

## Technischer Standard für die elektronische Einreichung von europäischen Patentanmeldungen und anderen Unterlagen

### 1. Hintergrund

Das vorliegende Dokument enthält die technischen Standards für die elektronische Einreichung von Dokumenten beim EPA. Sie basieren auf dem im Rahmen der dreiseitigen Zusammenarbeit vereinbarten PKI-Standard (Public Key Infrastructure), der in Anlage F Anhang I der Verwaltungsvorschriften zum PCT aufgenommen worden ist.

Eine PKI-Umgebung bietet verschiedene Möglichkeiten zur Verarbeitung vertraulicher Informationen und wird aufgrund der Verschlüsselung der Daten folgenden Erfordernissen gerecht:

- a) Authentizität: Es wird sichergestellt, daß Übermittlungen, Nachrichten und Absender echt sind und ein Empfänger berechtigt ist, bestimmte Kategorien von Informationen zu erhalten.
- b) Datenintegrität: Es wird gewährleistet, daß die Ausgangsdaten unverändert sind und nicht versehentlich oder mutwillig geändert, verfälscht oder zerstört wurden.
- c) Nachweisbarkeit: Ausreichend schlüssige und zuverlässige Nachweise bieten dem Absender von Daten (unter Mithilfe des Empfängers) die Gewähr, daß die Daten zugeestellt wurden, und verschaffen dem Empfänger Gewißheit über die Identität des Absenders, so daß keiner von beiden abstreiten kann, im Besitz der Daten gewesen zu sein, und auch Dritte die Integrität und die Herkunft der Daten überprüfen können.
- d) Vertraulichkeit: Es wird gewährleistet, daß die Informationen nur von Berechtigten eingesehen werden können.

Dieser Standard umfaßt neben den obligatorischen Erfordernissen für alle an der elektronischen Einreichung beteiligten Parteien auch eine Reihe fakultativer Erfordernisse.

### 2. Umfang

Dieser technische Standard deckt die Erfordernisse in folgenden Bereichen ab:

- a) Sicherheit und PKI
- b) elektronische Signatur
- c) Dokumentenformat
- d) Einreichung

### 3. Sicherheit und PKI

#### 3.1 Public Key Infrastructure

Im Rahmen dieses Standards wird das Datenpaket nach der PKI-Technologie zusammengestellt und übertragen. Wenn künftig andere praktikable Sicherheitstechnologien zur Verfügung stehen, können diese in aktualisierte Fassungen des Standards aufgenommen werden.

Die Umsetzung von PKI-Systemen muß den Empfehlungen entsprechen, die von der Working Group on PKI Interoperability (PKIX) der Internet Engineering Task Force (IETF) aufgestellt wurden und in IETF RFC 2459 dokumentiert sind.

Für die digitale Signatur und die Verschlüsselung müssen jeweils eigene Schlüsselpaare und digitale Zertifikate verwendet werden.

#### 3.2 Digitale Zertifikate

Soweit in diesem Standard die Verwendung digitaler Zertifikate vorgesehen ist, müssen diese der ITU-Empfehlung X.509 Version 3 zum Format von Zertifikaten entsprechen (ITU = International Telecommunication Union).

Für die Online-Kommunikation mit dem EPA ist ein digitales Zertifikat erforderlich.

Der Standard sieht zwei Kategorien digitaler Zertifikate vor:

*Hochwertiges Zertifikat:* Digitales Zertifikat, das eine Zertifizierungsstelle dem Anmelder ausstellt und das zur Authentifizierung der Identität des Anmelders verwendet werden kann. Die Zertifizierungsstelle muß in der vom EPA veröffentlichten Liste der anerkannten Zertifizierungsstellen aufgeführt sein (siehe 3.3).

*Einfaches Zertifikat:* Digitales Zertifikat, das das EPA dem Anmelder auf Antrag ausstellt. Für ein solches einfaches Zertifikat muß der Anmelder seinen Namen und seine E-Mail-Adresse angeben, seine Identität aber nicht nachweisen.

#### 3.3 Zertifizierungsstellen

Das EPA legt fest, welche Zertifizierungsstellen es anerkennt. Die Liste der anerkannten Zertifizierungsstellen wird auch einen Link zu den veröffentlichten PKI-Richtlinien dieser Zertifizierungsstellen umfassen.

Eine anerkannte Zertifizierungsstelle muß fortlaufend die Richtigkeit der elektronischen Zertifikate gewährleisten, die "nachweisen", daß der Betreffende tatsächlich derjenige ist, der er zu sein behauptet. Die Zertifizierungsstelle archiviert die Zertifizierungsdaten für alle von ihr ausgestellten Zertifikate in einer Verzeichnisstruktur, die der ITU-Empfehlung X.500 entspricht. Für die Veröffentlichung und den Abruf digitaler Benutzerzertifikate gibt es eine externe Schnittstelle entsprechend dem Lightweight Directory Access Protocol (LDAP) und RFC 1777 der IETF Network Working Group vom März 1995. Außerdem veröffentlicht die Zertifizierungsstelle Daten zur Sperrung von Zertifikaten gemäß dem Standard X.509.

Diese Sperrdaten werden vom EPA regelmäßig bezogen. Wird ein Zertifikat zur Authentifizierung einer Einzelperson verwendet, so konsultiert das EPA die von der betreffenden Zertifizierungsstelle veröffentlichten Sperrdaten, um sich zu vergewissern, daß das Zertifikat nicht gesperrt wurde.

#### 3.4 Digitale Signaturen

Digitale Signaturen, die bei der elektronischen Einreichung zur Unterzeichnung elektronischer Dokumente verwendet werden, müssen in Format und Anwendung der Definition des Datentyps "signierte Daten" unter "signed data content type" in der Version 1.5 des von RSA Laboratories festgelegten Standards PKCS#7 zur Syntax verschlüsselter Nachrichten (Cryptographic Message Syntax Standard) entsprechen.

Zur Erzeugung solcher Signaturen ist ein Zertifikat zu verwenden, das den in Abschnitt 3.2 dargelegten Erfordernissen genügt.

Alle digitalen Signaturen sind entsprechend den in der ITU-Empfehlung X.690 festgelegten DER-Codierungsregeln (Distinguished Encoding Rules) zu codieren.

### 3.5 Verschlüsselungsalgorithmen

Je nach Bedarf können symmetrische Algorithmen (geheimer Schlüssel) oder asymmetrische Algorithmen (öffentlicher Schlüssel) verwendet werden. Algorithmen, die nach dem nationalen Recht eines bestimmten Landes verboten sind, dürfen nicht für die elektronische Einreichung von Dokumenten aus diesem Land verwendet werden. In Hard- oder Software implementierte Algorithmen dürfen nicht in einer Weise verwendet werden, die gegen etwaige Exportbeschränkungen des Herkunftslandes der Hard- oder Software verstößt.

Soweit möglich ist zur asymmetrischen Verschlüsselung der rsaEncryption-Algorithmus und zur symmetrischen Verschlüsselung der dES-EDE3-CBC-Algorithmus zu verwenden. Derselbe asymmetrische Verschlüsselungsalgorithmus ist auch bei der Erstellung digitaler Zertifikate und Signaturen sowie bei der Versiegelung einzusetzen.

### 3.6 Versiegelung der Daten

Elektronische Dokumentendaten, die bei der elektronischen Einreichung aus Gründen der Vertraulichkeit verschlüsselt werden, müssen in Format und Anwendung der Definition des Datentyps "signierte und versiegelte Daten" unter "signed and enveloped data content type" in der Version 1.5 des von RSA Laboratories festgelegten Standards PKCS#7 zur Syntax verschlüsselter Nachrichten entsprechen.

### 3.7 Hash-Algorithmen

Aus dem Datenstrom der Nachricht ist mit dem sehr sicheren Einweg-Hash-Algorithmus SHA-1 der Hash-Wert zu ermitteln.

## 4. Signaturverfahren

Dieser Standard sieht verschiedene Arten von Signaturen vor, die bei der elektronischen Einreichung akzeptiert werden:

- a) einfache elektronische Signatur
  - i) Faksimile-Abbildung der Unterschrift des Benutzers
  - ii) Zeichenkette
- b) komplexe elektronische Signatur
  - i) digitale Signatur gemäß PKCS#7

**ANMERKUNG:** Der Benutzer muß zwar das eigentliche Dokument nicht unbedingt mit einer komplexen elektronischen Signatur versehen, braucht aber eine digitale Signatur gemäß PKCS#7, um die gebündelten Anmeldeunterlagen zum Paket zusammenzustellen (siehe 5.3). Ein Beispiel für ein gebündeltes und signiertes Paket ist in Abschnitt 6.1 dargestellt.

Die einfache elektronische Signatur wird im Bereich "party" des XML-Dokuments codiert (siehe nachstehender Teil der Dokumententypdefinition/DTD):

```

...
<!ELEMENT electronic-signature (basic-signature, enhanced-signature?) >
<!ATTLIST electronic-signature
    DATE-SIGNED CDATA #REQUIRED
    PLACE-SIGNED CDATA #IMPLIED >

    <!ELEMENT basic-signature (fax | text-string) >

        <!ELEMENT fax EMPTY >
        <!ATTLIST fax
            FILE-NAME ENTITY #REQUIRED >

        <!ELEMENT text-string (#PCDATA) >

    <!ELEMENT enhanced-signature (pkcs7) >

    <!ELEMENT pkcs7 EMPTY >
...

```

Eine einfache elektronische Signatur im XML-Dokument kann durch eine digitale Signatur der gebündelten Anmeldungsunterlagen ergänzt werden.

#### 4.1 Faksimile-Abbildung

Zur Erzeugung einer solchen Signatur muß die XML-Datei das Element <fax> und im Attribut FILE-NAME einen Verweis auf die externe Datei mit der Bitmap der Signatur enthalten:

```
...
<electronic-signature DATE-SIGNED="01/01/2000">
  <basic-signature>
    <fax FILE-NAME="signature.tif" />
  </basic-signature>
</electronic-signature>
...
```

Als Bitmap-Datei ist eine Abbildung des Formats TIFF-Gruppe 4, 300 dpi, einfacher Streifen, Intel-Codierung oder eine JFIF-(JPEG-)Datei vorgeschrieben.

