Beschluß des Präsidenten des Europäischen Patentamts vom 7. Dezember 2000 über die elektronische Einreichung von europäischen Patentanmeldungen und anderen Unterlagen

Der Präsident des Europäischen Patentamts (EPA), gestützt auf die Regeln 24 (1), 27a, 35 (2), 36 (5), 77 (2) d) und 101 EPÜ

und auf die für alle elektronischen Datensätze geltenden Grundanforderungen:

a) Authentizität, d. h. die Bestätigung, daß ein Dokument tatsächlich das Dokument ist, das es vorgeblich sein soll, und tatsächlich von der Person stammt, die vorgeblich der Autor sein soll

b) Integrität, d. h. die Unversehrtheit der Daten und insbesondere die Garantie, daß jede unberechtigte Veränderung oder Zerstörung aufgedeckt und verhindert werden kann

c) Vertraulichkeit, d. h. die Sicherstellung, daß die Existenz eines Dokuments oder sein Inhalt Nichtberechtigten nicht zur Kenntnis gelangt

d) Verbindlichkeit, d. h. die Sicherstellung, daß der Absender (unter Mithilfe des Empfängers) einen zuverlässigen Nachweis über den Eingang der Daten und der Empfänger einen zuverlässigen Nachweis der Identität des Absenders erhält, damit weder der Absender noch der Empfänger das Senden bzw. den Empfang der Daten abstreiten und ein Dritter ihre Integrität und ihren Ursprung überprüfen kann

sowie auf die folgenden grundlegenden Standards für die Verwaltung elektronischer Datensätze:

(1) Alle elektronisch eingereichten Unterlagen müssen sich in Papierform ausdrucken sowie verlustfrei und unverändert auf ein Archivierungsmedium übertragen lassen.

(2) Von den automatischen Systemen routinemäßig erfaßte Informationen über die Datensätze, sogenannte Metadaten, sind als Teil des elektronischen Datensatzes zu behandeln und durch die automatischen Systeme zu speichern.

(3) Elektronische Dokumente sind in einem vom Amt festzulegenden elektronischen Dateiformat zu übermitteln; ihre Archivierung hat ebenfalls in dem elektronischen Format zu erfolgen, in dem sie übermittelt wurden.

(4) Der Absender einer elektronischen Eingabe muß eine Empfangsbestätigung erhalten, aus der hervorgeht, daß das Amt die Unterlagen erhalten hat. Diese Empfangsbestätigung muß eine Identifikation des Amts sowie Datum und Uhrzeit des Eingangs (die dann als offizieller Zeitpunkt des Eingangs beim Amt gelten) enthalten und mit einer vom Amt gegebenenfalls vergebenen Referenz- oder Anmeldenummer versehen sein.

(5) Jedes Amt, das die elektronische Einreichung gestattet, muß auch die Einreichung in Papierform zulassen. Diese Papierunterlagen können anschließend gescannt werden, damit alle Unterlagen in einer einzigen elektronischen Akte abgelegt werden können.

(6) Es sind Vorkehrungen zu treffen, um die Authentizität und Integrität der elektronisch eingereichten Unterlagen sicherzustellen. Zu diesem Zweck ist eine Möglichkeit vorzusehen, die Identität des Absenders (Anmelder oder bevollmächtigter Vertreter) zu überprüfen und jede nach seiner Einreichung vorgenommene unberechtigte Veränderung eines Dokuments festzustellen.

(7) Systeme für die elektronische Einreichung müssen die Erstellung von Sicherungskopien und die Wiederherstellung von Daten gestatten, um elektronische Einreichungen gegen Systemausfälle zu schützen.

(8) Die elektronischen Datensätze sind so abzulegen, daß sie auf lange Zeit gespeichert und zugriffsbereit sind.

(9) Elektronische Dateien sind vor ihrer Bearbeitung auf Computerviren oder andere Arten bösartiger Software zu prüfen; gegebenenfalls sind geeignete Maßnahmen zu ergreifen, um den Anmeldetag aufrechtzuerhalten.

(10) Der Zugang zu den für die elektronische Einreichung genutzten Rechnern darf die Sicherheit anderer Computernetzwerke oder -anwendungen des Amts nicht gefährden.

(11) Systeme für die Verwaltung elektronischer Datensätze müssen Möglichkeiten für die Qualitätssicherung und -kontrolle der eingereichten Unterlagen bieten.

(12) Die Systeme für die Verwaltung elektronischer Datensätze müssen jegliche Ergänzungen oder Veränderungen der elektronischen Datensätze nachvollziehbar protokollieren, indem sie Eingangsinformationen oder sonstige Informationen über die Erstellung und jedwede Veränderung der Datensätze aufzeichnen.

(13) Sind vertrauliche Daten auf elektronischem Weg zugänglich, so ist der Zugang entsprechend zu sichern und darf nur berechtigten Nutzern offenstehen. Die Dateien sind durch geeignete Maßnahmen gegen etwaige Veränderungen zu schützen. Jeder Zugriff durch Anmelder, Vertreter oder andere berechtigte Personen mit elektronischen Mitteln ist durch Angaben über die Identität des Zugreifenden, das Datum (und wahlweise die Uhrzeit) des Zugriffs sowie Einzelheiten aller eingereichten Dokumente zu dokumentieren. Diese Angaben sind als vertrauliche Daten abzulegen.

(14) Der Öffentlichkeit ist in dem im EPÜ vorgesehenen Umfang Zugang zu den veröffentlichten europäischen Patentanmeldungen und Patenten zu gewähren.

(15) Alle elektronisch eingereichten Unterlagen sind bei Eingang auf einem schreibgeschützten Datenträger zu speichern.

beschließt:

Artikel 1
Einreichung europäischer Patentanmeldungen

Europäische Patentanmeldungen können beim EPA in elektronischer Form wie folgt eingereicht werden:

a) online über die Computer-Server des Europäischen Patentamts unter folgender Adresse:
https://secure.epoline.org

b) auf CD-R.

Europäische Patentanmeldungen können auch bei den zuständigen nationalen Behörden der Vertragsstaaten, die dies gestatten, in elektronischer Form eingereicht werden. Die nationalen Vorschriften der Vertragsstaaten, die die Einreichung von Erstanmeldungen beim nationalen Amt vorschreiben oder die die Einreichung bei einer anderen Behörde von einer vorherigen Zustimmung abhängig machen (Artikel 75 (2) EPÜ), bleiben unberührt.

Artikel 2
Standard für die elektronische Einreichung

Der technische Standard für die elektronische Einreichung, der als Anhang zu diesem Beschluß wiedergegeben ist (im folgenden "Standard" genannt), ist Bestandteil dieses Beschlusses. Jede künftige überarbeitete Fassung dieses Standards oder jeder künftige, von der Weltorganisation für geistiges Eigentum für die Einreichung nationaler Patentanmeldungen empfohlene Standard erlangt mit der Veröffentlichung eines entsprechenden Beschlusses des Präsidenten des Europäischen Patentamts Gültigkeit.

Artikel 3
Anfertigung von Unterlagen

Nach Artikel 1 eingereichte Unterlagen sind unter Verwendung von Software anzufertigen, die entweder vom EPA gebührenfrei zur Verfügung gestellt wird oder laut Bestätigung des EPA dem Standard entspricht.

Artikel 4
Form der Unterlagen

Die nach Artikel 1 eingereichten Unterlagen der europäischen Patentanmeldung einschließlich aller Zeichnungen müssen dem im Standard vorgegebenen Format entsprechen. Bei Anmeldungen, die nach Artikel 1 a) eingereicht werden und ein Sequenzprotokoll umfassen, braucht dieses nicht auf einem separaten Datenträger eingereicht zu werden.

Artikel 5
Erteilungsantrag

Ein nach Artikel 1 eingereichter Antrag auf Erteilung eines europäischen Patents soll zusätzlich zu den Angaben gemäß Regel 26 (2) EPÜ die elektronische Anschrift des Anmelders und gegebenenfalls des bestellten Vertreters enthalten.

Artikel 6
Lesbarkeit
Infizierte Dateien

(1) Sofort nach ihrem Eingang prüft das EPA nach Artikel 1 eingereichte europäische Patentanmeldungen dahingehend, ob sie

a) lesbar sind,

b) Computerviren oder andere Arten bösartiger Software enthalten.

(2) Ist eine europäische Patentanmeldung ganz oder teilweise unlesbar, so erachtet das EPA den Teil der Unterlagen, der unlesbar ist, als nicht eingegangen und wird nach Möglichkeit den Anmelder unverzüglich unterrichten.

(3) Stellt sich heraus, daß die europäische Patentanmeldung mit einem Computervirus infiziert ist oder andere bösartige Software enthält, so erachtet das EPA sie als nicht lesbar und ist nicht verpflichtet, sie zu öffnen oder zu bearbeiten. Das EPA versucht mit allen ihm zur Verfügung stehenden Mitteln, die Einreichung zu lesen, um einen Anmeldetag zuerkennen zu können. Es benachrichtigt den Anmelder nach Möglichkeit unverzüglich.

(4) Werden in der europäischen Patentanmeldung Mängel nach den Absätzen 2 oder 3 festgestellt und kann ein Anmeldetag deshalb nicht zuerkannt werden, so fordert das EPA den Anmelder nach Möglichkeit auf, die festgestellten Mängel innerhalb einer vom EPA zu bestimmenden Frist zu beseitigen. Der Anmeldetag ist der Tag, an dem die Mängel beseitigt sind. Werden die Mängel nicht rechtzeitig beseitigt, so wird die Anmeldung nicht als europäische Patentanmeldung behandelt.

Artikel 7
Prüfung bestimmter Formerfordernisse

Wird die europäische Patentanmeldung in einem Format eingereicht, das nicht Artikel 4 entspricht, so ergreift das EPA angemessene Maßnahmen, um die Einreichung zu lesen und ihr einen Anmeldetag zuzuerkennen. Scheitert dies, findet Artikel 6 (4) Anwendung. Gelingt dies, so ist der Anmelder aufzufordern, die Anmeldung innerhalb einer vom EPA zu bestimmenden Frist in dem in Artikel 4 vorgegebenen Format erneut einzureichen. Wird die Anmeldung nicht fristgerecht im vorgegebenen Format vorgelegt, so ist sie nach Maßgabe des Artikels 91 (3) EPÜ zurückzuweisen.

Artikel 8
Einreichung anderer Unterlagen

Wird die europäische Patentanmeldung nach Maßgabe des Artikels 1 eingereicht, können Vollmachten und Erfindernennung ebenfalls nach Maßgabe des Artikels 1 eingereicht werden. Die Artikel 3, 4 und 6 finden Anwendung. Werden diese Unterlagen in einem Format eingereicht, das nicht Artikel 4 entspricht, so ist der Anmelder aufzufordern, sie innerhalb einer vom EPA zu bestimmenden Frist in dem in Artikel 4 vorgegebenen Format erneut einzureichen. Wird eine Vollmacht nicht fristgerecht im vorgegebenen Format vorgelegt, so findet Regel 101 (4) EPÜ Anwendung. Wird eine Erfindernennung nicht fristgerecht im vorgegebenen Format vorgelegt, so findet Artikel 91 (5) EPÜ Anwendung.

Artikel 9
Originale – Stückzahl
Rechtlich maßgebliche Fassung

(1) Nach den Artikeln 1 und 8 eingereichte Unterlagen gelten für alle weiteren Verfahren vor dem Europäischen Patentamt als Originale und sind in einem Stück einzureichen.

(2) Ist ein Dokument auf CD-R nach Artikel 1 oder 8 eingereicht worden, so gilt die elektronische Fassung, die das EPA anhand der CD-R erstellt hat und die in der elektronischen Akte der europäischen Anmeldung aufbewahrt wird, als die rechtlich maßgebliche Fassung des Dokuments. Im Fall des Bestreitens können Überprüfungen anhand der ursprünglichen CD-R durchgeführt werden, die für die in Regel 95a EPÜ vorgesehene Zeitdauer aufzubewahren ist.

Artikel 10
Papierunterlagen zur Bestätigung

(1) Für die nach den Artikeln 1 und 8 eingereichten Unterlagen sind keine Papierunterlagen zur Bestätigung nachzureichen.

(2) Dennoch nachgereichte Papierunterlagen werden vom EPA nicht berücksichtigt, sofern es nicht ausdrücklich vom Anmelder darum gebeten wird. Eine Berücksichtigung dieser Papierunterlagen kann eine Änderung des Anmeldetags zur Folge haben.

(3) Nachgereichte Papierunterlagen müssen eindeutig als solche gekennzeichnet sein und entsprechende Angaben enthalten, anhand deren das EPA sie der betreffenden elektronischen Einreichung zuordnen kann.

Artikel 11
Unterschriften

(1) Für nach Artikel 1 eingereichte europäische Patentanmeldungen ist die im Antrag auf Erteilung eines europäischen Patents geforderte Unterschrift in einer der folgenden Formen zu erstellen:

a) Faksimile-Abbildung der eigenhändigen Unterschrift des Unterzeichners

b) elektronische Signatur, d. h. Daten in elektronischer Form, die anderen elektronischen Daten (Nachricht) beigefügt oder logisch mit ihnen verknüpft sind und dazu dienen, den Unterzeichner im Zusammenhang mit der Nachricht zu authentifizieren und sein Einverständnis mit dem Inhalt der Nachricht zu dokumentieren, oder

c) fortgeschrittene elektronische Signatur, d. h. eine elektronische Signatur, die folgende Anforderungen erfüllt:

i) Sie ist ausschließlich dem Unterzeichner zugeordnet.

ii) Sie wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann.

iii) Sie ist so mit den Daten, auf die sie sich bezieht, verknüpft, daß eine nachträgliche Veränderung der Daten erkannt werden kann.

(2) Eine elektronische Signatur im Sinne des Absatzes 1 b) ist eine Kette von Zeichen, vor und hinter der ein Schrägstrich (/) steht und die der Unterzeichner zum Nachweis seiner Identität sowie seiner Absicht, die jeweilige Nachricht abzuzeichnen, gewählt hat.

(3) Eine fortgeschrittene elektronische Signatur im Sinne des Absatzes 1 c) ist eine digitale Signatur, die mit einem Public-Key-Infrastructure-generierten Zertifikat und einem entsprechenden privaten Schlüssel erstellt wird.

(4) In allen übrigen Fällen, in denen gemäß EPÜ eine Unterschrift gefordert ist, muß das übermittelte Datenpaket durch eine fortgeschrittene elektronische Signatur im Sinne der Absätze 1 c) und 3 signiert sein. Einzelne Unterlagen des Datenpakets können auch nach Maßgabe des Absatzes 1 a) oder der Absätze 1 b) und 2 signiert sein.

(5) Fehlt im Antrag auf Erteilung eines europäischen Patents oder in sonstigen Unterlagen, die sich auf eine europäische Patentanmeldung beziehen und nach Artikel 1 a) eingereicht wurden, die Unterschrift des Anmelders oder genügt diese nicht den Anforderungen der jeweils zutreffenden Absätze 1 bis 4, so fordert das EPA den Anmelder auf, die festgestellten Mängel innerhalb einer vom EPA zu bestimmenden Frist zu beseitigen. Werden die Mängel nicht fristgerecht beseitigt, so gilt das Datenpaket als nicht eingegangen.

(6) Europäischen Patentanmeldungen und sonstigen Unterlagen, die auf CD-R eingereicht werden, ist eine Unterlage in Papierform mit einer eigenhändigen Unterschrift beizufügen, die den Anmelder und seinen Vertreter ausweist, eine Zustellanschrift angibt und die auf der CD-R gespeicherten Dateien auflistet.

Artikel 12
Empfangsbestätigung

(1) Der Empfang der nach Artikel 1 a) eingereichten Unterlagen ist während des Übertragungsvorgangs elektronisch zu bestätigen. Stellt sich heraus, daß die Übermittlung einer solchen Bestätigung fehlgeschlagen ist, so übermittelt das EPA die Bestätigung unverzüglich auf anderem Wege, sofern die ihm vorliegenden Angaben dies gestatten.

(2) Diese Empfangsbestätigung muß eine Identifikation des Amts, Datum und Uhrzeit des Eingangs, eine vom Amt vergebene Referenz- oder Anmeldenummer sowie eine Liste der übermittelten Dateien enthalten. Die Bestätigung muß ferner einen sogenannten Message-Digest, d. h. die Nachricht in komprimierter Form, umfassen.

(3) Die Bestätigung des Empfangs ist nicht gleichbedeutend mit der Zuerkennung eines Anmeldetags.

Artikel 13
Gebührenzahlungen

Die Regelungen für Gebührenzahlungen bleiben von diesem Beschluß unberührt.

Artikel 14
EPA-Bescheide und Mitteilungen

Das EPA bestimmt, welche Bescheide und Mitteilungen online zugestellt werden können. Die Anmelder müssen bei Einreichung der europäischen Patentanmeldung angeben, ob und welche Bescheide und Mitteilungen ihnen online zugestellt werden sollen. Anderenfalls werden alle Bescheide und Mitteilungen bis auf weiteres in Papierform zugestellt.

Artikel 15
Zustellungen

(1) Für die Zustellung von Bescheiden und Mitteilungen in Papierform gelten die Regeln 78 bis 80 EPÜ.

(2) Werden Bescheide und Mitteilungen online zugestellt, so setzt das EPA den Anmelder darüber in Kenntnis, daß ein Bescheid oder eine Mitteilung zum Abruf durch ihn bereitsteht. Dies erfolgt im Wege einer E-Mail an den Anmelder mit einer Verknüpfung zur Mailbox des Anmelders auf dem EPA-Server. Wird ein Bescheid oder eine Mitteilung nicht innerhalb von fünf Tagen nach Absenden der E-Mail abgerufen, wird eine Kopie in Papierform nach Absatz 1 zugestellt.

(3) Nach Absatz 2 zugestellte Bescheide und Mitteilungen gelten als am zehnten Tag nach dem Absendedatum der E-Mail eingegangen.

(4) Die Bestimmungen der Regeln 81 und 82 EPÜ bleiben unberührt.

Artikel 16
Fristen

Es gelten die Regeln 83 bis 85 EPÜ. Nur diejenigen Anmelder, die einer Online-Zustellung zugestimmt haben, können auch Fristverlängerungen online beantragen.

Artikel 17
Inkrafttreten

Dieser Beschluß tritt am 8. Dezember 2000 in Kraft.

Geschehen zu München am 7. Dezember 2000.

Ingo KOBER
Präsident

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 unversehrt 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 zugestellt 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 Anmeldungsunterlagen 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:

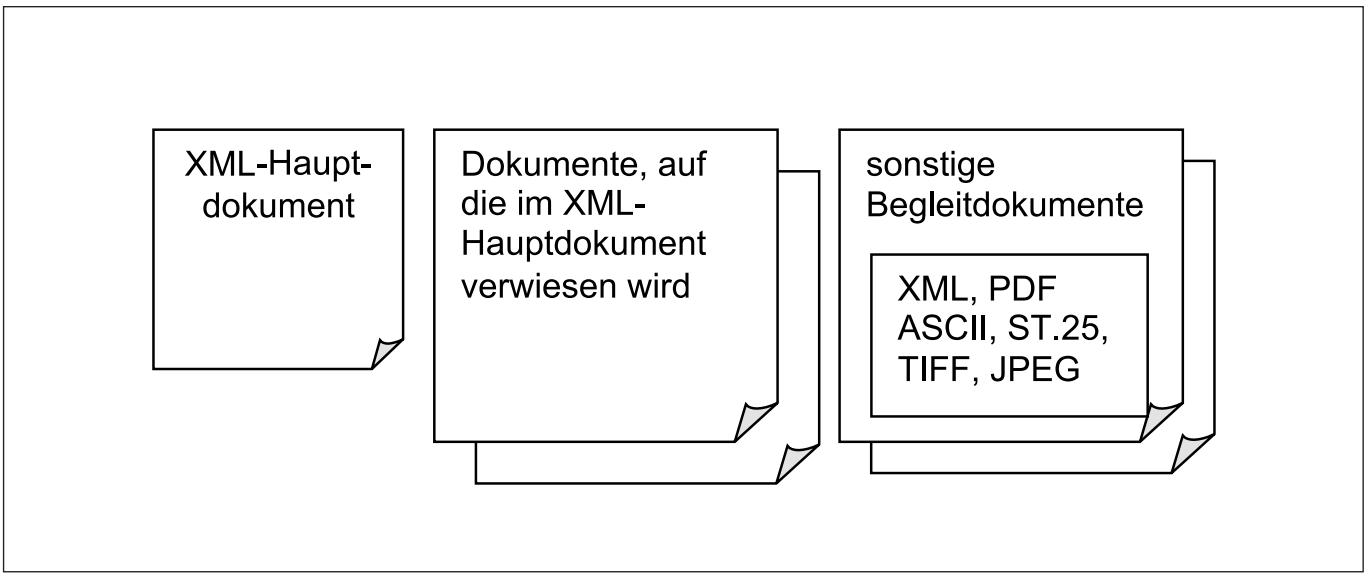
```
...
<electronic-signature DATE-SIGNED="01/01/2000">
     <enhanced-signature>
          <pkcs7 />
     </enhanced-signature>
</electronic-signature>
...
```

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.

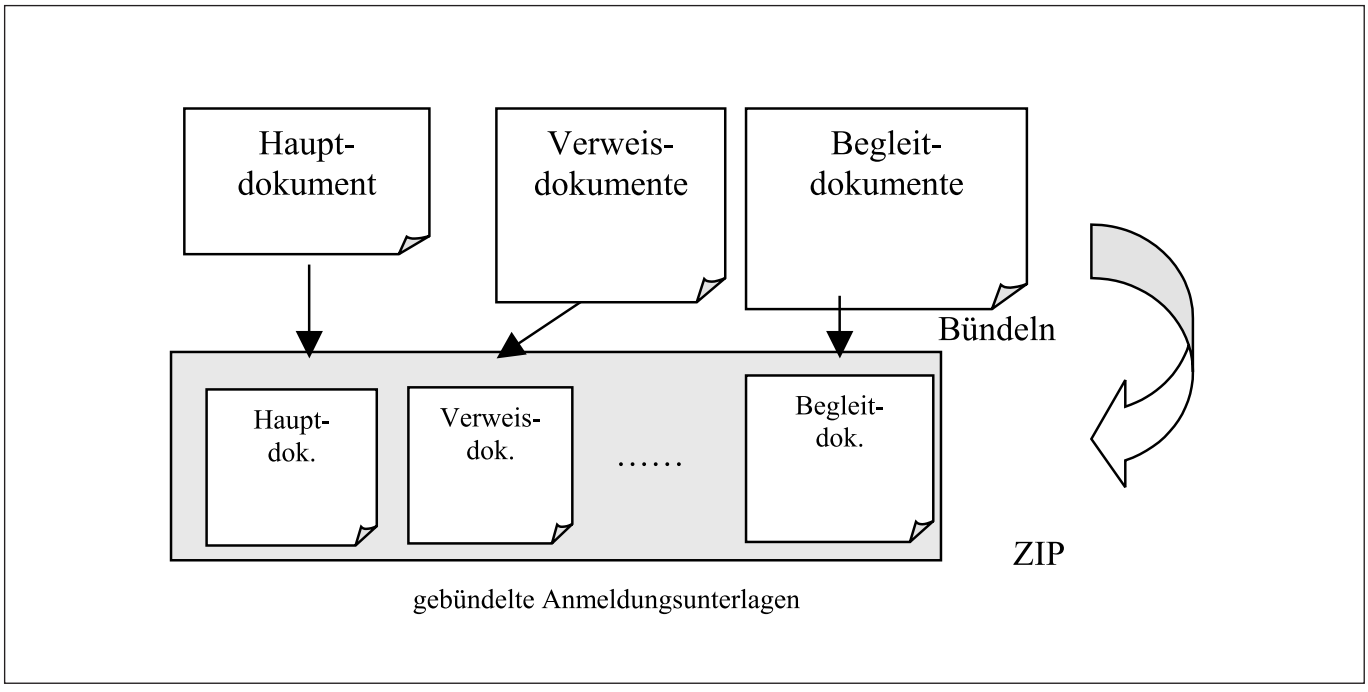
5.1.1.3 ASCII
Ein in reinem ASCII-Text erstelltes Dokument kann als externes Dokument in die gebündelten Anmeldungsunterlagen aufgenommen werden. Dann muß das XML-Hauptdokument die Codeseite des ASCII-Texts enthalten.

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).

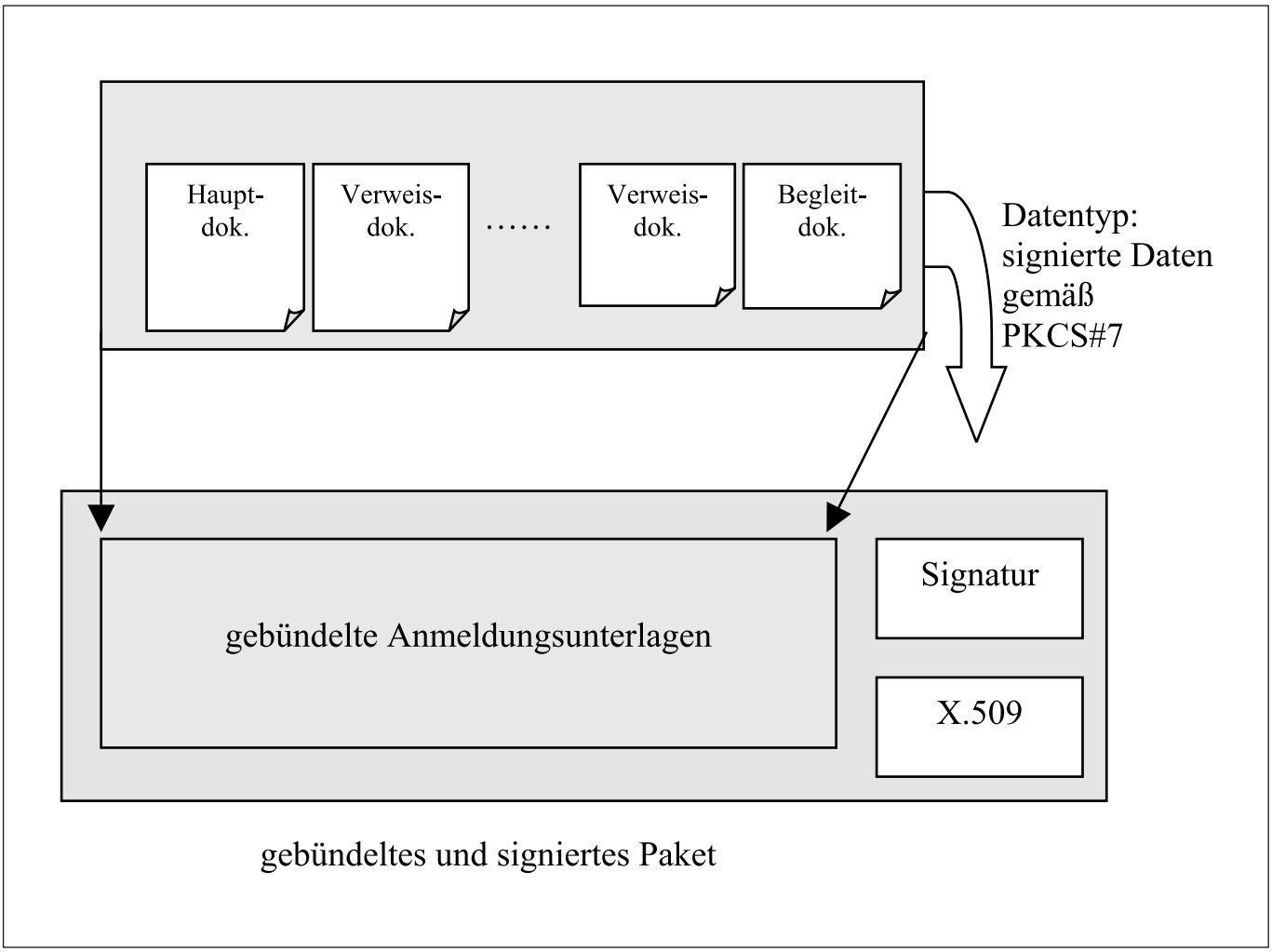
Alle in diesem Standard genannten Teile des Dokuments müssen im ZIP-Format zusammengefaßt werden. Die eingereichte ZIP-Datei muß alle externen Dateien enthalten, auf die in der Anmeldung verwiesen wird. Im Hauptverzeichnis der ZIP-Datei enthaltene Dateinamen müssen der Spezifikation für das jeweilige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

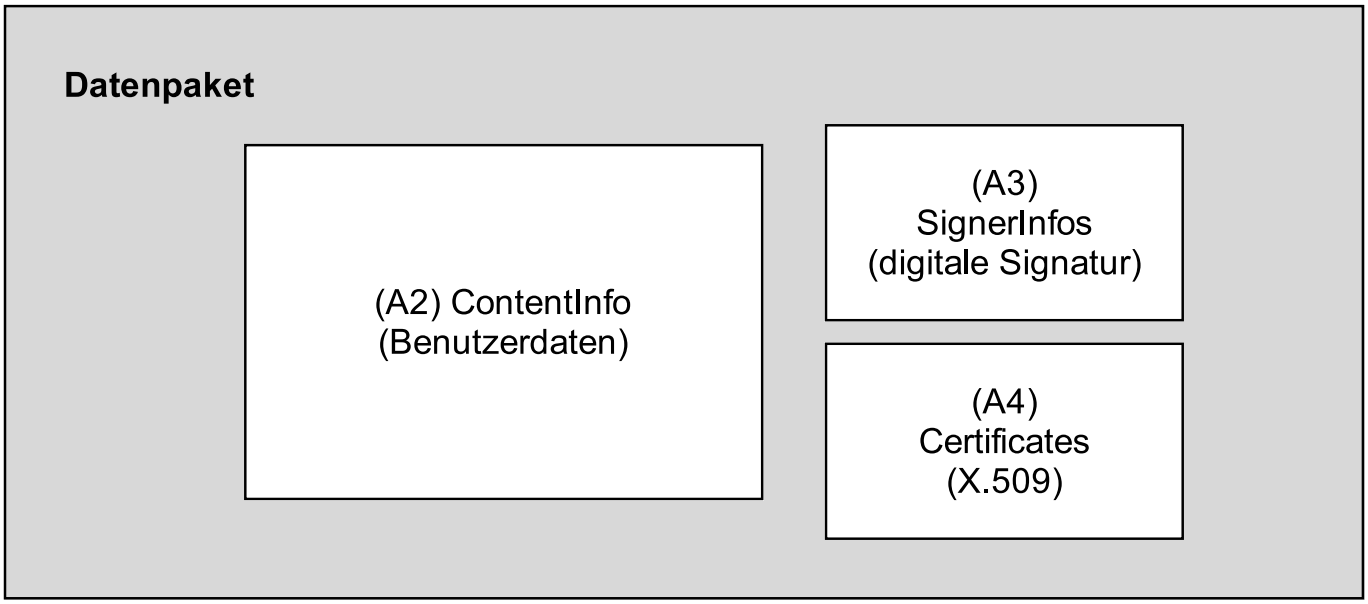
Nach dem ZIP-Standard kann die Komprimierungssoftware mit verschiedenen Komprimierungsalgorithmen arbeiten. Als standardmäßiges Komprimierungsverfahren ist das "Deflation"-Verfahren zu wählen.

