszahl (Random number)
SE	Sicherheitsumgebung (Security Environment)
SFI	Short File Identifier
SHA	Sicherer Hash-Algorithmus (Secure Hash Algorithm)
SK	Geheimer Schlüssel (Secret Key)
SM	Sichere Nachrichtenübermittlung (Secure Messaging)
SN	Laufende Nummer (Serial Number)
SSCD	Sichere Signaturerstellungseinheit (Secure Signature Creation Device)
SSD	Sicherheitsdienstdeskriptor (Secure Service Descriptor)
UQB	Verwendungskennzeichner (Usage Qualifier)

5 Wahl zusätzlicher Dienste

Zusätzliche Dienste werden üblicherweise im Zusammenhang mit Anwendungen genutzt, die digitale Signaturen verwenden.

Ein hinreichend bekannter zusätzlicher Dienst ist die **Client/Server-Authentisierung**. In diesem Fall wird die Chipkarte als eine Krypto-Toolbox verwendet, z. B. um eine Challenge mit einem in der Chipkarte gespeicherten privaten Schlüssel zu verschlüsseln. Dies ist besonders bei Anwendungen hilfreich, bei denen zur Client/Server-Authentisierung ein Gerät erforderlich ist, das nicht manipuliert werden kann. Eine Chipkarte weist diese manipulationssichere Eigenschaft auf und kann daher wirksam zur Unterstützung der Anwendung in diesem Zusammenhang eingesetzt werden.

Eine **Dokumentenentschlüsselung** ist ein weiterer bekannter Dienst, der von dem Schnittstellengerät ausgeführt werden kann. Eine Endgeräteanwendung empfängt ein Dokument, das typischerweise mit einem symmetrischen Schlüssel verschlüsselt ist. Der symmetrische Schlüssel ist ebenfalls mit einem weiteren öffentlichen Schlüssel verschlüsselt. Die Chipkarte enthält den entsprechenden privaten Schlüssel, dechiffriert den symmetrischen Schlüssel und sendet diesen zurück an die Endgeräteanwendung.

Zwar besteht die übliche Verwendung einer Signaturkarte in der Generierung einer digitalen Signatur, jedoch ist es auch möglich, dass eine Anwendung vor hat, eine Signatur mit einem in der Chipkarte gespeicherten öffentlichen Schlüssel zu überprüfen. In diesem Fall wird zur **Signaturüberprüfung** ein zusätzlicher Dienst aufgerufen.

In der Chipkarte vorgesehene zusätzliche Dienste erfordern das Vorhandensein einer entsprechenden Sicherheitsumgebung. Die jeweiligen Sicherheitsumgebungen sind in Anhang C beschrieben.

Zusätzlich zu den in DF.CIA enthaltenen beschreibenden Informationen (siehe EN 14890-1:2008, Abschnitt 16) können Informationen erforderlich sein, die in Sicherheitsdienstdeskriptoren (Security Service Descriptors, SSD) dargestellt werden können. Das Prinzip der SSD ist in Anhang A beschrieben.

Vor Verwendung zusätzlicher Dienste kann eine Benutzerüberprüfung erforderlich sein. Das Passwort für diese Benutzerüberprüfung muss sich von dem zur Signaturgenerierung verwendeten Passwort unterscheiden. Dadurch soll der Zweck des Signaturgenerierungspassworts einzig als „Willenserklärung“ im Fall einer Signaturgenerierung aufrechterhalten werden.