#### 4.2 Zeichenkette

Zur Erzeugung einer solchen Signatur muß das XML-Dokument das Element <text-string> mit einer Zeichenkette enthalten, die in Schrägstriche ("/") gesetzt ist und als "handschriftliche" Unterschrift des Benutzers gilt:

```
...
<electronic-signature DATE-SIGNED="01/01/2000">
  <basic-signature>
    <text-string>/janedoe/</text-string>
  </basic-signature>
</electronic-signature>
...
```

Die Zeichenkette ist eine Folge von Zeichen (ohne Schrägstrich "/"), die der Benutzer als elektronische Signatur wählt. Beispiele:

```
...
<text-string>/John Smith/</text-string>
<text-string>/Tobeornottobe/</text-string>
<text-string>/1345728625235/</text-string>
<text-string>/Günter François/</text-string>
...
```

#### 4.3 Digitale Signatur gemäß PKCS#7

Signierte Daten gemäß PKCS#7 werden aus der elektronischen Nachricht erzeugt, indem der Unterzeichner den Hash-Wert mit seinem privaten Signaturschlüssel verschlüsselt. Wenn sie versandt werden, umfassen sie auch eine Kopie des digitalen Zertifikats des Unterzeichners.

Die Verwendung einer Signatur gemäß PKCS#7 ist in der XML-Datei durch das Element <pkcs7> anzugeben:

```
...
<electronic-signature DATE-SIGNED="01/01/2000">
  <enhanced-signature>
    <pkcs7 />
  </enhanced-signature>
</electronic-signature>
...
```

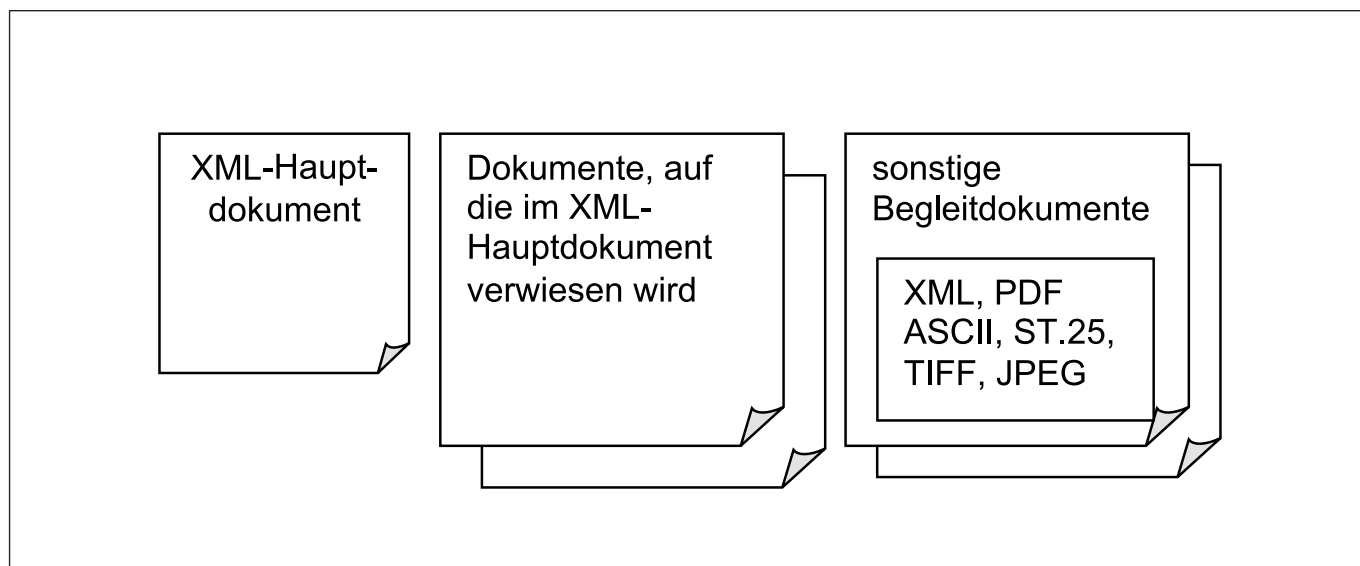
### 5. Datenformat

Beim Zusammenstellen der Dokumente zu einem Paket werden die Daten, die Auskunft darüber geben, was übertragen wird, mit den übertragenen Daten zu einem einzigen binären Objekt, den sogenannten gebündelten Anmeldungsunterlagen (WAD - Wrapped Application Documents), zusammengefaßt und dann mit einer geeigneten digitalen Signatur versehen und verschlüsselt.

#### 5.1 Vorbereitung der Dokumente

Zu jedem eingereichten Dokument gibt es ein XML-Hauptdokument, das gegebenenfalls explizite Verweise auf alle Unterlagen enthält, die zusammen übermittelt werden. Diese Verweisdokumente bilden eine logische Einheit mit dem Hauptdokument (z. B. eine neue Patentanmeldung). Darüber hinaus können zu einem Hauptdokument noch Begleitdokumente vorliegen (z. B. Erfindernennung oder Gebührenzahlung).

Das XML-Hauptdokument muß einer der nachstehend spezifizierten Dokumententypdefinitionen (DTD) entsprechen. Bei den Verweisdokumenten (externen Einheiten) handelt es sich in der Regel um eingebettete Abbildungen, Tabellen, Zeichnungen oder andere Verbunddokumente, die auf der Grundlage von XML, ST.25, PDF, ASCII, TIFF oder JFIF (JPEG) codiert sein können. Die Begleitdokumente sind eigenständige, aber zugehörige Dokumente im XML-, ST.25-, PDF-, ASCII- oder Bild-Format. Begleitdokumente im XML-Format müssen ebenfalls einer der nachstehend spezifizierten DTD entsprechen.



**5.1.1 Zeichencodierte Formate**

**5.1.1.1 XML**

Alle XML-Dokumente müssen einer der nachstehend spezifizierten DTD entsprechen. Anmelder können XML-Dokumente, die diesem Standard genügen, mit der Client-Software des EPA für die elektronische Einreichung erstellen.

Der codierte Zeichensatz für alle XML-Dokumente darf nicht über den des ISO/IEC-Standards 10646:2000 (Unicode 3) hinausgehen. Das Standard-Codierungssystem für XML-Dokumente ist UTF-8.

**5.1.1.2 ST.25**

Ein Dokument, das mit SGML-Tags für Sequenzprotokolle entsprechend WIPO-ST.25 erstellt wurde, kann als externes Dokument in die gebündelten Anmeldungsunterlagen aufgenommen werden.

**5.1.1.3 ASCII**

Ein in reinem ASCII-Text erstelltes Dokument kann als externes Dokument in die gebündelten Anmeldungsunterlagen aufgenommen werden. Dann muß das XML-Hauptdokument die Codeseite des ASCII-Texts enthalten.

**5.1.2 PDF**

Die bei der elektronischen Einreichung verwendeten PDF-Dokumente müssen folgenden Erfordernissen genügen:

- a) kompatibel mit PDF Version 1.3
  - b) Text nicht komprimiert (zur Erleichterung der Suche)
  - c) Text nicht verschlüsselt
  - d) keine digitalen Signaturen
  - e) keine eingebetteten OLE-Objekte
  - f) Alle Fonts müssen eingebettet sein, dem Standard PS17 entsprechen oder auf Adobe® Multiple Master (MM) Fonts basieren.
- Das PDF-Format hat sich zum De-facto-Standard für den Austausch formatierter Dokumente im Internet entwickelt.

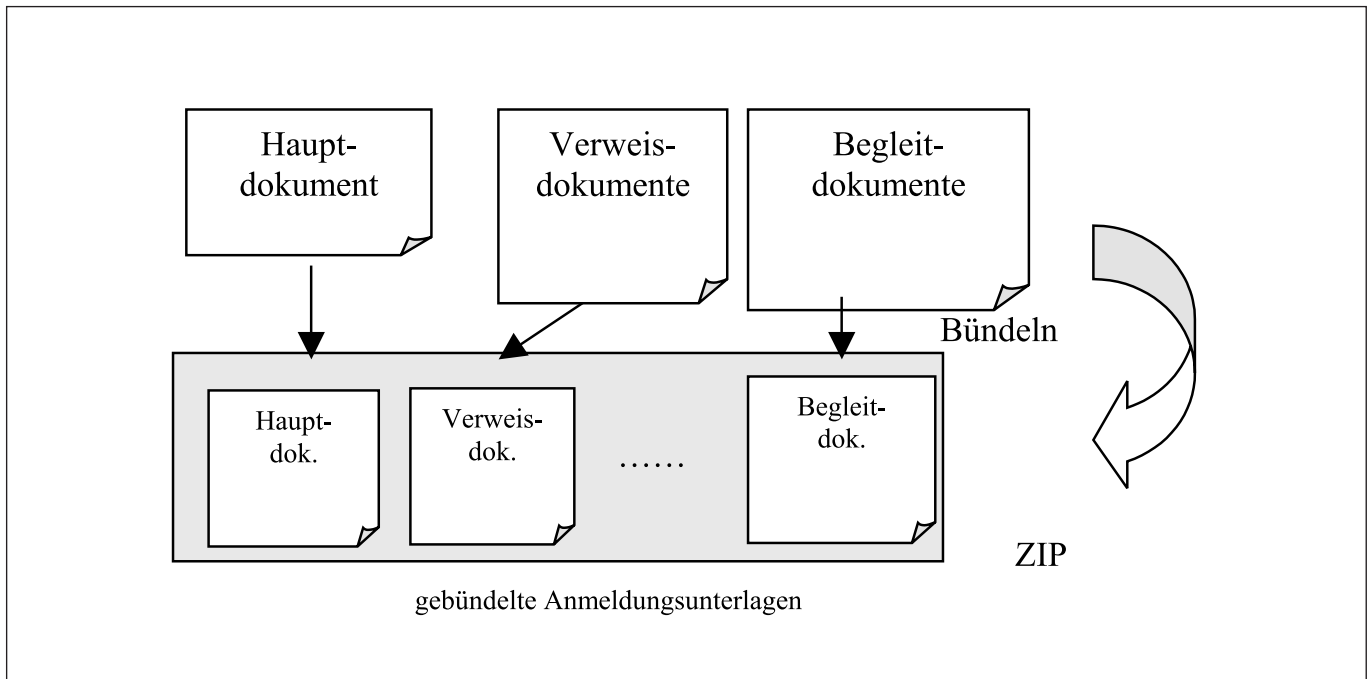
**5.1.3 Abbildungen**

Die Faksimile-Abbildungen, die bei der elektronischen Einreichung verwendet werden, müssen folgenden Erfordernissen genügen:

- Format
  - TIFF Version 6.0 mit Komprimierung Gruppe 4, einfacher Streifen, Intel-Codierung oder
  - JFIF (JPEG)
- 200, 300 oder 400 dpi
- A4-Format

**5.2 Bündelung der Dokumente**

Das Hauptdokument wird mit allen externen Verweisdokumenten und allen Begleitdokumenten zu einem einzigen Datenblock zusammengefaßt. Dieser Datenblock – die gebündelten Anmeldungsunterlagen – wird nach dem ZIP-Standard erstellt. Zur Zusammenstellung der Dokumentendateien einer elektronischen Anmeldung müssen die Anmelder eine Software für die Archivierung und Komprimierung im ZIP-Format verwenden.



