E

WIPO

PCT/AI/1 Add.4 Prov.
ORIGINAL: English
DATE: June 9, 2000

WORLD INTELLECTUAL PROPERTY ORGANIZATION
GENEVA

PATENT COOPERATION TREATY (PCT)

ADMINISTRATIVE INSTRUCTIONS UNDER THE PATENT COOPERATION TREATY:

PROPOSED MODIFICATIONS RELATING TO THE ELECTRONIC FILING, PROCESSING, STORAGE AND RECORDS MANAGEMENT OF INTERNATIONAL APPLICATIONS

(ANNEX F, APPENDIX I: TECHNICAL STANDARD FOR THE ON-LINE EXCHANGE OF INDUSTRIAL PROPERTY DOCUMENTS IN A PKI ENVIRONMENT)

prepared by the International Bureau for consideration at a PCT informal consultation meeting on electronic filing, Geneva, July 11 to 14, 2000

INTRODUCTION

1. At its twenty-eighth (16th extraordinary) session, held in Geneva in March 2000, the PCT Union Assembly considered the implementation of electronic filing and processing of international applications. The Assembly's discussions were based on document PCT/A/28/3, which included proposed modifications of the Administrative Instructions under the PCT,[1] and the comments of delegations and user representatives on that document which were reproduced in documents PCT/A/28/3 Add.2 to Add.5. The discussions also took into account the documents reproduced in document PCT/A/28/3 Add.1 relating to the development of the necessary technical standard to enable implementation of electronic filing and processing of international applications. The Assembly agreed that proposed new Part 7 of the Administrative Instructions under the PCT (Instructions Relating to Electronic Filing, Processing, Storage and Records Management of International Applications) and draft Annex F of the Administrative Instructions (Standard for Electronic Filing, Processing, Storage and Records Management of International Applications) needed extensive redrafting, and that further consultations on the redrafted versions were necessary (see the Assembly's report, document PCT/A/28/5, paragraph 24).[2]

2. This and related documents[3] contain a redraft of the necessary implementing provisions of the Administrative instructions for the purposes of continuing the consultation under Rule 89.2(b) which was begun in conjunction with the twenty-eighth session of the Assembly. The documents are as follows:

PCT/AI/1 Add.2 Prov., containing redrafted Part 7;

PCT/AI/1 Add.3 Prov., containing redrafted Annex F, Introduction;

[1] References in this document to "Articles," "Rules" and "Sections" are, respectively, to those of the Patent Cooperation Treaty (PCT), of the Regulations under the PCT ("the Regulations") and of the Administrative Instructions under the PCT ("the Administrative Instructions"), or to such provisions as proposed to be amended or added, as the case may be. The current texts are available on WIPO's Internet site at http://www.wipo.int/eng/pct/texts/index.htm. References to "national law," "national applications," "national Offices," etc., include reference to regional law, regional applications, regional Offices, etc.

[2] The report and other documents for the Assembly's session are available on WIPO's Internet site at http://www.wipo.int/eng/document/govbody/wo_pct/index_28.htm.

[3] This and other documents for consideration by the PCT informal consultation meeting on electronic filing are available on WIPO's Internet site at http://www.wipo.int/eng/meetings/2000/pct_ef/index.htm.

PCT/AI/1 Add.4 Prov., containing redrafted Annex F, Appendix I (Technical Standard for the On-Line Exchange of Industrial Property Documents in a PKI Environment);

PCT/AI/1 Add.5 Prov., containing redrafted Annex F, Appendix II (XML DTDs for Industrial Property Document Exchange);

PCT/AI/1 Add.6 Prov., containing redrafted Annex F, Appendix III (Electronic Filing Using Physical Media).

[Annex F, Appendix I, follows]

PROPOSED MODIFICATIONS OF THE
ADMINISTRATIVE INSTRUCTIONS UNDER THE PCT

ANNEX F
STANDARD FOR ELECTRONIC FILING, PROCESSING, STORAGE AND RECORDS MANAGEMENT OF INTERNATIONAL APPLICATIONS

Appendix I
Technical Standard for the On-line Exchange of Industrial Property Documents in a PKI Environment

Table of Contents

1 Background

This document presents the technical requirements for the on-line exchange of industrial property documents in a PKI environment including on-line filing.

This standard sets out mandatory requirements for all applicants and offices participating in such exchanges as well as optional requirements. All optional elements are indicated in *italics*.

2 Scope

This technical standard covers the 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 the present version of the standard, the packaging and transmission are performed using PKI technology. When feasible alternative security technologies become available, they may be incorporated in updates to the standard. The technical specification of this standard therefore currently requires the use of PKI.

The implementation of PKI shall comply with the recommendations established by the Internet Engineering Task Force (IETF) Working Group on PKI Interoperability (PKIX) and documented in IETF RFC 2459.

The implementation of PKI shall use separate key pairs and digital certificates for the purpose of authentication and confidentiality. *Optional: An industrial property Office or recognized Certification Authority may decide to offer Key Recovery for the confidentiality key pair when allowed (or required) under national laws.*

3.2 Certificates

The standard foresees two classes of digital certificates:

Recognized Certificate: The applicant is already in possession of a digital certificate issued by a trusted third party that identifies him. This certificate is then used both for creating the packages as well as for the transfer of the data.