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: **sha-1 OBJECT IDENTIFIER ::={iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 26}**
Objektbezeichner für RSA-Verschlüsselung	Der Objektbezeichner für RSA-Verschlüsselung ist im Standard *PKCS#1 - RSA Encryption* wie folgt definiert: **pkcs-1 OBJECT IDENTIFIER ::={iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1} rsaEncryption OBJECT IDENTIFIER ::={pkcs-1 1}**
Objektbezeichner für Triple DES	dES-EDE3-CBC OBJECT IDENTIFIER ::={iso(1) member-body(2) us(840) rsadsi(113549) encryptionAlgorithm(3) 7}

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 **Satz** 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 **Satz** 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.

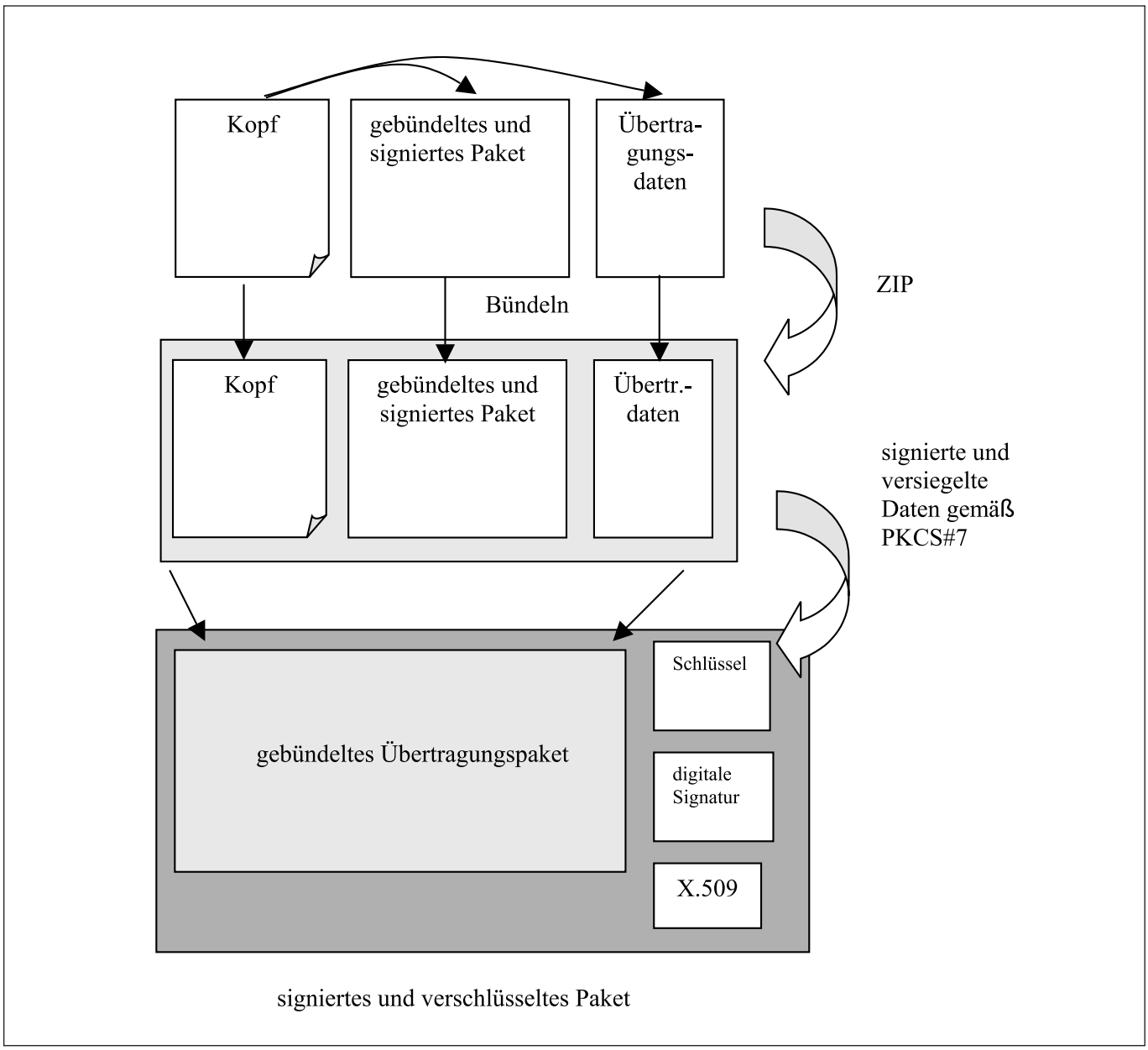
Je nach Paketart enthält das Paket verschiedene Datenelemente, darunter:
1. Datenelement "Kopf"
2. gebündeltes und signiertes Paket, das durch Bündelung und Signatur der Anmeldungsunterlagen entsteht
3. Übertragungsdaten, z. B. Zeitpunkt der Übertragung

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.

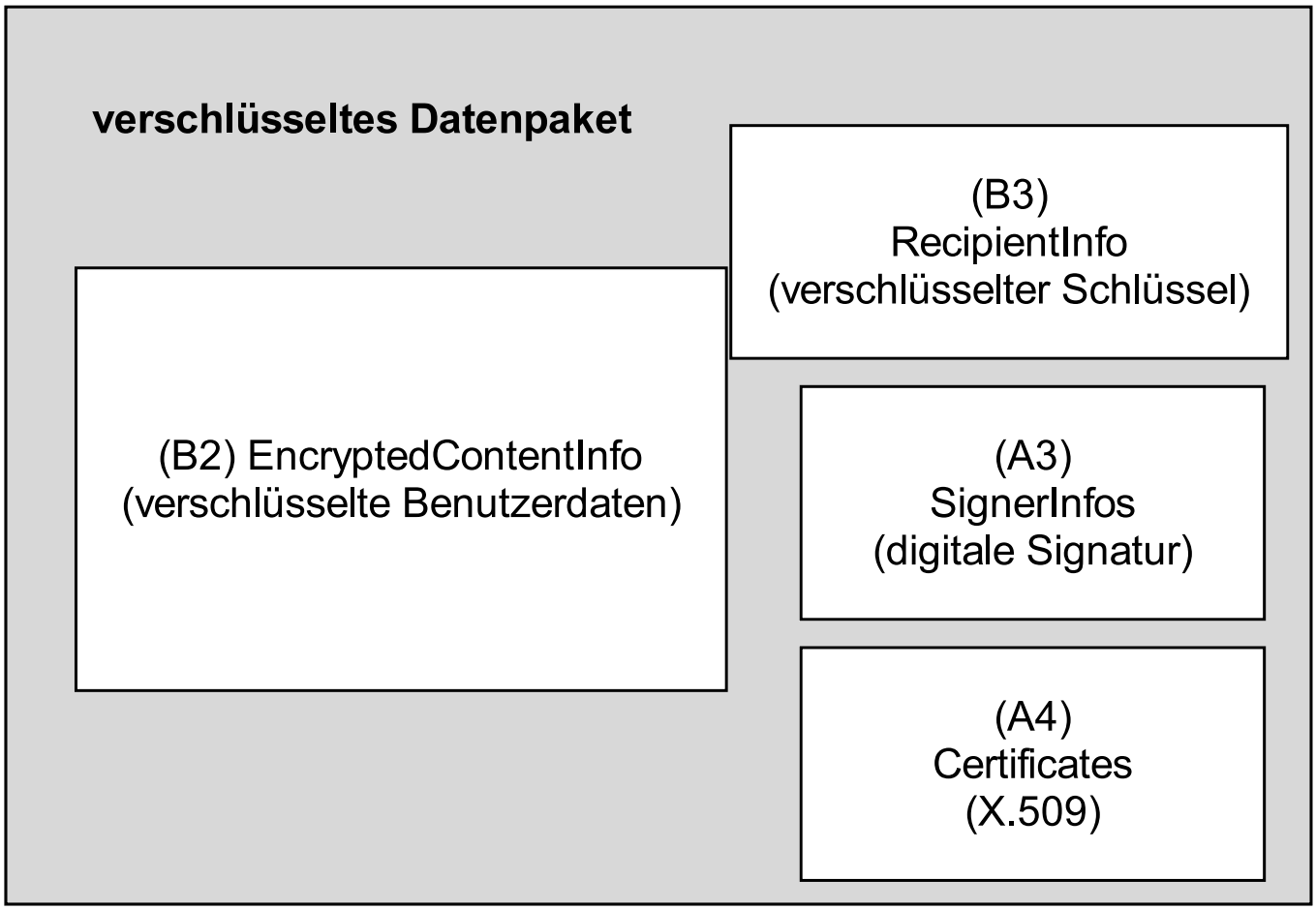
Für die Erstellung des signierten und verschlüsselten Pakets gilt folgendes Verfahren:
a) Erstellung eines gebündelten Übertragungspakets durch weitere Bündelung des gebündelten und signierten Pakets und der für die Übertragung verwendeten Datenelemente mittels ZIP
b) Erstellung eines signierten und 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)

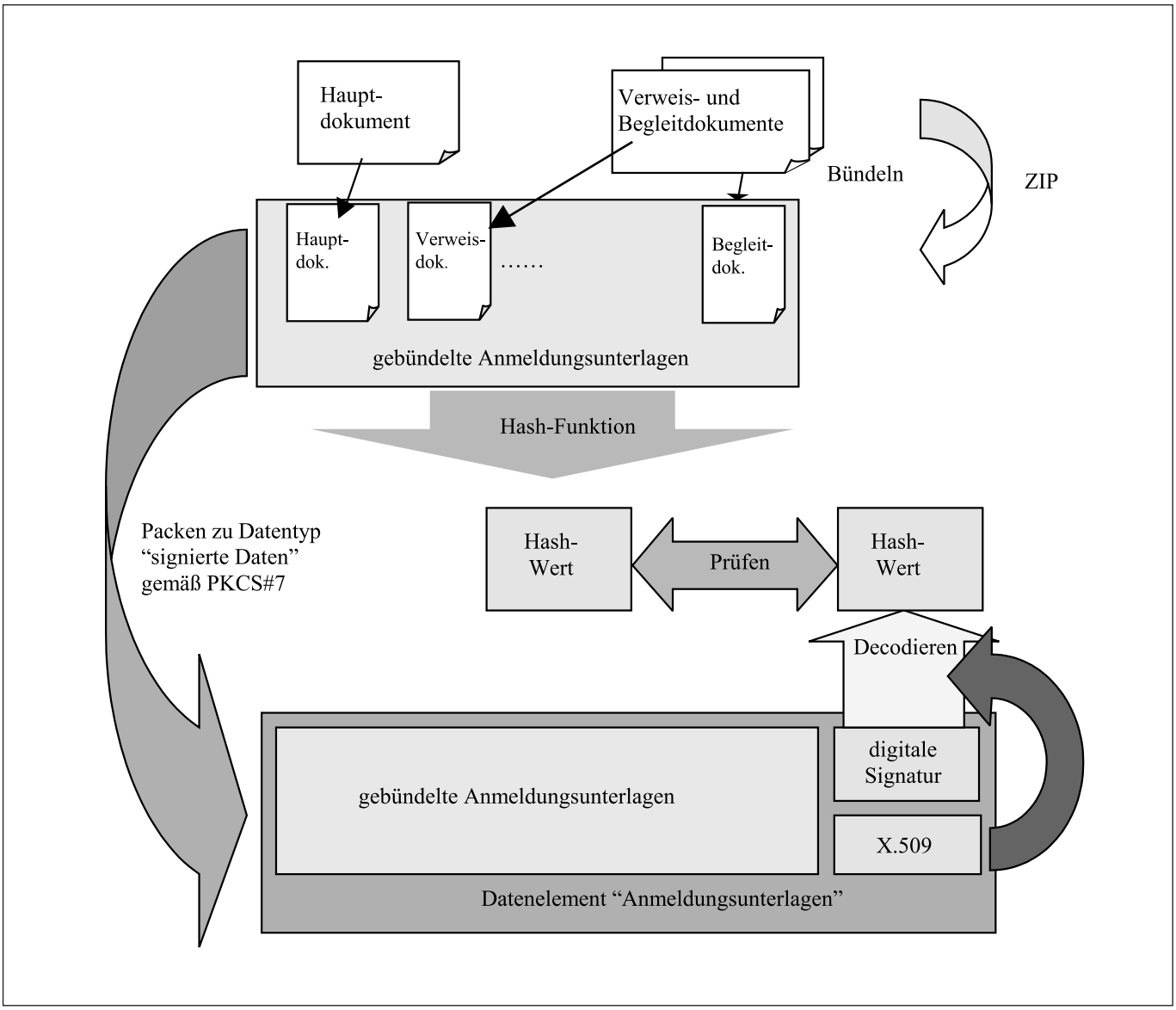
Tabelle B2: EncryptedContentInfo – oberste Ebene

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 unverwechselbare 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.

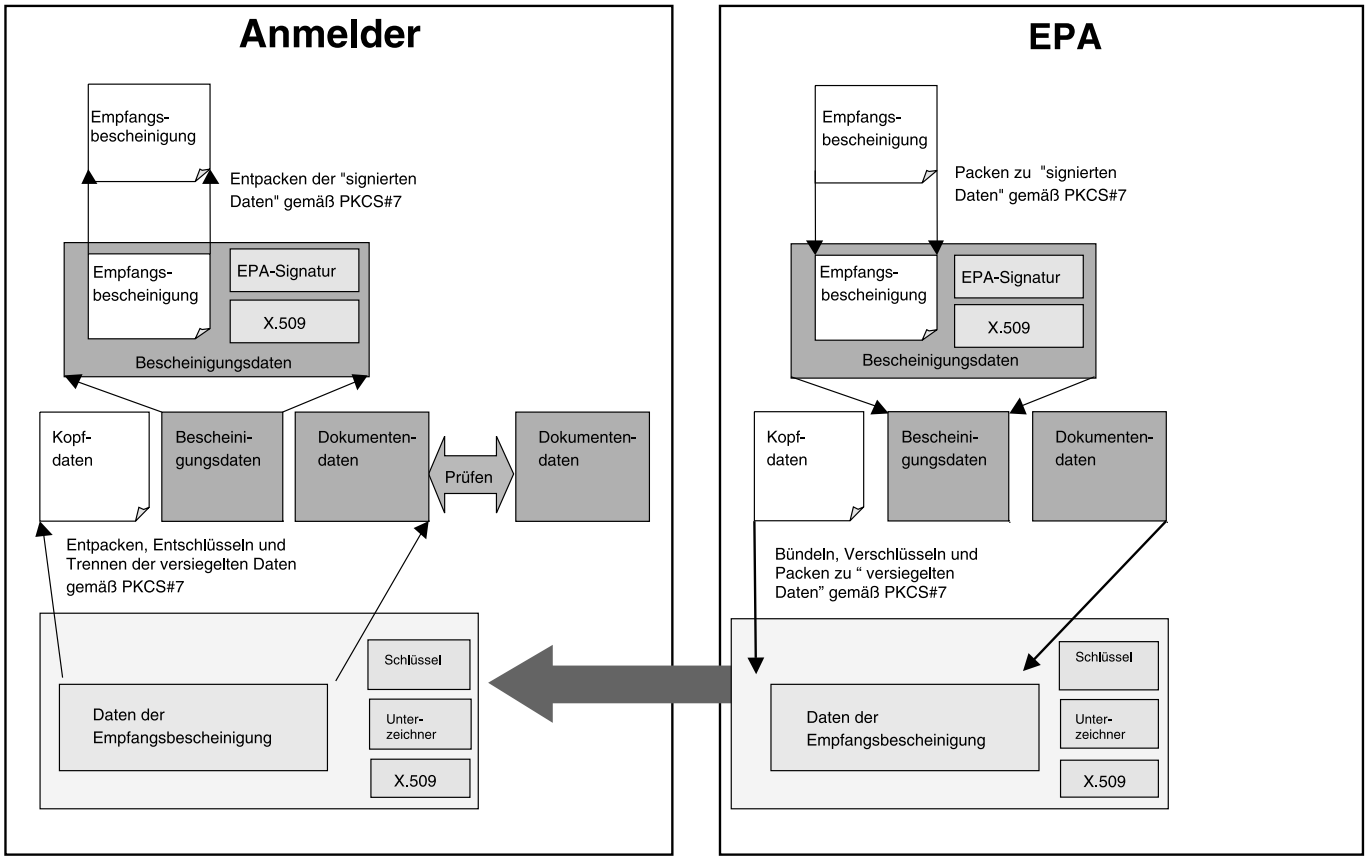


6.2.1 Prüfung des Hash-Werts
Das EPA nimmt die gebündelten Anmeldungsunterlagen entgegen, öffnet die darin enthaltenen Datenelemente und weist ihnen entsprechend den Angaben im Datenelement "Kopf" ihre Funktion zu.

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".

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

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 Anmeldungsunterlagen (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.

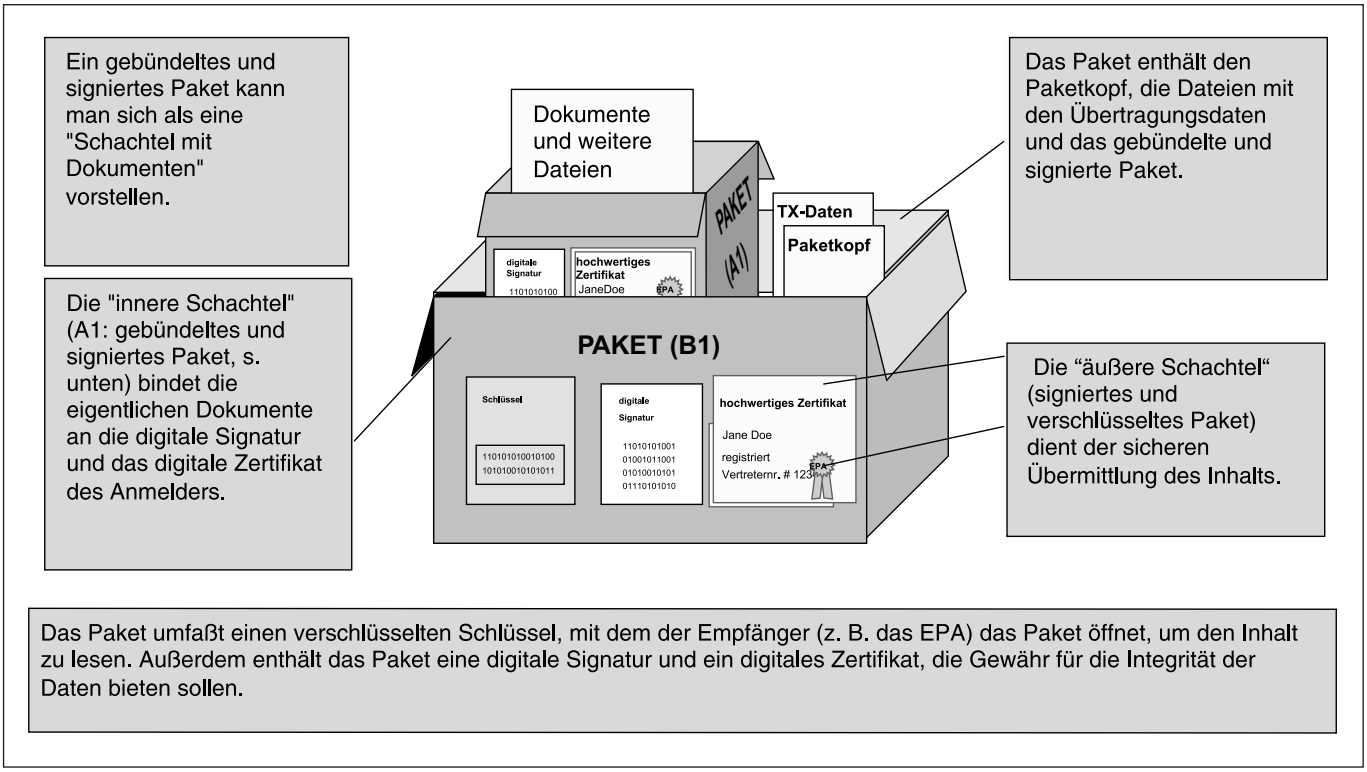


Abbildung 1: Signiertes und verschlüsseltes Paket

Vereinfachte Darstellung des gebündelten und signierten Pakets

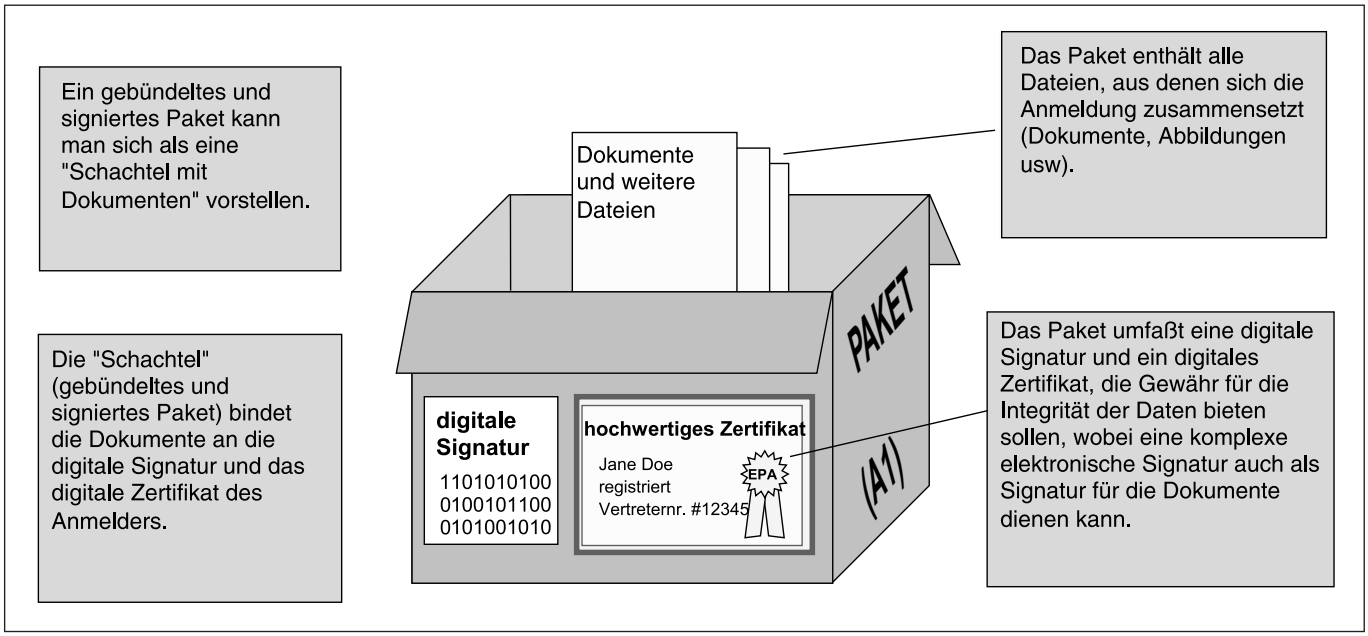


Abbildung 2: Gebündeltes und signiertes Paket

Aufbau des Objekts "gebündelte Anmeldungsunterlagen"