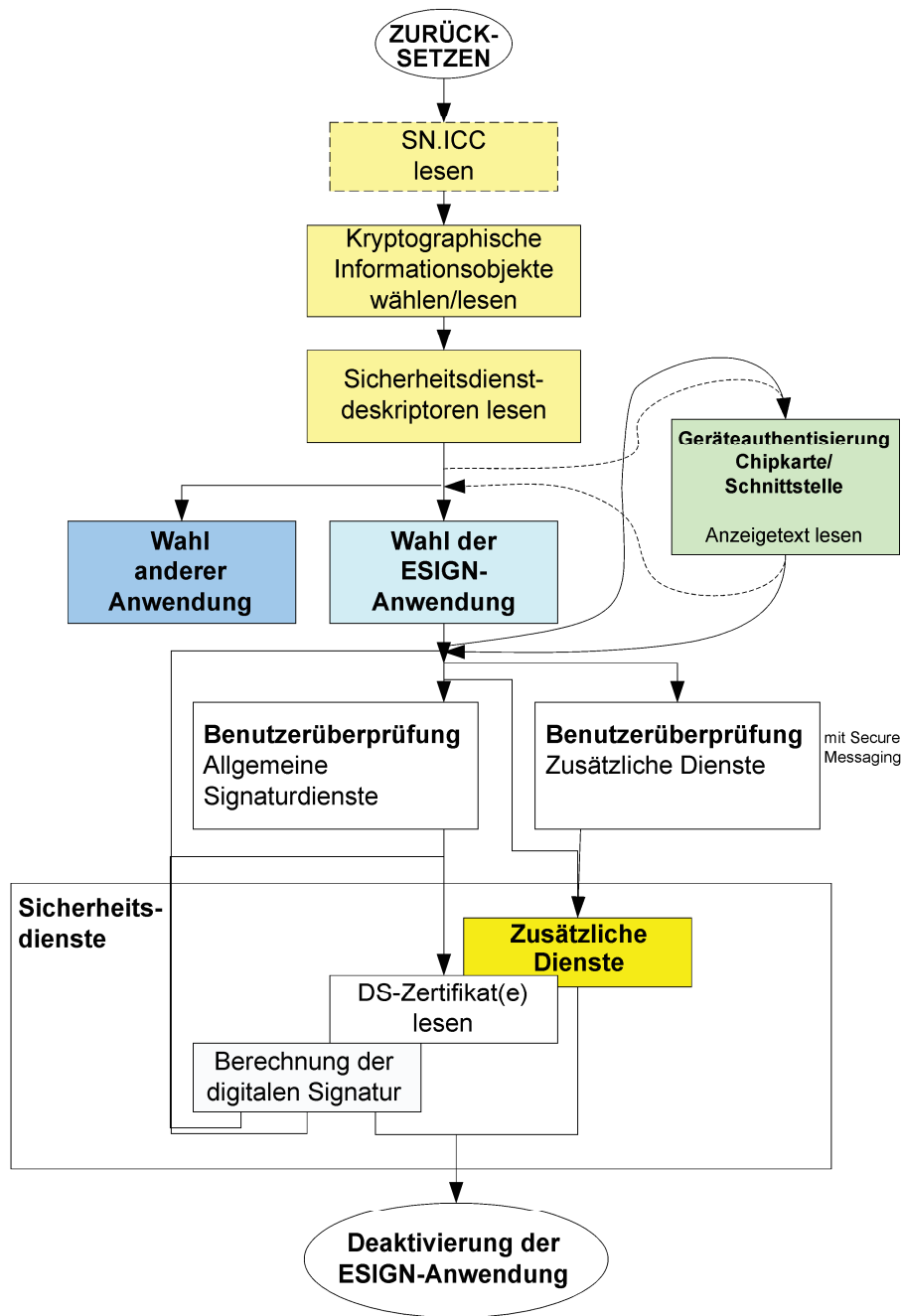


Bild 1 — Beispiel für die Wahl zusätzlicher Dienste

Bild 1 zeigt die Wahl zusätzlicher Dienste im Zusammenhang mit der E-Sign-Anwendung. Für einige zusätzliche Dienste ist möglicherweise eine Benutzerüberprüfung erforderlich. Einzelheiten zu den Zugriffsbedingungen sind in den entsprechenden Sicherheitsumgebungen beschrieben.

6 Client/Server-Authentisierung

6.1 Allgemeines

Um bestimmten Komponenten wie z. B. Servern Zugriffsrechte zu gewähren, ist eine PK-basierte Authentisierungsprozedur durchzuführen. Eine derartige Client/Server-Authentisierung (siehe 3.2) ist ein Prozess, der von einer erforderlichen Geräteauthentisierung unabhängig ist.