Ad-hoc Certificate: The applicant is not in possession of such a recognized certificate, in which case the technical transfer of data is done using an “ad-hoc” digital certificate issued to the user (e.g. as part of the registration of the on-line filing client or obtained from an unrecognized Certification Authority). In obtaining this certificate the applicant must provide his name and e-mail address.

In both cases, the digital certificate shall comply with the International Telecommunication Union (ITU) X.509 Version 3 Recommendation for certificate format.

Optional: Certificates may be stored either on a Smart Card or on a diskette or hard drive

3.3 Certification Authorities

Each receiving Office shall specify Certification Authorities acceptable to that receiving Office. This list of "recognized" Certification Authorities will be published by the International Bureau including a link to the published PKI policy statement of those Certification Authorities.

Meanwhile, the member states will work with the International Bureau to establish a coordinated set of guidelines by which these PKI policy statements can be assessed. In the longer term, it is intended that these guidelines will be used to arrive at a list of Certification Authorities acceptable to all receiving Offices. The International Bureau would then publish this list.

A recognized Certification Authority is responsible for maintaining the accuracy of the electronic certificates that "prove" a party is who he says he is. The Certification Authority must store certificate information for all certificates it issues in a directory structure complying with ITU Recommendation X.500. Such systems shall provide an external interface for publishing and retrieving user digital certificates that complies with the Lightweight Directory Access Protocol (LDAP) using IETF Network Working Group RFC 1777 dated March 1995. In addition, the Certification Authority must publish a Certificate Revocation List using X.509 Version 2.

Each industrial property Office shall subscribe to the Certificate Revocation List for all Certification Authorities that it accepts. Whenever a certificate is used to authenticate an individual, these Certificate Revocation Lists shall be consulted by the industrial property Office to ensure that the certificate has not been revoked.

3.4 Digital Signatures

Digital signatures used to sign electronic documents for industrial property Document Exchange shall conform to the format and practice specified in RSA Laboratories, PKCS#7 – Cryptographic Message Syntax Standard Version 1.5 definition of 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 shall be encoded using DER rules.

3.5 Encryption Algorithms

Both symmetric (secret key) and asymmetric (public key) algorithms may be used as necessary. Algorithms that are prohibited under national law of a country shall not be used for industrial property Document Exchange from that country. Algorithms implemented in hardware or software shall not be used in any manner that is contrary to export restrictions of the country of origin for the hardware or software. Any algorithm used between industrial property Offices must be disclosed to both parties.

Optional: For asymmetric encryption algorithm, rsaEncryption is recommended. As a symmetric encryption algorithm, dES-EDE3-CBC is recommended. The same asymmetric encryption algorithm should be used for digital certificates, digital signatures and envelopes.

3.6 Data Encryption

Electronic document data that is encrypted to ensure confidentiality for industrial property Document Exchange shall conform to the format and practice specified in RSA Laboratories, PKCS#7 – Cryptographic Message Syntax Standard Version 1.5 definition of Signed and Enveloped-data content type.

3.7 Message Digest Algorithms

The message stream shall be input to the strong one-way message digest algorithm SHA-1 to create a message digest.

4 Signatures Mechanisms

For industrial property Document Exchange a number of signature types have been defined as possible. Each receiving Office and designated Office can choose from the following list the types it will accept:

- (a) Basic Electronic Signatures
    - (i) Facsimile image of the users signature
    - (ii) Text String
    - (iii) Click Wrap
- (b) Enhanced Electronic Signature
    - (i) PKCS#7 Signature

The Basic Electronic Signature is encoded within the “party” structure of the XML document shown below:

```
…
<!ELEMENT electronic-signature
              (date-signed,
              place-signed,
              signature-type,
              (signature-file, signature-mark)) >
…
```

A Basic Electronic Signature within the XML document may be supplemented by the addition of a Digital Signature to the Wrapped Documents.

4.1 Facsimile Signature

To create this type of signature, the user must include signature-type=”facsimile” and an external entity reference (e.g. signature-file=“signature.tif”) in the XML document that points to the file containing the bitmap of the signature. This bitmap file must be a 300dpi single strip, Intel Encoded TIFF Group 4 Image.

4.2 Text String Signature

To create this type of signature, the user must include signature-type=”mark” and a text string in the XML document in the format:

signature-mark=”/text-string/”

where text-string is a string of UTF-8 encoded characters, not including the forward slash “/” character, chosen by the user as their electronic signature. Valid examples include:

signature-mark=”/John Smith/”
signature-mark=”/Tobeornottobe/”
signature-mark=”/1345728625235/”
signature-mark=”/Günter François/”

4.3 Click Wrap Signature

To create this type of signature, the user must click on a button in the User Interface marked “I accept”. This is encoded in the XML document as signature-type=”click-wrap”, signature-mark= “click-wrap-signature-accepted”.

4.4 PKCS#7 Signature

This is a PKCS#7 Signed Data Type generated from the electronic message by the act of the signer invoking the use of their private authentication key to encrypt the message digest. The PKCS#7 Signed Data Type includes a copy of the Digital Certificate of the signer issued by a recognized Certification Authority.

The use of a PKCS#7 signature must be indicated in the XML file by the use of the signature-type=”PKCS#7” and signature-mark=”use-digital-signature”.