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

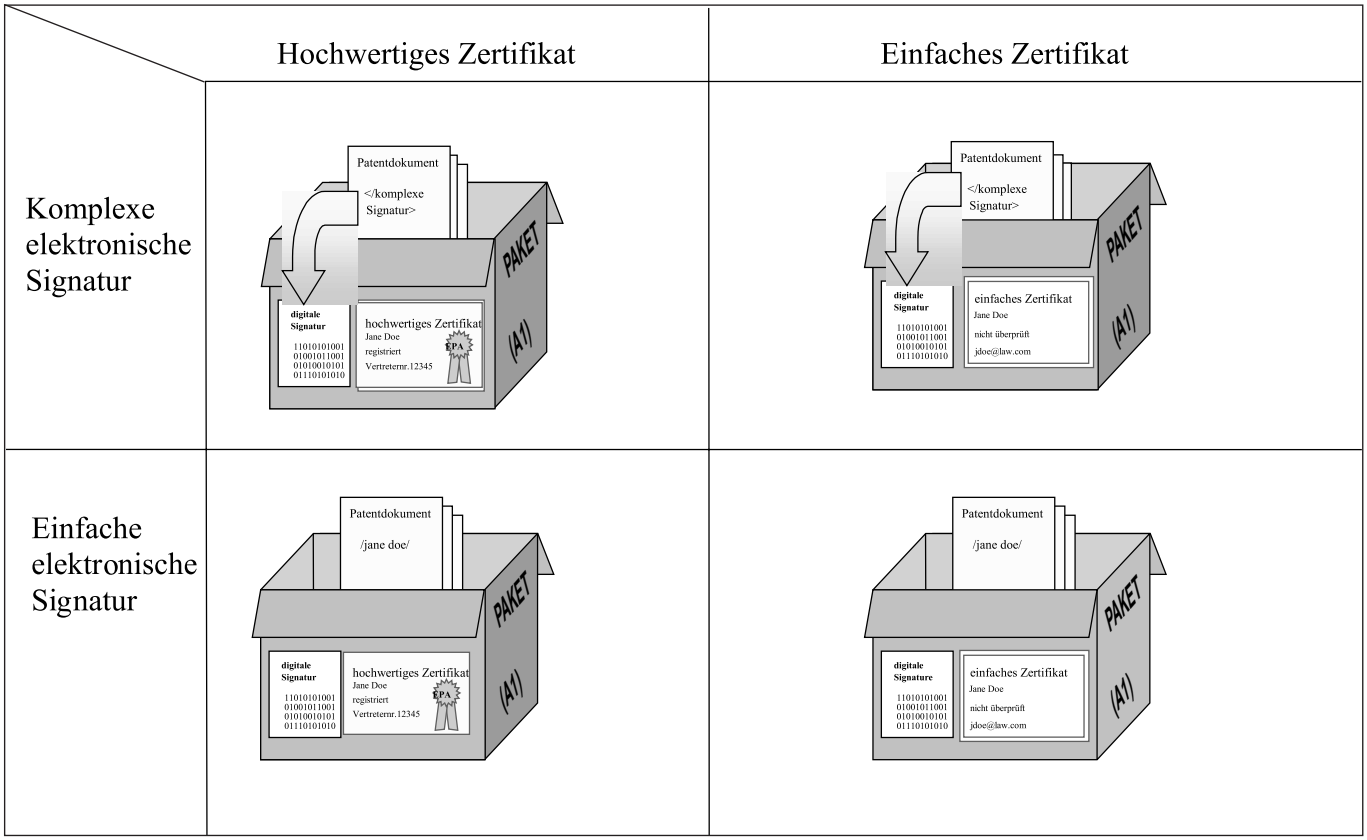


Abbildung 3: Arten von Zertifikaten/Signaturen

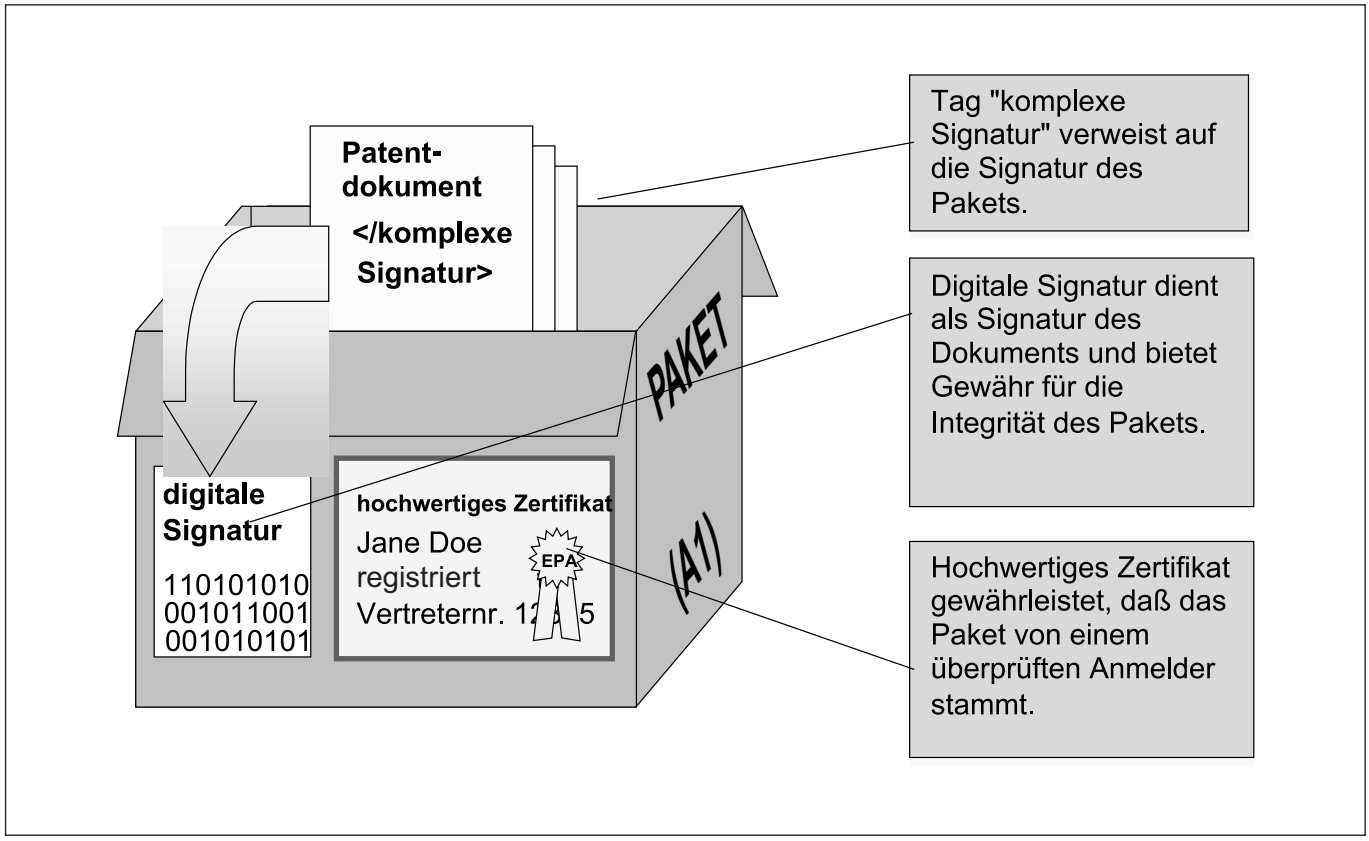


Abbildung 4: Komplexe elektronische Signatur/hochwertiges Zertifikat

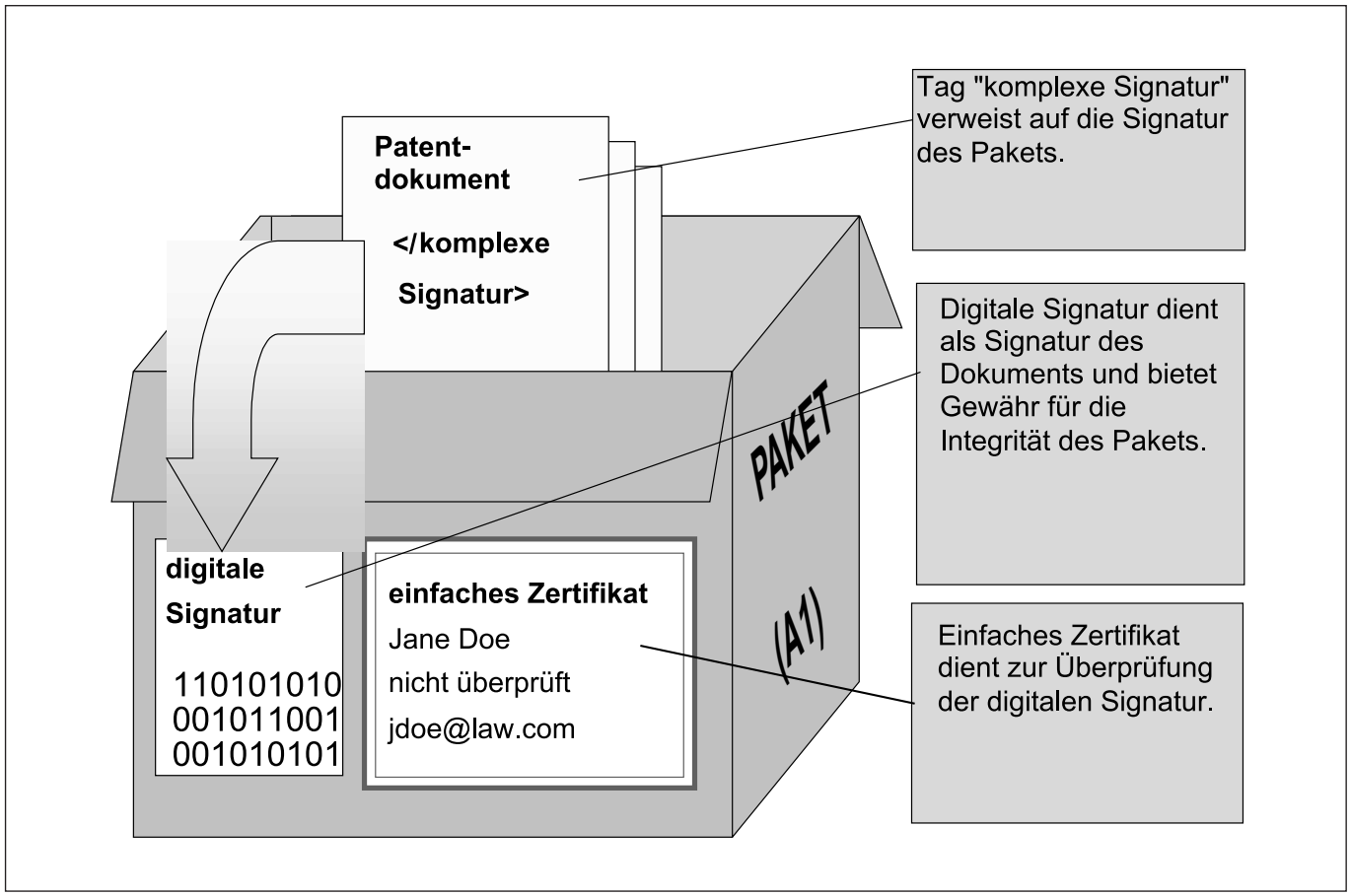


Abbildung 5: Komplexe elektronische Signatur/einfaches Zertifikat

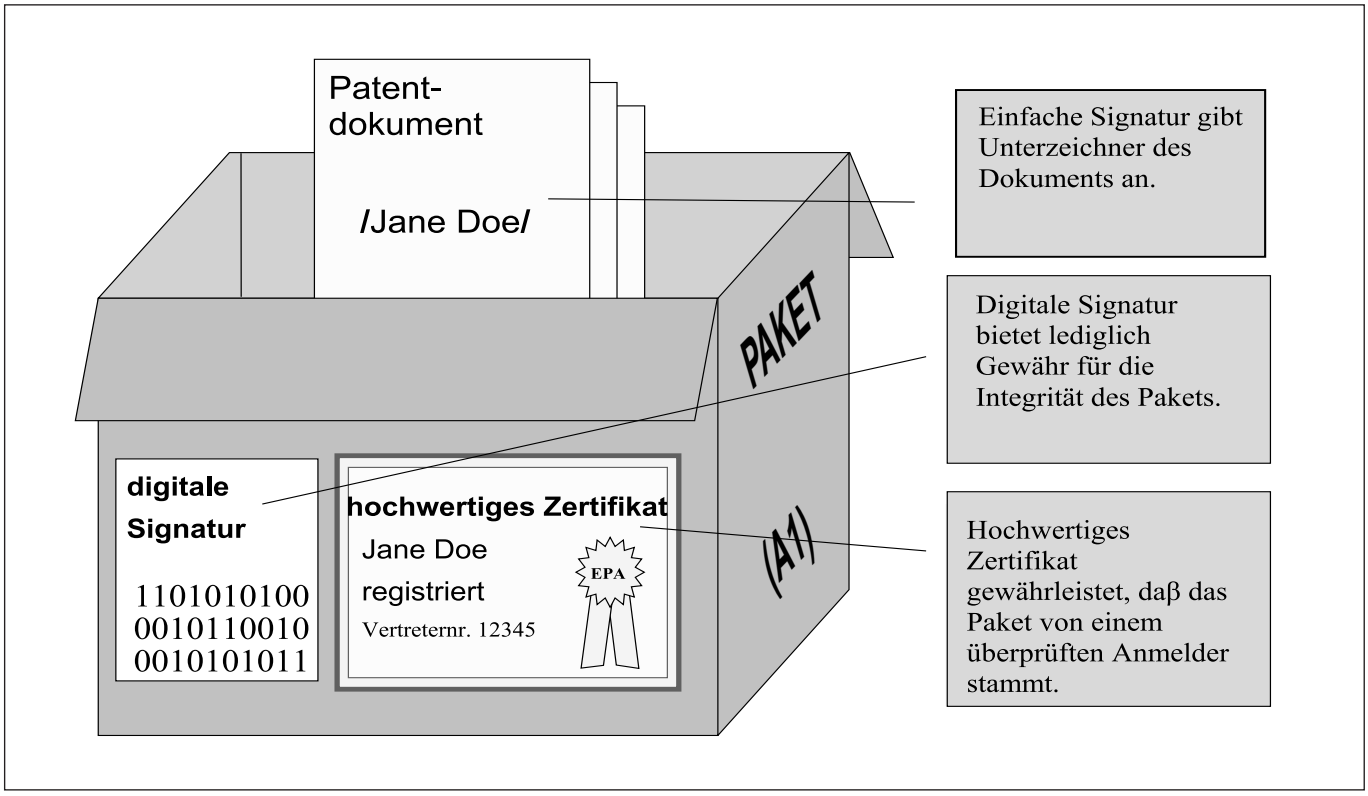


Abbildung 6: Einfache elektronische Signatur/hochwertiges Zertifikat

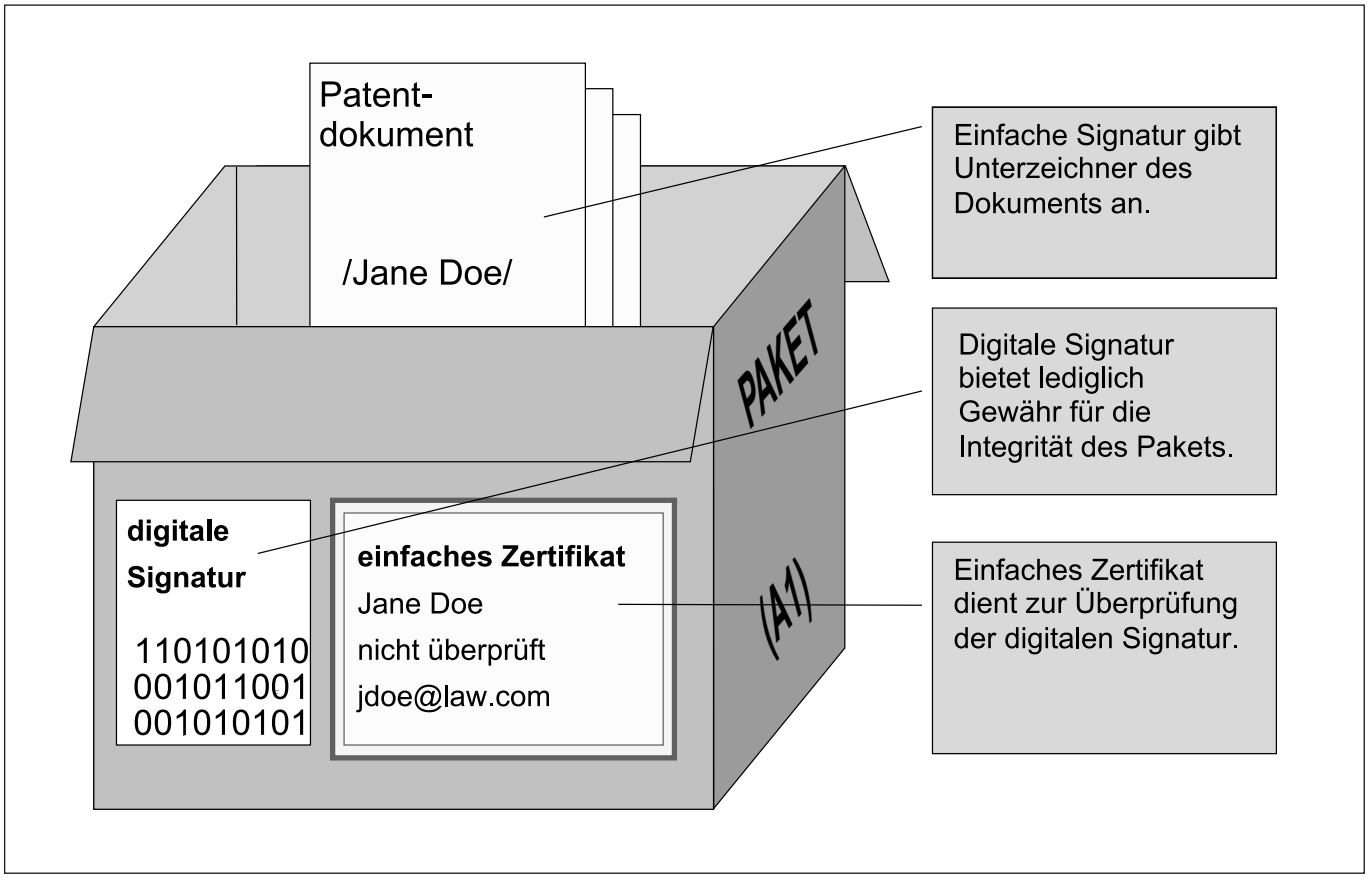


Abbildung 7: Einfache elektronische Signatur/einfaches Zertifikat

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.

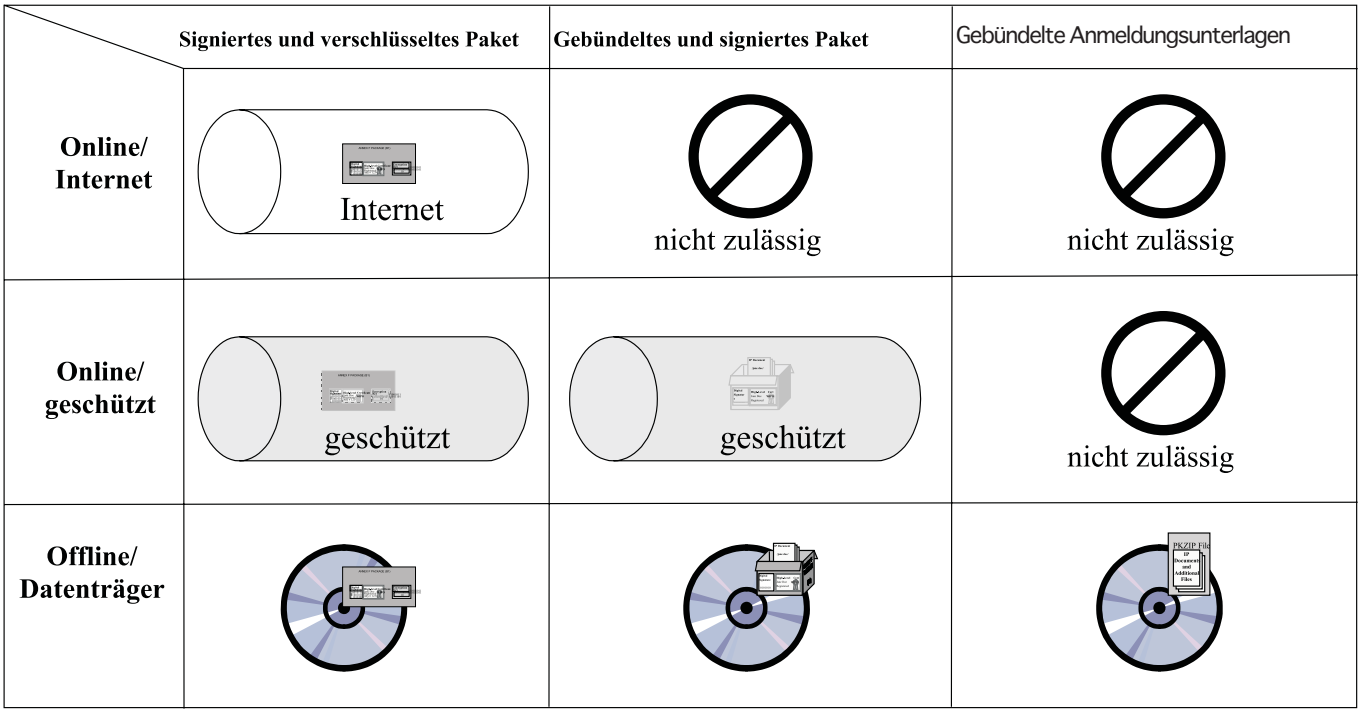


Abbildung 8: Übertragungsprotokolle und zulässige Pakete

Decision of the President of the European Patent Office dated 7 December 2000 on the electronic filing of European patent applications and subsequent documents

The President of the European Patent Office (EPO), having regard to Rules 24(1), 27a, 35(2), 36(5), 77(2)(d) and 101 EPC,

having regard to the basic requirements to be fulfilled by any electronic record, namely

(a) authenticity – ie confirmation that a document is what it purports to be, and was authored by the person who purports to have done so,

(b) integrity – ie consistency of the data and, in particular, detecting and preventing its unauthorised alteration or destruction,

(c) confidentiality – ie ensuring that a document's existence or content is not disclosed to unauthorised persons, and

(d) non-repudiation – ie ensuring that the sender (with the recipient's co-operation) has reliable evidence that the data has been delivered, and that the recipient has reliable evidence of the identity of the sender, so that neither party can successfully deny sending or receiving the data and a third party can verify its integrity and origin,

having regard to the basic standards of electronic records management, namely that

(1) all documents filed electronically must be capable of being printed as paper and transferred to archival media without loss of content or material alteration;

(2) information that is routinely collected by the automated systems concerning the record, often called metadata, is to be considered part of the electronic records and maintained by the automated systems;

(3) electronic documents must be submitted in an Office-designated electronic file format; archive copies must also be retained in the electronic format in which they are submitted;

(4) all electronic submissions must generate a positive acknowledgment to the submitter indicating that the Office has received the submission. The positive acknowledgment must include the identity of the Office, the date and time of the submission's receipt (which is the Office's receipt date/time) and any Office-assigned reference or application number;

(5) every Office that accepts electronic filing must also provide for the submission of paper documents. These paper documents may be imaged to facilitate the creation of a single electronic case file;

(6) a mechanism must be provided to ensure the authenticity and integrity of the electronically filed document. This requires the ability to verify the identity of the submitter (the applicant or authorised representative) as well as the ability to verify that a document has not been altered without authorisation since it was filed;

(7) electronic filing systems must provide backup and recovery mechanisms to protect electronic filings against system failures;

(8) the electronic records must be maintained for long-term access and retention;

(9) electronic files must be scanned for computer viruses and other forms of malicious logic prior to processing, with appropriate action being taken in order to preserve the filing date, if possible;

(10) access to computers used for electronic filing must not jeopardise the security of other Office networks and applications;

(11) electronic records management systems must provide mechanisms for quality assurance and quality control of the submitted documents;

(12) the electronic records management systems must maintain an audit trail of all additions to or alterations of the electronic records, recording the receipt information or other information about the generation of each record and of all changes to the records;

(13) if access to confidential data by electronic means is allowed, this access must be secure and available to authorised viewers only. Measures to assure the protection of these files from alteration must be taken. Such access by applicants, representatives or authorised members of the public by electronic means must be documented as to the identity of the party, the date (and optionally time) of the transaction, and the details of any submissions. Such documentation should be maintained as confidential data;

(14) to the extent provided for in the EPC, adequate public access to the published European patent applications and patents must be provided; and

(15) all electronic submissions should upon receipt be copied to a read-only medium,

has decided as follows:

Article 1
Filing of European patent applications

European patent applications may be filed with the EPO in electronic form as follows:

(a) online, at the European Patent Office's computer servers at the following address:
https://secure.epoline.org or

(b) on CD-R.

European Patent applications may also be filed in electronic form with the competent national authorities of those contracting states which so permit. The national provisions of the contracting states prescribing initial filing with the national authority or prior authorisation before filing with another authority (Article 75(2) EPC) are unaffected.

Article 2
Standard on electronic filing

The Technical Standard for Electronic Filing, annexed to this decision (referred to thereafter as "the Standard"), shall form an integral part of it. Any future amended version of this standard or any future standard recommended by the World Intellectual Property Organisation for the online filing of national patent applications shall become applicable after the publication of a corresponding decision of the President of the European Patent Office.

Article 3
Preparation of documents

Documents filed in accordance with Article 1 shall be prepared using software either provided free of charge by the EPO or certified by the EPO as conforming to the Standard.

Article 4
Presentation of documents

The documents making up the European patent application, including any drawings, filed in accordance with Article 1 shall be in the format specified in the Standard. Any sequence listing contained in applications filed in accordance with Article 1(a) need not be submitted on a separate data carrier.

Article 5
Request for grant

Any request for grant of a European patent filed in accordance with Article 1 shall comprise, in addition to the information pursuant to Rule 26(2) EPC, the electronic address of the applicant and of any representative appointed.

Article 6
Legibility
Infected files

(1) Promptly upon receipt, the EPO shall check European patent applications filed in accordance with Article 1 for

(a) legibility and

(b) computer viruses and other forms of malicious logic.

(2) In so far as the European patent application is illegible in whole or in part, the EPO shall regard that part of the document which is illegible as not having been received and shall, if possible, promptly notify the applicant accordingly.

(3) If the European patent application is found to be infected with a computer virus or malicious logic, the EPO shall regard it as illegible and need not open or process it. The EPO shall use all means reasonably available to it to read the submission for the purposes of according a filing date and shall, if possible, promptly notify the applicant accordingly.

(4) Where the European patent application is found to be deficient under paragraphs 2 or 3, so that no filing date can be accorded, the EPO shall, if possible, invite the applicant to correct the deficiencies within a time limit to be set by it. The filing date shall be the date on which the deficiencies are remedied. If the deficiencies are not remedied in due time, the application shall not be dealt with as a European patent application.

Article 7
Examination for certain physical requirements

If the European patent application is filed in a format not complying with Article 4, the EPO shall make reasonable efforts to read the submission for the purpose of according it a filing date. If unsuccessful, Article 6(4) shall apply. If successful, the EPO shall set the applicant a time limit for re-submitting the application in a format complying with Article 4. If the application is not re-submitted in the prescribed format in due time, it shall be refused in accordance with Article 91(3) EPC.

Article 8
Filing of other documents

Where the European patent application is filed in accordance with Article 1, any authorisation or designation of inventor may also be filed in accordance with Article 1. Articles 3, 4 and 6 shall apply. If these documents are filed in a format not complying with Article 4, the applicant shall be invited to re-submit them in a format complying with Article 4 within a time limit to be set by the EPO. If an authorisation is not re-submitted in the prescribed format in due time, Rule 101(4) EPC shall apply. If a designation of inventor is not re-submitted in the prescribed format in due time, Article 91(5) EPC shall apply.

Article 9
Original documents – Number of copies
Authentic version

(1) Any documents filed in accordance with Articles 1 and 8 shall be the original documents for the purposes of all subsequent proceedings before the EPO. They shall be filed in one copy.

(2) Where documents have been filed on CD-R in accordance with Article 1 or 8, the electronic version obtained by the EPO from the CD-R and kept in the electronic file of the European patent application shall be deemed to be the authentic version of the document. In the event of any dispute, verification may be effected by comparison with the originally filed CD-R, which shall be kept for the period prescribed in Rule 95a EPC.

Article 10
Paper confirmation

(1) No confirmation on paper is required for documents filed in accordance with Articles 1 and 8.

(2) The EPO shall take no action in respect of any paper confirmation nonetheless filed, unless clearly instructed by the applicant to do so. Such action may result in a new filing date being accorded.

(3) Any paper confirmation filed must be clearly marked as such and must contain the information necessary for the EPO to be able to attribute it to the electronic submission concerned.

Article 11
Signatures

(1) When the European patent application is filed in accordance with Article 1, the signature required in the request for grant of a European patent shall be provided in one of the following forms:

(a) as a facsimile image of the signer's handwritten signature;

(b) as an electronic signature, ie data in electronic form which is attached to or logically associated with other electronic data (data message) and which serves as a method of authenticating the signatory in relation to the data message and indicates his or her approval of the information contained in the data message; or

(c) as an advanced electronic signature, ie an electronic signature which meets the following requirements:

(i) it is uniquely linked to the signatory;

(ii) it is created using means that the signatory can maintain under his or her sole control; and

(iii) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

(2) An electronic signature within the meaning of paragraph 1(b) is a series of characters chosen by the signatory to express his or her identity and intent to sign the data message in question, and is preceded and followed by the forward slash (/).

(3) An advanced electronic signature within the meaning of paragraph 1(c) is a digital signature produced using a Public Key Infrastructure-generated certificate and the corresponding private key.

(4) In all other cases where a signature is required under the EPC, an advanced electronic signature within the meaning of paragraphs 1(c) and 3 must be produced in respect of the packaged submission. Individual documents within the package may be signed also in accordance with paragraph 1(a) or paragraphs 1(b) and 2.

(5) If the request for grant of a European patent or any other submission relating to a European patent application and filed in accordance with Article 1(a) is not signed, or the signature furnished does not comply with paragraphs 1 to 4 as appropriate, the EPO shall set the applicant a time limit for correcting the deficiency. If the deficiency is not corrected in due time, the submission shall be deemed not to have been received.

(6) European patent applications and other submissions filed on CD-R must be accompanied by a paper document bearing a handwritten signature, identifying the applicant and the applicant's representative, indicating an address for correspondence and listing the files contained in the CD-R.

Article 12
Acknowledgment of receipt

(1) The receipt of submissions filed in accordance with Article 1(a) shall be acknowledged electronically within the submission session. Where it becomes apparent that such acknowledgment was not successfully transmitted, the EPO shall promptly transmit the acknowledgment by other means where the necessary indications furnished to the EPO so permit.

(2) The acknowledgment shall include the identity of the Office, the date and time of the document's receipt, an Office-assigned reference or application number and a list of the files transferred. The acknowledgment shall also contain a message digest of the submission.

(3) Acknowledgment of receipt shall not imply the accordance of a filing date.

Article 13
Fee payments

The arrangements for fee payments shall remain unaffected by this decision.

Article 14
EPO communications

The EPO shall specify which communications may be notified online. Applicants shall indicate, upon filing the European patent application, which communications, if any, they wish to be notified online. Communications shall otherwise continue until further notice to be notified in paper form.

Article 15
Notifications

(1) If communications are notified on paper, Rules 78 to 80 EPC shall apply.

(2) If communications are notified online, the EPO shall inform the applicant that a communication is awaiting collection by the applicant. Such information shall be in the form of an e-mail containing a link to the applicant's mailbox at the EPO server. If a communication is not collected within five days from dispatch of the e-mail information, a paper copy shall be notified in accordance with paragraph 1.

(3) Communications notified in accordance with paragraph 2 shall be deemed to have been received on the tenth day following the date of dispatch of the e-mail information.

(4) Rules 81 and 82 EPC shall remain unaffected.

Article 16
Time limits

Rules 83 to 85 EPC shall apply. Only applicants who have agreed to receive notifications online may also request time-limit extensions online.

Article 17
Entry into force

This decision shall enter into force on 8 December 2000.

Done at Munich, 7 December 2000.

Ingo KOBER
President

Technical standard for the electronic filing of European patent applications and subsequent documents

1 Background

This document contains the technical standards for the electronic filing of documents with the EPO. It is based on the Trilateral Public Key Infrastructure (PKI)-based standard that has been incorporated into Annex F, Appendix I of the PCT Administrative Instructions.

A PKI environment provides a suite of services for processing sensitive information. Through the use of cryptography, PKI can satisfy the requirements for:
(a) Authentication – by ensuring that transmissions, messages and originators are valid, and that a recipient is authorised to receive specific categories of information.
(b) Data integrity – by ensuring that data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.
(c) Non-repudiation – by ensuring strong and substantial evidence is available to the sender of data that the data has been delivered (with the co-operation of the recipient), and to the recipient of the sender's identity, so that neither party can successfully deny having possessed the data, and a third party can verify its integrity and origin.
(d) Confidentiality – by ensuring that the information can be read by authorised entities only.

This standard sets out the mandatory requirements for all parties participating in electronic filing, as well as a number of optional requirements.

2 Scope

This technical standard covers requirements in the following areas:
(a) Security and PKI
(b) Electronic signatures
(c) Document format requirements
(d) Submission

3 Security and PKI

3.1 Public Key Infrastructure

In this standard, packaging and transmission are performed using PKI technology. When feasible alternative security technologies become available, they may be incorporated in updates to the standard.

PKI must be implemented in accordance with the recommendations established by the Internet Engineering Task Force (IETF) Working Group on PKI Interoperability (PKIX) and documented in IETF RFC 2459.

Separate key pairs and digital certificates must be used for the digital signature and encryption.

3.2 Digital certificates

Where the standard specifies use of a digital certificate, the certificate must comply with the International Telecommunication Union (ITU) X.509 (version 3) recommendation for certificate format.

A digital certificate is required when communicating with the EPO online.

The standard provides for two classes of digital certificate:

High-level certificate: a digital certificate issued by a certification authority to the applicant, which can be used to authenticate the identity of the applicant. The certification authority must appear on the list of "recognised" certification authorities published by the EPO (see 3.3 below).

Low-level certificate: a digital certificate provided by the EPO to the applicant on request. To receive a low-level certificate, the applicant must provide his name and e-mail address, but is not required to furnish proof of identity.

3.3 Certification authorities

The EPO will specify which certification authorities it accepts. This list of "recognised" certification authorities will include a link to the published PKI policy statement of each of these authorities.

Recognised certification authorities are responsible for maintaining the accuracy of the electronic certificates that "prove" a party is who he says he is. Certification authorities store certificate information for all the certificates they issue in a directory structure complying with ITU recommendation X.500. Such systems provide an external interface for publishing and retrieving user digital certificates that complies with the Lightweight Directory Access Protocol (LDAP) using the IETF Network Working Group's RFC 1777 dated March 1995. In addition, certification authorities publish revocation information about certificates drawn up in accordance with the X.509 standard.

The EPO will subscribe to this revocation information. Whenever a certificate is used to authenticate an individual, the EPO will consult the revocation information published by the certification authority concerned to ensure that the certificate has not been revoked.

3.4 Digital signatures

Digital signatures used to sign electronic documents for electronic filing must conform to the format and practice specified in RSA Laboratories' PKCS#7 Cryptographic Message Syntax Standard (version 1.5) with regard to the definition of the signed-data content type.

To build these signatures, a certificate meeting the requirements set out in Section 3.2 above must be used.

All digital signatures must be encoded using the distinguished encoding rules (DER) defined in ITU recommendation X.690.

3.5 Cryptographic algorithms
Both symmetric (secret key) and asymmetric (public key) algorithms may be used as required. Algorithms prohibited under the national law of a country may not be used for the electronic filing of documents from that country. Algorithms implemented in hardware or software may not be used in any manner contrary to the export restrictions of the country of origin of the hardware or software.

Where possible, the rsaEncryption algorithm is to be used for asymmetric encryption and the dES-EDE3-CBC algorithm for symmetric encryption. The same asymmetric encryption algorithm should be used to create digital certificates, digital signatures and envelopes.

3.6 Data enveloping
Electronic document data that is encrypted to ensure confidentiality for electronic filing must conform to the format and practice specified in RSA Laboratories' PKCS#7 Cryptographic Message Syntax Standard (version 1.5) with regard to the definition of the signed and enveloped data content type.

3.7 Message digest algorithms
The message stream must be input to the strong one-way message digest algorithm SHA-1 to create a message digest.

4 Signature mechanisms

This standard provides for a number of signature types acceptable for electronic filing:
(a) Basic electronic signatures
  (i) Facsimile image of the user's signature
  (ii) Text string
(b) Enhanced electronic signature
  (i) PKCS#7 digital signature

NOTE: Although users may choose not to utilise an enhanced electronic signature mechanism for the document itself, a PKCS#7 digital signature is required to package the wrapped application document as described in section 5.3. See Section 6.1 for an example of a wrapped and signed package.

The basic electronic signature is encoded within the "party" structure of the XML document as specified by the portion of the Document Type Definition (DTD) shown below:

```
...
<!ELEMENT electronic-signature   (basic-signature, enhanced-signature?) >
<!ATTLIST electronic-signature
      DATE-SIGNEDC       DATA    #REQUIRED
      PLACE-SIGNEDC      DATA    #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  >
...
```

A basic electronic signature within an XML document may be supplemented by the addition of a digital signature to the wrapped application documents.

4.1 Facsimile signature
To create this type of signature, the XML file must include the <fax> element and an external entity reference set in the FILE-NAME attribute that points to the file containing the bitmap of the signature, as shown below:

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

This bitmap file must be a 300dpi single strip, Intel encoded TIFF Group 4 image or a JFIF (JPEG) file.