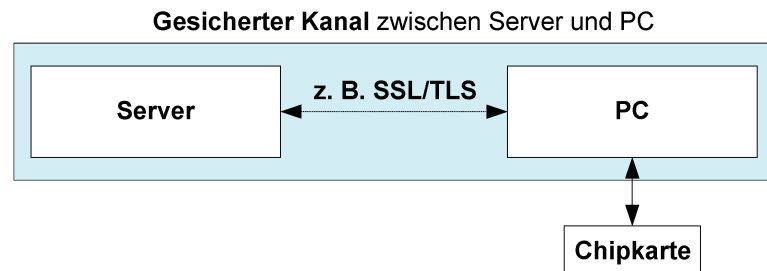


Bild 2 — Beispiel für eine Client/Server-Authentisierung

In dem oben stehenden Beispiel wird durch die Client/Server-Authentisierung ein gesicherter Kanal zwischen einem abgesetzten Server und einem PC eingerichtet. Die Chipkarte wird als eine kryptographische Toolbox verwendet, um dem PC die kryptographische Funktionalität zu verleihen.

Dieses Dokument unterstützt nicht die Authentisierung des Servers (siehe 3.1). Das Zertifikat des Servers sowie das Serverprotokoll sind anwendungsspezifisch und liegen daher außerhalb des Anwendungsbereichs dieses Dokuments.

6.2 Client/Server-Protokolle

Dieses Dokument behandelt die Berechnung der digitalen Signatur durch die Karte, und zwar unter Anwendung des privaten Schlüssels zur Authentisierung in dem Befehl INTERNAL AUTHENTICATE (COMPUTE DIGITAL SIGNATURE) auf die im Datenfeld des Befehls enthaltene Authentisierungseingabe nach Formatierung der Eingabe.

Das zur Client/Server-Authentisierung verwendete Schlüsselpaar muss sich von den Geräteauthentisierungsschlüsseln bzw. den Signaturerstellungsschlüsseln unterscheiden. Der zusammen mit dem kennzeichnenden Namen des Karteninhabers gespeicherte öffentliche Teil dieses Schlüsselpaars ist durch ein Zertifikat (üblicherweise X.509 [7]) zertifiziert. Ein derartiges Zertifikat wird von der Chipkarte nicht interpretiert.

Relevante Authentisierungsprozeduren sind z. B.:

- PK-Kerberos-Protokoll (zur Login-Authentisierung);
- SSL/TLS-Protokoll;
- WTLS-Protokoll.

Alle oben stehenden Protokolle beruhen auf den gleichen kryptographischen Algorithmen. Vor allem verwenden diese Protokolle im Fall von RSA alle das Paddingformat PKCS #1. Daher beschreibt dieses Dokument nur das Paddingformat PKCS #1.

6.3 Vor der Client/Server-Authentisierung durchzuführende Schritte

Die vor einer Client/Server-Authentisierung durchzuführenden Schritte sind anwendungsspezifisch. Daher schreibt dieses Dokument die Durchführung dieser Schritte nicht obligatorisch vor.

Die in Anhang C vorgeschlagenen Zugriffsbedingungen legen eine Benutzerprüfung als obligatorischen Schritt vor der Client/Server-Authentisierung fest.

Die Verweisung auf das im Zusammenhang mit der Client/Server-Authentisierung zur Benutzerüberprüfung zu verwendende Passwort ist in den Informationen von DF.CIA beschrieben.

6.4 Paddingformat

6.4.1 PKCS #1 v 1-5

Im Fall von RSA wird die Authentisierungseingabe T nach [6] PKCS # 1, Version 2.1, und Unterabschnitt 9.2 „EMSA-PKCS1-v1-5“ formatiert. Zu bestimmten Algorithmen, siehe 6.5.6.