Die zur Erstellung der ZIP-Datei verwendete Software muß den in der "PKZIP® Application Note" von PKWARE® veröffentlichten Spezifikationen des ZIP-Dateiformats entsprechen (revidierte Fassung vom 1.8.1998).

Alle in diesem Standard genannten Teile des Dokuments müssen im ZIP-Format zusammengefaßt werden. Die eingereichte ZIP-Datei muß alle externen Dateien enthalten, auf die in der Anmeldung verwiesen wird. Im Hauptverzeichnis der ZIP-Datei enthaltene Dateinamen müssen der Spezifikation für das jeweilige Betriebssystem entsprechen.

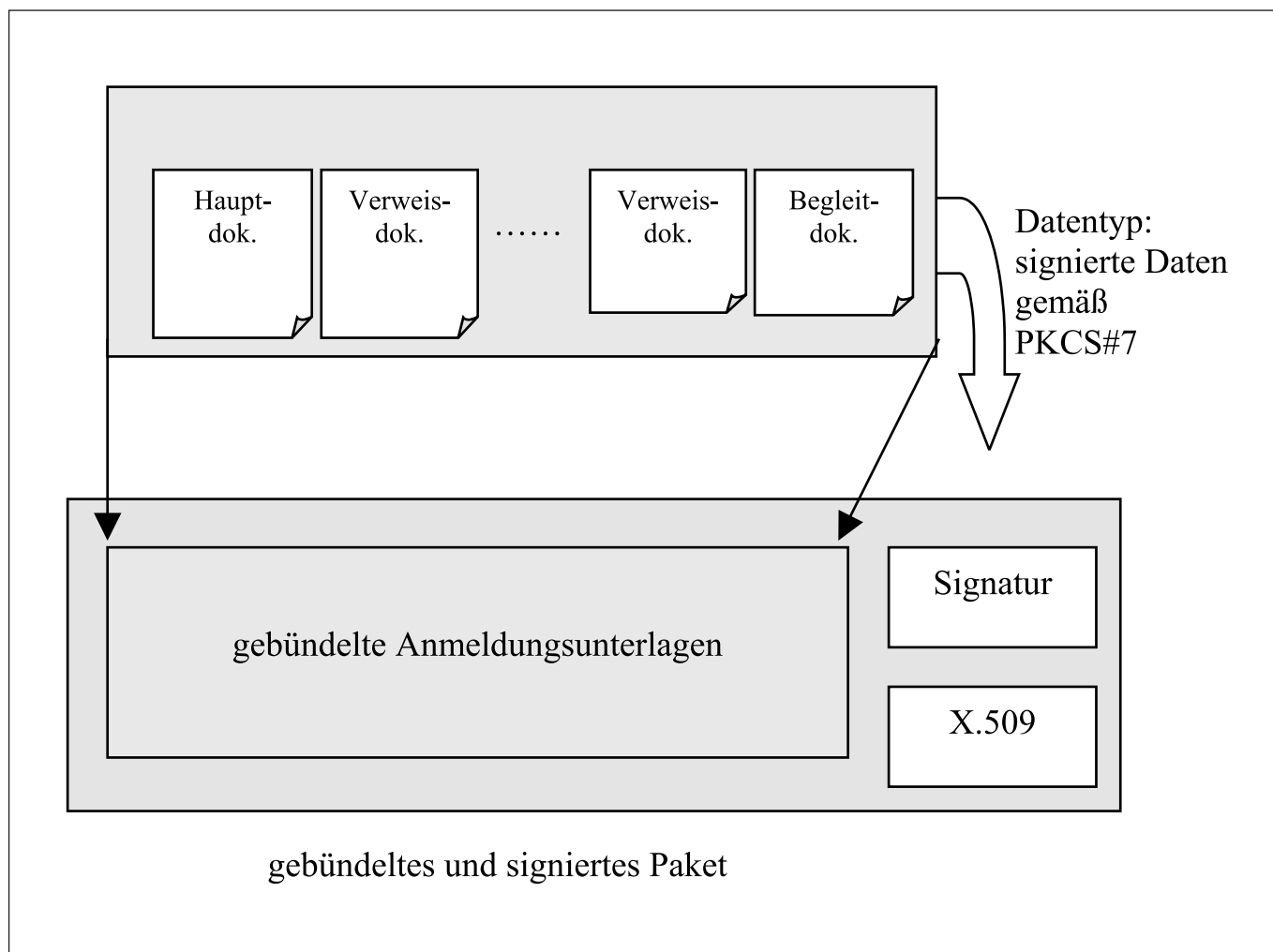
Eine ZIP-Datei muß eine flache Verzeichnisstruktur aufweisen. Wenn eine Sammlung von Dateien in die ZIP-Datei eingebettet werden muß, sind diese als eine einzige flache eingebettete ZIP-Datei aufzunehmen.

Nach dem ZIP-Standard kann die Komprimierungssoftware mit verschiedenen Komprimierungsalgorithmen arbeiten. Als standardmäßiges Komprimierungsverfahren ist das "Deflation"-Verfahren zu wählen.

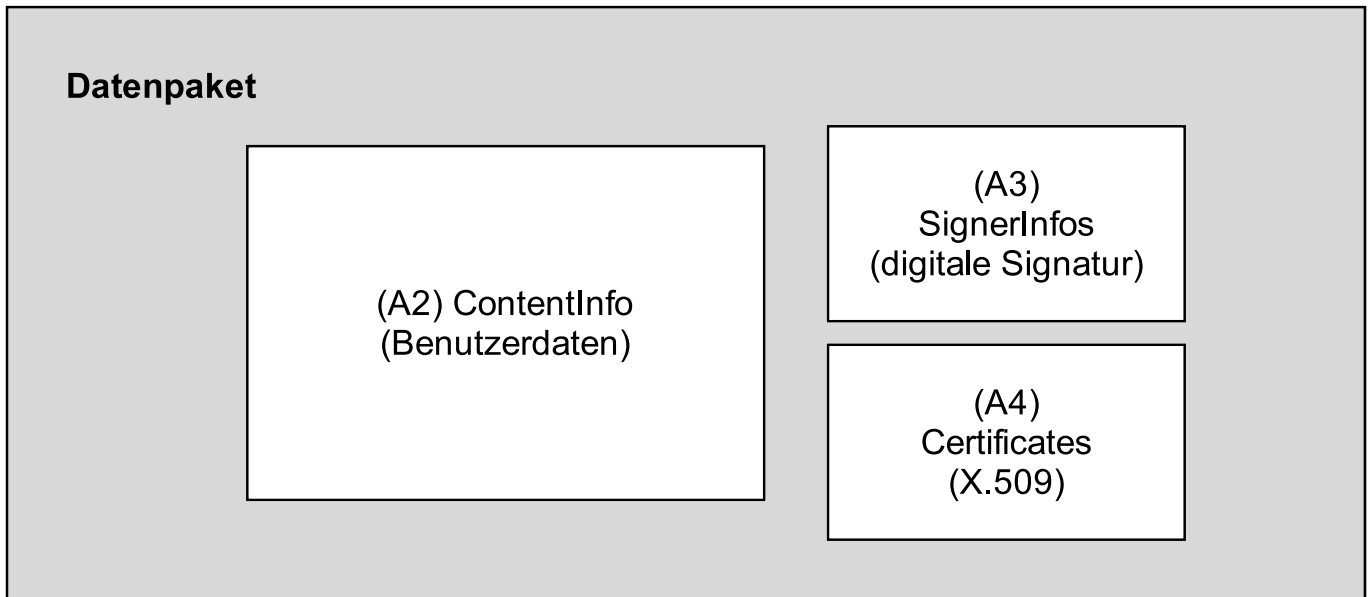
### 5.3 Signatur der gebündelten Anmeldungsunterlagen

Zur Bindung der Person, die das Paket zusammenstellt, an die gebündelten elektronischen Anmeldungsunterlagen wird eine digitale Signatur hinzugefügt und so das gebündelte und signierte Paket erstellt. Die Signatur gewährleistet, daß diese Person identifiziert werden kann und der Empfänger etwaige unbefugte Veränderungen während des Übertragungsvorgangs feststellen kann.

Zur Erzeugung eines Datentyps "signierte Daten" für die Signatur ist PKCS#7 zu verwenden.



**(A1) Signed Data <oberste Ebene>  
(digitale Versiegelung für die Signatur gemäß PKCS#7)**



Regeln für die digitale Versiegelung der Daten zur Zertifizierung gemäß PKCS#7

Objektbezeichner für SHA-1	Der gewählte Objektbezeichner für SHA-1 ist in OIW interconnection protocols, Teil 12 wie folgt definiert: <b>sha-1 OBJECT IDENTIFIER ::= {iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 26}</b>
Objektbezeichner für RSA-Verschlüsselung	Der Objektbezeichner für RSA-Verschlüsselung ist im Standard <i>PKCS#1 - RSA Encryption</i> wie folgt definiert: <b>pkcs-1 OBJECT IDENTIFIER ::= {iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1}</b> <b>rsaEncryption OBJECT IDENTIFIER ::= {pkcs-1 1}</b>
Objektbezeichner für Triple DES	<b>dES-EDE3-CBC OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) encryptionAlgorithm(3) 7}</b>

**Tabelle A1: SignedData – oberste Ebene**

Nr.	Bezeichnung	Bezeichnung in PKCS#7	Inhalt
1	Version	Version	ganzzahligen Wert '1' setzen
2	Satz von Algorithmusbezeichnern	DigestAlgorithms	
2.1	Algorithmusbezeichner	AlgorithmIdentifier	nur EINEN Satz von Algorithmusbezeichnern setzen {sha-1}
3	Information zum Inhalt	ContentInfo	eine Information zum Inhalt setzen (s. Tabelle A2)
4	Zertifikate	Certificates	ein Zertifikat setzen (s. Tabelle A4)
5	Sperrlisten	Crls	nicht belegt (keine Daten setzen)
6	Information zum Unterzeichner	SignerInfos	eine Information zum Unterzeichner setzen (s. Tabelle A3)

**Tabelle A2: ContentInfo** – oberste Ebene

Nr.	Bezeichnung	Bezeichnung in PKCS#7	Inhalt
1	Art des Inhalts	ContentType	Objektbezeichner setzen {pkcs-7 1}
2	Inhalt	Content	Benutzerdaten setzen (binär)