4.2 Text string signature
To create this type of signature, the XML document must include the <text-string> element containing a text string that represents the user's "wet" (ink) signature, enclosed in slash "/" characters, as shown in the example below:

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

The text string must be a string of characters, not including the forward slash "/" character, chosen by the user as his electronic signature, as shown in the following examples:

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

4.3 PKCS#7 digital signature
The PKCS#7 signed data type is generated from the electronic message by the signer, who uses his private signing key to encrypt the message digest. It includes a copy of the digital certificate of the signer when sent.

The use of a PKCS#7 signature must be indicated in the XML file by the <pkcs7> element, as shown below:

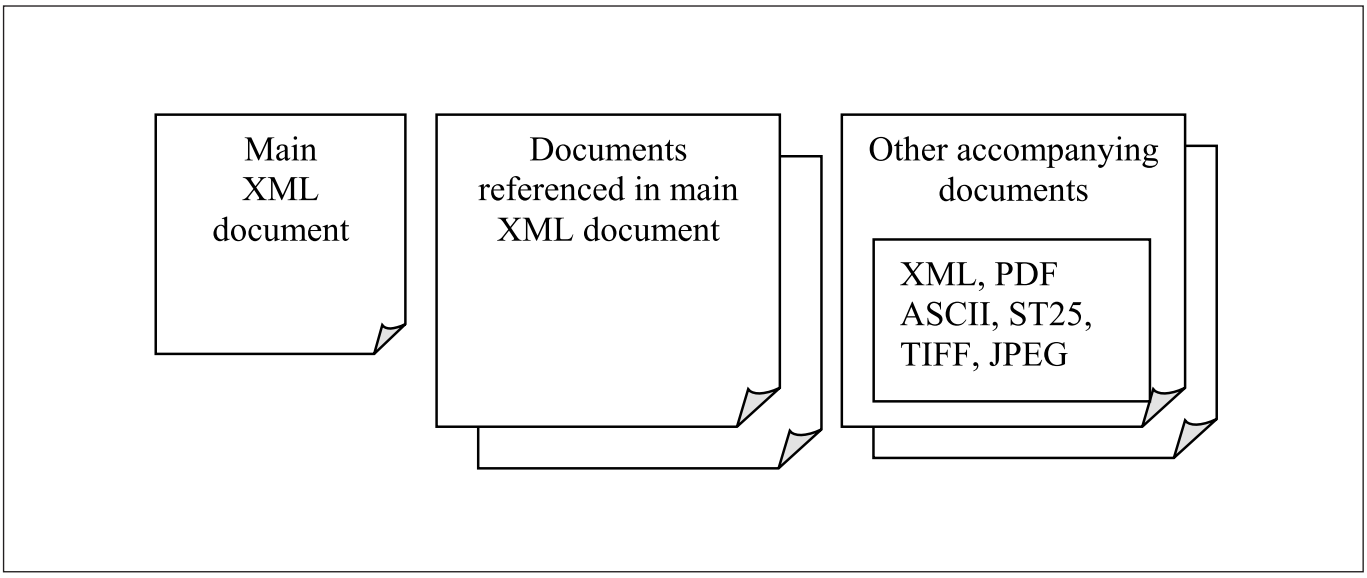
```
...
<electronic-signature DATE-SIGNED="01/01/2000">
      <enhanced-signature>
            <pkcs7 />
      </enhanced-signature>
</electronic-signature>
...
```

5 Data format requirements

The document packaging mechanism is used to combine the data about what is being transmitted with the contents of the transmission to form a single binary object called a wrapped application document (WAD), and then to apply the appropriate digital signatures and encryption.

5.1 Document preparation
For each document filed there is a main XML document that may explicitly reference all documents to be sent in a single package. These referenced documents are logically part of the main document (eg a new patent application). In addition, a filing may include other accompanying documents (eg designation of inventor or fee payment).

The main XML document must conform to one of the DTDs specified below. The referenced documents (external entities) are typically embedded images, tables, drawings or other compound documents and may be encoded as either XML, ST25, PDF, ASCII, TIFF or JFIF(JPEG). The accompanying documents are separate, but related, documents that may be encoded as either XML, ST25, PDF, ASCII or Image. Any accompanying XML documents must also conform to one of the DTDs specified below.



5.1.1 Character-coded formats

5.1.1.1 XML
All XML documents must conform to one of the DTDs specified below. Applicants will be able to create XML documents conforming to this standard by using the EPO's client software for electronic filing.

The coded character set used for all XML documents must be confined within that specified by ISO/IEC 10646:2000 (Unicode 3.0). The standard character-encoding scheme for XML documents is UTF-8.

5.1.1.2 ST.25
A document created using WIPO ST.25 SGML tags for sequence listings may be included in a WAD as an external document.

5.1.1.3 ASCII
A document created as plain ASCII text may be included in a WAD as an external document. In this case, the main XML document must include the code page of the ASCII text.

5.1.2 PDF
PDF documents for use in electronic filing must meet the following requirements:

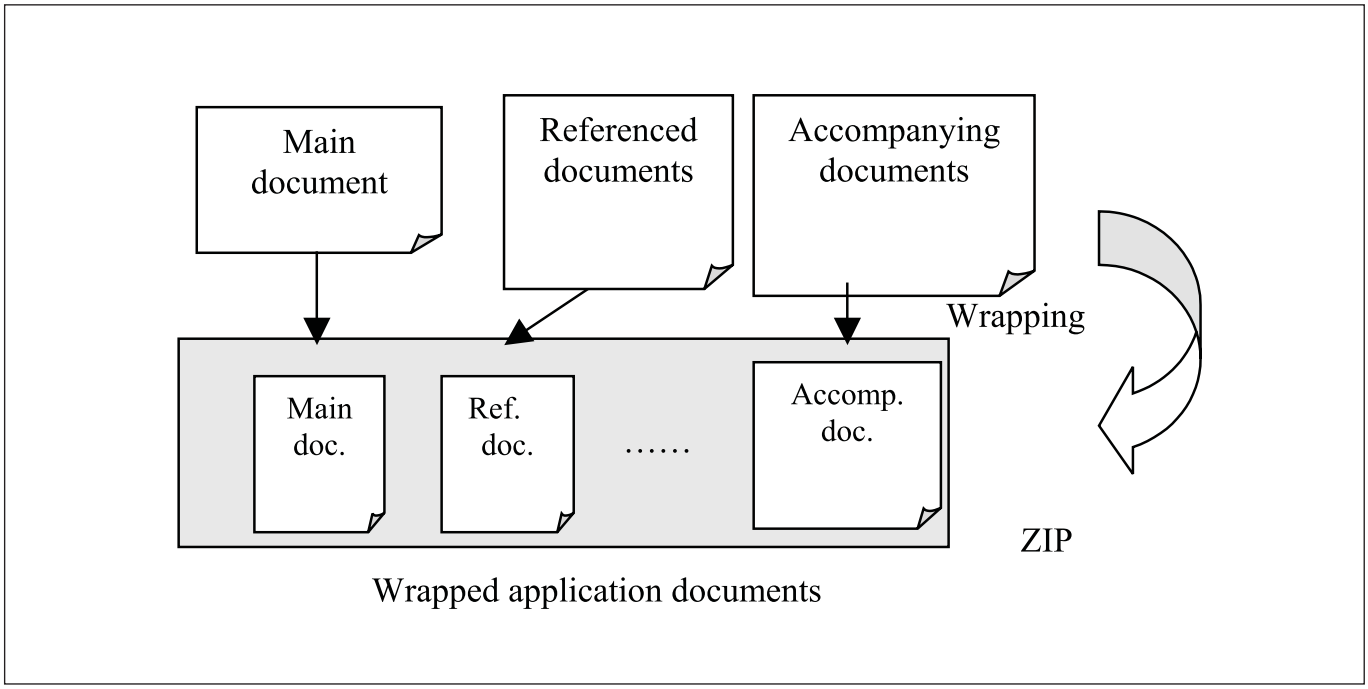
(a) PDF V1.3 compatible
(b) Non-compressed text to facilitate searching
(c) Unencrypted text
(d) No digital signatures
(e) No embedded OLE objects
(f) All fonts must either be embedded, standard PS17 or built from Adobe® Multiple Master (MM) fonts

The PDF format has become the de facto standard for the exchange of formatted documents on the Internet.

5.1.3 Images
Facsimile images used in electronic filing must meet the following requirements:

- Format
  - TIFF V6.0 with Group 4 compression, single strip, Intel encoded or
  - JFIF(JPEG)
- 200, 300 or 400 dpi
- A4 size

5.2 Wrapping documents
The main document and any externally referenced documents and accompanying documents are wrapped and treated as one data block. This data block, called the wrapped application documents (WAD), is created using the ZIP wrapping standard. Applicants must use ZIP format archiving and compression software to package the document files constituting an electronic application.



The software used to create the ZIP file must conform to the ZIP file format specification as published in the PKWARE® PKZIP® Application Note (revised: 8.1.1998).

The files to be zipped must include all parts of the document identified elsewhere in this standard. All external files referenced by the application must be included in the ZIP file submission. File names included in the central directory of the ZIP file must comply with the specification for the applicable operating system.

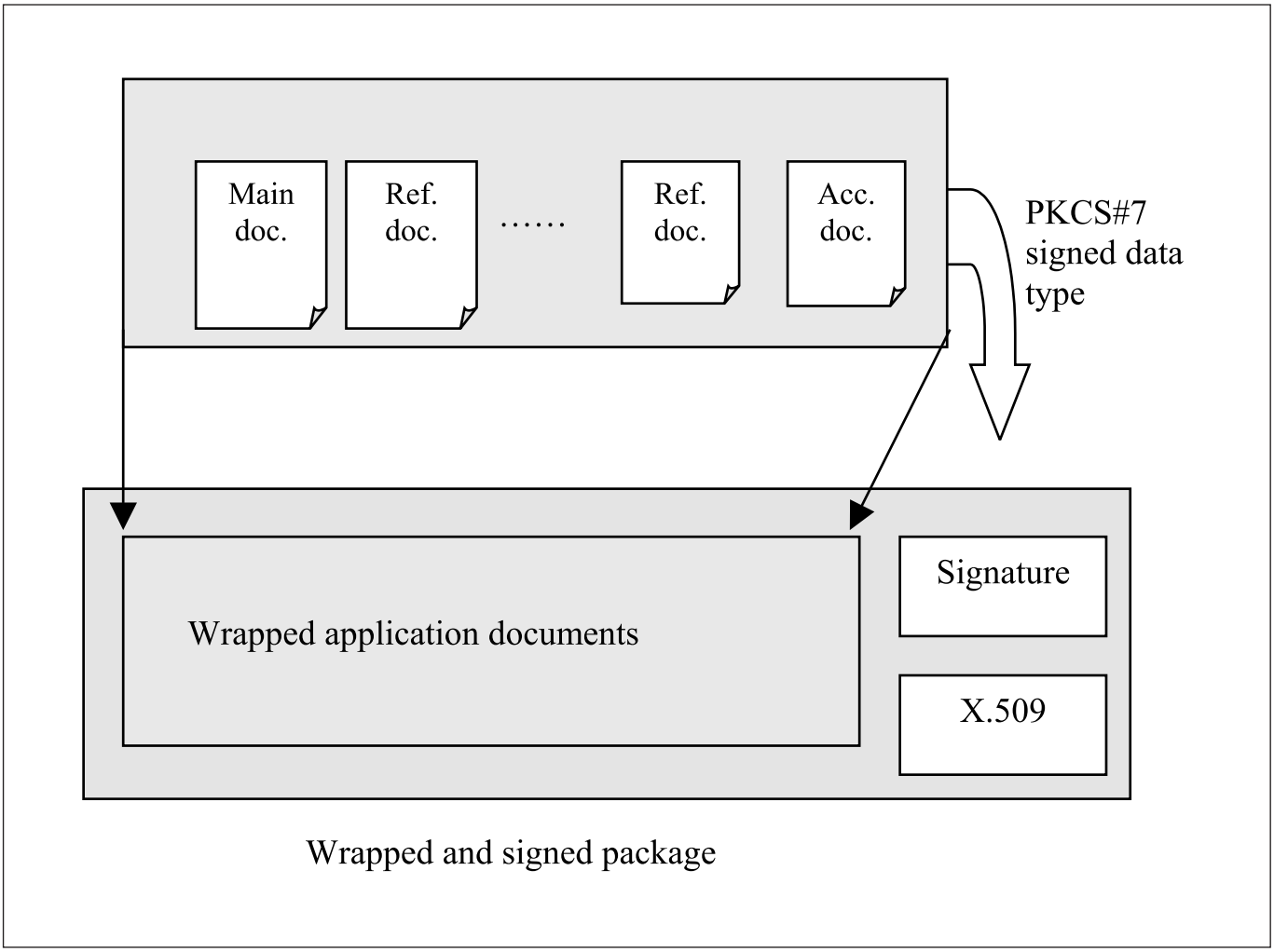
All ZIP files must have a flat directory structure. If a collection of files needs to be embedded in the ZIP file, then these should be included as a single flat embedded ZIP file.

The ZIP standard allows the compression software to select from among a number of compression algorithms. The default compression method must be "Deflation".

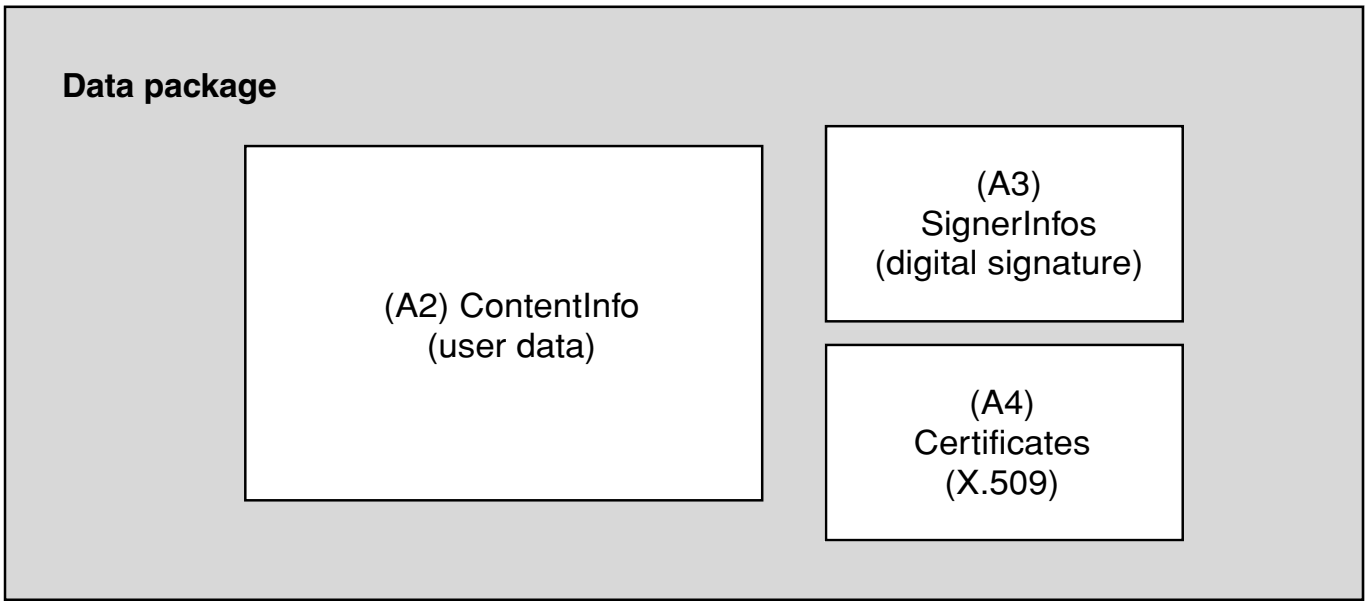
5.3 Signing wrapped application documents

To bind the person creating the package to the electronic wrapped application documents, a digital signature is added to create the wrapped and signed package. The purpose of adding the signature is to identify the person creating the package and to enable the recipient to detect any unauthorised alteration during transmission.

PKCS#7 is used to produce a signed data type for the signature.



(A1) SignedData <top level>
(PKCS#7 digital envelope for signature)



Rules for producing the PKCS#7 digital envelope for certification

Object identifier for sha-1	The object identifier adopted for SHA-1 is defined in OIW interconnection protocols (Part 12) as follows: **Sha-1 OBJECT IDENTIFIER ::= {iso (1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 26}**
Object identifier for RSA encryption	The object identifier for RSA encryption is defined in *RSA Encryption Standard PKCS#1* as follows: **Pkcs-1 OBJECT IDENTIFIER ::= iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1} RsaEncryption OBJECT IDENTIFIER ::={pkcs-1 1}**
Object identifier for triple DES	dES-EDE3-CBC OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) encryptionAlgorithm(3) 7}

Table A1 SignedData – top level

No.	Item name	PKCS#7 item	Content
1	Version	Version	Set integer value '1'
2	Set of algorithm identifiers	DigestAlgorithms	
2.1	Algorithm identifier	AlgorithmIdentifier	Set ONE **set** of algorithm identifiers {sha-1} only
3	Content information	ContentInfo	Set one content information (see table A2)
4	Certificates	Certificates	Set one Certificates (see table A4)
5	Certificate revocation lists	Crls	Not used (set no data)
6	Signer information	SignerInfos	Set one SignerInfos (see table A3)

Table A2 ContentInfo – top level

No.	Item name	PKCS#7 item	Content
1	Content type	ContentType	Set object identifier {pkcs-7 1}
2	Content	Content	Set user data (binary)

Table A3 SignerInfos – top level

No.	Item name	PKCS#7 item	Content
1	Version	Version	Set integer value '1'
2	Issuer and serial number	IssuerAndSerialNumber	Issuer of certificate and certificate serial number in acc. with X.509 (signer's certificate)
3	Set of digest algorithms	DigestAlgorithm	
3.1	Algorithm identifier	AlgorithmIdentifier	Set ONE **set** of algorithm identifiers {sha-1} only to make digest of digital signature
4	Authenticated attributes	AuthenticatedAttributes	Not used (set no data)
5	Digest encryption algorithm	DigestEncryptionAlgorithm	Algorithm OBJECT identifier of digest encryption (recommended algorithm: rsaEncryption)
6	Encrypted digest	EncryptedDigest	Digest data encrypted using signer's private key
7	Unauthenticated attributes	UnauthenticatedAttributes	Not used (set no data)

Table A4 Certificates – top level

No.	Item name	PKCS#7 item	Content
1	Set of certificates	ExtendedCertificatesAnd Certificates	
1.1	X.509 certificate	Certificate (defined in X.509)	Set ONE **set** of X.509 certificate data only

6 Submission

6.1 Transmission package

The EPO may decide not to use the enveloping mechanism described in this section as the encryption mechanism for transmission where channel level encryption such as SSL or physical media such as CD-R are used.

The actual transmission data exchanged between the applicant and the EPO is called a package.

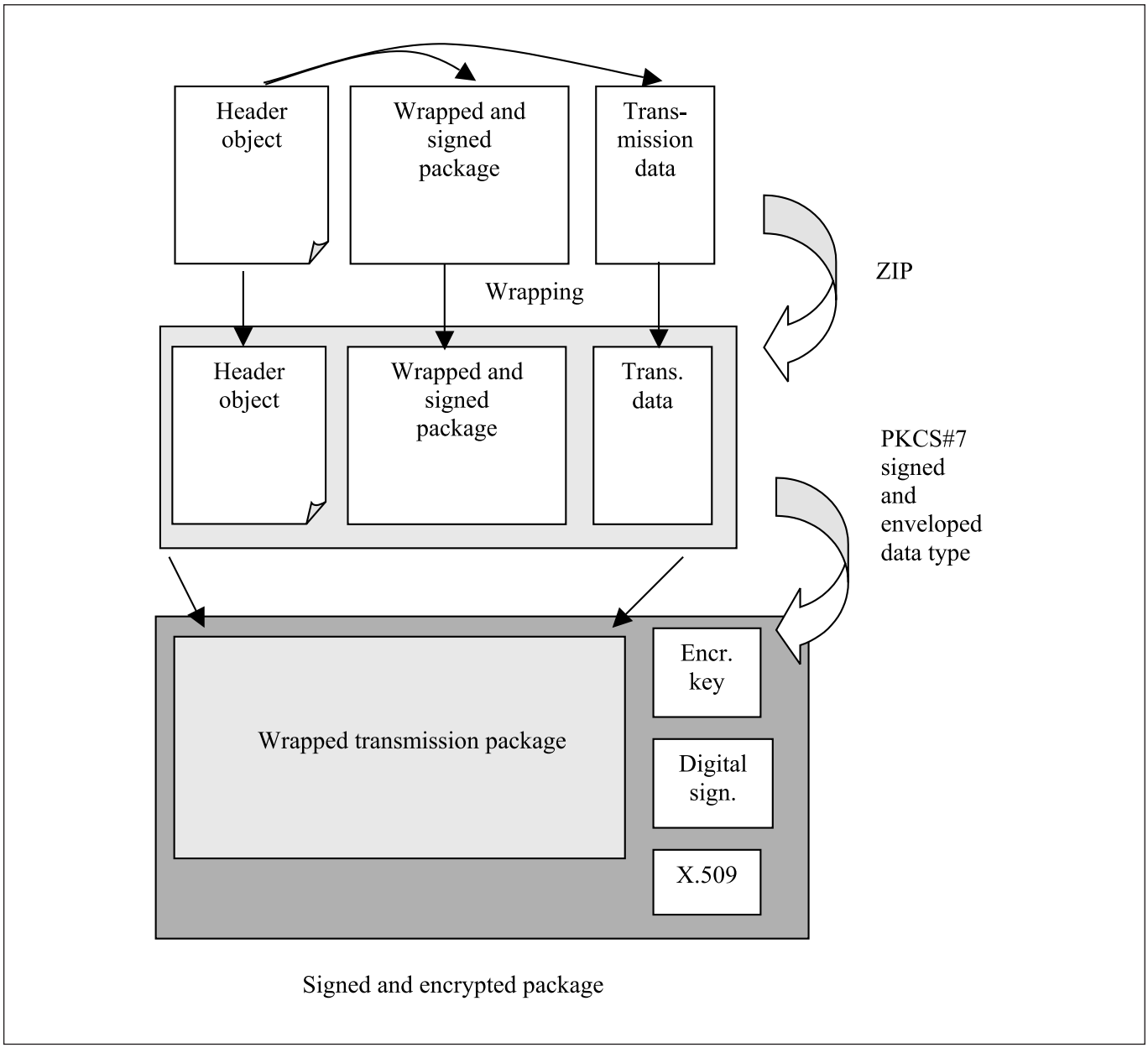
A package contains various data items depending on the type of package. These include:
1. Header object data item
2. Wrapped and signed package made by wrapping and signing the application documents
3. Transmission data such as time of transmission.

The header object data item indicates the package type, file name of data item, etc. It is always found in the signed and encrypted package, and is written in XML.

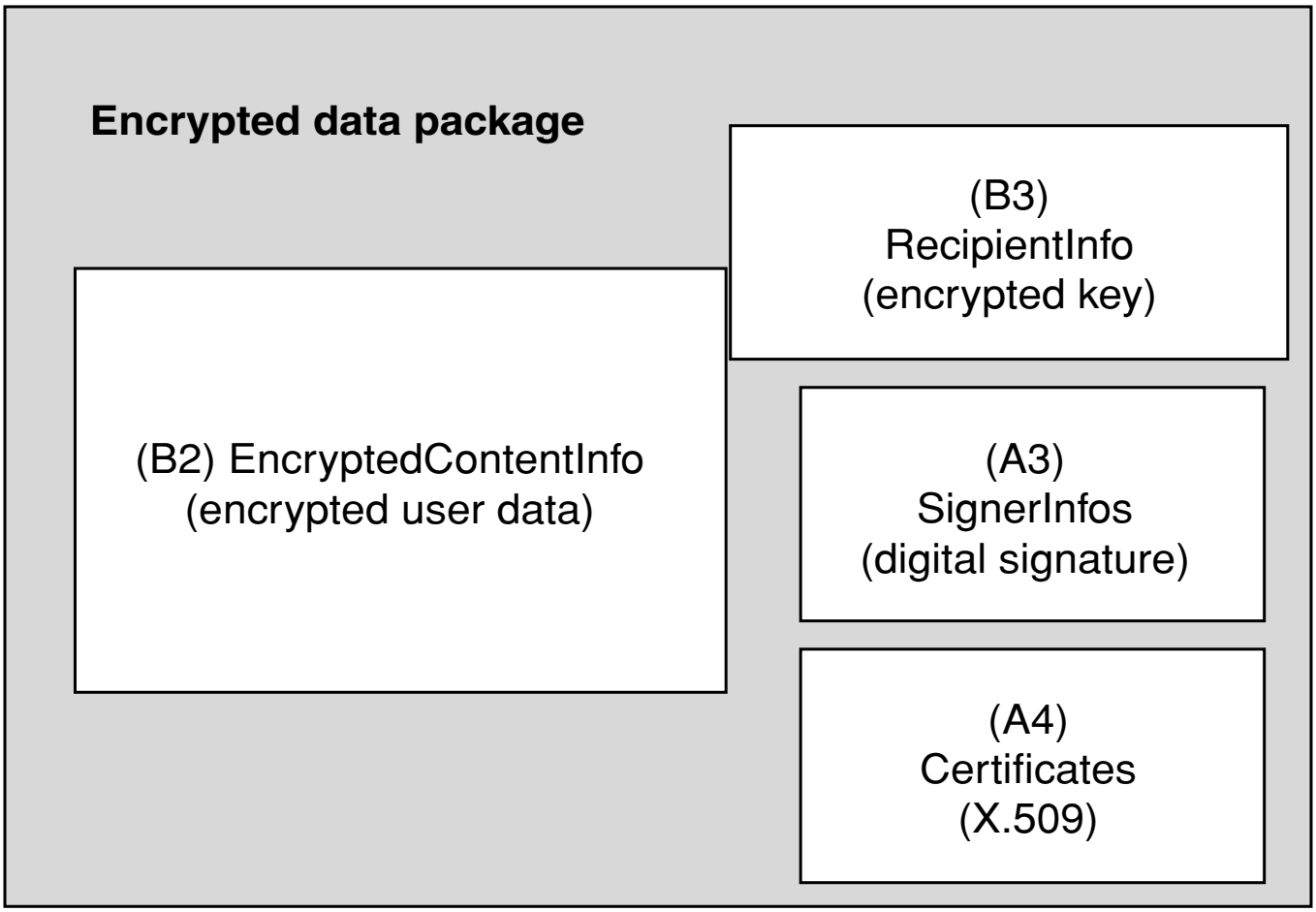
The procedure for creating signed and encrypted packages is as follows:
(a) Create a wrapped transmission package by wrapping the wrapped and signed package with the data items used for transmission using ZIP
(b) Create a signed and encrypted package for network transmission by encrypting using the PKCS#7 signed and enveloped data type.

The purpose of the signature is to ensure the combination and contents of the individual data items, and to enable the recipient to detect any unauthorised alterations during transmission. Encryption is to prevent the unauthorised interception of data during communication.

The digital signature for the wrapped and signed package may be produced by either the applicant or his representative. The person that starts the transmission produces the digital signature for the final signed and encrypted package.



(B1) SignedAndEnveloped Data <top level>
(PKCS#7 digital envelope for transmission)



Rules for producing the PKCS#7 digital envelope for transmission

Table B1 SignedAndEnvelopedData – top level

No.	Item name	PKCS#7 item	Content
1	Version	Version	Set integer value '1'
2	Recipient information	RecipientInfos	Set ONE **set** of RecipientInfo only (see table B3)
2	Set of algorithm identifiers	DigestAlgorithms	
2.1	Algorithm identifier	AlgorithmIdentifier	Set ONE **set** of algorithm identifiers {sha-1} only
3	Encrypted Content information	EncryptedContentInfo	Set one EncryptedContentInfo (see table B2)
4	Certificates	Certificates	Set one Certificates (see table A4)
5	Certificate revocation lists	Crls	Not used (set no data)
6	Signer information	SignerInfos	Set one SignerInfos (see table A3)

Table B2 EncryptedContentInfo – top level

No.	Item name	PKCS#7 item	Content
1	Content type	ContentType	Set object identifier {pkcs-7 1}
2	Content encryption algorithm	ContentEncryptionAlgorithm	Algorithm OBJECT identifier of content encryption (recommended algorithm: dES-EDE3-CBC)
3	Encrypted content	EncryptedContent	Encrypted user data

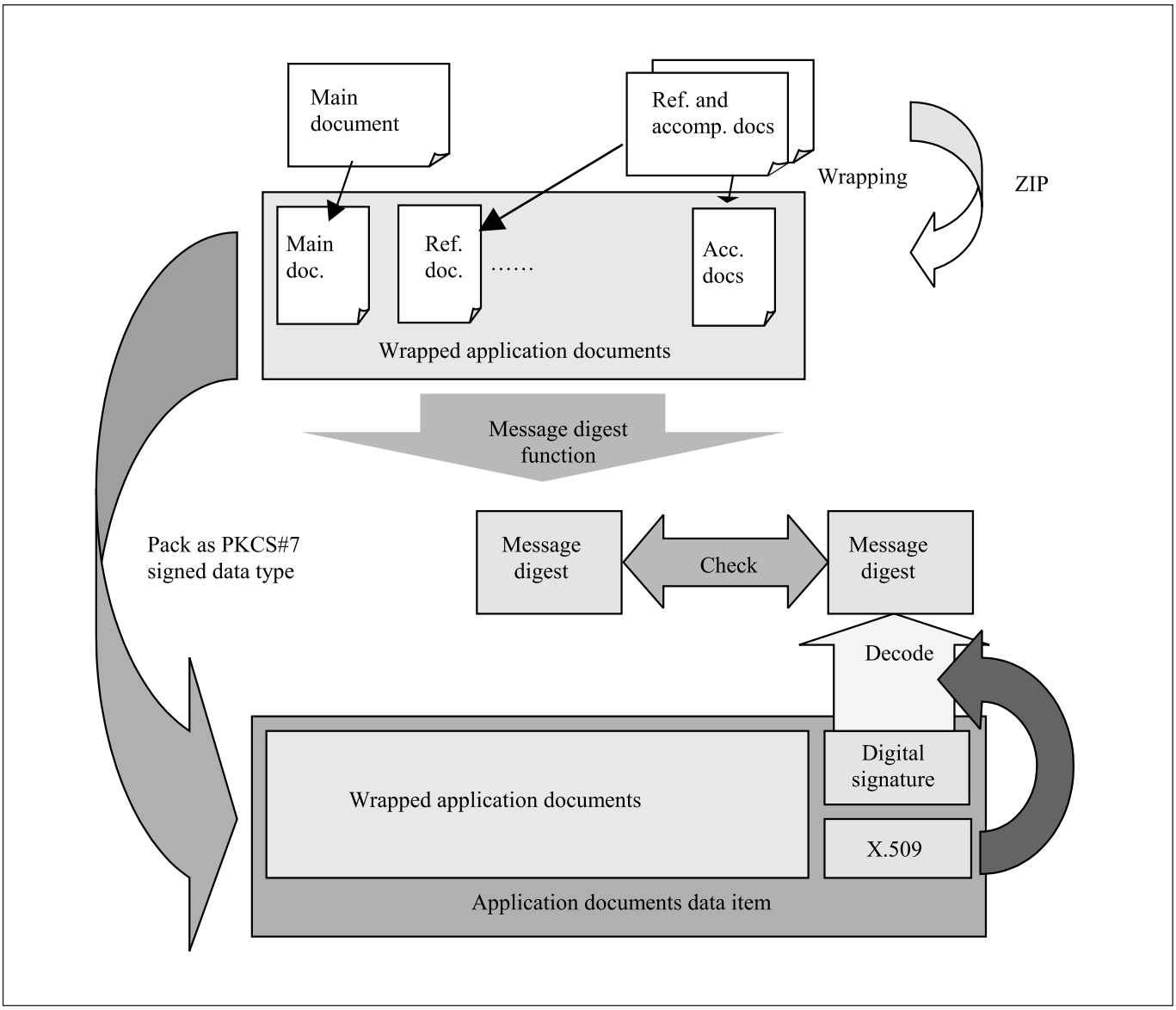
Table B3 RecipientInfo – top level

No.	Item name	PKCS#7 item	Content
1	Version	Version	Set integer value '1'
2	Issuer and serial number	IssuerAndSerialNumber	Issuer and serial number of certificate including public key for encrypting user data encryption key
3	Key encryption algorithm	KeyEncryptionAlgorithm	Algorithm OBJECT identifier for encrypting user data encryption key (recommended algorithm: rsaEncryption)
4	Encrypted key	EncryptedKey	Encrypted decryption key for user data

6.2 Transmission mechanism

The transmission mechanism operates as follows:

- An electronic session is established between the applicant and the EPO.
- The applicant transmits the signed and encrypted package.
- When the signed and encrypted package is received, its contents are checked for the presence of viruses and the wrapped application documents object is processed to create its unique message digest.
- This digest is compared with the message digest included in the wrapped and signed package. If they match, an acknowledgement of receipt is sent to the applicant. If they do not, the applicant is informed accordingly. The session is then ended.