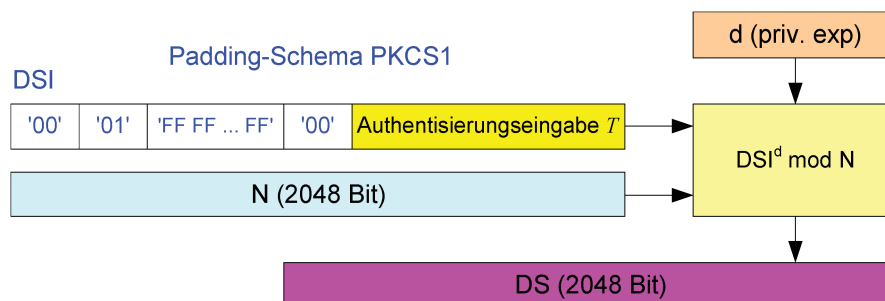


Bild 3 — Beispiel für 2048-Bit-DSI nach PKCS #1 V1.5

Das Padding erfolgt durch einen Oktettstrang, der aus acht Oktetten mit dem Wert 'FF' (Länge ≥ 8) besteht. Aus Sicherheitsgründen muss die Authentisierungseingabe kleiner oder gleich 40 % der Länge des Moduls sein. Der formatierte Oktettstrang muss aus k Oktetten bestehen, wobei k die in Oktetten angegebene Länge des Moduls des privaten Schlüssels zur Authentisierung ist.

Die Digest-Info ist in EN 14890-1:2008, 13.3.3 beschrieben.

6.4.2 DSI nach PKCS #1 V2.x (PSS)

Das DSI-Format nach PKCS #1 V2.2 weist den folgenden Aufbau auf. Die Nachricht M stellt die Authentisierungseingabe T dar:

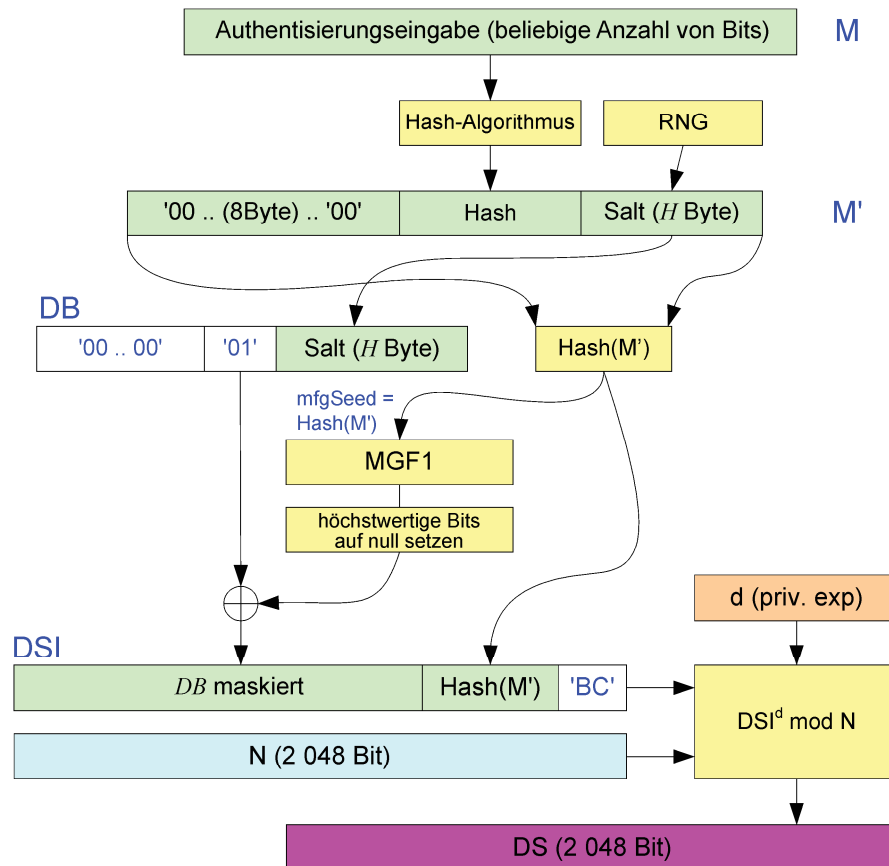


Bild 4 — Beispiel für 2048-Bit-DSI nach PKCS #1 V2.1

Die höchstwertigen Bits der Länge $[8 \times \text{Key.ModulusByteLength} - (\text{Key.ModulusBitLength} - 1)]$ der Ausgabe der MGF1-Funktion werden auf null gesetzt, um eine DSI-Eingabe bereitzustellen, die kleiner als der Modul N ist. Die MGF1-Funktion ist beschrieben in [6] [PKCS 1, Version 2.1, Unterabschnitt B.2.1].