**Tabelle A3: SignerInfos** – oberste Ebene

Nr.	Bezeichnung	Bezeichnung in PKCS#7	Inhalt
1	Version	Version	ganzzahligen Wert '1' setzen
2	Ausgabestelle und laufende Nummer	IssuerAndSerialNumber	Ausgabestelle und laufende Nummer des Zertifikats gemäß X.509 (Zertifikat des Unterzeichners)
3	Satz von Hash-Algorithmen	DigestAlgorithm	
3.1	Algorithmusbezeichner	AlgorithmIdentifier	zur Erzeugung des Hash-Werts der digitalen Signatur NUR EINEN <b>Satz</b> VON Algorithmusbezeichnern setzen {sha-1}
4	authentifizierte Attribute	AuthenticatedAttributes	nicht belegt (keine Daten setzen)
5	Algorithmus zur Verschlüsselung des Hash-Werts	DigestEncryptionAlgorithm	Objektbezeichner für den Algorithmus zur Verschlüsselung des Hash-Werts (empfohlener Algorithmus: rsaEncryption)
6	verschlüsselter Hash-Wert	EncryptedDigest	Hash-Wert, der mit privatem Schlüssel des Unterzeichners verschlüsselt wird
7	nicht authentifizierte Attribute	UnauthenticatedAttributes	nicht belegt (keine Daten setzen)

**Tabelle A4: Certificates** – oberste Ebene

Nr.	Bezeichnung	Bezeichnung in PKCS#7	Inhalt
1	Satz von Zertifikaten	ExtendedCertificatesAndCertificates	
1.1	Zertifikat gemäß X.509	Certificate (gemäß Definition in X.509)	nur EINEN <b>Satz</b> von Zertifikatdaten gemäß X.509 setzen

**6. Einreichung**

**6.1 Übertragungspaket**

Das EPA kann auf die in diesem Abschnitt beschriebene Versiegelung zur Verschlüsselung für Übertragungszwecke verzichten, wenn eine Verschlüsselung auf der Ebene des Kanals wie SSL oder ein Datenträger wie CD-R eingesetzt wird.

Die tatsächlich übertragenen Daten, die zwischen dem Anmelder und dem EPA ausgetauscht werden, werden als Paket bezeichnet.

Je nach Paketart enthält das Paket verschiedene Datenelemente, darunter:

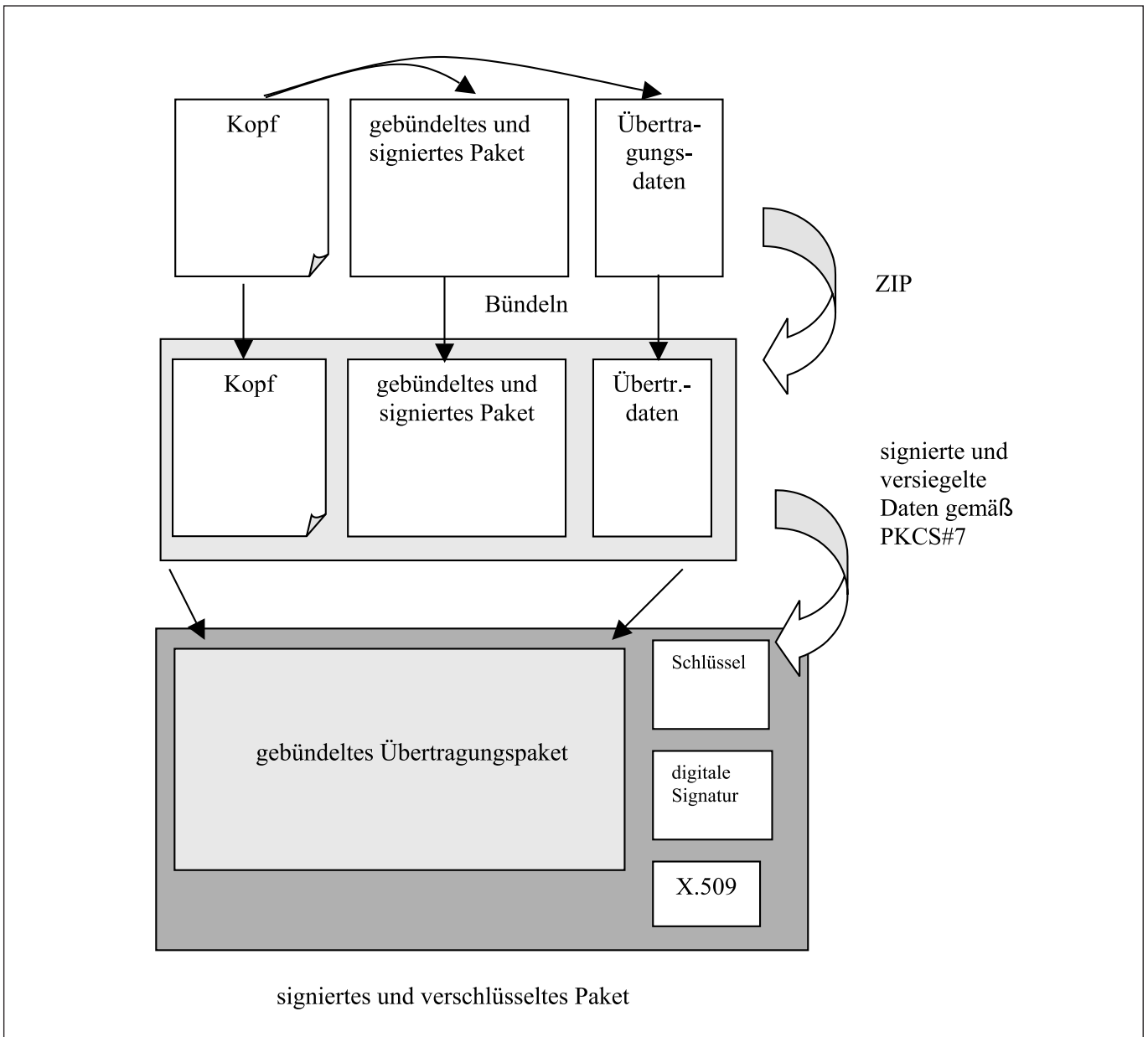
1. Datenelement "Kopf"
2. gebündeltes und signiertes Paket, das durch Bündelung und Signatur der Anmeldungsunterlagen entsteht
3. Übertragungsdaten, z. B. Zeitpunkt der Übertragung

Das Datenelement "Kopf" gibt Aufschluß über die Art des Pakets, den Dateinamen des Datenelements usw. Es befindet sich immer im signierten und verschlüsselten Paket und ist in XML abgefaßt.

Für die Erstellung des signierten und verschlüsselten Pakets gilt folgendes Verfahren:  
 a) Erstellung eines gebündelten Übertragungspakets durch weitere Bündelung des gebündelten und signierten Pakets und der für die Übertragung verwendeten Datenelemente mittels ZIP  
 b) Erstellung eines signierten und verschlüsselten Pakets für die Übertragung im Netz durch Verschlüsselung entsprechend der Definition des Datentyps "signierte und versiegelte Daten" unter "signed and enveloped data type" in PKCS#7

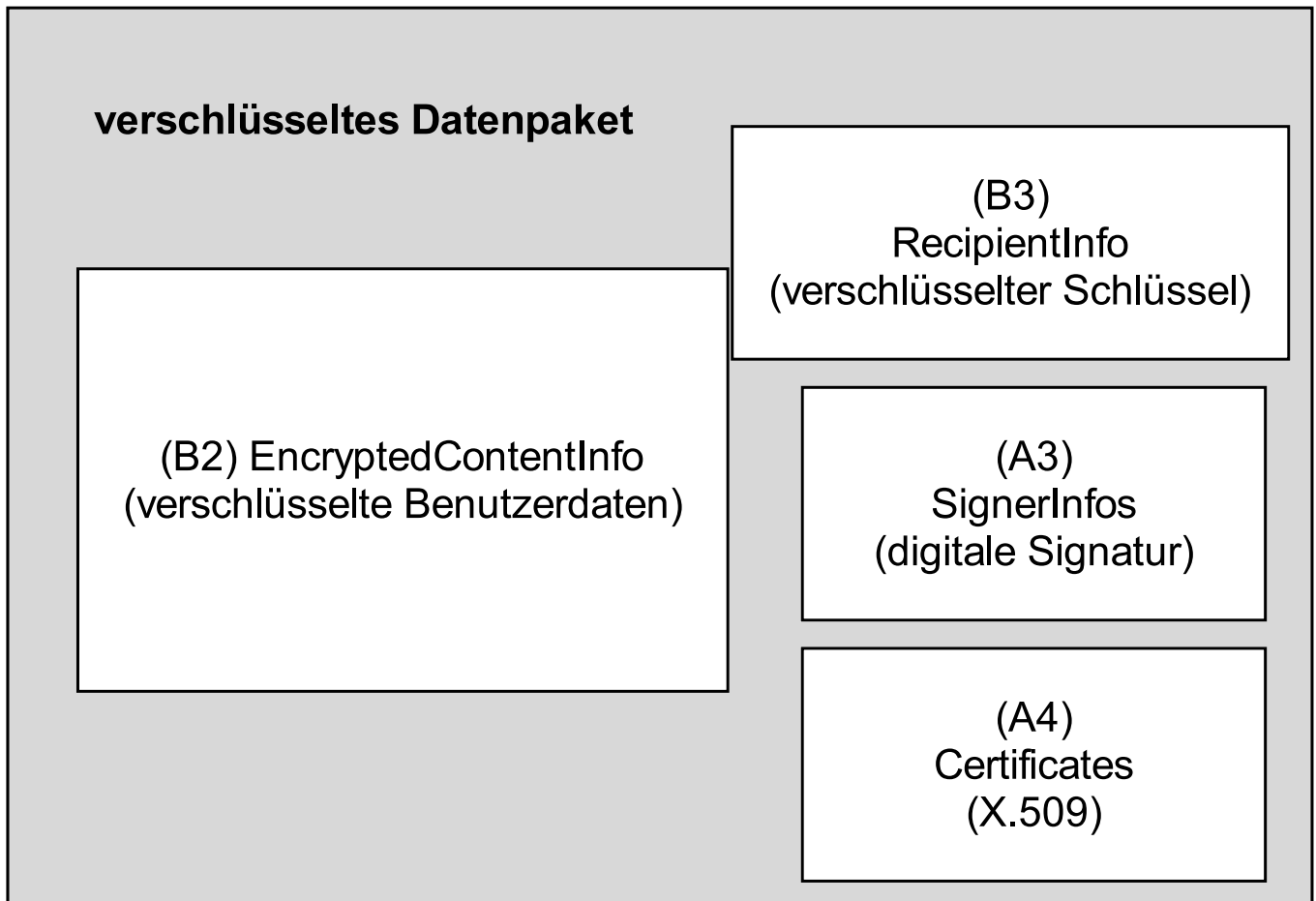
Die Signatur soll für Kombination und Inhalt der einzelnen Datenelemente bürgen und gewährleisten, daß der Empfänger feststellen kann, ob bei der Übertragung unbefugte Änderungen vorgenommen wurden. Die Verschlüsselung soll verhindern, daß Daten bei der Übertragung unbefugt abgefangen werden.