6.2.1 Checking the message digest

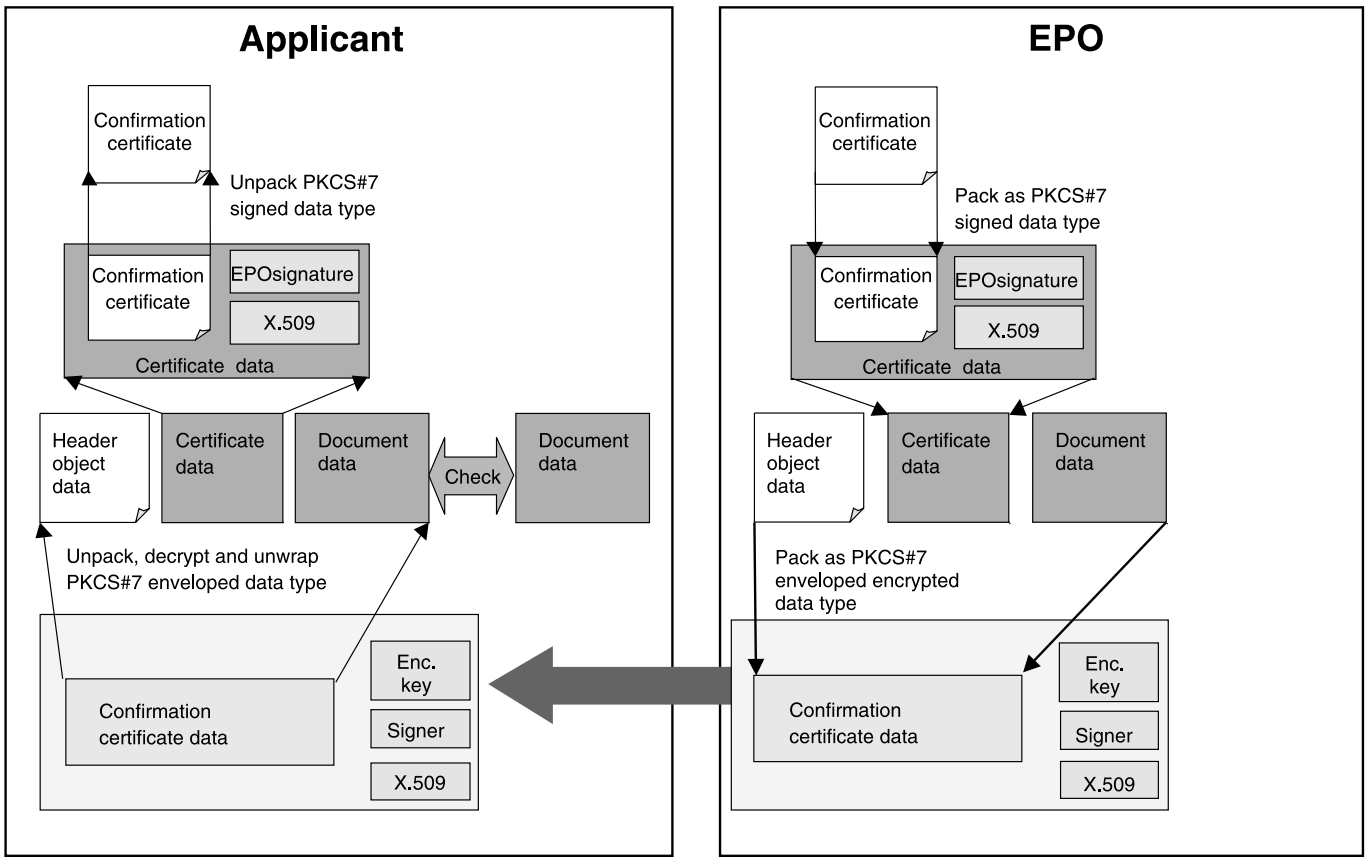
When the EPO receives the wrapped application documents, it opens the data items in them and ascertains the role of each one according to the information in the header object.

6.2.2 Confirmation certificate

The confirmation certificate data item includes a certificate data item, a header object data item indicating that the corresponding packet is a confirmation certificate, and, optionally, the application documents data item received with the new application.

In the event of a communications or message digest comparison problem, the confirmation certificate contains information about the problem.

The confirmation certificate is packaged as a signed and encrypted package, as described above.



The confirmation certificate is used to inform the applicant of the receipt of the application and must contain an XML version of this information. It may also contain a formatted version of the data in PDF. These files are combined in a single ZIP file and signed using the EPO's digital certificate.

6.3 Transmission protocol

The EPO uses a transfer protocol based on HTTP in conjunction with SSL.

7 Physical media

The EPO also accepts electronic filing on CD-R. Each CD-R should contain one application only, in the form of a signed WAD written into the root directory. The name of the signed WAD file should be "WAD.ZIP". The accompanying paper form should include details of the application or document and should refer to the "WAD.ZIP" file on the CD-R. The CD-R volume name should be based on the applicant's reference number.

Annex – Diagrams illustrating the standard

The following diagrams and text provide additional (simplified) information about the standard.

Simplified anatomy of a signed and encrypted package

Figure 1 illustrates, for non-technical readers, the components of the signed and encrypted package mechanism specified in this standard. The diagram has been intentionally simplified to obscure technical detail that may distract the reader from the key issues of the package design. For example, the ZIP wrapping has been left out, and encoding standards for objects are not addressed.

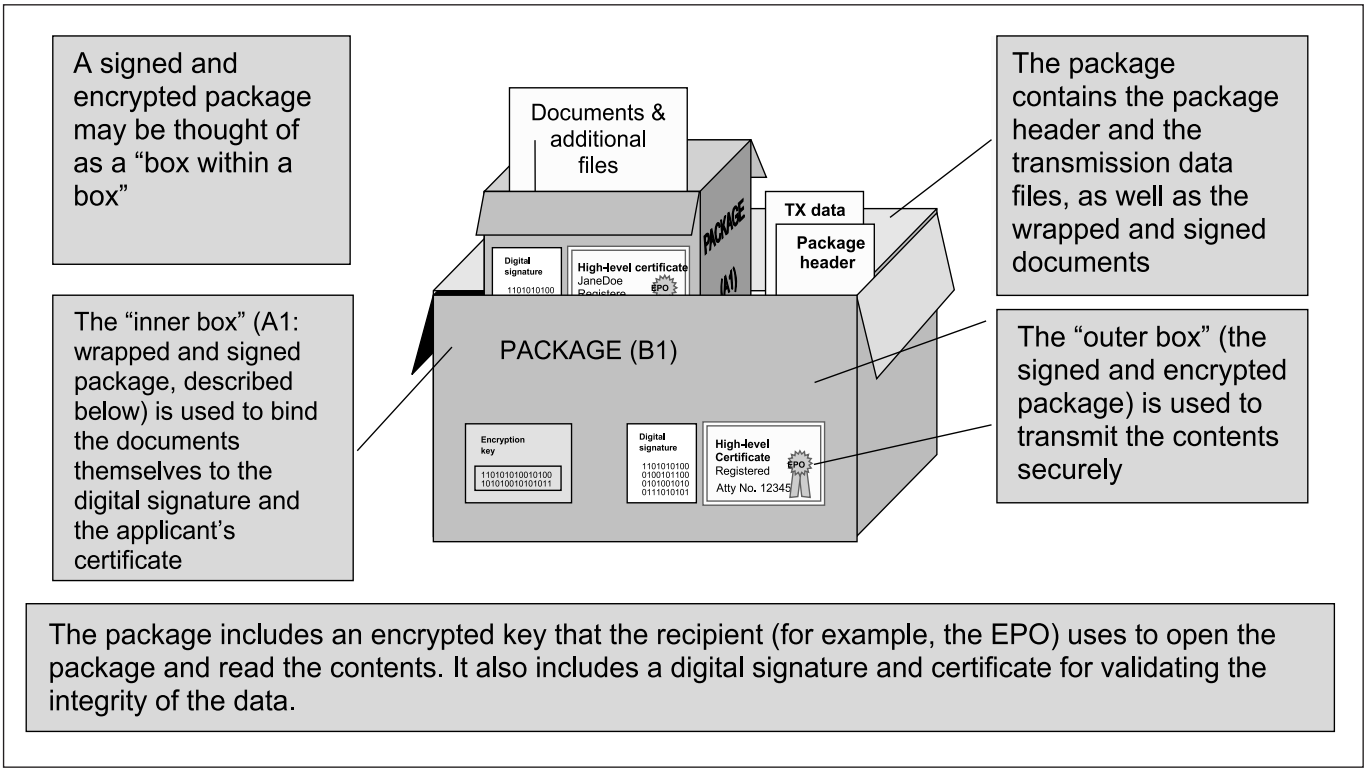


Figure 1: Signed and encrypted package

Simplified anatomy of a wrapped and signed package

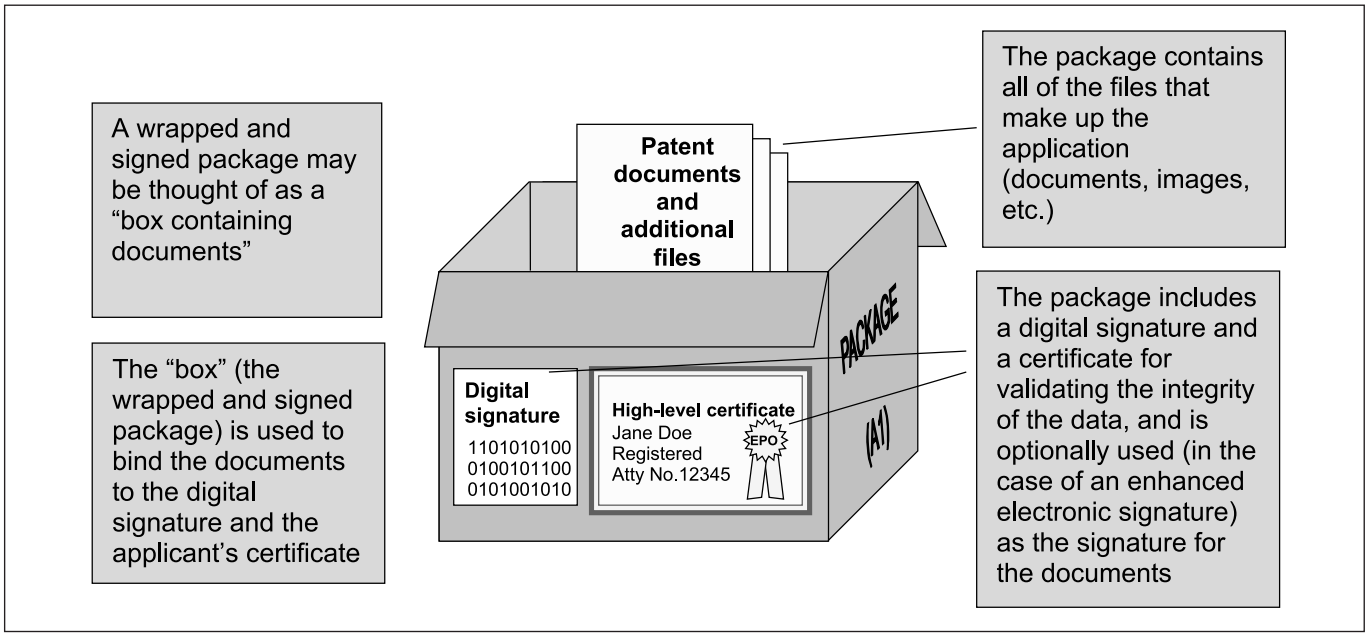


Figure 2: Wrapped and signed package

Anatomy of the wrapped application documents object

The wrapped application documents object in section 5 defines how documents are "wrapped" together. In the case of offline submission on physical media, the further steps of creating the wrapped and signed package and the signed and encrypted package are optional. A wrapped application documents object consists of files that have been 'zipped' together into a single file and placed in the root directory of the physical media.

Certificate/signature types

The diagrams in Figures 3 to 7 illustrate the differences between the types of "digital certificate" and "electronic signature" options as specified in the standard. Each diagram shows a "box" representing the wrapped and signed package.

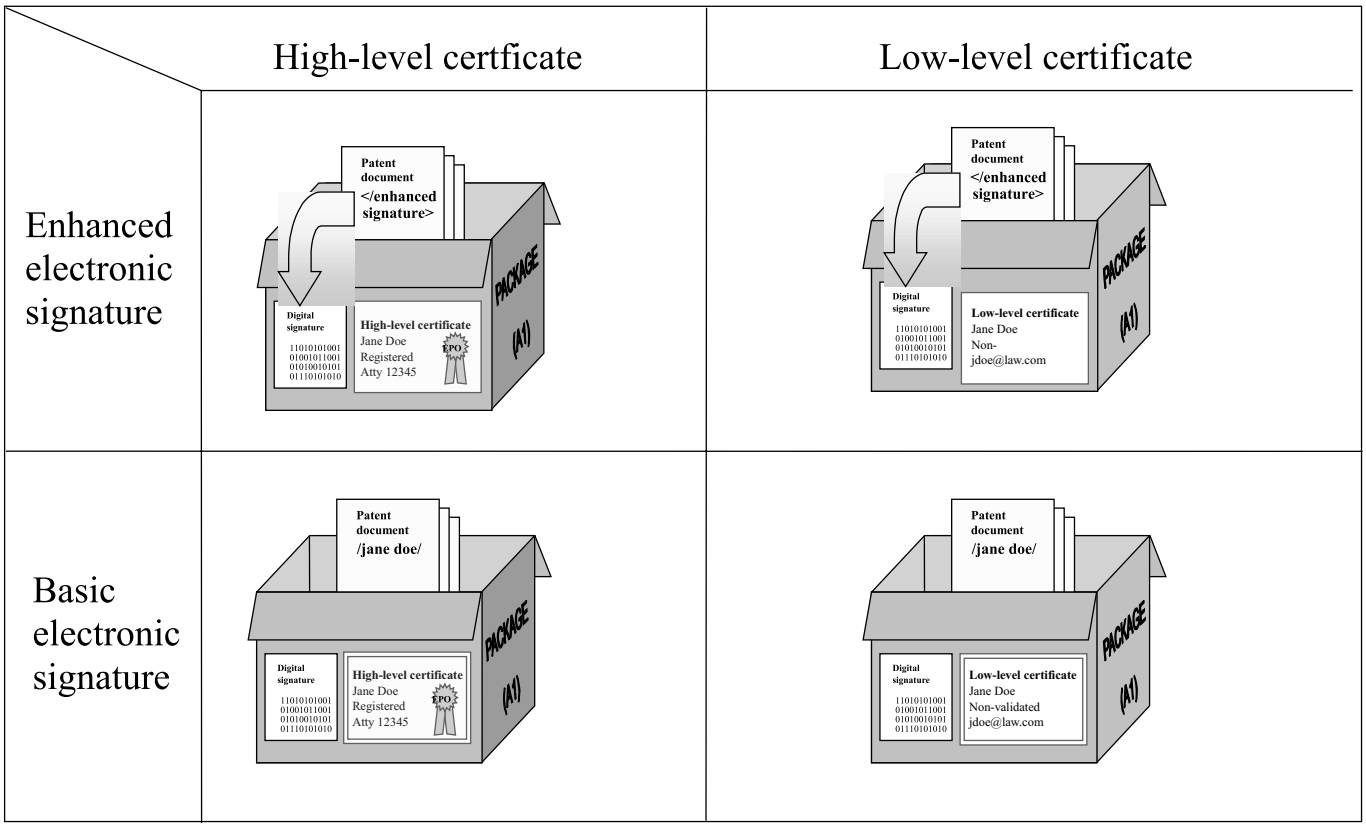


Figure 3: Certificate/signature types

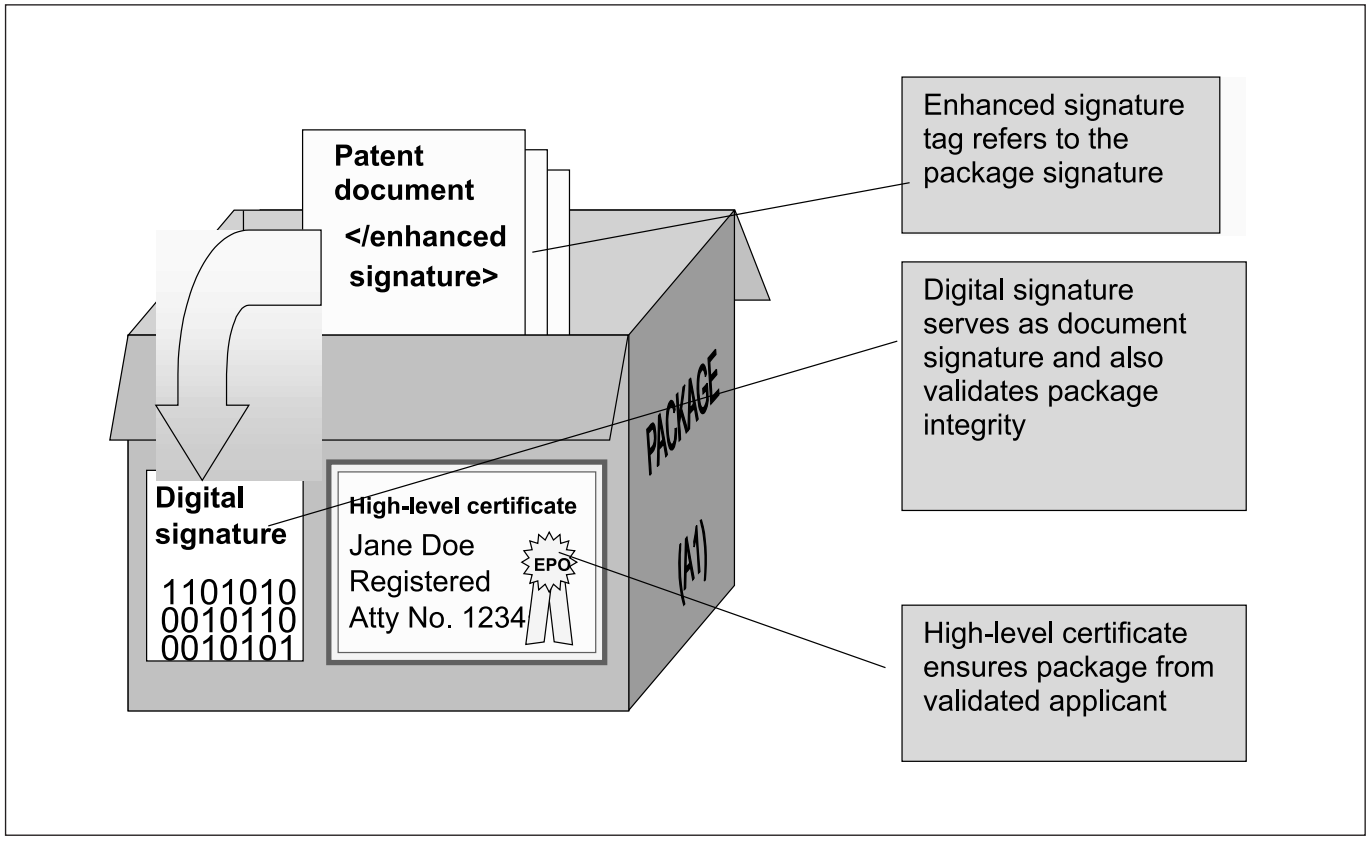


Figure 4: Enhanced electronic signature/high-level certificate

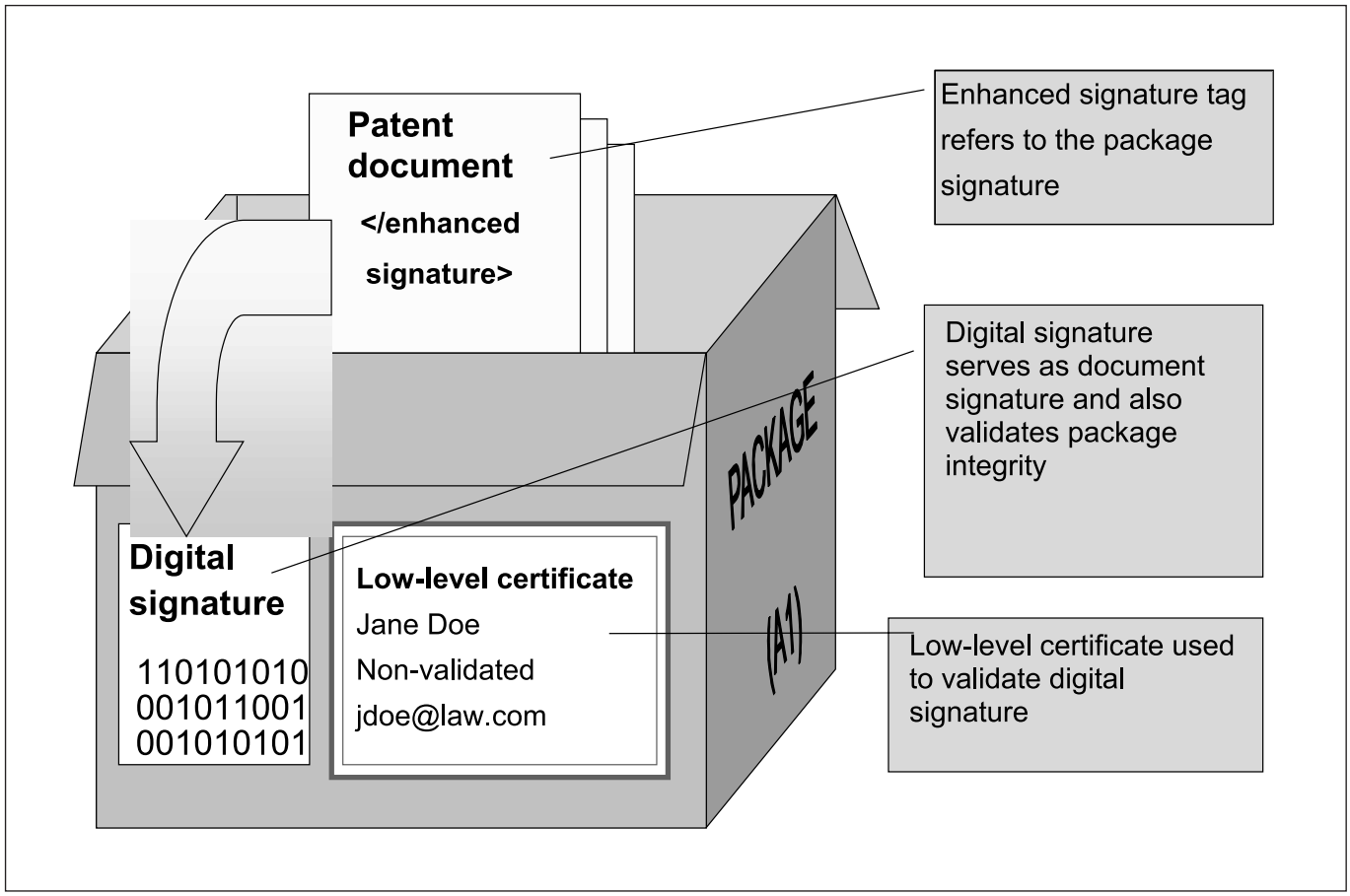


Figure 5: Enhanced electronic signature/low-level certificate

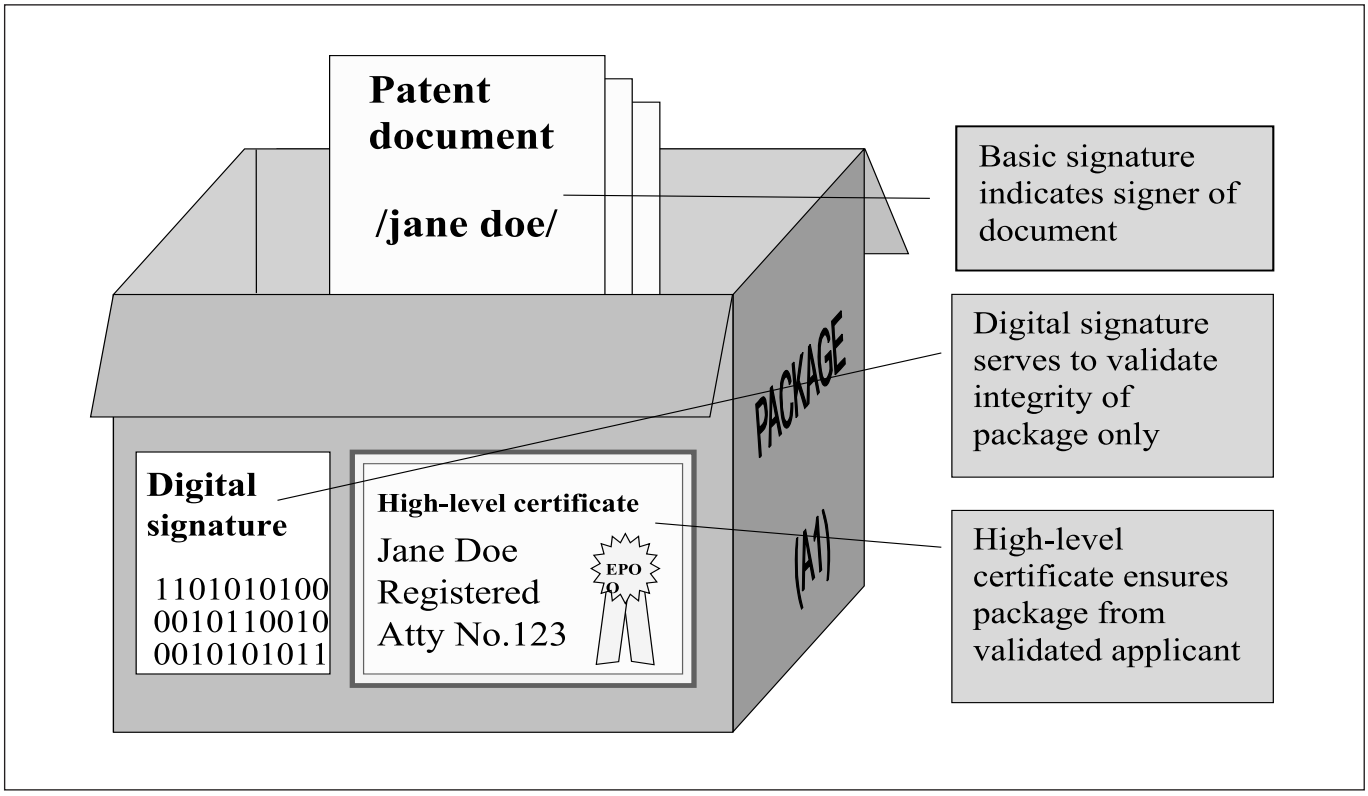


Figure 6: Basic electronic signature/high-level certificate

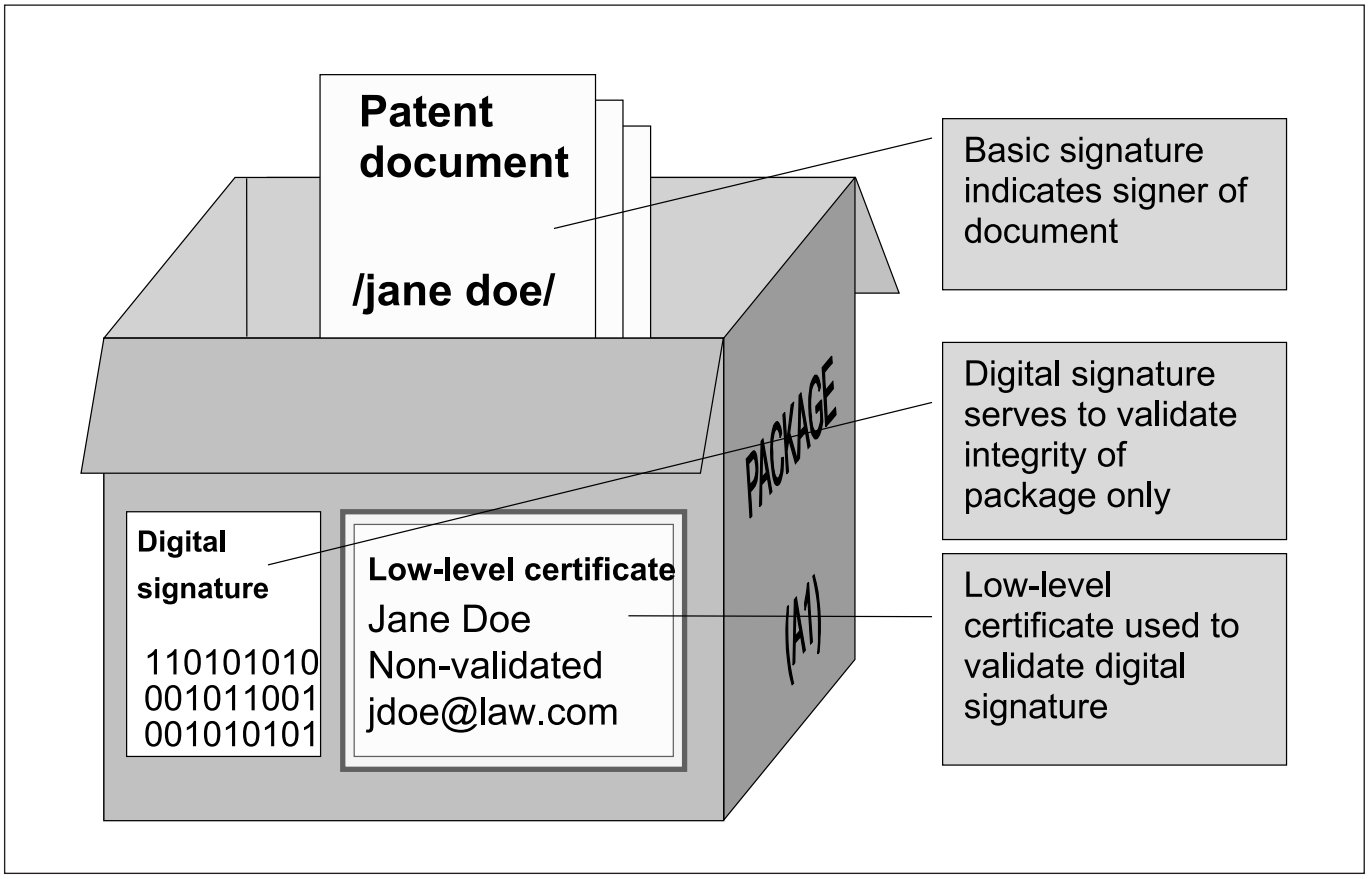


Figure 7: Basic electronic signature/low-level certificate

Transmission mechanism/packaging combinations

Figure 8 shows the various transmission mechanism/packaging combinations that are permissible. The following applies to each transmission mechanism:
(a) Online/internet: a signed and encrypted package must be used.
(b) Online/secure (channel encryption such as a private network): a signed and encrypted package or wrapped and signed package must be used.
(c) Offline/physical media: either a signed and encrypted package, a wrapped and signed package, or a wrapped application documents package may be used.