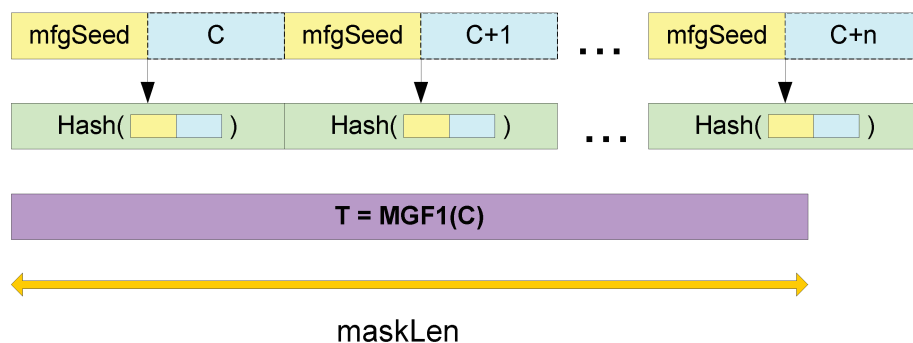


Bild 5 — Beispiel für die Maskengenerierungsfunktion MGF1

Die Länge des Salt ist identisch mit der Digest-Länge H des Hash-Algorithmus. Die Länge von DB berechnet sich nach:

$$\text{Length}(DB) = N - H - 1 = \text{maskLen}$$

Dabei ist

N die Byte-Länge des Moduls;

H die Digest-Länge des Hash-Algorithmus.

Die Länge von *mfgSeed* ist identisch mit H , die Länge von C beträgt 4 Byte, wie in [6] festgelegt. Der Anfangswert von C ist null. Die Verkettung von $[mfgSeed || C]$ -Paaren wird an der Länge von *maskLeng* rechtstrunkiert.

Es ergibt sich folgende digitale Signatureingabe.

Tabelle 1 — Digitale Signatureingabe (DSI) — Format nach PKCS #1, Version 2.x

T	L	V
—	—	masked DB = $DB \oplus \text{MGF1}(\text{Hash}(M'), \text{Key.Length} - H - 1)$ Hash(M') 'BC' = Padding nach ISO 9796 (Option 1)

6.5 Client/Server-Protokoll

6.5.1 Allgemeines

Tabelle 2 zeigt die Ausführungsabfolge der RSA-Client/Server-Authentisierung. Dieses Dokument behandelt nur die interne Authentisierung.

Tabelle 2 — Ausführungsabfolge Client/Server-Authentisierung

Stufe	Schritt	Schnittstellengerät	Übertragung	Chipkarte
1	—	... vorangehende Schritte (z. B. Benutzerüberprüfung), die anwendungsspezifisch für Client/Server-Authentisierung sind		anwendungsspezifischer Protokollablauf
INTERNE AUTHENTISIERUNG — Server (Schnittstellengerät) authentisiert Client (Chipkarte)				
2	1	READ BINARY des Zertifikats (üblicherweise X.509)		Zertifikat
	2	MSE:SET PrK.CH.AUT		
	3	INTERNAL AUTHENTICATE oder COMPUTE DIGITAL SIGNATURE		
Client (Chipkarte) ist durch Server (Schnittstellengerät) authentisiert				
3	—	... nachfolgende Schritte, die anwendungsspezifisch für aktuelle Client/Server-Authentisierung sind		nicht in diesem Dokument festgelegt

6.5.2 Schritt 1 — Zertifikat lesen

Verfügt das Schnittstellengerät nicht bereits über das Authentisierungszertifikat des Clients (der Chipkarte), kann es dieses aus einer globalen Datendatei EF.C.CH.AUT auslesen. Das Zertifikat C.CH.AUT des Clients kann öffentliche Algorithmengrößen enthalten, die vom Client/Server-Authentisierungsalgorithmus abhängen.