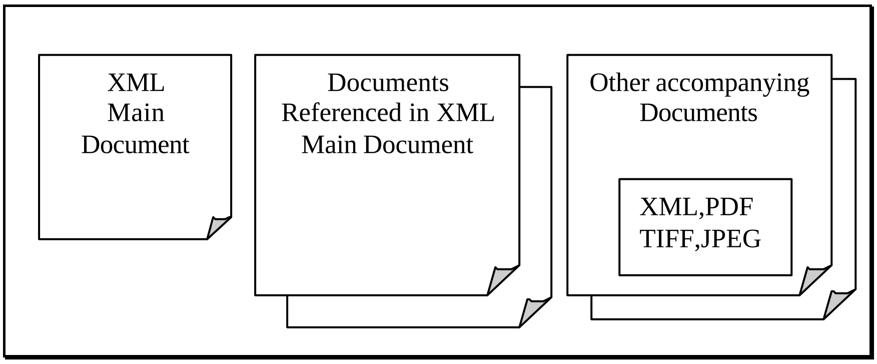
5 Data Format Requirements

The document packaging mechanism is used to combine into a single binary object both the data about what is being transmitted with the contents of the transmission and to then apply the appropriate digital signatures and encryption.

5.1 Document Preparation

For each industrial property Document Exchange there is an XML Main Document that may explicitly reference and be hyper-linked to other documents. These referenced documents are logically part of the Main Document (e.g. a New Patent Application). In addition, a document exchange may include other accompanying documents (e.g. Designation of Inventor or a Fee Payment).

The XML Main Document must conform to one of the DTDs specified in Appendix II. The Referenced Documents (external entities) are typically embedded images, tables, drawings or other compound documents and may be encoded as either XML, PDF, TIFF and JFIF(JPEG). The accompanying documents are separate, but related documents that may be encoded as either XML, PDF or Image.



The Trilateral Offices and WIPO are committed to the principle of establishing an open standards environment for electronic exchange of Intellectual Property documents. A notable result of this is: the standard for submitting electronic documents emphasize the use of open standards and will not promote proprietary vendor formats for electronic documents. The reasons for this policy include avoiding the need to maintain the record copies of electronic filings in specific versions of proprietary formats over which the offices have no control.

One desirable feature of commonly used proprietary word processor systems is that they package their electronic documents as a single file such as a .doc or .wps. The proprietary .doc, .wps and other word processor formats combine text, processing instructions, page layout information, raster graphics, vector drawings, tables and other types of data in a single proprietary word processor file.

The Trilateral Offices have selected an open systems alternative to word processor files where electronic documents will be based on using the eXtensible Markup Language (XML) which is being developed to deliver structured data on the World Wide Web. XML documents, like HTML web pages, consist of a character coded text file and zero or more additional files that may be more text or contain binary data such as images and drawings. A typical XML patent application electronic document will consist of a collection of files. An example would be a text file for each procedural document submitted as part of the application plus a text file for the specification of the invention that is accompanied by multiple graphics files (one graphics file for each drawing in the specification). While the XML approach has freed the offices from investing in proprietary word processor formats, the simplicity of the single word processor document file has been lost.

5.1.1 Images

The facsimile images for use in industrial property document exchange must meet the following requirements:

(a) Format
  (i) TIFF V6.0 with Group 4 compression, Single Strip, Intel Encoded or
  (ii) JFIF(JPEG)
(b) 200, 300 or 400 dpi
(c) Maximum size A4 or Letter size

5.1.2 PDF

The PDF documents for use in industrial property document exchange must meet the following requirements:

(a) Acrobat V3 compatible
(b) Non-compressed text to facilitate searching
(c) Un-encrypted text
(d) No Digital Signatures
(e) No embedded OLE objects
(f) All Fonts must either be embedded, Standard PS17 or built from Adobe MM fonts

5.1.3 XML

All XML documents must conform to one of the DTDs specified in Appendix II.

The character set for all XML documents must be either UTF-8 encoded Unicode UCS-2 (ISO/IEC 10646:193) or ISO-2022-JP encoded JIS-X0208. For PCT Applications, Chinese GB2312 and Korean KSC 5601 are also acceptable.

In addition to the above, each receiving Office may specify a character encoding scheme as described in [IETF RFC 2277] and [IETF RFC 2130] and inform the International Bureau of the specification. In this case, the following must be defined:

(a) Coded character set (mapping from a set of letters to that of integral numbers) as described in [IETF RFC 2277] and [IETF RFC 2130].
(b) Glyph set to indicate a set of integral numbers with that of letters.
(c) Translation rules between the coded character sets, if several coded character sets are used in the system.

5.1.4 ST25

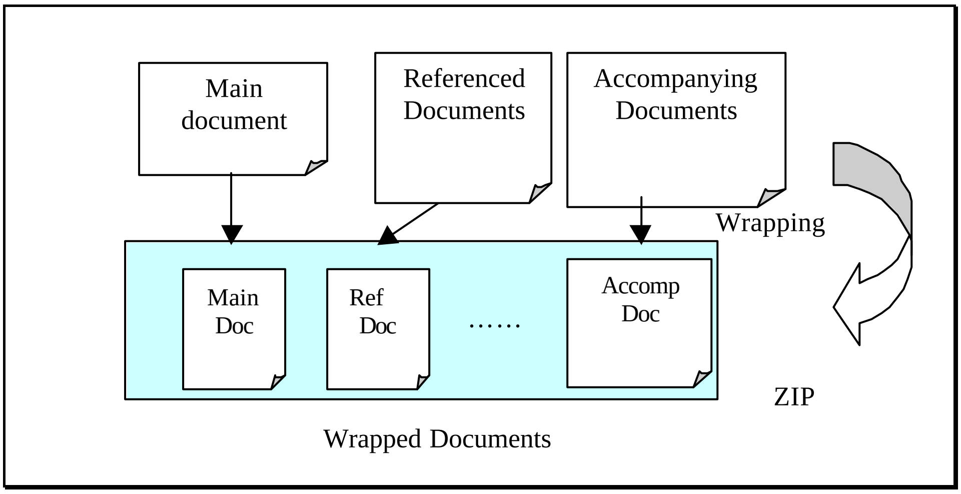
A document created using the WIPO ST25 SGML tags for sequence listings can be included as an external document in a WAD.