Die digitale Signatur für das gebündelte und signierte Paket kann vom Anmelder oder von seinem Vertreter erzeugt werden. Die digitale Signatur für das endgültige signierte und verschlüsselte Paket erzeugt derjenige, der die Übertragung einleitet.





**(B1) SignedAndEnveloped Data <oberste Ebene>**  
**(digitale Versiegelung für die Signatur gemäß PKCS#7)**



Regeln für die digitale Versiegelung zur Übertragung  
gemäß PKCS#7

**Tabelle B1: SignedAndEnvelopedData – oberste Ebene**

Nr.	Bezeichnung	Bezeichnung in PKCS#7	Inhalt
1	Version	Version	ganzzahligen Wert '1' setzen
2	Information zum Empfänger	RecipientInfos	NUR EINEN Satz von Informationen zum Empfänger setzen (s. Tabelle B3)
2	Satz von Algorithmusbezeichnern	DigestAlgorithms	
2.1	Algorithmusbezeichner	AlgorithmIdentifier	NUR EINEN Satz von Algorithmusbezeichnern setzen (sha-1)
3	Information zum verschlüsselten Inhalt	EncryptedContentInfo	eine Information zum verschlüsselten Inhalt setzen (s. Tabelle B2)
4	Zertifikate	Certificates	ein Zertifikat setzen (s. Tabelle A4)
5	Sperrlisten	Crls	nicht belegt (keine Daten setzen)
6	Information zum Unterzeichner	SignerInfos	eine Information zum Unterzeichner setzen (s. Tabelle A3)

**Tabelle B2: EncryptedContentInfo** – oberste Ebene

Nr.	Bezeichnung	Bezeichnung in PKCS#7	Inhalt
1	Art des Inhalts	ContentType	Objektbezeichner setzen {pkcs-7 1}
2	Verschlüsselungs- algorithmus für den Inhalt	ContentEncryptionAlgorithm	Objektbezeichner für den Algorithmus zur Verschlüsselung des Inhalts (empfohlener Algorithmus: dES-EDE3-CBC)
3	verschlüsselter Inhalt	EncryptedContent	verschlüsselte Benutzerdaten

**Tabelle B3: RecipientInfo** – oberste Ebene

Nr.	Bezeichnung	Bezeichnung in PKCS#7	Inhalt
1	Version	Version	ganzzahligen Wert '1' setzen
2	Ausgabestelle und laufende Nummer	IssuerAndSerialNumber	Ausgabestelle und laufende Nummer des Zertifikats, das den öffentlichen Schlüssel zur Verschlüsselung des Schlüssels für die Benutzerdaten enthält
3	Algorithmus zur Verschlüsselung des Schlüssels	KeyEncryptionAlgorithm	Objektbezeichner für den Algorithmus zur Verschlüsselung des Schlüssels für die Benutzerdaten (empfohlener Algorithmus: rsaEncryption)
4	verschlüsselter Schlüssel	EncryptedKey	verschlüsselter Schlüssel zur Entschlüsselung der Benutzerdaten

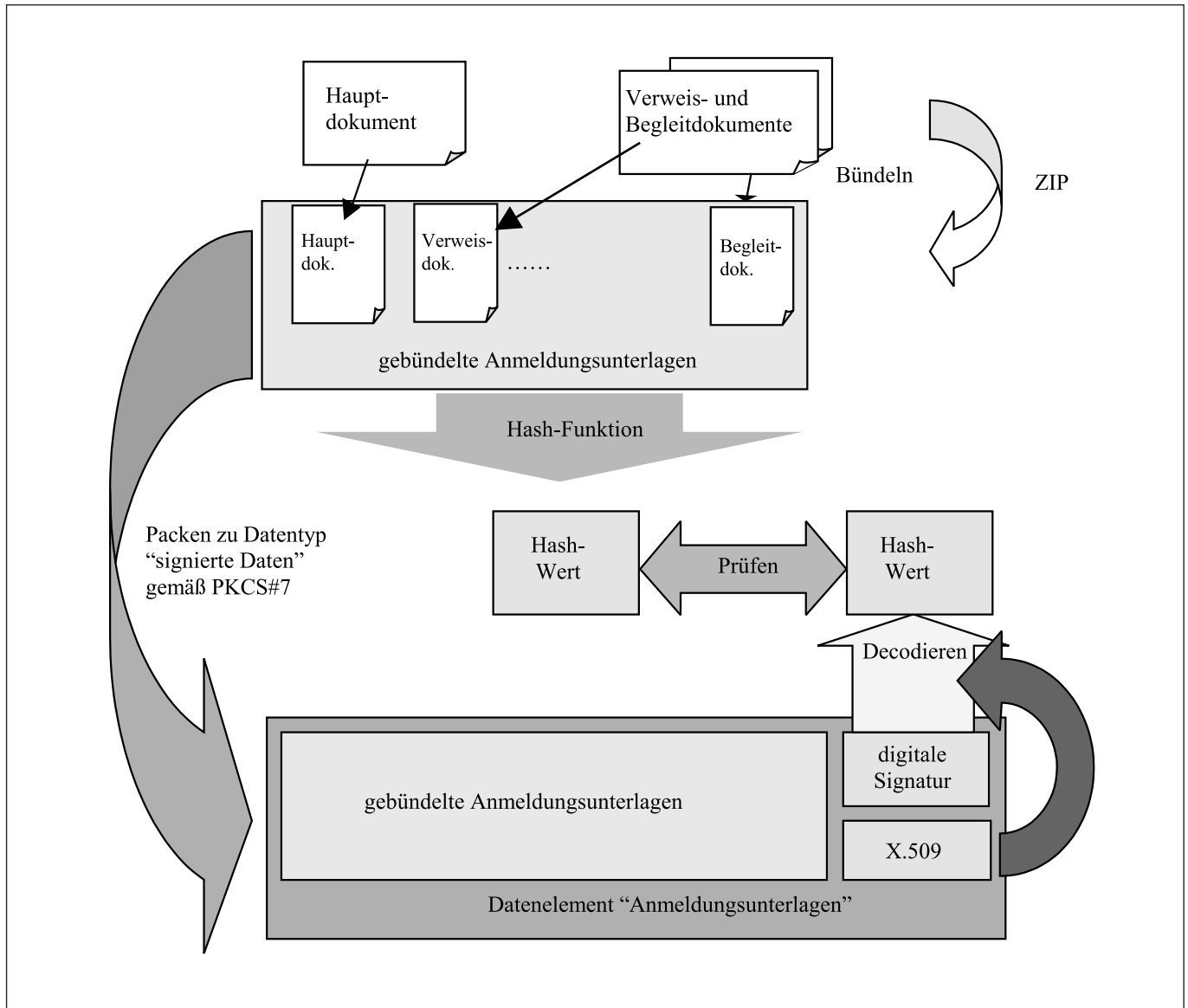
**6.2 Übertragungsverfahren**

Das Übertragungsverfahren läuft wie folgt ab:

- Zwischen dem Anmelder und dem EPA wird eine elektronische Verbindung hergestellt.
- Der Anmelder übermittelt das signierte und verschlüsselte Paket.
- Bei Eingang des signierten und verschlüsselten Pakets wird sein Inhalt auf Viren überprüft und der unverwech-

selbare Hash-Wert der gebündelten Anmeldungsunterlagen ermittelt.

- Dieser Hash-Wert wird mit dem im gebündelten und signierten Paket enthaltenen Hash-Wert verglichen. Bei Übereinstimmung erhält der Anmelder eine Empfangsbescheinigung; stimmen die Werte nicht überein, so wird der Anmelder entsprechend unterrichtet. Dann wird die Verbindung beendet.



**6.2.1 Prüfung des Hash-Werts**

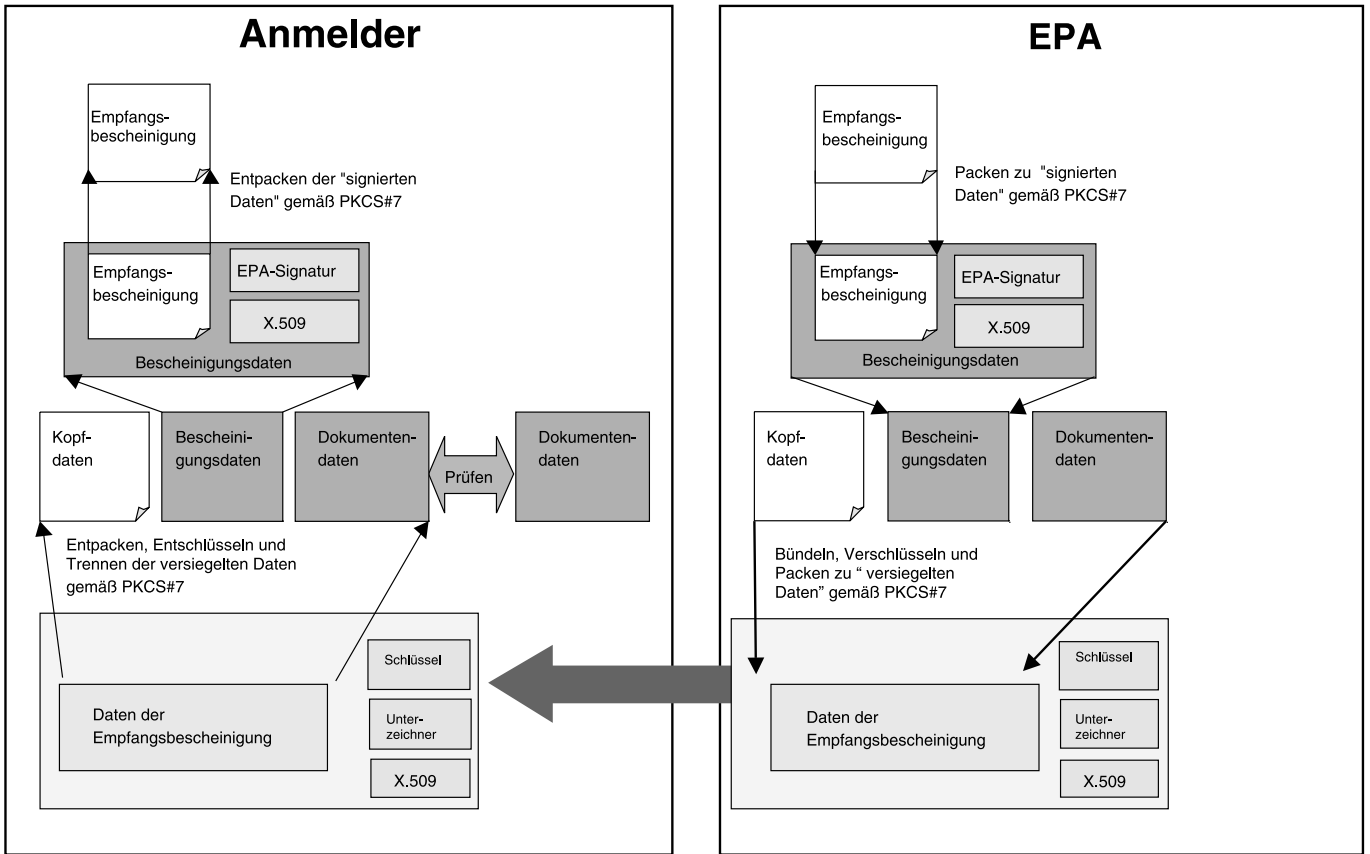
Das EPA nimmt die gebündelten Anmeldungsunterlagen entgegen, öffnet die darin enthaltenen Datenelemente und weist ihnen entsprechend den Angaben im Datenelement "Kopf" ihre Funktion zu.