Ausführungsabfolge

Tabelle 3 — EF.C.CH.AUT lesen — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'B0' READ BINARY
P1	'85' Beispiel: SFI = 05
P2	'00' Offset = 0
Le-Feld	'00'

Zu Aufbau und Inhalt der APDU, siehe ISO/IEC 7816-4:2005, 7.2.3.

Der Aufbau und die Codierung von C.CA_{ICC}.CS_AUT dürfen der Beschreibung in 14.15 entsprechen, können jedoch auch ein anderes, der E-SIGN-Anwendung nicht bekanntes Format aufweisen. Das tatsächliche Format ist anwendungsspezifisch und liegt außerhalb des Anwendungsbereichs dieser Norm.

Tabelle 4 — EF.C.CH.AUT lesen — Antwort

Antwortparameter	Bedeutung
Datenfeld	EF.C.CH.AUT in EF gespeicherte Klartextdaten
SW1-SW2	siehe ISO/IEC 7816-4

ANMERKUNG Sofern nicht mit READ BINARY die Datei unter Verwendung eines Short File Identifier (SFI) gewählt wird, muss vor dem Lesen der Datei ein entsprechender SELECT(EF)-Befehl ausgeführt werden

6.5.3 Schritt 2 — Signierschlüssel für Client/Server-Authentisierung setzen

Der MSE-Befehl setzt den Schlüsselbezeichner des privaten Client/Server-Authentisierungsschlüssels der Chipkarte, der zur anschließenden Berechnung der digitalen Signatur zu verwenden ist.

Ausführungsabfolge

Tabelle 5 — Schlüsselreferenz für interne Authentisierung wählen — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'22' MANAGE SECURITY ENVIRONMENT
P1	'41' SET für interne Authentisierung
P2	'A4'
Lc-Feld	'xx'
Datenfeld	CRT-Datenfeld mit AlgId(PrK.CH.AUT) und KeyRef(PrK.CH.AUT)

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

Der Aufbau und die Codierung der Schlüsselreferenzdaten ist in 11.2.2 festgelegt.

Das Antwortdatenfeld bleibt leer.

Tabelle 6 — Schlüsselreferenz für interne Authentisierung wählen — Antwort

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

Alternativ kann der Befehl COMPUTE DIGITAL SIGNATURE verwendet werden.

Alternative Ausführungsabfolge

Tabelle 7 — Schlüsselreferenz für interne Authentisierung wählen — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'22' MANAGE SECURITY ENVIRONMENT
P1	'41' SET für interne Authentisierung
P2	'B6' digitale Signatur DST
Lc-Feld	'xx'
Datenfeld	CRT-Datenfeld mit AlgID(PrK.CH.AUT) und KeyRef(PrK.CH.AUT)

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

Der Aufbau und die Codierung der Schlüsselreferenzdaten ist in 11.2.1 festgelegt.

Das Antwortdatenfeld bleibt leer.

Tabelle 8 — Schlüsselreferenz für interne Authentisierung wählen — Antwort

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

6.5.4 Schritt 3 — Interne Authentisierung

Das Schnittstellengerät sendet eine Challenge im Datenfeld des Befehls INTERNAL AUTHENTICATE. Die Chipkarte berechnet unter Verwendung ihres im vorangegangenen Schritt gewählten privaten Schlüssels eine Signatur über der Challenge.

Ausführungsabfolge

Tabelle 9 — INTERNAL AUTHENTICATE — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'88' INTERNAL AUTHENTICATE
P1	'00' keine Algorithmusinformation
P2	'00' Schlüsselreferenz — keine
Lc-Feld	'xx'
Datenfeld	Daten Authentisierungseingabe <i>T</i> , siehe unten
Le-Feld	'00'

Zu Aufbau und Inhalt der APDU, siehe ISO/IEC 7816-4, 7.5.2.

Das Format der digitalen Signatureingabe ist in 6.5.6 beschrieben.

Die zur Client/Server-Authentisierung verwendbaren Algorithmen sind in 11.1.1 beschrieben.

Die Antwortdaten enthalten die Signatur.