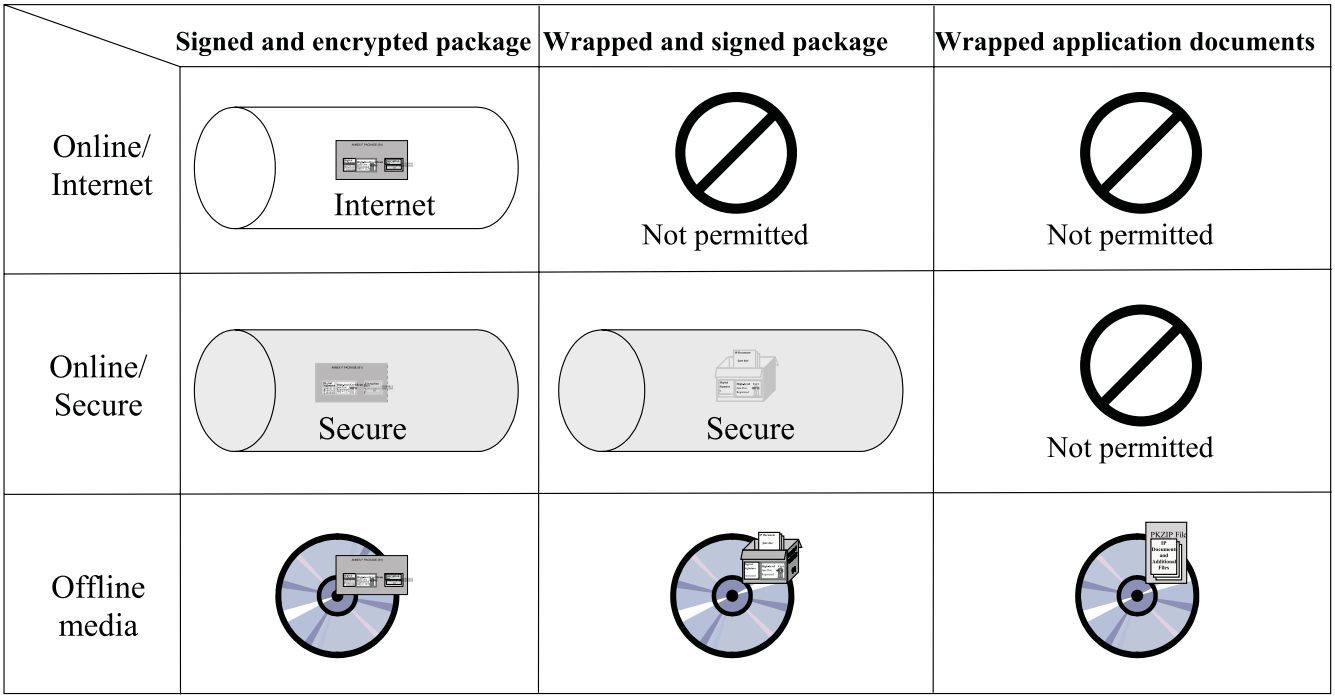


Figure 8: Transmission protocols and packages permitted

Décision du Président de l'Office européen des brevets du 7 décembre 2000, relative au dépôt électronique de demandes de brevet européen et de documents produits ultérieurement

Le Président de l'Office européen des brevets (OEB), vu les règles 24(1), 27bis, 35(2), 36(5), 77(2)d) et 101 CBE,

vu les conditions de base que doit remplir toute pièce électronique, à savoir :

a) l'authenticité, c'est-à-dire la confirmation qu'un document est bien ce qu'il prétend être et que son auteur est bien la personne censée en être l'auteur ;

b) l'intégrité, c'est-à-dire la cohérence des données, notamment pouvoir déceler et éviter l'altération et la destruction non autorisées de ces données ;

c) la confidentialité, c'est-à-dire veiller à ce que l'existence ou le contenu d'un document ne soient pas divulgués à des personnes non autorisées, et

d) la non-répudiation, c'est-à-dire veiller à ce que l'expéditeur (avec la collaboration du destinataire) dispose de preuves fiables du fait que les données ont bien été transmises, et que le destinataire dispose de preuves fiables concernant l'identité de l'expéditeur, afin qu'aucune des parties ne puisse nier de manière crédible avoir envoyé ou reçu les données, et qu'un tiers puisse en vérifier l'intégrité et l'origine,

vu les normes de base en matière de gestion des pièces électroniques, à savoir que :

(1) tous les documents déposés sous forme électronique doivent pouvoir être imprimés sur papier et transférés sur un support d'archivage sans perte de contenu, ni altération matérielle ;

(2) les renseignements recueillis à chaque fois par les systèmes informatiques au sujet des pièces électroniques, souvent appelés métadonnées, doivent également être considérés comme faisant partie desdites pièces et conservés par ces systèmes informatiques ;

(3) les documents électroniques doivent être envoyés dans un format de fichier électronique défini par l'office, et les copies d'archive doivent également être conservées dans le format électronique dans lequel elles ont été envoyées ;

(4) tous les dépôts électroniques doivent faire l'objet d'un accusé de réception adressé à l'expéditeur pour indiquer que l'office a bien reçu le document. L'accusé de réception doit indiquer l'identité de l'office, la date et l'heure de réception du document (qui seront la date et l'heure officielles de réception par l'office), ainsi que tout numéro de référence ou de demande attribué par l'office, le cas échéant ;

(5) tout office qui accepte le dépôt électronique doit aussi permettre l'envoi de documents sur papier. Ces documents sur papier peuvent être scannés de façon à faciliter la création d'un dossier électronique unique ;

(6) un mécanisme doit être prévu afin de garantir l'authenticité et l'intégrité du document déposé sous forme électronique. Cela suppose la possibilité de vérifier l'identité de l'expéditeur (le déposant ou son mandataire), ainsi que la possibilité de vérifier qu'un document n'a pas été modifié sans autorisation depuis son dépôt ;

(7) tout système de dépôt électronique doit prévoir des mécanismes de sauvegarde et de restauration pour protéger les dépôts électroniques contre ses propres défaillances ;

(8) les pièces électroniques doivent être conservées et accessibles à long terme ;

(9) l'absence de virus et d'autres formes de logiciels nuisibles doit être vérifiée dans tous les fichiers électroniques avant leur traitement, et des mesures appropriées doivent être prises afin de préserver, si possible, la date de dépôt ;

(10) l'accès aux ordinateurs utilisés pour le dépôt électronique ne doit pas mettre en péril la sécurité des autres réseaux et applications de l'office ;

(11) les systèmes de gestion des pièces électroniques doivent prévoir des mécanismes d'assurance et de contrôle de la qualité des documents produits ;

(12) les systèmes de gestion des pièces électroniques doivent mettre en oeuvre une piste de contrôle gardant trace de toutes les adjonctions ou modifications apportées aux pièces électroniques et y consigner les renseignements concernant la réception et la production de chaque pièce ainsi que de toute modification apportée à une pièce ;

(13) si l'accès à des données confidentielles par des moyens électroniques est permis, il doit être sécurisé et réservé à un public autorisé. Des mesures doivent être prises pour protéger ces fichiers contre toute altération. Lorsqu'un déposant, un mandataire ou des membres autorisés du public ont accès à des fichiers par des moyens électroniques, des renseignements doivent être consignés sur l'identité de la partie concernée, sur la date (et éventuellement l'heure) de la transaction et sur tout envoi de documents. Ces renseignements doivent rester confidentiels ;

(14) dans la mesure prévue par la CBE, le public doit pouvoir avoir accès aux demandes de brevet européen et aux brevets européens publiés ; et

(15) tout document électronique doit à sa réception être copié sur un support à lecture seule,

décide :

Article premier
Dépôt de demandes de brevet européen

Les demandes de brevet européen peuvent être déposées à l'OEB sous forme électronique comme suit :

a) en ligne, auprès des serveurs informatiques de l'Office européen des brevets, à l'adresse suivante : **https://secure.epoline.org** ou

b) sur CD-R.

Les demandes de brevet européen peuvent être également déposées sous forme électronique auprès des services nationaux compétents des Etats contractants qui autorisent ce mode de dépôt. Les dispositions nationales des Etats contractants qui prescrivent qu'un premier dépôt doit être effectué auprès de l'Office national ou que le dépôt auprès d'une autre autorité est soumis à une autorisation préalable (article 75(2) CBE) ne sont pas affectées.

Article 2
Norme relative au dépôt électronique

La norme technique relative au dépôt électronique figurant en annexe (dénommée ci-après "la norme") est partie intégrante de la présente décision. Toute version future remaniée de cette norme ou toute norme future recommandée par l'Organisation Mondiale de la Propriété Intellectuelle pour le dépôt électronique de demandes nationales de brevet sera applicable après publication d'une décision correspondante du Président de l'Office européen des brevets.

Article 3
Etablissement des pièces

Les pièces déposées conformément à l'article premier doivent être établies à l'aide soit du logiciel fourni gratuitement par l'OEB, soit d'un logiciel certifié par l'OEB comme étant conforme à la norme.

Article 4
Présentation des pièces

Les pièces de la demande de brevet européen, y compris les dessins, déposées conformément à l'article premier, doivent être présentées dans le format spécifié dans la norme. Les listes de séquences figurant dans les demandes déposées conformément à l'article premier, alinéa a) ne doivent pas être présentées sur un support séparé de données.

Article 5
Requête en délivrance

Toute requête en délivrance d'un brevet européen, déposée conformément à l'article premier, doit comporter, outre les informations requises à la règle 26(2) CBE, l'adresse électronique du demandeur, ainsi que celle de tout mandataire éventuellement désigné.

Article 6
Lisibilité
Fichiers infectés

(1) L'OEB vérifie dès leur réception si les demandes de brevet européen déposées conformément à l'article premier

a) sont lisibles et

b) si elles contiennent des virus informatiques ou d'autres formes de logiciels nuisibles.

(2) Si la demande de brevet européen est illisible en totalité ou en partie, l'OEB considère que la partie du document qui est illisible n'a pas été reçue et, si possible, en avise rapidement le demandeur.

(3) S'il est constaté que la demande de brevet européen est infectée par un virus informatique ou par un logiciel nuisible, l'OEB la considère comme illisible et n'est tenu ni de l'ouvrir, ni de la traiter. L'OEB met en oeuvre tous les moyens dont il dispose normalement pour lire le document afin de pouvoir lui attribuer une date de dépôt et, si possible, avise rapidement le demandeur.

(4) S'il est constaté que la demande de brevet européen présente les défauts visés aux paragraphes 2 et 3, et qu'il n'est pas possible par conséquent de lui accorder une date de dépôt, l'OEB invite si possible le demandeur à remédier à ces défauts dans un délai qu'il lui impartit. La date de dépôt sera celle à laquelle il aura été remédié aux défauts. S'il n'est pas remédié en temps utile à ces défauts, la demande n'est pas traitée en tant que demande de brevet européen.

Article 7
Examen relatif au respect de certaines conditions de forme

Si la demande de brevet européen est présentée dans un format non conforme à celui spécifié à l'article 4, l'OEB s'efforce dans une mesure raisonnable de lire les pièces déposées aux fins de l'attribution d'une date de dépôt. S'il n'y parvient pas, l'article 6(4) est applicable. S'il y parvient, l'OEB invite le demandeur, dans un délai qu'il lui impartit, à présenter de nouveau sa demande dans un format conforme à celui spécifié à l'article 4. Si la demande n'est pas représentée en temps utile dans le format prescrit, elle est rejetée conformément à l'article 91(3) CBE.

Article 8
Dépôt d'autres pièces

Si la demande de brevet européen est déposée conformément à l'article premier, tout pouvoir ainsi que toute désignation d'inventeur peuvent également être déposés conformément à l'article premier. Les articles 3, 4 et 6 sont applicables. Si ces pièces sont présentées dans un format non conforme à celui spécifié à l'article 4, le demandeur est invité à les représenter dans un format conforme à celui spécifié à l'article 4, dans un délai que lui impartit l'OEB. Si un pouvoir n'est pas représenté en temps utile dans le format prescrit, la règle 101(4) CBE s'applique. Si la désignation de l'inventeur n'est pas représentée en temps utile dans le format prescrit, l'article 91(5) CBE s'applique.

Article 9
Pièces originales – nombre d'exemplaires
Version authentique

(1) Les pièces déposées conformément aux articles premier et 8 sont réputées être les pièces originales pour toutes les procédures engagées par la suite devant l'OEB. Elles sont produites en un exemplaire.

(2) Lorsqu'un document a été déposé sur CD-R conformément à l'article premier ou 8, la version électronique du document obtenue par l'OEB à partir du CD-R et stockée dans le dossier électronique de la demande de brevet européen est réputée être la version authentique du document. En cas de contestation par le déposant ou par des tiers, des vérifications pourront être effectuées à l'aide du CD-R original qui sera conservé pendant la période prévue à la règle 95bis CBE.

Article 10
Confirmation sur papier

(1) Il n'est pas exigé de confirmation sur papier pour les documents déposés conformément aux articles premier et 8.

(2) L'OEB ne tiendra pas compte des confirmations sur papier qui auraient pu néanmoins être produites, à moins que le demandeur ne le lui ait expressément demandé, auquel cas l'OEB pourra être amené à modifier la date de dépôt déjà accordée.

(3) Toute confirmation sur papier qui aura été produite devra être clairement signalée en tant que telle et contenir les informations permettant à l'OEB de la rattacher à la pièce correspondante déposée par voie électronique.

Article 11
Signatures

(1) Lorsque la demande de brevet européen est déposée conformément aux dispositions de l'article premier, la signature requise dans la requête en délivrance d'un brevet européen doit figurer sous l'une des formes suivantes :

a) image en fac-similé de la signature manuscrite du signataire ;

b) signature électronique, c'est-à-dire données sous forme électronique rattachées ou associées logiquement à d'autres données électroniques (message électronique), utilisées comme méthode d'authentification du signataire du message et servant à indiquer qu'il approuve les informations contenues dans ce message ; ou

c) signature électronique avancée, c'est-à-dire signature électronique remplissant les conditions suivantes :

i) être liée uniquement au signataire ;

ii) être créée par des moyens que le signataire peut garder sous son contrôle exclusif ; et

iii) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données puisse être détectée.

(2) Une signature électronique au sens du paragraphe 1 b) est constituée d'une série de caractères choisis par le signataire pour exprimer son identité et signifier son intention de signer le message électronique en question ; cette série de caractères est précédée et suivie d'une barre oblique (/).

(3) Une signature électronique avancée au sens du paragraphe 1 c) est une signature numérique produite à l'aide d'un certificat généré par une infrastructure à clé publique et de la clé privée correspondante.

(4) Dans tous les autres cas où une signature est requise en vertu de la CBE, le paquet de données transmises doit être assorti d'une signature électronique avancée au sens du paragraphe 1 c) et du paragraphe 3. Les pièces à l'intérieur de ce paquet peuvent également être signées conformément au paragraphe 1 a) ou aux paragraphes 1 b) et 2.

(5) Si la requête en délivrance d'un brevet européen ou tout autre document relatif à une demande de brevet européen, déposés conformément à l'article premier, lettre a, ne comportent pas de signature ou si la signature apposée n'est pas conforme aux dispositions pertinentes des paragraphes 1 à 4, l'OEB invite le demandeur à remédier à cette irrégularité dans un délai qu'il lui impartit. S'il n'est pas remédié en temps utile à cette irrégularité, le document est réputé n'avoir pas été reçu.

(6) Les demandes de brevet européen et autres documents produits sur CD-R doivent être accompagnés d'un document sur papier qui doit porter une signature manuscrite, permettre l'identification du demandeur ainsi que de son mandataire et comporter également une adresse pour la correspondance et une liste des fichiers contenus sur le CD-R.

Article 12
Accusé de réception

(1) La réception des documents déposés conformément à l'article premier a) est confirmée électroniquement pendant la session de transmission. S'il s'avère que cette confirmation n'a pas été transmise avec succès, l'OEB transmet rapidement cette confirmation par d'autres moyens, s'il dispose des informations voulues pour ce faire.

(2) L'accusé de réception devra indiquer l'identité de l'Office, la date et l'heure de la réception du document, un numéro de référence ou de dépôt attribué par l'Office, ainsi qu'une liste des fichiers transmis. L'accusé de réception comportera aussi un condensé numérique des documents transmis.

(3) L'accusé de réception n'équivaut pas à l'attribution d'une date de dépôt.

Article 13
Paiement des taxes

Les dispositions relatives au paiement des taxes ne sont pas affectées par la présente décision.

Article 14
Notifications de l'OEB

L'OEB précisera quelles notifications peuvent être signifiées en ligne. Lors du dépôt de la demande de brevet européen, les demandeurs indiqueront s'ils souhaitent que des notifications leur soient signifiées en ligne, et, dans l'affirmative, préciseront lesquelles. Les notifications continueront sinon à leur être signifiées sur papier jusqu'à nouvel ordre.

Article 15
Significations

(1) Les significations effectuées sur papier sont régies par les règles 78, 79 et 80 CBE.

(2) Lorsque des notifications sont signifiées en ligne, l'OEB informe le demandeur qu'une notification lui a été adressée et qu'il doit la récupérer. A cet effet, l'OEB envoie au demandeur un courrier électronique contenant un lien avec la boîte aux lettres du demandeur dans le serveur de l'OEB. Si une notification n'est pas récupérée dans un délai de cinq jours à compter de l'envoi du courrier électronique, il est procédé à une signification sur papier conformément au paragraphe 1.

(3) Les notifications signifiées conformément au paragraphe 2 sont réputées reçues le dixième jour suivant la date d'envoi du courrier électronique.

(4) Les dispositions des règles 81 et 82 CBE ne sont pas affectées par la présente décision.

Article 16
Délais

Les règles 83, 84 et 85 CBE sont applicables en matière de délais. Seuls les demandeurs qui ont accepté de recevoir des significations en ligne peuvent également requérir des prorogations de délais en ligne.

Article 17
Entrée en vigueur

La présente décision prend effet le 8 décembre 2000.

Fait à Munich, le 7 décembre 2000.

Ingo KOBER
Président

Technical standard for the electronic filing of European patent applications and subsequent documents

1 Background

This document contains the technical standards for the electronic filing of documents with the EPO. It is based on the Trilateral Public Key Infrastructure (PKI)-based standard that has been incorporated into Annex F, Appendix I of the PCT Administrative Instructions.

A PKI environment provides a suite of services for processing sensitive information. Through the use of cryptography, PKI can satisfy the requirements for:
(a) Authentication – by ensuring that transmissions, messages and originators are valid, and that a recipient is authorised to receive specific categories of information.
(b) Data integrity – by ensuring that data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.
(c) Non-repudiation – by ensuring strong and substantial evidence is available to the sender of data that the data has been delivered (with the co-operation of the recipient), and to the recipient of the sender's identity, so that neither party can successfully deny having possessed the data, and a third party can verify its integrity and origin.
(d) Confidentiality – by ensuring that the information can be read by authorised entities only.

This standard sets out the mandatory requirements for all parties participating in electronic filing, as well as a number of optional requirements.

2 Scope

This technical standard covers requirements in the following areas:
(a) Security and PKI
(b) Electronic signatures
(c) Document format requirements
(d) Submission

3 Security and PKI

3.1 Public Key Infrastructure

In this standard, packaging and transmission are performed using PKI technology. When feasible alternative security technologies become available, they may be incorporated in updates to the standard.

PKI must be implemented in accordance with the recommendations established by the Internet Engineering Task Force (IETF) Working Group on PKI Interoperability (PKIX) and documented in IETF RFC 2459.

Separate key pairs and digital certificates must be used for the digital signature and encryption.

3.2 Digital certificates

Where the standard specifies use of a digital certificate, the certificate must comply with the International Telecommunication Union (ITU) X.509 (version 3) recommendation for certificate format.

A digital certificate is required when communicating with the EPO online.

The standard provides for two classes of digital certificate:

High-level certificate: a digital certificate issued by a certification authority to the applicant, which can be used to authenticate the identity of the applicant. The certification authority must appear on the list of "recognised" certification authorities published by the EPO (see 3.3 below).

Low-level certificate: a digital certificate provided by the EPO to the applicant on request. To receive a low-level certificate, the applicant must provide his name and e-mail address, but is not required to furnish proof of identity.

3.3 Certification authorities

The EPO will specify which certification authorities it accepts. This list of "recognised" certification authorities will include a link to the published PKI policy statement of each of these authorities.

Recognised certification authorities are responsible for maintaining the accuracy of the electronic certificates that "prove" a party is who he says he is. Certification authorities store certificate information for all the certificates they issue in a directory structure complying with ITU recommendation X.500. Such systems provide an external interface for publishing and retrieving user digital certificates that complies with the Lightweight Directory Access Protocol (LDAP) using the IETF Network Working Group's RFC 1777 dated March 1995. In addition, certification authorities publish revocation information about certificates drawn up in accordance with the X.509 standard.

The EPO will subscribe to this revocation information. Whenever a certificate is used to authenticate an individual, the EPO will consult the revocation information published by the certification authority concerned to ensure that the certificate has not been revoked.

3.4 Digital signatures

Digital signatures used to sign electronic documents for electronic filing must conform to the format and practice specified in RSA Laboratories' PKCS#7 Cryptographic Message Syntax Standard (version 1.5) with regard to the definition of the signed-data content type.

To build these signatures, a certificate meeting the requirements set out in Section 3.2 above must be used.

All digital signatures must be encoded using the distinguished encoding rules (DER) defined in ITU recommendation X.690.

3.5 Cryptographic algorithms
Both symmetric (secret key) and asymmetric (public key) algorithms may be used as required. Algorithms prohibited under the national law of a country may not be used for the electronic filing of documents from that country. Algorithms implemented in hardware or software may not be used in any manner contrary to the export restrictions of the country of origin of the hardware or software.

Where possible, the rsaEncryption algorithm is to be used for asymmetric encryption and the dES-EDE3-CBC algorithm for symmetric encryption. The same asymmetric encryption algorithm should be used to create digital certificates, digital signatures and envelopes.

3.6 Data enveloping
Electronic document data that is encrypted to ensure confidentiality for electronic filing must conform to the format and practice specified in RSA Laboratories' PKCS#7 Cryptographic Message Syntax Standard (version 1.5) with regard to the definition of the signed and enveloped data content type.

3.7 Message digest algorithms
The message stream must be input to the strong one-way message digest algorithm SHA-1 to create a message digest.

4 Signature mechanisms

This standard provides for a number of signature types acceptable for electronic filing:
(a) Basic electronic signatures
  (i) Facsimile image of the user's signature
  (ii) Text string
(b) Enhanced electronic signature
  (i) PKCS#7 digital signature

NOTE: Although users may choose not to utilise an enhanced electronic signature mechanism for the document itself, a PKCS#7 digital signature is required to package the wrapped application document as described in section 5.3. See Section 6.1 for an example of a wrapped and signed package.

The basic electronic signature is encoded within the "party" structure of the XML document as specified by the portion of the Document Type Definition (DTD) shown below:

```
...
<!ELEMENT electronic-signature   (basic-signature, enhanced-signature?) >
<!ATTLIST electronic-signature
      DATE-SIGNEDC       DATA    #REQUIRED
      PLACE-SIGNEDC      DATA    #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  >
...
```

A basic electronic signature within an XML document may be supplemented by the addition of a digital signature to the wrapped application documents.

4.1 Facsimile signature
To create this type of signature, the XML file must include the <fax> element and an external entity reference set in the FILE-NAME attribute that points to the file containing the bitmap of the signature, as shown below:

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

This bitmap file must be a 300dpi single strip, Intel encoded TIFF Group 4 image or a JFIF (JPEG) file.

4.2 Text string signature
To create this type of signature, the XML document must include the <text-string> element containing a text string that represents the user's "wet" (ink) signature, enclosed in slash "/" characters, as shown in the example below:

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

The text string must be a string of characters, not including the forward slash "/" character, chosen by the user as his electronic signature, as shown in the following examples:

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

4.3 PKCS#7 digital signature
The PKCS#7 signed data type is generated from the electronic message by the signer, who uses his private signing key to encrypt the message digest. It includes a copy of the digital certificate of the signer when sent.

The use of a PKCS#7 signature must be indicated in the XML file by the <pkcs7> element, as shown below:

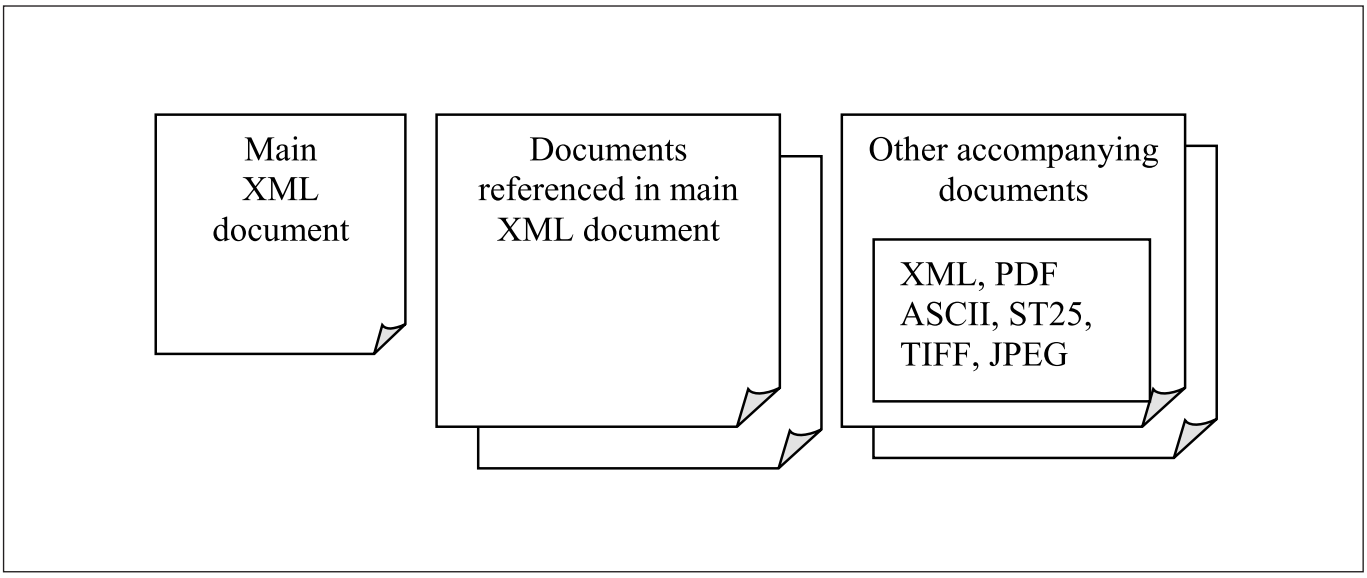
```
...
<electronic-signature DATE-SIGNED="01/01/2000">
      <enhanced-signature>
            <pkcs7 />
      </enhanced-signature>
</electronic-signature>
...
```

5 Data format requirements

The document packaging mechanism is used to combine the data about what is being transmitted with the contents of the transmission to form a single binary object called a wrapped application document (WAD), and then to apply the appropriate digital signatures and encryption.

5.1 Document preparation
For each document filed there is a main XML document that may explicitly reference all documents to be sent in a single package. These referenced documents are logically part of the main document (eg a new patent application). In addition, a filing may include other accompanying documents (eg designation of inventor or fee payment).

The main XML document must conform to one of the DTDs specified below. The referenced documents (external entities) are typically embedded images, tables, drawings or other compound documents and may be encoded as either XML, ST25, PDF, ASCII, TIFF or JFIF(JPEG). The accompanying documents are separate, but related, documents that may be encoded as either XML, ST25, PDF, ASCII or Image. Any accompanying XML documents must also conform to one of the DTDs specified below.



5.1.1 Character-coded formats

5.1.1.1 XML
All XML documents must conform to one of the DTDs specified below. Applicants will be able to create XML documents conforming to this standard by using the EPO's client software for electronic filing.

The coded character set used for all XML documents must be confined within that specified by ISO/IEC 10646:2000 (Unicode 3.0). The standard character-encoding scheme for XML documents is UTF-8.

5.1.1.2 ST.25
A document created using WIPO ST.25 SGML tags for sequence listings may be included in a WAD as an external document.

5.1.1.3 ASCII
A document created as plain ASCII text may be included in a WAD as an external document. In this case, the main XML document must include the code page of the ASCII text.