5.1.5 ASCII

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

5.2 Wrapping the Documents

The Main Document with any Externally Referenced Documents and Accompanying Documents are wrapped and treated as one data block. This data block is called the Wrapped Application Documents and is created using the wrapping standard (ZIP). Applicants shall use ZIP format archiving and compression software to package the document files constituting an electronic application.



The software used to create the ZIP file shall conform to the ZIP format standard as published in the PKWARE® PKZIP® Application Note (Revised: 08/01/1998) on the PKWARE® web page http://www.pkware.com/appnote.html.

The files to be zipped shall include all parts of the document identified elsewhere in this specification. All external files referenced by the Specification of the Invention must be included in the ZIP file submission. Filenames included in the central directory of the ZIP file shall comply with the specification for the applicable operating system given elsewhere in this specification.

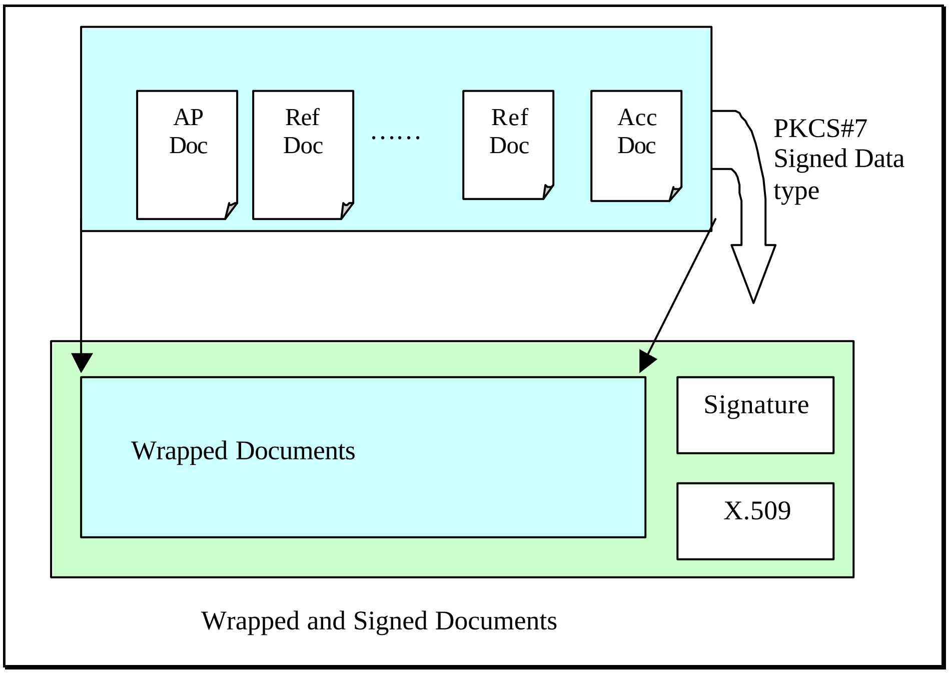
All ZIP files must have a flat directory structure. If a collection of files needs to be embedded in the ZIP file, then these should be included as a single flat embedded ZIP file.

The ZIP standard allows the compression software to select from among a number of compression algorithms. The default compression method shall be “Deflation” with the normal compression option. This format can be most readily dealt with by UNZIP packages. The “Shrinking” compression method shall not be used because it makes use of a patented Lempel-Ziv-Welch (LZW) compression algorithm protected by a patent held by the UNISYS Corporation.

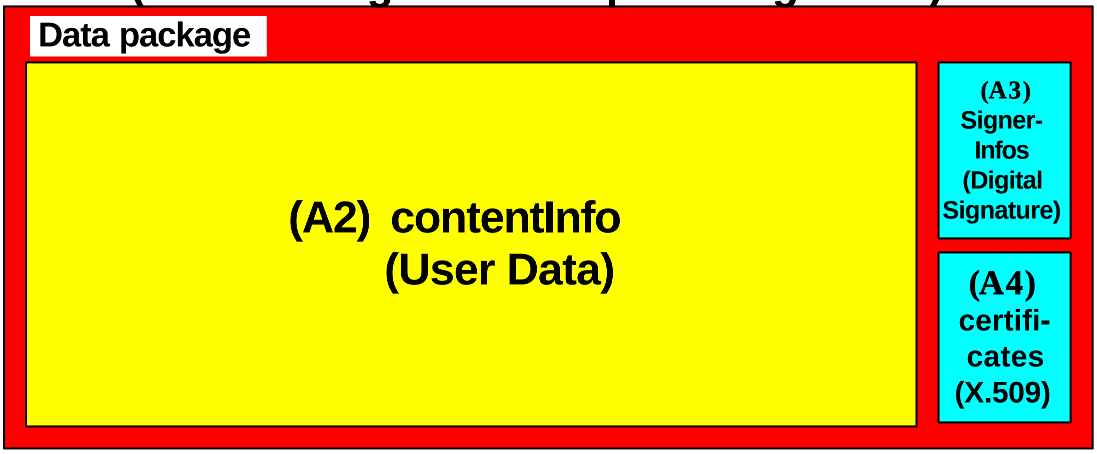
5.3 Signing the Wrapped Application Documents

To bind the person creating the package to the electronic Wrapped Application Documents, a Digital Signature is added to create the Signed Wrapped Application Documents data item. The purpose of adding the signature is to identify the person creating the package and to ensure that the recipient is able to detect any unauthorized alteration during the transmission.