Tabelle 10 — INTERNAL AUTHENTICATE — Antwort

Antwortparameter	Bedeutung
Datenfeld	RSA: $SIG = DS^a[PrK.IFD.CS.AUT](DSI)$, wobei DSI nach 6.4 formatiert ist. ECDSA: Für den ECDSA-Algorithmus ist das Signaturformat in B.4 beschrieben.
SW1-SW2	siehe ISO/IEC 7816-4
^a DS ist als einfache RSA-Potenzierung zu verstehen. Es bedeutet keine Eingabeformatierungsschicht, außer der hier bereits festgelegten.	

Alternativ kann der Befehl COMPUTE DIGITAL SIGNATURE verwendet werden.

Alternative Ausführungsabfolge

Tabelle 11 — COMPUTE DIGITAL SIGNATURE — Befehls-APDU

Befehlsparameter	Bedeutung
CLA	nach ISO/IEC 7816-4
INS	'2A' PERFORM SECURITY OPERATION
P1	'9E' erwartetes Antwort-DO
P2	'9A' zu signierende Daten
Lc-Feld	'xx'
Datenfeld	Daten Authentisierungseingabe <i>T</i> , siehe unten
Le-Feld	'00'

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

Das Format der digitalen Signatureingabe ist in 6.5.6 beschrieben.

Die zur Client/Server-Authentisierung verwendbaren Algorithmen sind in 11.1.1 beschrieben.

Die Antwortdaten enthalten die Signatur.

Tabelle 12 — COMPUTE DIGITAL SIGNATURE — Antwort

Antwortparameter	Bedeutung
Datenfeld	RSA: $SIG = DS^a[PrK.IFD.CS.AUT](DSI)$, wobei DSI nach 6.4 formatiert ist. ECDSA: Für den ECDSA-Algorithmus ist das Signaturformat in B.4 beschrieben.
SW1-SW2	siehe ISO/IEC 7816-4
^a DS ist als einfache RSA-Potenzierung zu verstehen. Es bedeutet keine Eingabeformatierungsschicht, außer der hier bereits festgelegten.	

Während das Schnittstellengerät lediglich die Authentisierungseingabe *T* sendet, führt die Chipkarte das Padding nach Bild 3 durch. Im weiteren Textverlauf ist eine Unterscheidung zwischen diesen Alternativen nicht notwendig.

6.5.5 Ausführungsabfolge für Client/Server-Authentisierung

Die Chipkarte generiert eine Signatur mit der Größe des Moduls über den Eingabedaten, die in gepaddeter Form vorliegen muss, sodass sie die Größe des Moduls aufweist.