5.1.2 PDF
PDF documents for use in electronic filing must meet the following requirements:

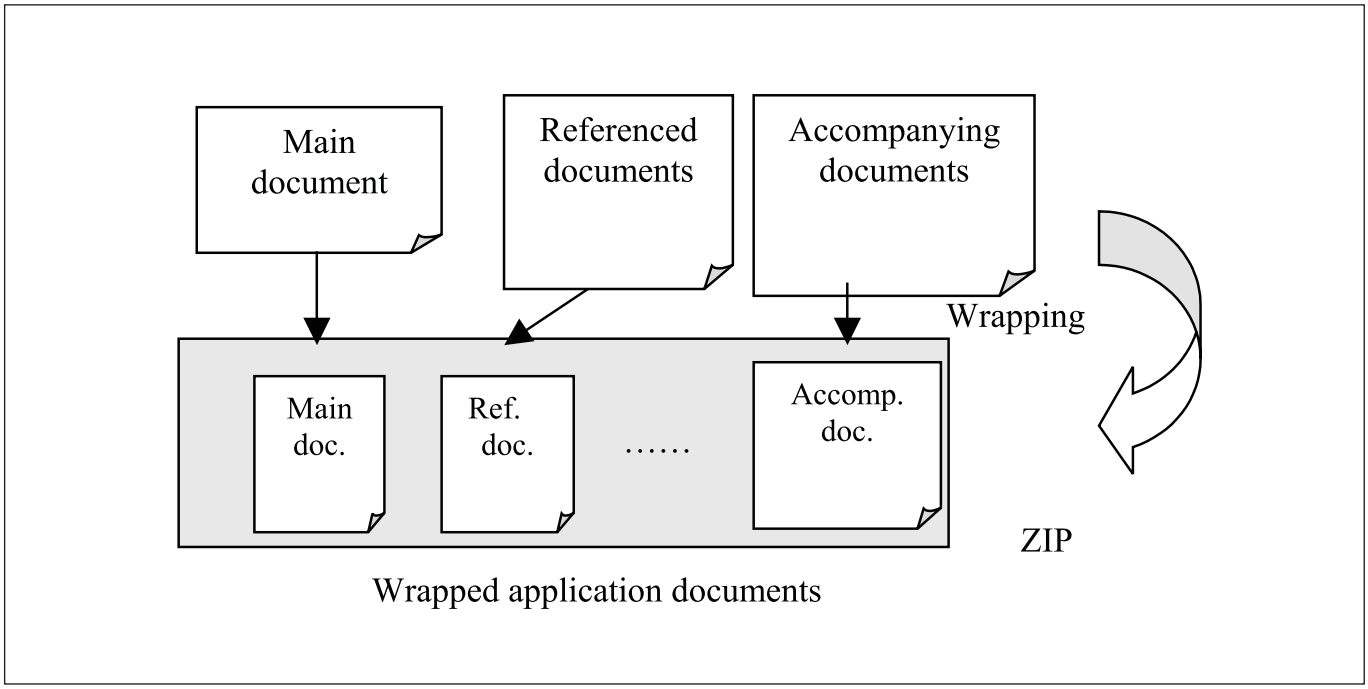
(a) PDF V1.3 compatible
(b) Non-compressed text to facilitate searching
(c) Unencrypted text
(d) No digital signatures
(e) No embedded OLE objects
(f) All fonts must either be embedded, standard PS17 or built from Adobe® Multiple Master (MM) fonts

The PDF format has become the de facto standard for the exchange of formatted documents on the Internet.

5.1.3 Images
Facsimile images used in electronic filing must meet the following requirements:

- Format
  - TIFF V6.0 with Group 4 compression, single strip, Intel encoded or
  - JFIF(JPEG)
- 200, 300 or 400 dpi
- A4 size

5.2 Wrapping documents
The main document and any externally referenced documents and accompanying documents are wrapped and treated as one data block. This data block, called the wrapped application documents (WAD), is created using the ZIP wrapping standard. Applicants must use ZIP format archiving and compression software to package the document files constituting an electronic application.



The software used to create the ZIP file must conform to the ZIP file format specification as published in the PKWARE® PKZIP® Application Note (revised: 8.1.1998).

The files to be zipped must include all parts of the document identified elsewhere in this standard. All external files referenced by the application must be included in the ZIP file submission. File names included in the central directory of the ZIP file must comply with the specification for the applicable operating system.

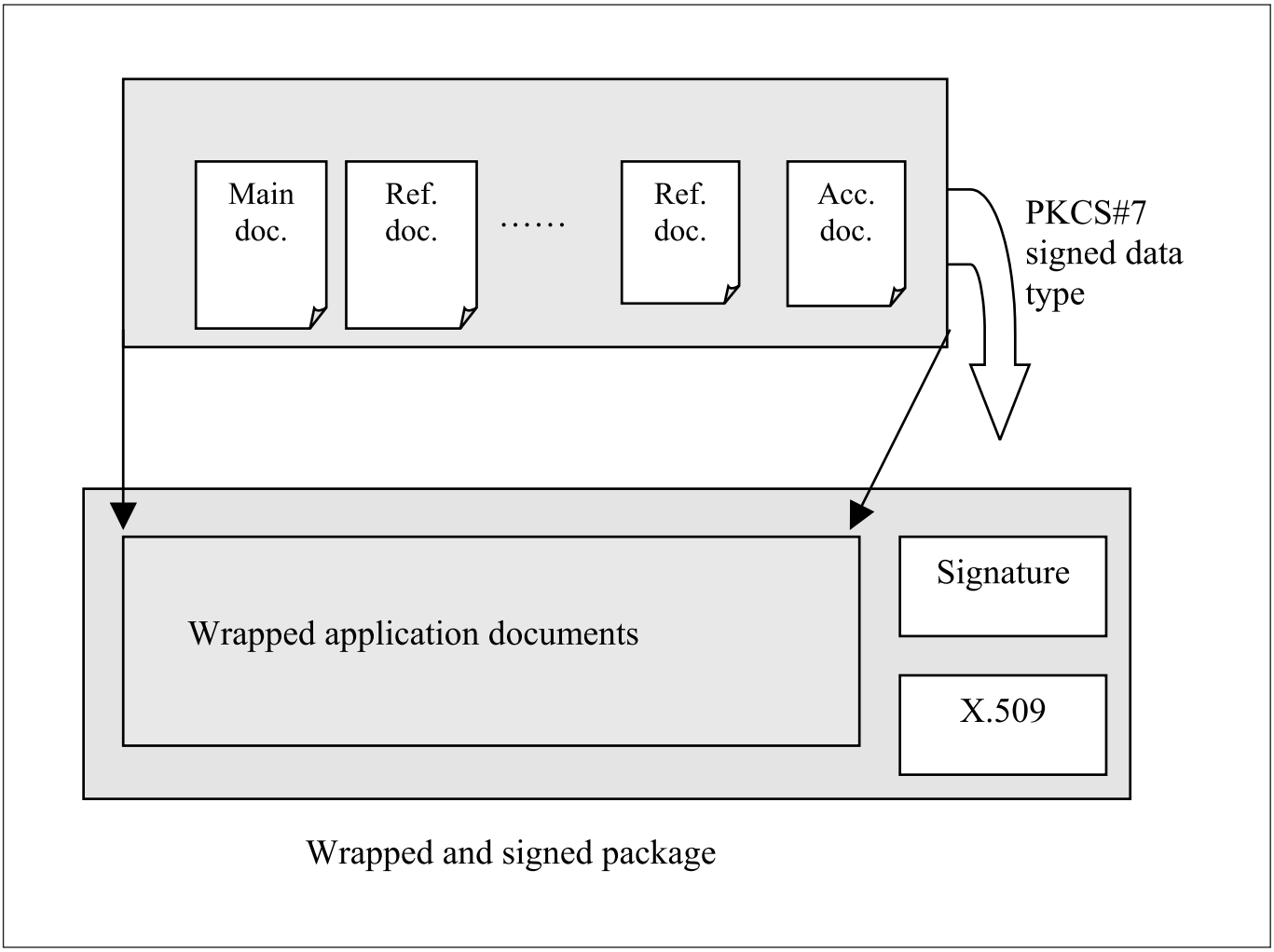
All ZIP files must have a flat directory structure. If a collection of files needs to be embedded in the ZIP file, then these should be included as a single flat embedded ZIP file.

The ZIP standard allows the compression software to select from among a number of compression algorithms. The default compression method must be "Deflation".

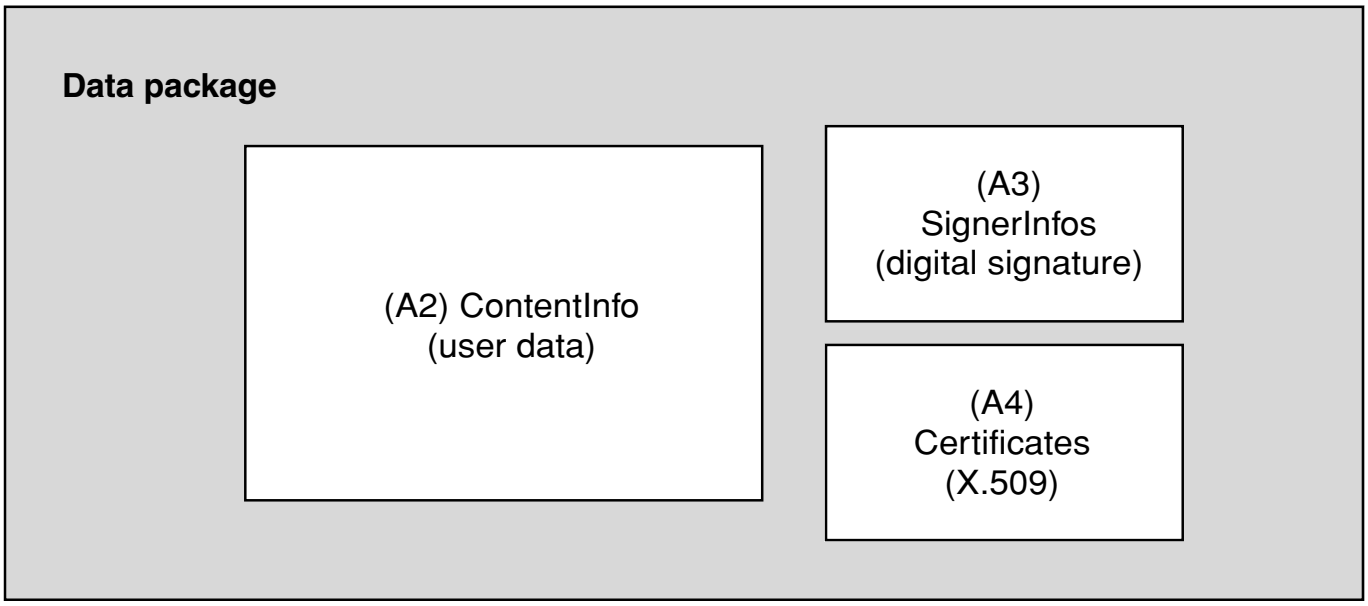
5.3 Signing wrapped application documents

To bind the person creating the package to the electronic wrapped application documents, a digital signature is added to create the wrapped and signed package. The purpose of adding the signature is to identify the person creating the package and to enable the recipient to detect any unauthorised alteration during transmission.

PKCS#7 is used to produce a signed data type for the signature.



(A1) SignedData <top level>
(PKCS#7 digital envelope for signature)



Rules for producing the PKCS#7 digital envelope for certification

Object identifier for sha-1	The object identifier adopted for SHA-1 is defined in OIW interconnection protocols (Part 12) as follows: **Sha-1 OBJECT IDENTIFIER ::= {iso (1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 26}**
Object identifier for RSA encryption	The object identifier for RSA encryption is defined in *RSA Encryption Standard PKCS#1* as follows: **Pkcs-1 OBJECT IDENTIFIER ::= iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1} RsaEncryption OBJECT IDENTIFIER ::={pkcs-1 1}**
Object identifier for triple DES	dES-EDE3-CBC OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) encryptionAlgorithm(3) 7}

Table A1 SignedData – top level

No.	Item name	PKCS#7 item	Content
1	Version	Version	Set integer value '1'
2	Set of algorithm identifiers	DigestAlgorithms	
2.1	Algorithm identifier	AlgorithmIdentifier	Set ONE **set** of algorithm identifiers {sha-1} only
3	Content information	ContentInfo	Set one content information (see table A2)
4	Certificates	Certificates	Set one Certificates (see table A4)
5	Certificate revocation lists	Crls	Not used (set no data)
6	Signer information	SignerInfos	Set one SignerInfos (see table A3)

Table A2 ContentInfo – top level

No.	Item name	PKCS#7 item	Content
1	Content type	ContentType	Set object identifier {pkcs-7 1}
2	Content	Content	Set user data (binary)

Table A3 SignerInfos – top level

No.	Item name	PKCS#7 item	Content
1	Version	Version	Set integer value '1'
2	Issuer and serial number	IssuerAndSerialNumber	Issuer of certificate and certificate serial number in acc. with X.509 (signer's certificate)
3	Set of digest algorithms	DigestAlgorithm	
3.1	Algorithm identifier	AlgorithmIdentifier	Set ONE **set** of algorithm identifiers {sha-1} only to make digest of digital signature
4	Authenticated attributes	AuthenticatedAttributes	Not used (set no data)
5	Digest encryption algorithm	DigestEncryptionAlgorithm	Algorithm OBJECT identifier of digest encryption (recommended algorithm: rsaEncryption)
6	Encrypted digest	EncryptedDigest	Digest data encrypted using signer's private key
7	Unauthenticated attributes	UnauthenticatedAttributes	Not used (set no data)

Table A4 Certificates – top level

No.	Item name	PKCS#7 item	Content
1	Set of certificates	ExtendedCertificatesAnd Certificates	
1.1	X.509 certificate	Certificate (defined in X.509)	Set ONE **set** of X.509 certificate data only

6 Submission

6.1 Transmission package

The EPO may decide not to use the enveloping mechanism described in this section as the encryption mechanism for transmission where channel level encryption such as SSL or physical media such as CD-R are used.

The actual transmission data exchanged between the applicant and the EPO is called a package.

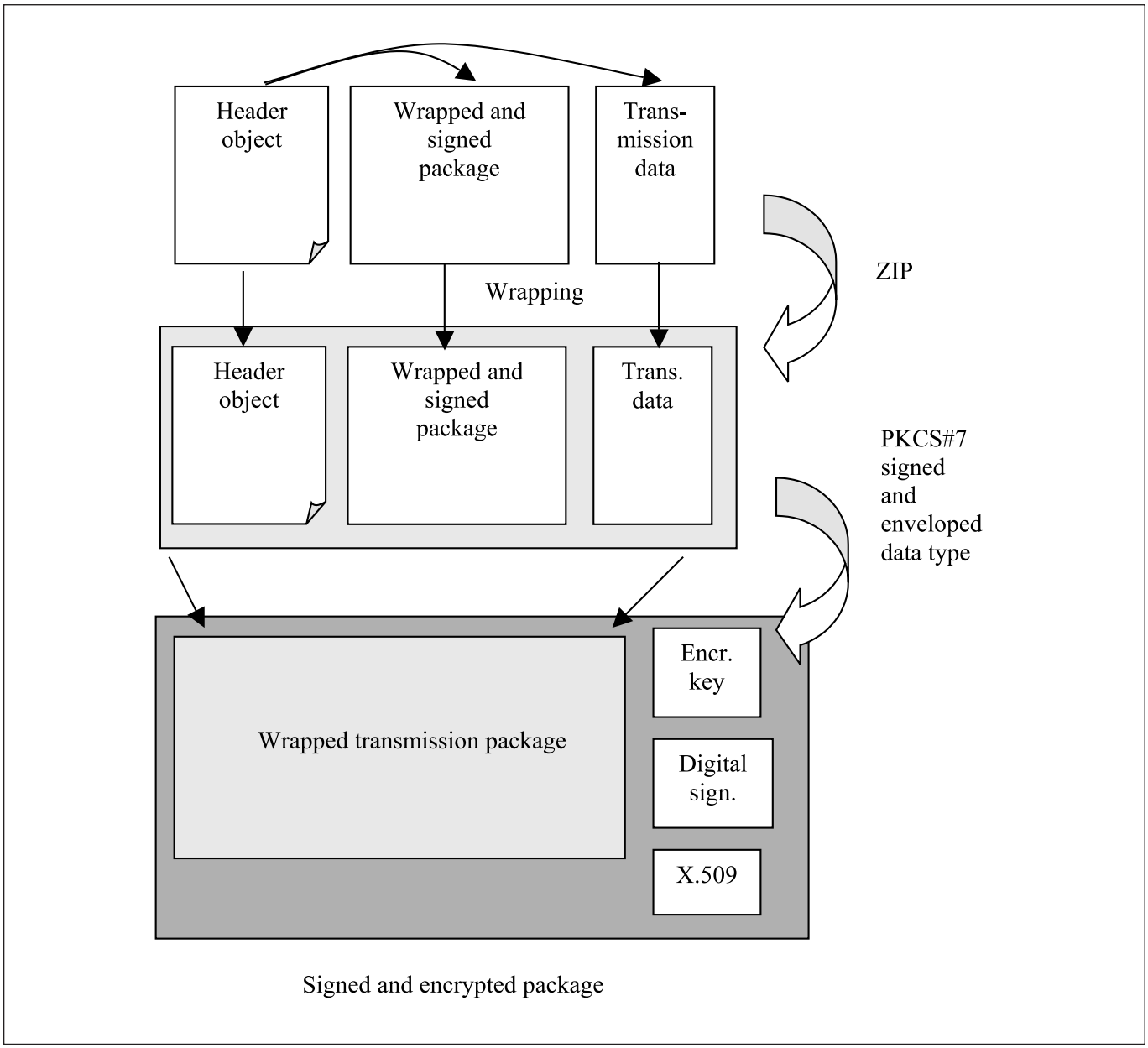
A package contains various data items depending on the type of package. These include:
1. Header object data item
2. Wrapped and signed package made by wrapping and signing the application documents
3. Transmission data such as time of transmission.

The header object data item indicates the package type, file name of data item, etc. It is always found in the signed and encrypted package, and is written in XML.

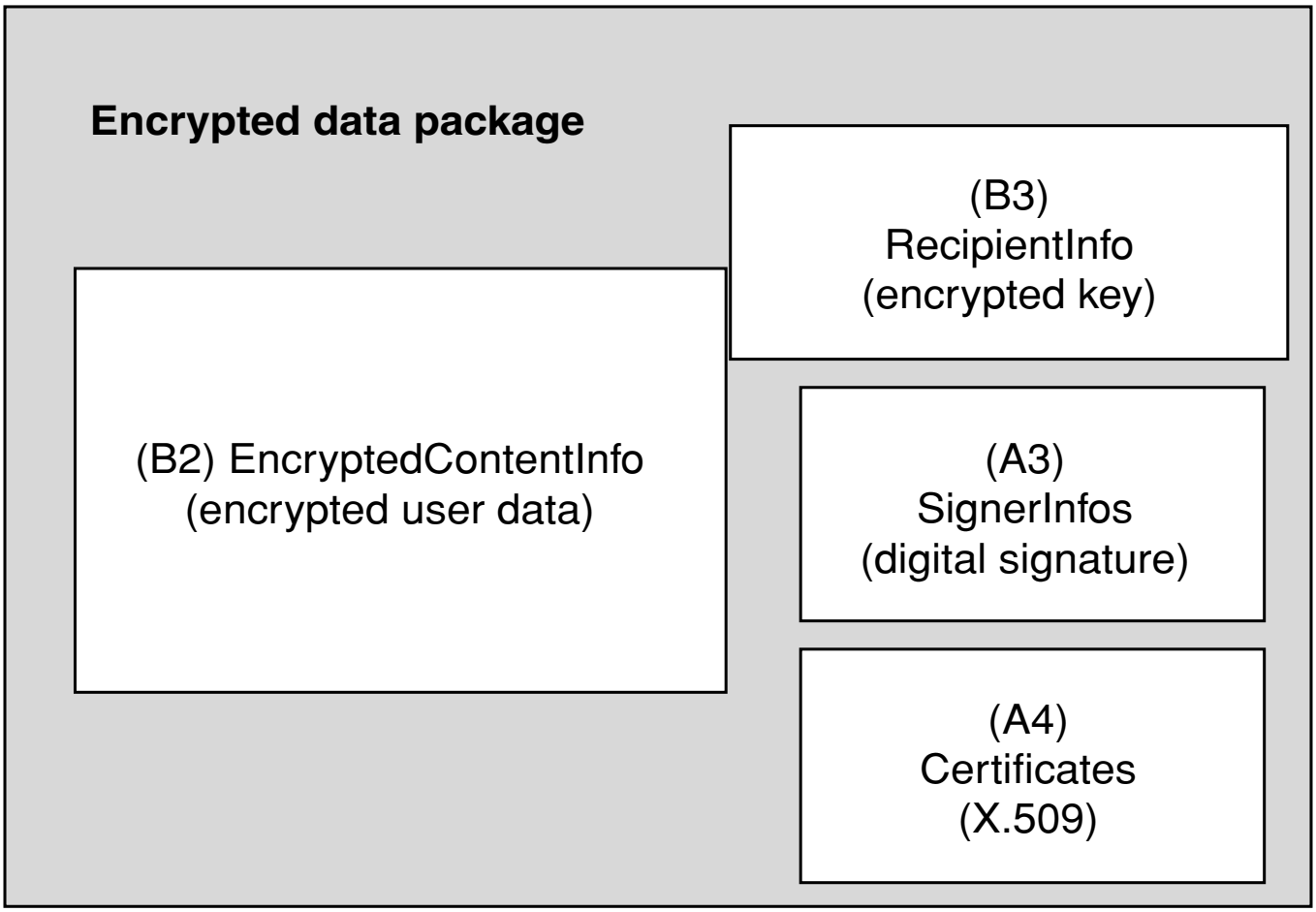
The procedure for creating signed and encrypted packages is as follows:
(a) Create a wrapped transmission package by wrapping the wrapped and signed package with the data items used for transmission using ZIP
(b) Create a signed and encrypted package for network transmission by encrypting using the PKCS#7 signed and enveloped data type.

The purpose of the signature is to ensure the combination and contents of the individual data items, and to enable the recipient to detect any unauthorised alterations during transmission. Encryption is to prevent the unauthorised interception of data during communication.

The digital signature for the wrapped and signed package may be produced by either the applicant or his representative. The person that starts the transmission produces the digital signature for the final signed and encrypted package.



(B1) SignedAndEnveloped Data <top level>
(PKCS#7 digital envelope for transmission)



Rules for producing the PKCS#7 digital envelope for transmission

Table B1 SignedAndEnvelopedData – top level

No.	Item name	PKCS#7 item	Content
1	Version	Version	Set integer value '1'
2	Recipient information	RecipientInfos	Set ONE **set** of RecipientInfo only (see table B3)
2	Set of algorithm identifiers	DigestAlgorithms	
2.1	Algorithm identifier	AlgorithmIdentifier	Set ONE **set** of algorithm identifiers {sha-1} only
3	Encrypted Content information	EncryptedContentInfo	Set one EncryptedContentInfo (see table B2)
4	Certificates	Certificates	Set one Certificates (see table A4)
5	Certificate revocation lists	Crls	Not used (set no data)
6	Signer information	SignerInfos	Set one SignerInfos (see table A3)

Table B2 EncryptedContentInfo – top level

No.	Item name	PKCS#7 item	Content
1	Content type	ContentType	Set object identifier {pkcs-7 1}
2	Content encryption algorithm	ContentEncryptionAlgorithm	Algorithm OBJECT identifier of content encryption (recommended algorithm: dES-EDE3-CBC)
3	Encrypted content	EncryptedContent	Encrypted user data

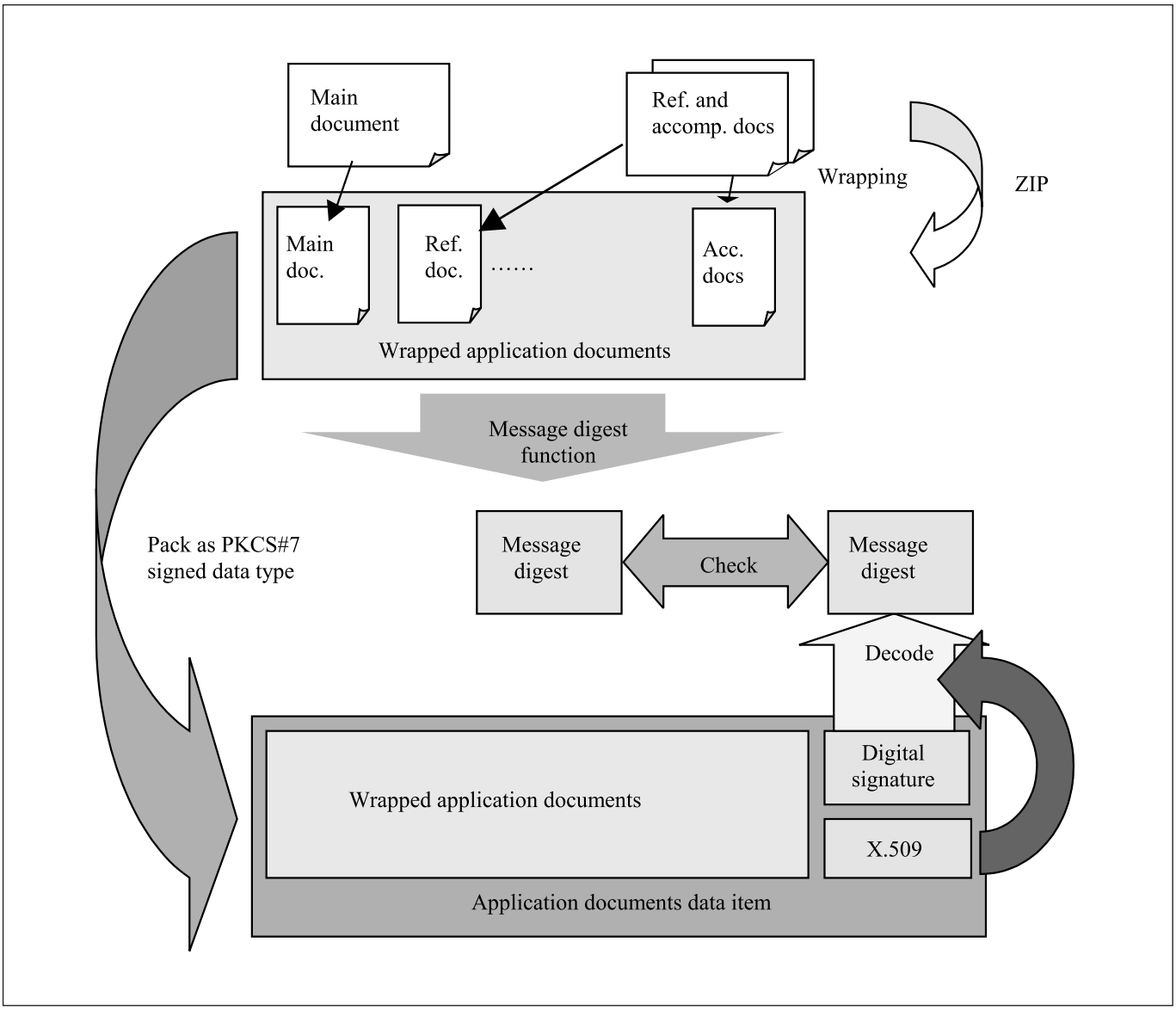
Table B3 RecipientInfo – top level

No.	Item name	PKCS#7 item	Content
1	Version	Version	Set integer value '1'
2	Issuer and serial number	IssuerAndSerialNumber	Issuer and serial number of certificate including public key for encrypting user data encryption key
3	Key encryption algorithm	KeyEncryptionAlgorithm	Algorithm OBJECT identifier for encrypting user data encryption key (recommended algorithm: rsaEncryption)
4	Encrypted key	EncryptedKey	Encrypted decryption key for user data

6.2 Transmission mechanism

The transmission mechanism operates as follows:

- An electronic session is established between the applicant and the EPO.
- The applicant transmits the signed and encrypted package.
- When the signed and encrypted package is received, its contents are checked for the presence of viruses and the wrapped application documents object is processed to create its unique message digest.
- This digest is compared with the message digest included in the wrapped and signed package. If they match, an acknowledgement of receipt is sent to the applicant. If they do not, the applicant is informed accordingly. The session is then ended.



6.2.1 Checking the message digest

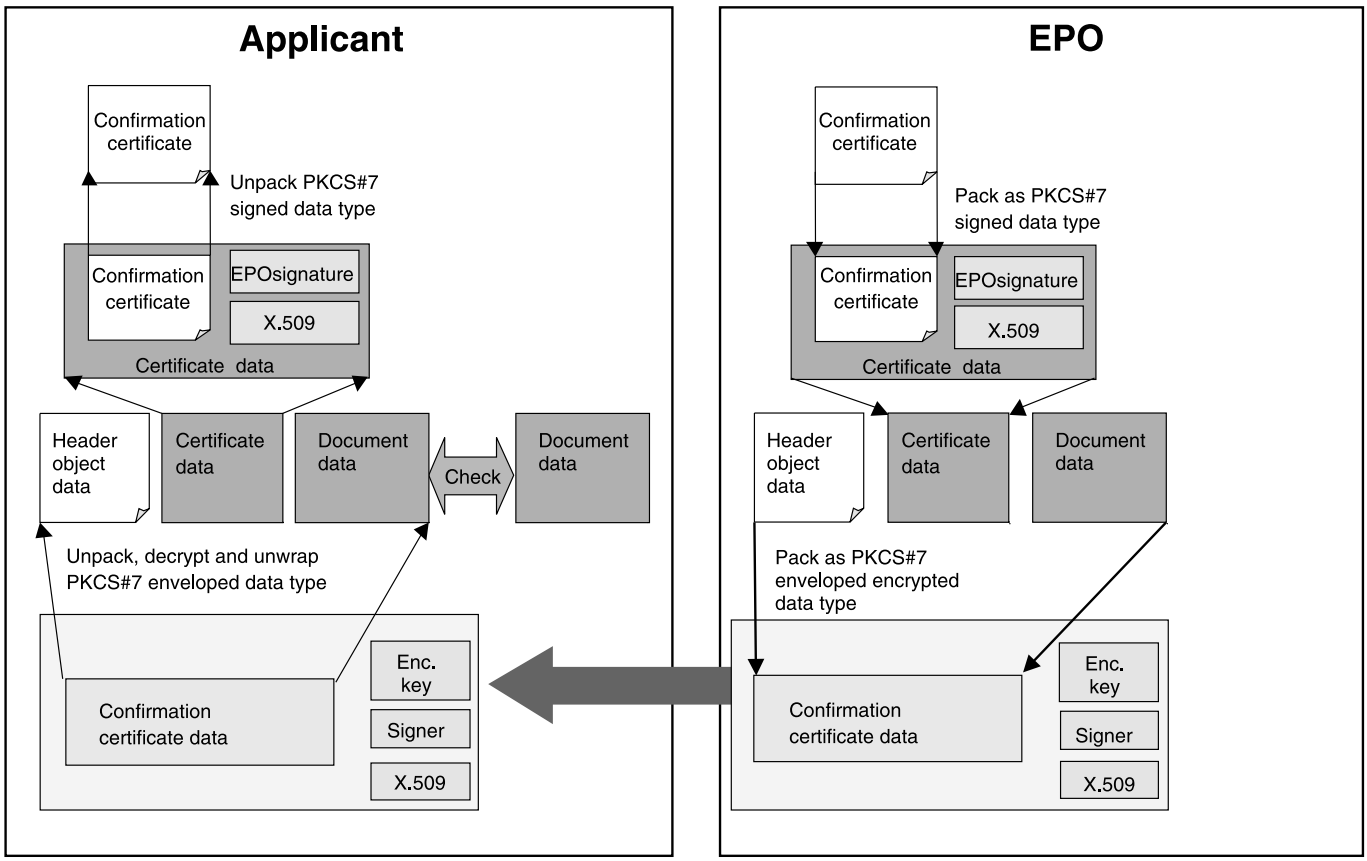
When the EPO receives the wrapped application documents, it opens the data items in them and ascertains the role of each one according to the information in the header object.