Im Falle von Problemen bei der Übertragung oder beim Vergleich der Hash-Werte enthält die Empfangsbescheinigung Informationen zum aufgetretenen Problem.

**6.2.2 Empfangsbescheinigung**

Das Datenelement "Empfangsbescheinigung" umfaßt ein Datenelement "Bescheinigung", ein Datenelement "Kopf", das das entsprechende Paket als Empfangsbescheinigung ausweist, und fakultativ bei einer neuen Anmeldung ein Datenelement "Anmeldungsunterlagen".

Die Empfangsbescheinigung wird in Form eines signierten und verschlüsselten Pakets zusammengestellt (siehe vorstehende Beschreibung).



Die Empfangsbescheinigung unterrichtet den Anmelder über den Eingang der Anmeldung und muß eine XML-Version dieser Angaben enthalten. Darüber hinaus kann sie auch eine Version der Daten im PDF-Format umfassen. Diese Dateien werden zu einer einzigen ZIP-Datei zusammengefaßt und mit dem digitalen Zertifikat des EPA signiert.

### 6.3 Übertragungsprotokoll

Das EPA setzt ein Übertragungsprotokoll auf der Grundlage von HTTP in Verbindung mit SSL ein.

### 7. Datenträger

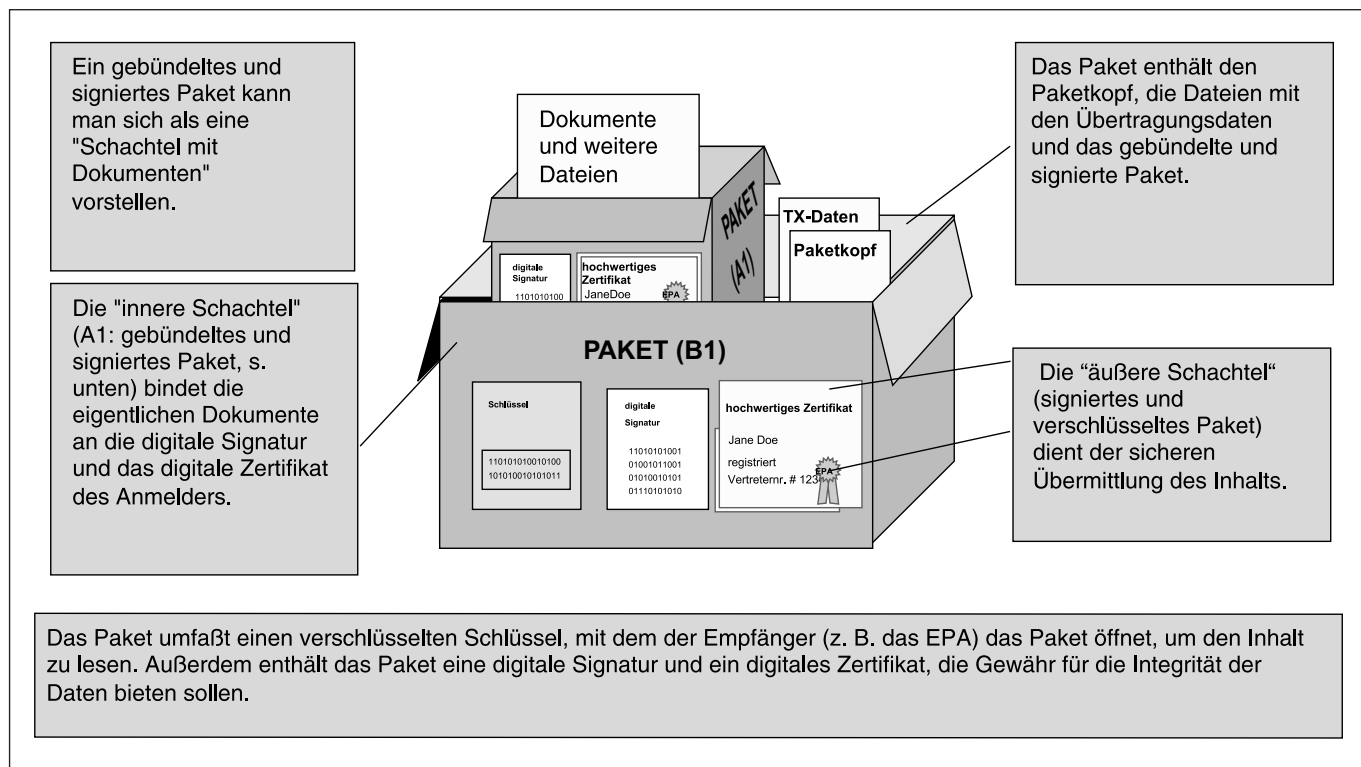
Das EPA akzeptiert auch eine elektronische Einreichung auf CD-R. Die CD-R darf nur eine Anmeldung in Form der signierten gebündelten Anwendungsunterlagen (WAD – Wrapped Application Documents) enthalten, die im Stammverzeichnis zu speichern sind und den Dateinamen "WAD.ZIP" haben sollten. Das Begleitschreiben muß nähere Einzelheiten zur Anmeldung bzw. zum Dokument umfassen und auf die "WAD.ZIP"-Datei auf der CD-R verweisen. Die Bezeichnung der CD-R muß auf der Anmeldernummer basieren.

**Anlage – Schaubilder zur Erläuterung des Standards**

Die folgenden Schaubilder und Textpassagen enthalten zusätzliche (vereinfachte) Erläuterungen zum Standard.

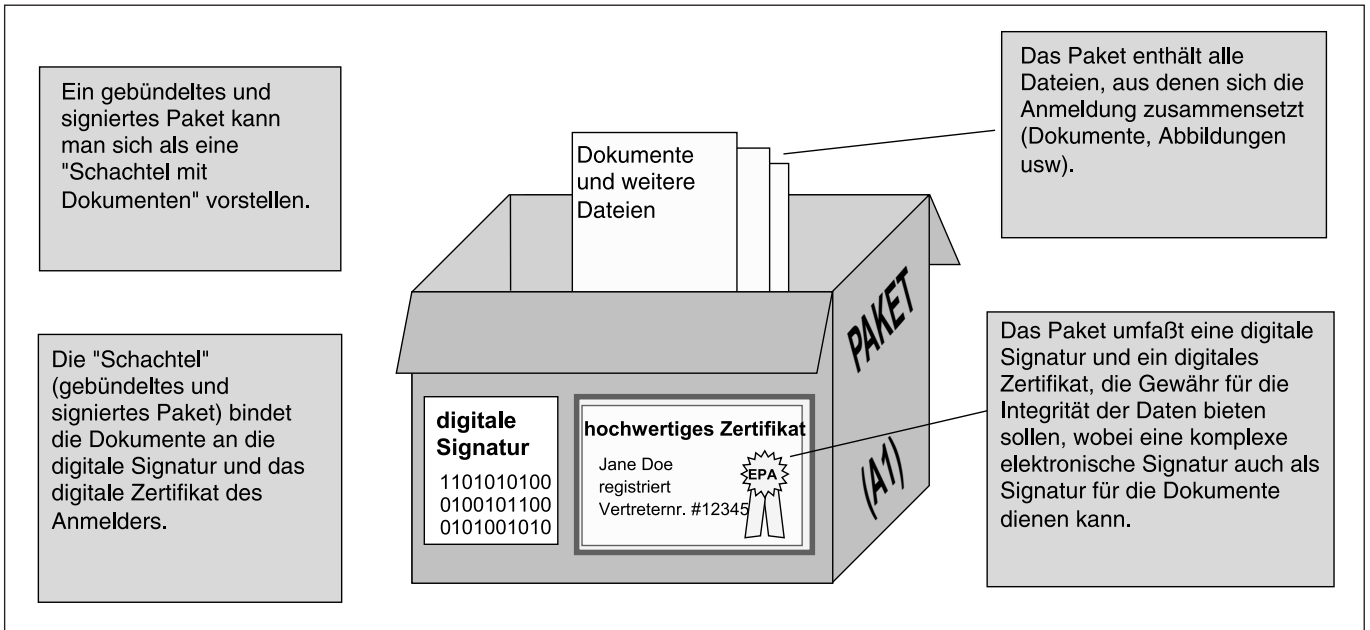
**Vereinfachte Darstellung des signierten und verschlüsselten Pakets**

Abbildung 1 veranschaulicht für den Laien, aus welchen Bestandteilen sich das signierte und verschlüsselte Paket gemäß dem vorliegenden Standard zusammensetzt. Die Abbildung wurde bewußt vereinfacht und verzichtet auf technische Details, die den Leser von den wesentlichen Aspekten des Paketaufbaus ablenken könnten. So wird in der Abbildung nicht auf die Bündelung zu einer "ZIP"-Datei und die Codierungsstandards für Objekte eingegangen.