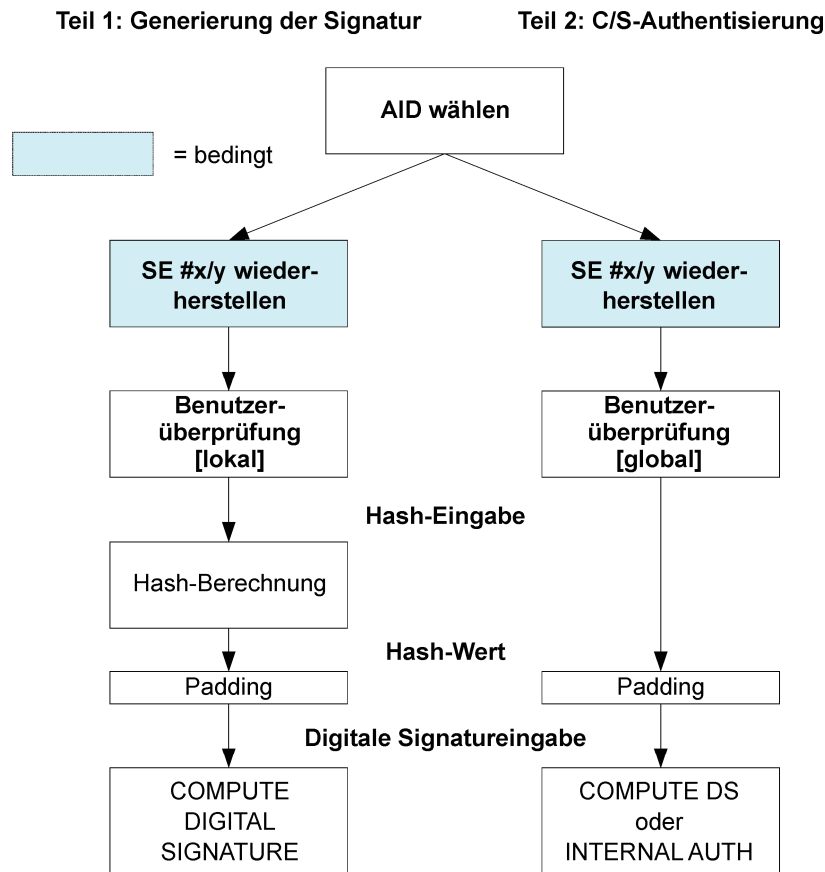


Bild 6 — Vergleich der Vorgänge in der Chipkarte bei der Signaturerstellung und der C/S-Authentisierung

- Die Wahl einer Sicherheitsumgebung ist obligatorisch, wenn zur Signaturerstellung und zur Client/Server-Authentisierung der Befehl COMPUTE DS verwendet wird. Durch Verwendung unterschiedlicher Befehle werden Mehrdeutigkeiten in Bezug auf die Verwendung von COMPUTE DS vermieden, somit ist die Wahl einer Sicherheitsumgebung nicht erforderlich.
- Für die C/S-Authentisierung wird die Authentisierungseingabe vom PC generiert und an die Chipkarte gesendet. Die Chipkarte stellt das Padding im Format PKCS #1 bereit und berechnet die digitale Signatur. Zumindest ein Teil des Paddings muss in der Chipkarte erfolgen, um bestehende Angriffe auf die Schlüssel zu vermeiden.
- Die Digest-Info liegt im Datenfeld des Befehls COMPUTE DIGITAL SIGNATURE vor. Dieser Mechanismus unterscheidet sich von der in Teil 1 beschriebenen Berechnung einer digitalen Signatur.
- Die Benutzerüberprüfung erfolgt mit Passwortreferenzen, die für die Signaturerstellung [lokales Passwort] und für die C/S-Authentisierung [globales Passwort] unterschiedlich sind.

6.5.6 Befehlsdatenfeld für die Client/Server-Authentisierung

6.5.6.1 RSA

Tabelle 13 — Befehlsdatenfeld für KERBEROS-Protokoll [3]

T	L	V	Bytes
—	—	$T = \text{DigestInfo}$	

Tabelle 14 — Befehlsdatenfeld für SSL/TLS

T	L	V	Bytes
—	—	$T = H_MD5 \parallel H_SHA1$, siehe [4] und [5]	

Tabelle 15 — Befehlsdatenfeld für WTLS

T	L	V	Bytes
—	—	$T = H_SHA1$, siehe [4]	

Die Chipkarte muss das Padding nach Bild 3 oder Bild 4 ausführen. Der Wert T ist entsprechend den oben stehenden Tabellen zu entnehmen.

6.5.6.2 ECDSA

Für ECDSA wird der Wert T mit Bits führender Nullen gepaddet.

6.5.6.3 Weitere Algorithmen

Alle übrigen Algorithmen verwenden die gepaddete (PKCS-#1-)Authentisierungseingabe im Datenfeld.

Tabelle 16 — Eingabe für weitere Algorithmen

T	L	V	Bytes
—	—	Authentisierungseingabe	

7 Rollenauthentisierung

7.1 Rollenauthentisierung der Karte

Diese Funktion ist optional.

Die C/S-Authentisierung beruht auf einem internen Authentisierungsprotokoll, bei dem der Server (Schnittstellengerät) die Karte (Chipkarte) authentisiert. Dazu liest das Schnittstellengerät das Zertifikat der Karte (üblicherweise ein X.509-Zertifikat), das eine Erweiterung (entsprechend X.509) bereitstellen kann, die die Rolle bezeichnet, die dem Karteninhaber zum Zweck des Zugriffs auf einige auf dem Server gehostete reservierte Daten verliehen wurde. Der differentielle Zugriff auf diese Daten wird vom Server entsprechend den durch die Zertifikaterweiterungen definierten Regeln gesteuert. Diese Rollenauthentisierung der Karte ist anwendungsspezifisch und in diesem Dokument nicht weiter beschrieben.