PKCS#7 is used to produce a Signed Data Type for the signature.



(A1) Signed Data <Top Level>
(PKCS#7 Digital Envelope for signature)


Data package
(A2) contentInfo (User Data)
(A3) Signer-Infos (Digital Signature)
(A4) certifi-cates (X.509)

Rules for producing the PKCS#7 digital envelope for certification

Object identifier for sha-1	The object identifier for SHA-1 that we adopt is defined in OIW interconnection protocols: Part 12. The definition is below: **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*. The definition is below:
	Pkcs-1 OBJECT IDENTIFIER ::= iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1}
	RsaEncryption OBJECT IDENTIFIER ::={pkcs-1 1}

Object identifier of 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 ONLY ONE **set of** algorithm identifiers {sha-1}
3	Content information	ContentInfo	Set one content info (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 its serial number defined in X.509 spec. (for signer's certificate)
3	Set of digest algorithms	DigestAlgorithm	
3.1	Algorithm identifier	AlgorithmIdentifier	Set ONLY ONE **set of** algorithm identifiers {sha-1} for making digest of digital signature.
4	Authenticated attributes	AuthenticatedAttributes	Not used (Set no data)
5	Digest encryption algorithm	DigestEncryptionAlgoritm	Algorithm OBJECT identifier of digest encryption (recommended algorithm : rsaEncryption[2])
6	Encrypted digest	EncryptedDigest	Message digested data; content is encrypted with 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	ExtendedCertificatesAndCertificates	
1.1	The X.509 certificate	Certificate (defined in X.509 spec.)	Set ONLY ONE **set of** X.509 certificate data

Optional: If the encryption algorithm, which is used in the digital certificates added to a digital signature, is different from the algorithm described in this specification, the receiving Office must notify International Bureau of the algorithm.

6 Submission

A receiving Office may decide not to use the enveloping mechanism described in this section as the encryption mechanism for transmission, because of the use of channel level encryption such as SSL. In the case of the transmission between Offices, it is not needed to use these encryption mechanisms, because of using private network like TriNet.

6.1 Transmission Package

A package is the actual transmission data that is exchanged between the applicant and the receiving Office.

The package contains various data items according to the individual package type. Data items include:

(a) Header Object Data item
(b) Document Data item that is made by wrapping and signing Documents
(c) Transmission Data such as time of transmission.

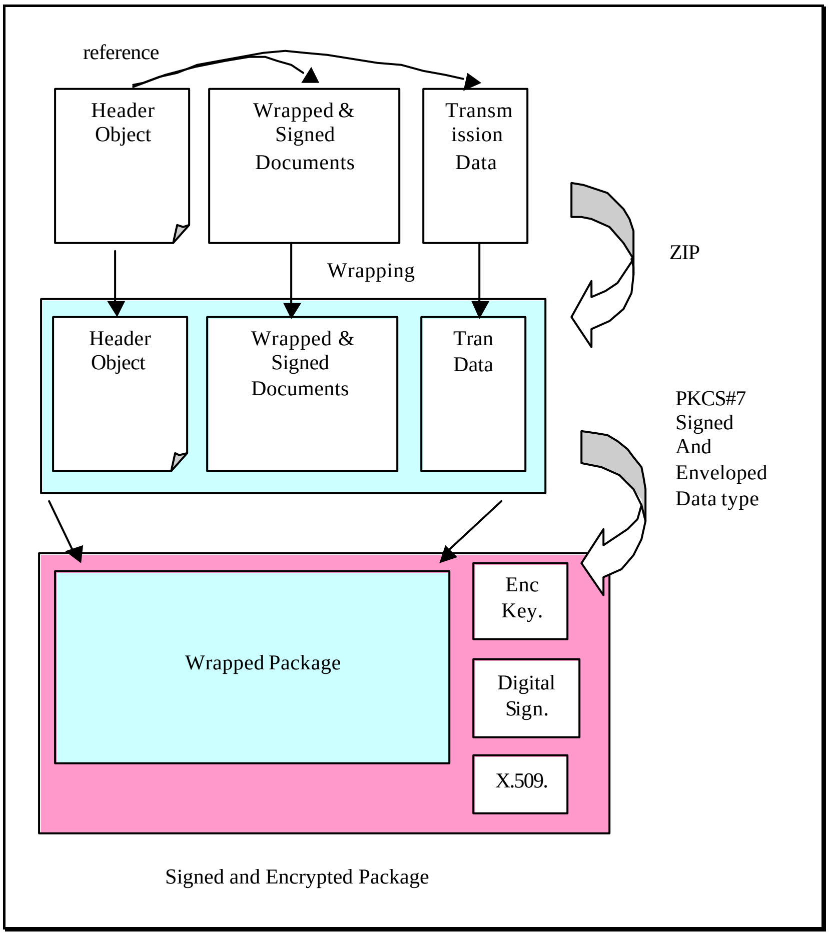
The Header Object Data item indicates the package type, file name of data item, etc. The Header Object Data item is always found in the package. The Header Object Data item is written in XML in accordance with DTD defined in Appendix II.