**Abbildung 1: Signiertes und verschlüsseltes Paket**

**Vereinfachte Darstellung des gebündelten und signierten Pakets**



**Abbildung 2: Gebündeltes und signiertes Paket**

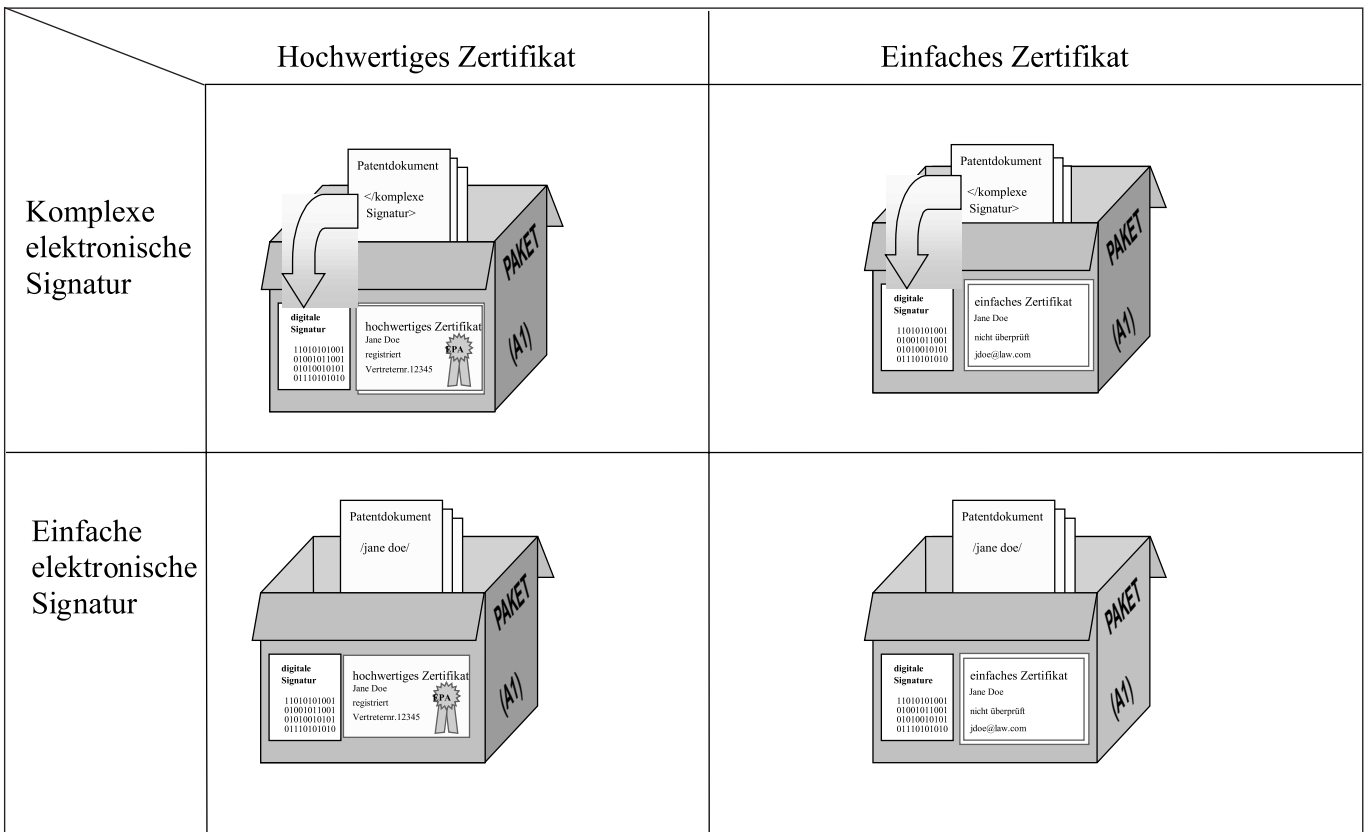
**Aufbau des Objekts "gebündelte Anmeldeunterlagen"**

In Abschnitt 5 wird festgelegt, wie die Dokumente zu "gebündelten Anmeldeunterlagen" zusammengefaßt werden. Im Falle der Offline-Einreichung auf Datenträgern sind die weiteren Schritte zur Erstellung des gebündelten und signierten Pakets sowie des signierten und verschlüs-

selten Pakets fakultativ. Die gebündelten Anmeldeunterlagen bestehen aus Dateien, die zu einer einzigen "ZIP"-Datei zusammengefaßt und im Stammverzeichnis des Datenträgers gespeichert sind.

**Arten von Zertifikaten/Signaturen**

Die Abbildungen 3 bis 7 sollen den Unterschied zwischen den im Standard festgelegten verschiedenen Arten von digitalen Zertifikaten und elektronischen Signaturen veranschaulichen. Jedes Schaubild zeigt eine "Schachtel", die das gebündelte und signierte Paket darstellt.