6.2.2 Confirmation certificate

The confirmation certificate data item includes a certificate data item, a header object data item indicating that the corresponding packet is a confirmation certificate, and, optionally, the application documents data item received with the new application.

In the event of a communications or message digest comparison problem, the confirmation certificate contains information about the problem.

The confirmation certificate is packaged as a signed and encrypted package, as described above.



The confirmation certificate is used to inform the applicant of the receipt of the application and must contain an XML version of this information. It may also contain a formatted version of the data in PDF. These files are combined in a single ZIP file and signed using the EPO's digital certificate.

6.3 Transmission protocol

The EPO uses a transfer protocol based on HTTP in conjunction with SSL.

7 Physical media

The EPO also accepts electronic filing on CD-R. Each CD-R should contain one application only, in the form of a signed WAD written into the root directory. The name of the signed WAD file should be "WAD.ZIP". The accompanying paper form should include details of the application or document and should refer to the "WAD.ZIP" file on the CD-R. The CD-R volume name should be based on the applicant's reference number.

Annex – Diagrams illustrating the standard

The following diagrams and text provide additional (simplified) information about the standard.

Simplified anatomy of a signed and encrypted package

Figure 1 illustrates, for non-technical readers, the components of the signed and encrypted package mechanism specified in this standard. The diagram has been intentionally simplified to obscure technical detail that may distract the reader from the key issues of the package design. For example, the ZIP wrapping has been left out, and encoding standards for objects are not addressed.

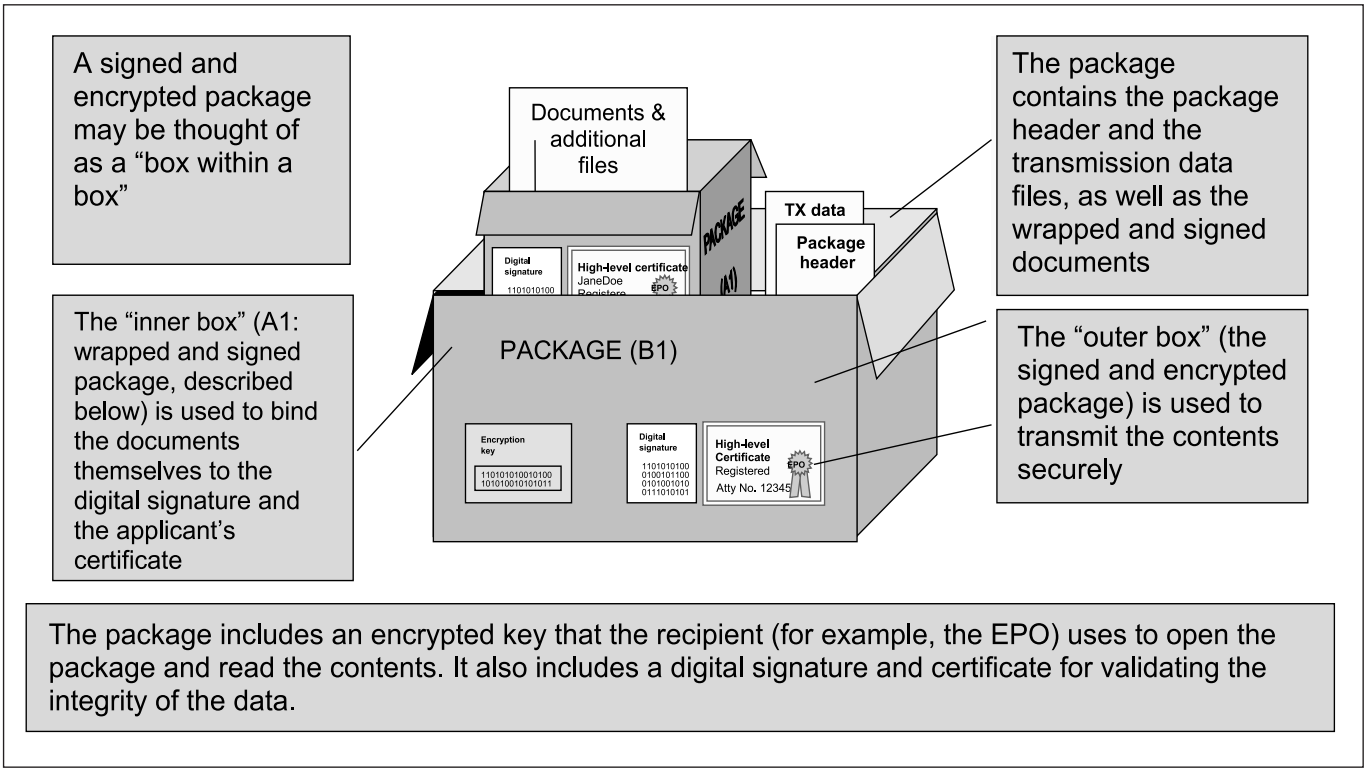


Figure 1: Signed and encrypted package

Simplified anatomy of a wrapped and signed package

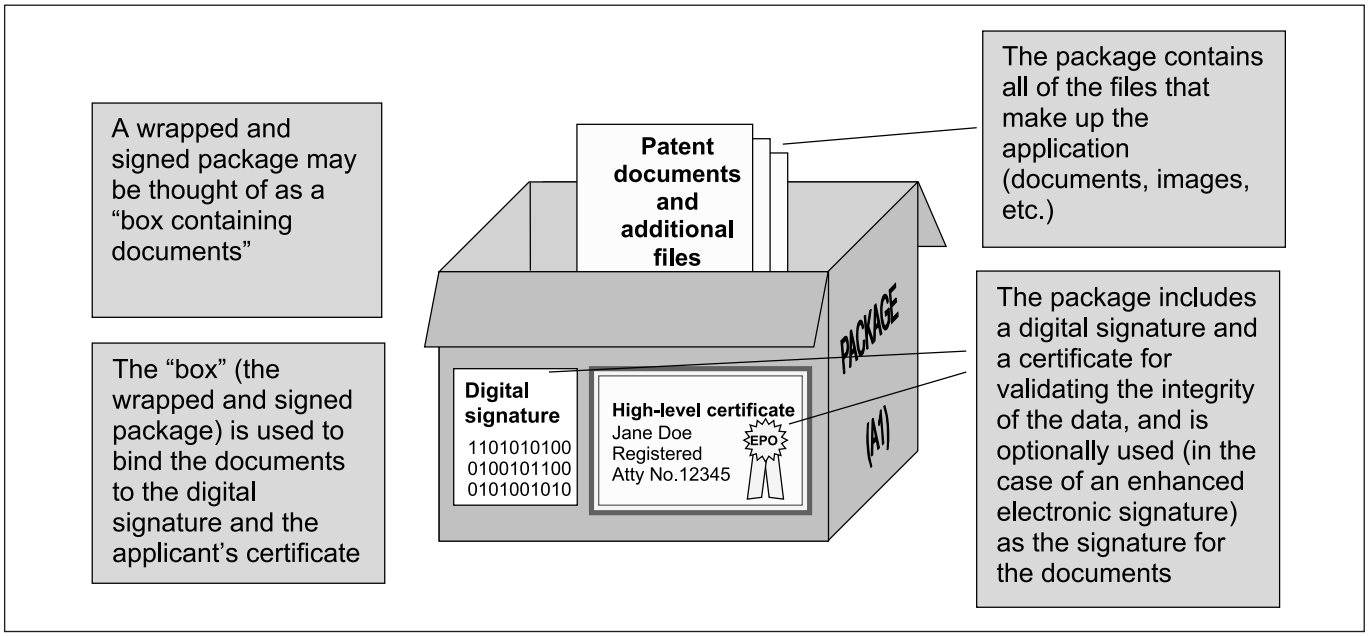


Figure 2: Wrapped and signed package

Anatomy of the wrapped application documents object

The wrapped application documents object in section 5 defines how documents are "wrapped" together. In the case of offline submission on physical media, the further steps of creating the wrapped and signed package and the signed and encrypted package are optional. A wrapped application documents object consists of files that have been 'zipped' together into a single file and placed in the root directory of the physical media.

Certificate/signature types

The diagrams in Figures 3 to 7 illustrate the differences between the types of "digital certificate" and "electronic signature" options as specified in the standard. Each diagram shows a "box" representing the wrapped and signed package.

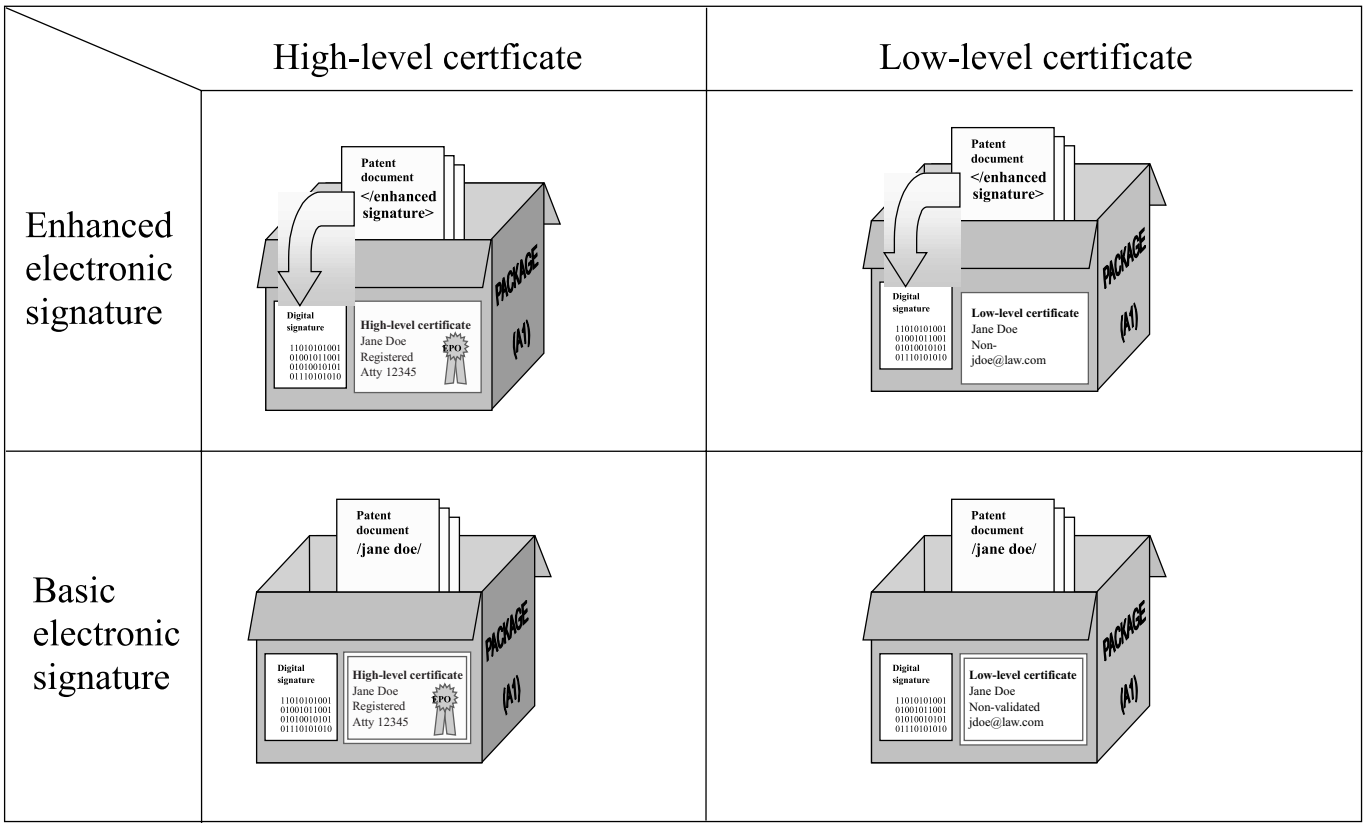


Figure 3: Certificate/signature types

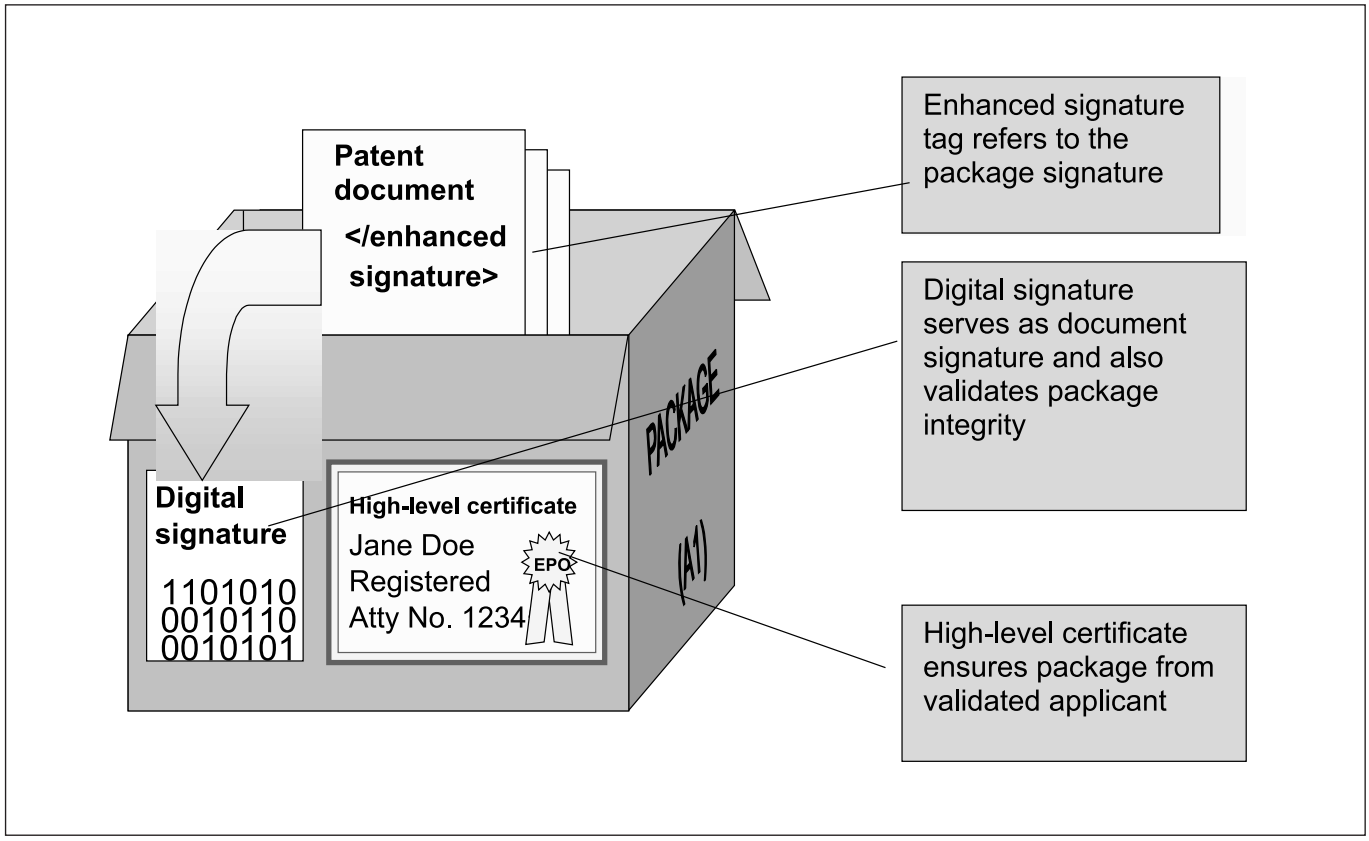


Figure 4: Enhanced electronic signature/high-level certificate

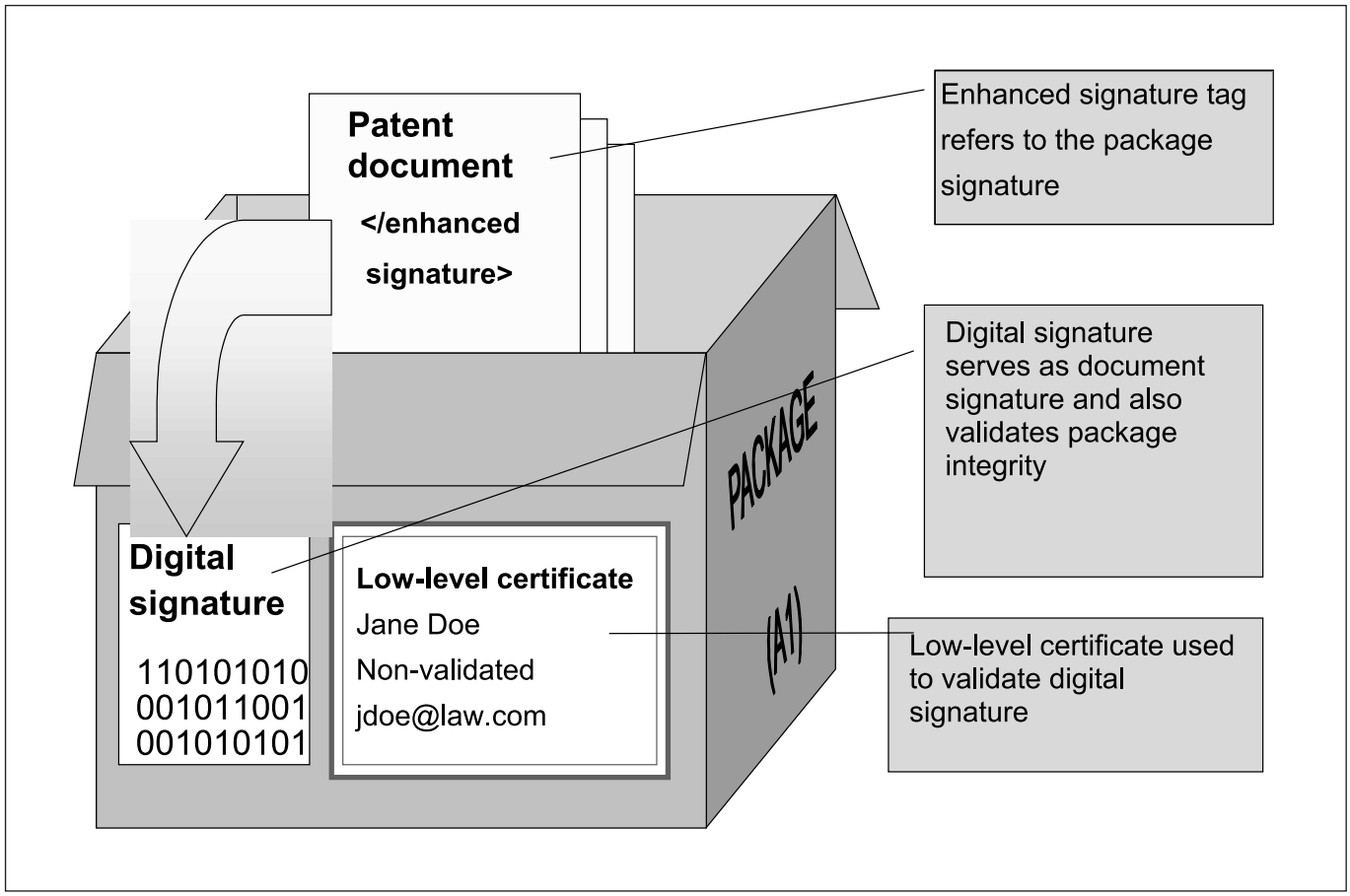


Figure 5: Enhanced electronic signature/low-level certificate

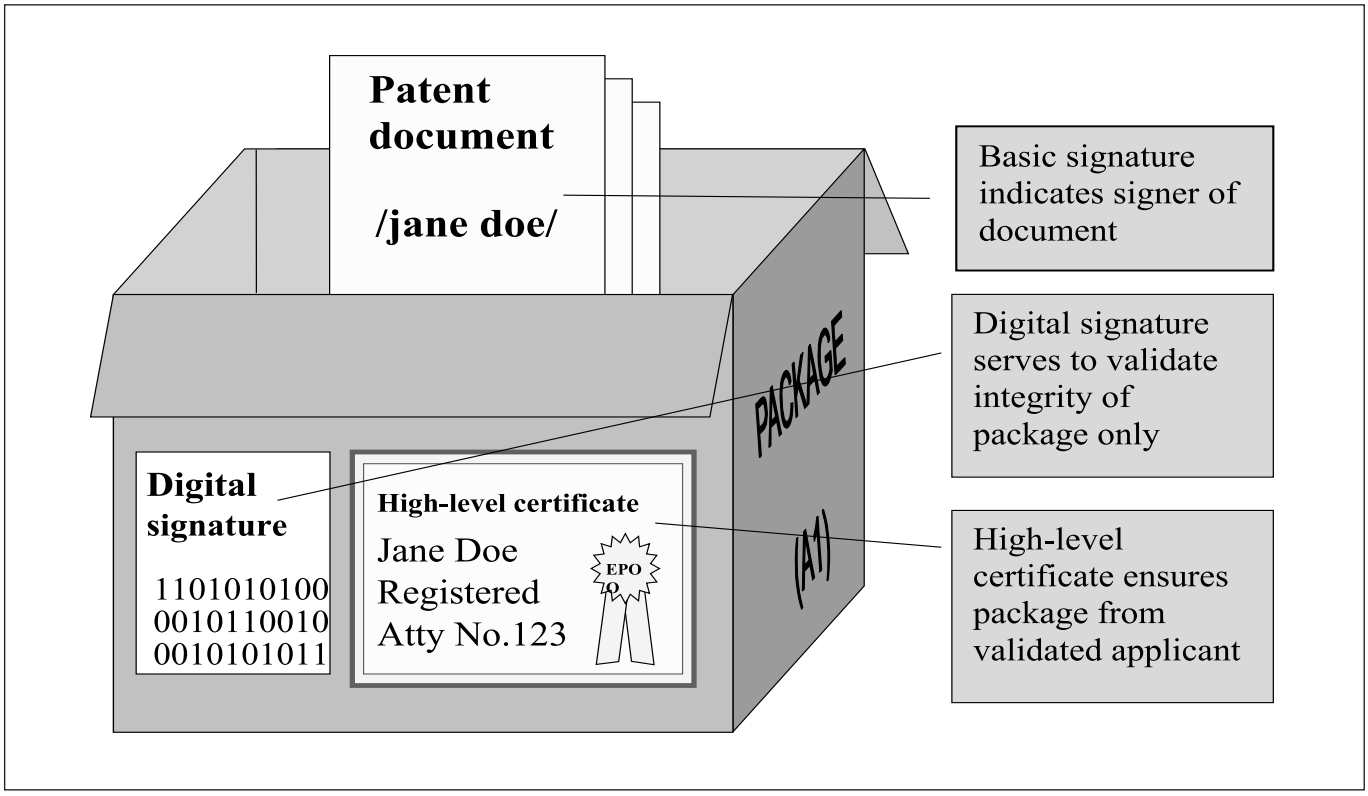


Figure 6: Basic electronic signature/high-level certificate

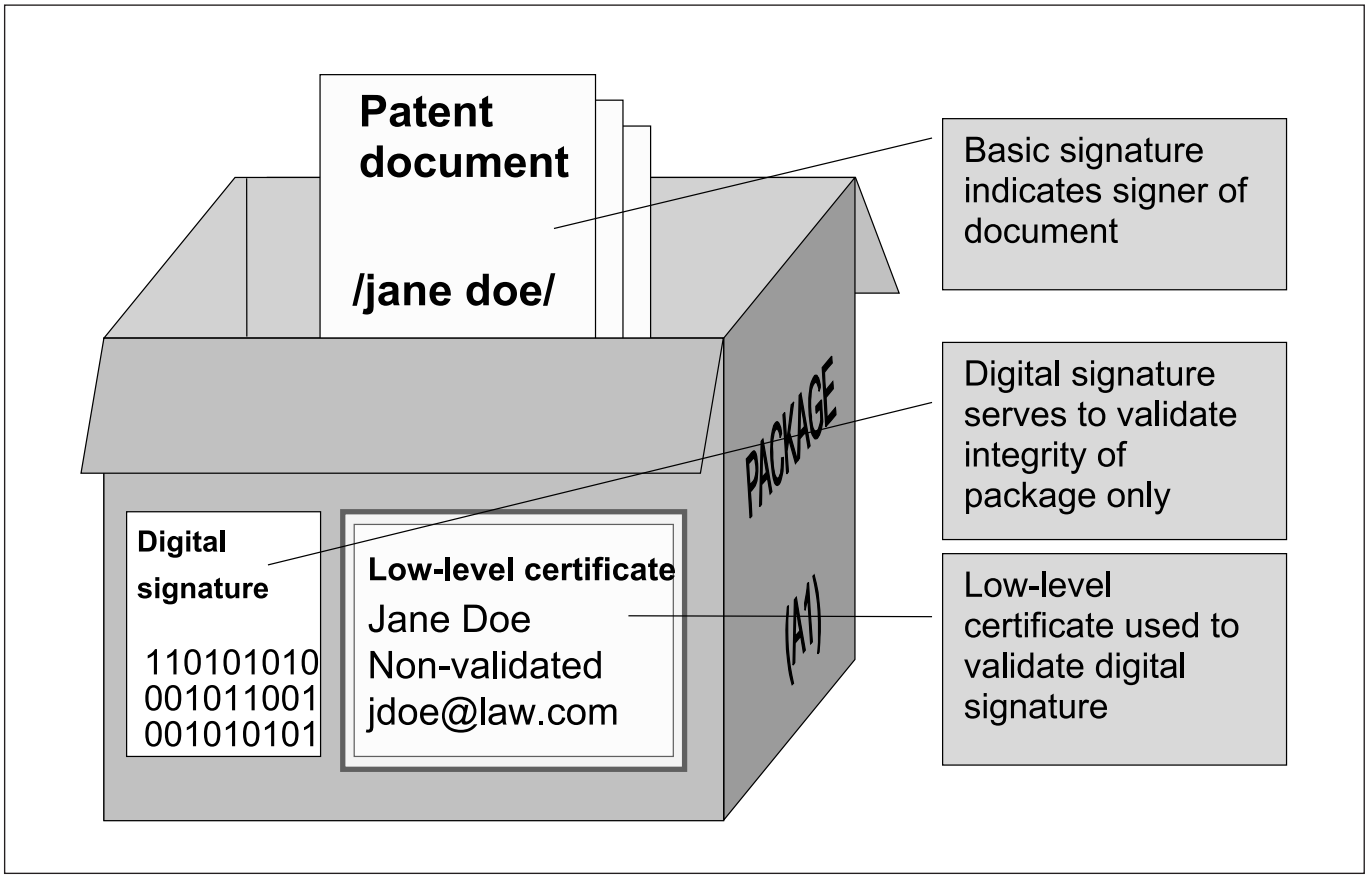


Figure 7: Basic electronic signature/low-level certificate

Transmission mechanism/packaging combinations

Figure 8 shows the various transmission mechanism/packaging combinations that are permissible. The following applies to each transmission mechanism:
(a) Online/internet: a signed and encrypted package must be used.
(b) Online/secure (channel encryption such as a private network): a signed and encrypted package or wrapped and signed package must be used.
(c) Offline/physical media: either a signed and encrypted package, a wrapped and signed package, or a wrapped application documents package may be used.

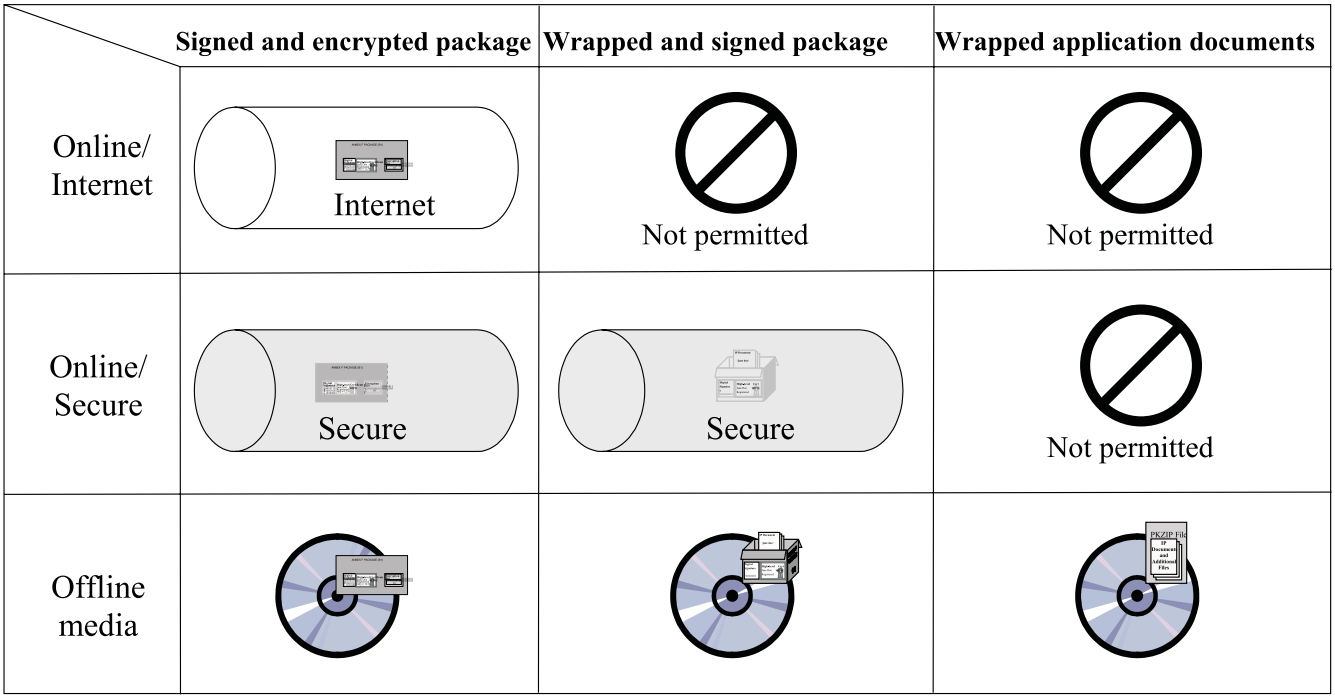


Figure 8: Transmission protocols and packages permitted