The procedure for creating the package is as follows:

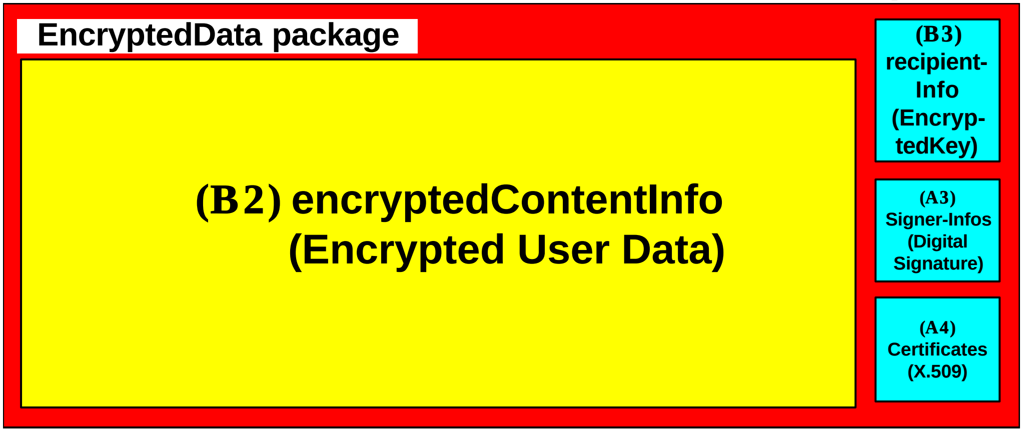
(a) Create a wrapped package by wrapping the Signed WAD with the data items used for transmission using ZIP
(b) Create a signed and encrypted package for network transmission by encrypting using the Signed And Enveloped Data Type in PKCS#7

The purpose of the signature is to assure the combination and contents of individual data items, and to ensure that the recipient is able to detect any unauthorized alterations during the transmission. Encryption is to prevent unauthorized interception during data communications.

The Digital Signature for the Wrapped Application Documents may be produced either by the applicant or their representatives. The person that starts the transmission produces the Digital Signature for the final Signed and Enveloped Data Type.


reference
Header Object
Wrapped & Signed Documents
Transmission Data
Wrapping
ZIP
Header Object
Wrapped & Signed Documents
Tran Data
PKCS#7 Signed And Enveloped Data type
Wrapped Package
Enc Key.
Digital Sign.
X.509.
Signed and Encrypted Package

(B1) SignedAndEnvelopedData <Top Level>
(PKCS#7 Digital Envelope for Transmission)


EncryptedData package
(B2) encryptedContentInfo
(Encrypted User Data)
(B3) recipient-Info (Encryp-tedKey)
(A3) Signer-Infos (Digital Signature)
(A4) Certificates (X.509)

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 ONLY ONE **set of** recipientInfo (see table B3)
2	Set of algorithm identifiers	DigestAlgorithms	

2.1	Algorithm identifier	AlgorithmIdentifier	Set ONLY ONE **set of** algorithm identifiers {sha-1}
3	Encrypted Content information	EncryptedContentInfo	Set one encrypted content info (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

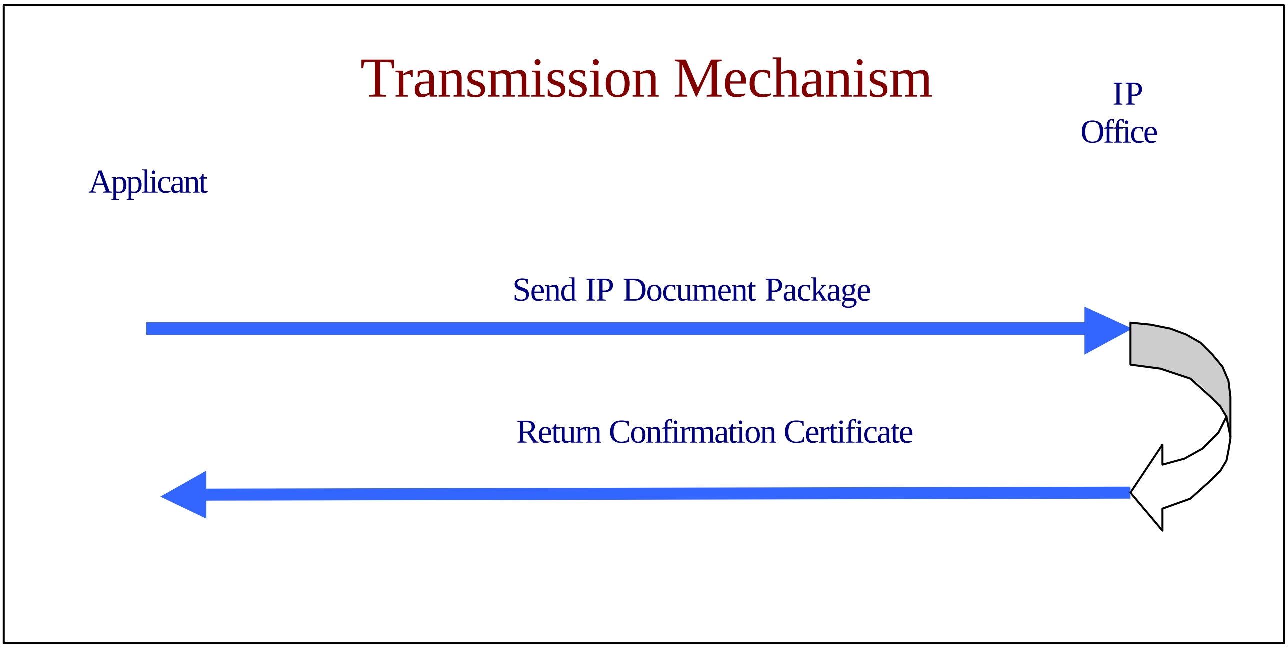
No.	Item name	PKCS#7 item	Content
1	Content type	ContentType	Set object identifier {pkcs-7 1}
2	Content encryption algorithm	ContentEncryptionAlgorithm	Algorithm OBJECT identifier of content encryption (recommended algorithm : dES-EDE3-CBC)
3	Encrypted content	EncryptedContent	Encrypted user data