**Abbildung 3: Arten von Zertifikaten/Signaturen**

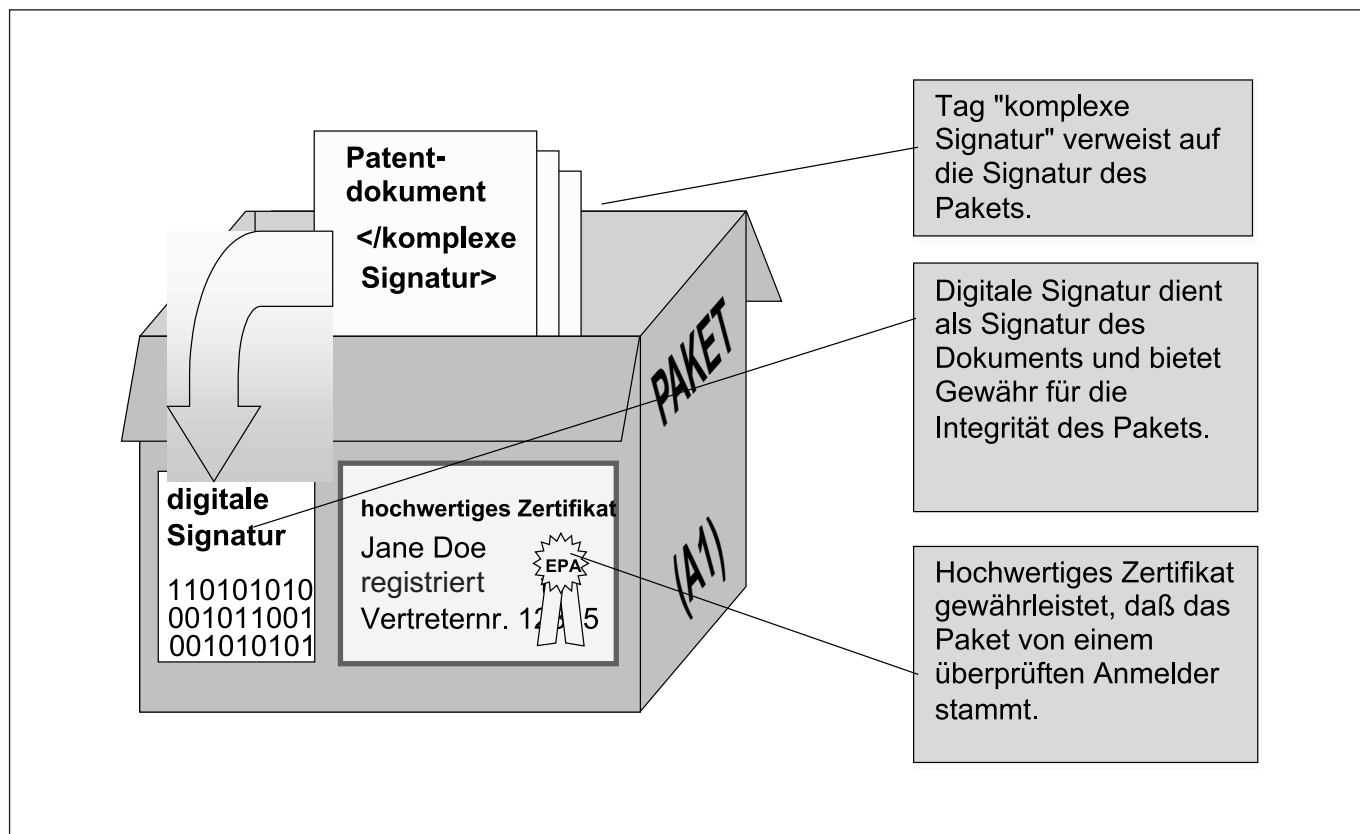


Abbildung 4: Komplexe elektronische Signatur/hochwertiges Zertifikat

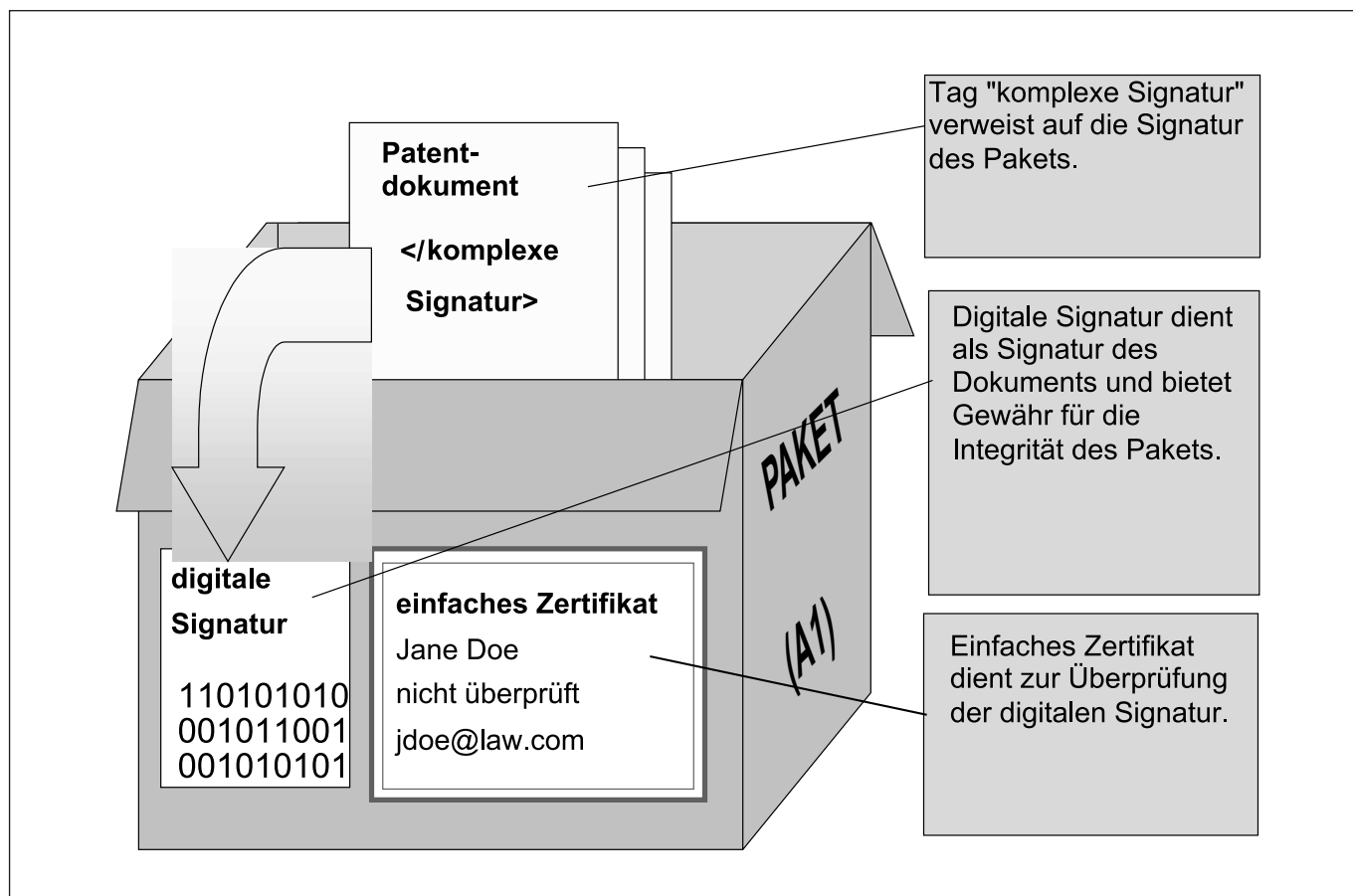


Abbildung 5: Komplexe elektronische Signatur/einfaches Zertifikat

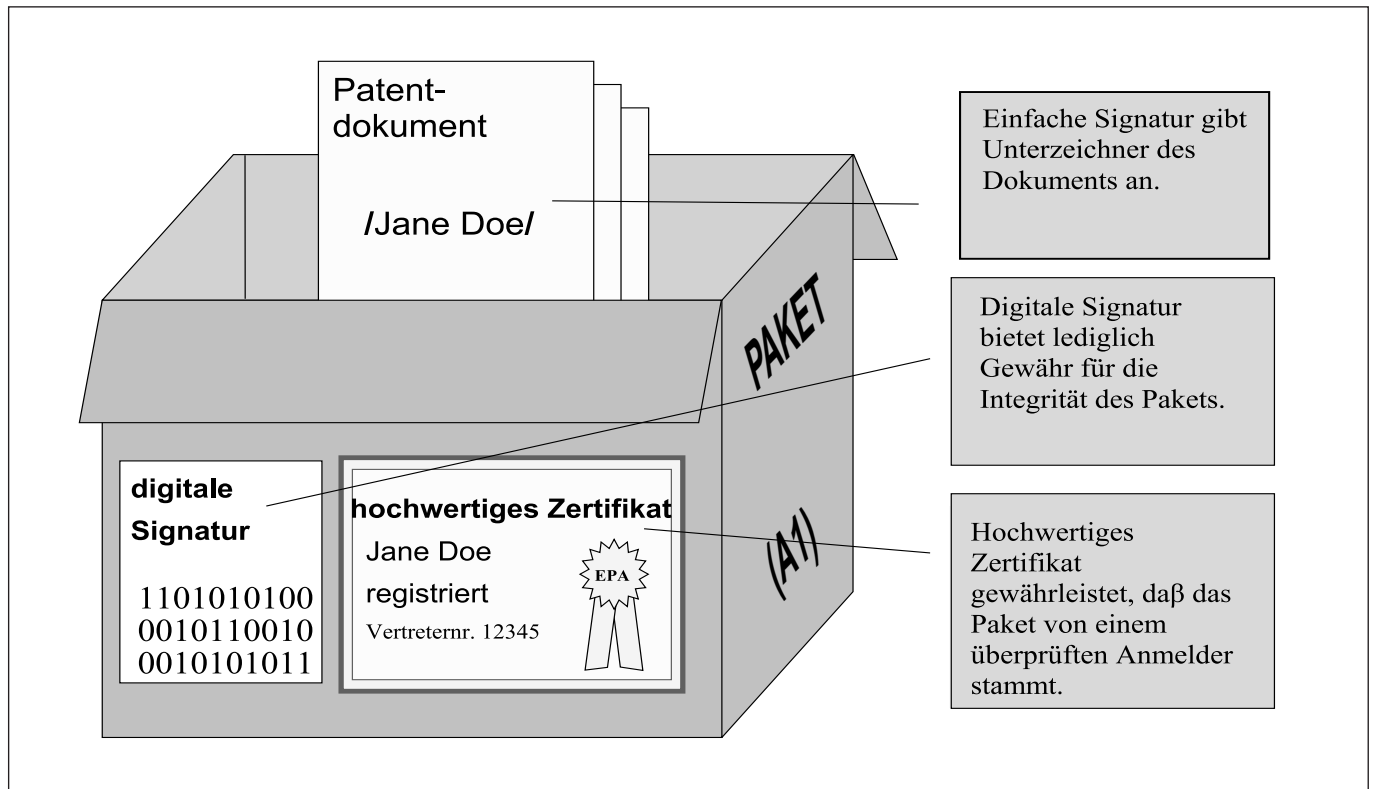


Abbildung 6: Einfache elektronische Signatur/hochwertiges Zertifikat

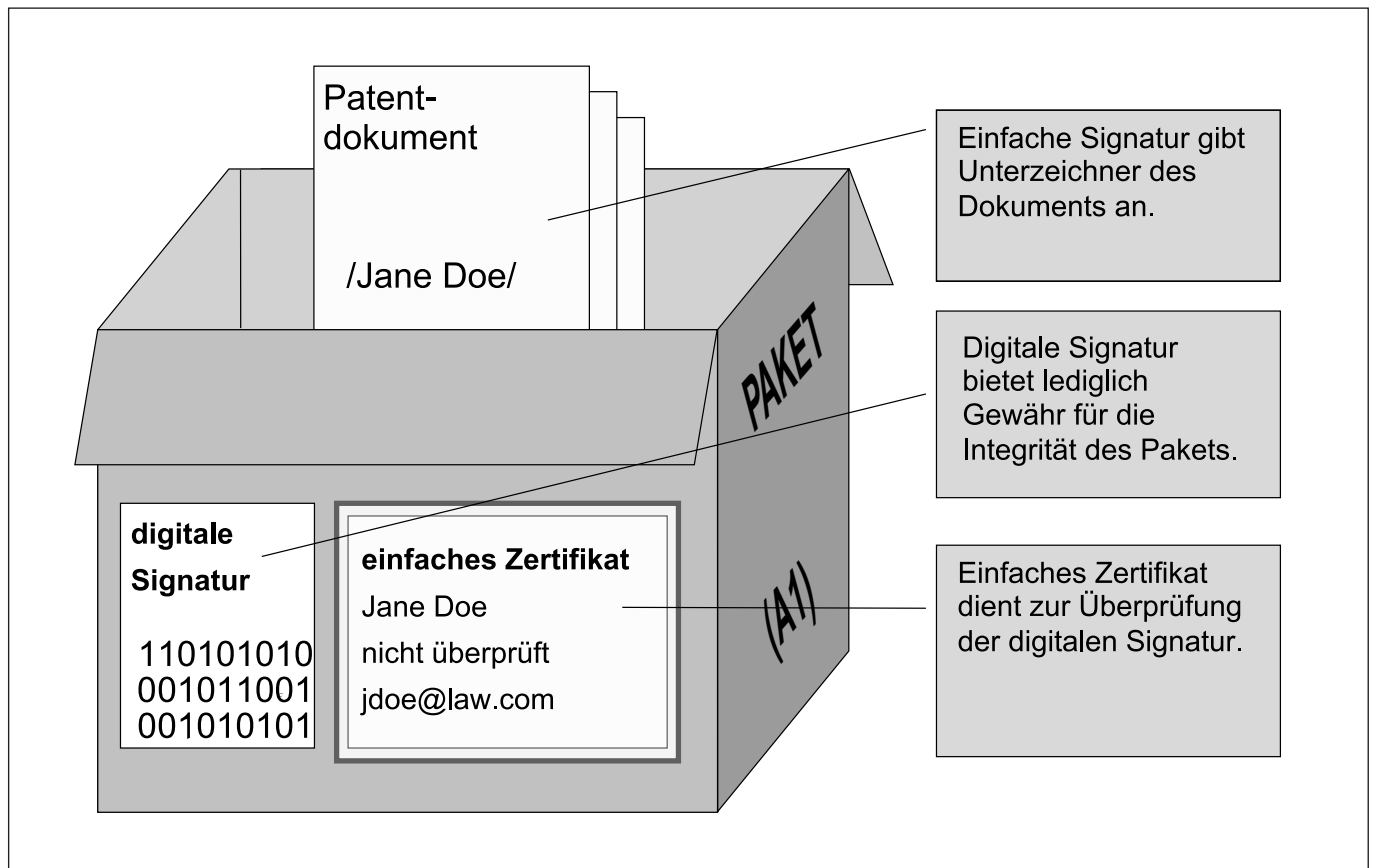


Abbildung 7: Einfache elektronische Signatur/einfaches Zertifikat



**Kombinationen von Übertragungsverfahren und Paketarten**

Abbildung 8 zeigt die zulässigen Kombinationsmöglichkeiten von Übertragungsverfahren und Paketarten. Generell gilt für die verschiedenen Übertragungsverfahren folgendes:

a) Online/Internet: Es ist ein signiertes und verschlüsseltes Paket zu verwenden.

b) Online/geschützt (Verschlüsselung auf Kanalebene, z. B. privates Netz): Es ist ein signiertes und verschlüsseltes Paket oder ein gebündeltes und signiertes Paket zu verwenden.

c) Offline/Datenträger: Es kann ein signiertes und verschlüsseltes Paket, ein gebündeltes und signiertes Paket oder ein Paket mit den gebündelten Anmeldungsunterlagen verwendet werden.

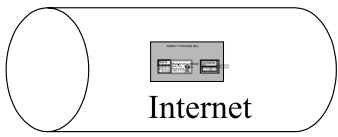








	Signiertes und verschlüsseltes Paket	Gebündeltes und signiertes Paket	Gebündelte Anmeldungsunterlagen
Online/ Internet	 Internet	 nicht zulässig	 nicht zulässig
Online/ geschützt	 geschützt	 geschützt	 nicht zulässig
Offline/ Datenträger			

Abbildung 8: Übertragungsprotokolle und zulässige Pakete