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 certificates that includes the 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:



(a) An electronic session is established between the applicant and the industrial property Office.

(b) The applicant transmits the complete set of files constituting the industrial property Document package.

(c) On receipt of the full set of files, the documents are then checked for the presence of viruses and processed to develop their unique message digest.

(d) This digest is compared to the message digest included in the Signed Wrapped Application Documents. If they match, an acknowledgement of receipt is sent to the applicant. If they do not match, the applicant is informed accordingly. The session is then ended.

6.2.1 Virus Scanning

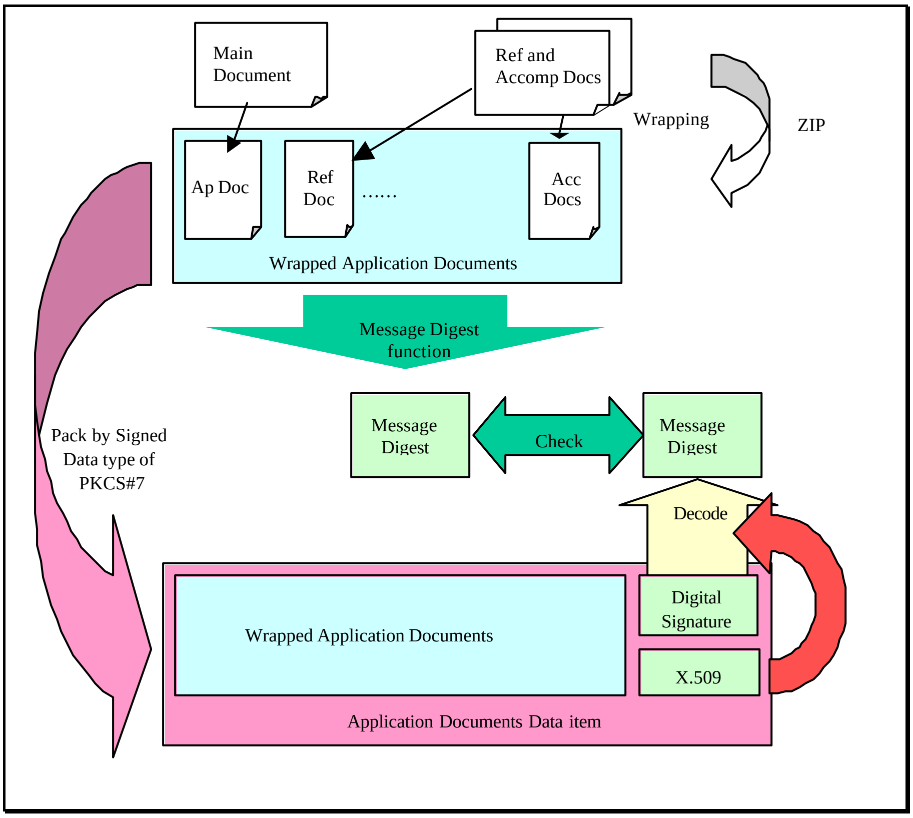
The receiving Office shall scan electronic submissions for the presence of viruses.

Virus scanning software will be made available by the International Bureau to all receiving Offices participating in the WIPONET project.

The WIPONET project will distribute manuals containing security guidelines to participating Offices. These manuals will also contain recommendations on the methodology for virus scanning of electronic submissions.

The Administrative Instructions specify the steps to be taken upon detection of possible virus infection.

6.2.2 Checking the Message Digest



The industrial property Office then receives the package, opens the data items in the package and decides the role of individual data items in accordance with the documentation in the Header Object Data items.

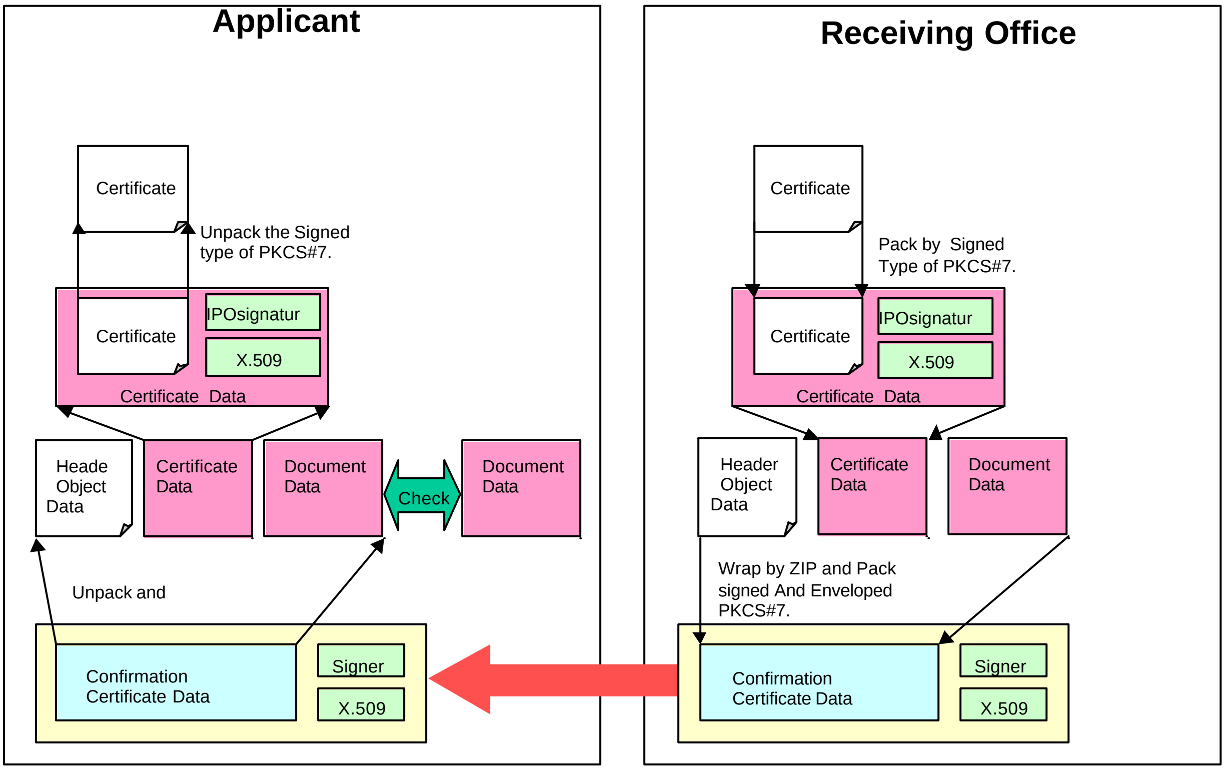
6.2.3 Confirmation Certificate

The Confirmation Certificate Data item includes a Certificate Data item, a Header Object Data item specifying that the corresponding packet is a Confirmation Certificate, and an Application Documents Data item received with a New Application as an option.

In the event of a communications or message digest comparison problems, the Confirmation Certificate contains information about the problem detected

The Confirmation Certificate is created by wrapping and packing the Data item using Signed And Enveloped Data type in PKCS#7.

Confirmation Certificate



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 contain a formatted version of the data in PDF, TIFF and JFIF(JPEG). These files are combined in a single ZIP file and signed using the Digital Certificate of the industrial property Office.

6.3 Transmission Protocol

To increase the probability of successful validation, a reliable transport layer protocol shall be used for all transfers between offices. The reliable transport layer protocol serves to assure that all data in transmission has been transferred and re-assembled correctly between the sending and receiving software applications.

Each receiving Office shall specify the transfer protocol acceptable between the receiving Office and applicant. As the transfer protocol, the FTP or the HTTP protocol is recommended.

Optional: The security of communication provided by the encryption within a PKCS#7 Signed And Enveloped Data type will normally be sufficient but, if an industrial property Office considers it necessary, it may opt for channel level encryption such as SSL or IP Sec to enhance this security.

6.4 Physical media

Each receiving Office may choose the physical media instead of, or in addition to online filing. The standard such as labeling and physical packaging requirements are defined in Appendix III.

7 Types of Document Exchange

The industrial property Document Exchange Standard is designed to cover all types of interaction between Applicants, Representatives and industrial property Offices. The following types of exchange have been defined in detail:

7.1 New PCT Applications

The procedure for creating the required data format is as follows.

(a) Create an XML document as specified in the New PCT Application DTD in Appendix II.
(b) Create a wrapped package by wrapping the XML document and Signed wrapped application document sent by applicant using ZIP.
(c) Add the digital signature of submitter using the Signed Data Type in PKCS#7.
(d)

7.2 Receiving Office to International Bureau

The procedure for creating the data format is as follows.

(e) Create an XML document that includes the filing date, application number and an external reference to the signed WAD submitted by the applicant
(f) Create a wrapped package by wrapping the XML document and Signed WAD using ZIP.
(g) Add the digital signature of the receiving Office using the Signed Data Type in PKCS#7.
(h)

7.3 Receiving Office to International Searching Authority

The same procedure as for receiving Office to International Bureau is used.

7.4 International Bureau to designated Office(elected Office)

The data exchanged between the International Bureau and the designated Office is not only the application document. The data format will be specified by argument between the International Bureau and the designated Office. If a designated Office cannot receive the document format (e.g. PDF), the International Bureau shall send the document after conversion into a format which is acceptable to the designated Office.

8 Reference Implementations

As part of the preparation of this standard, the Trilateral offices are preparing two reference implementations (both in JAVA and C++ running on Windows NT) that allows other developers to re-use and extend the basic source code provided to build client and procedure specific implementations.

The reference implementations covers the following areas:

(a) ZIP
(b) PKCS#7

(c) Wrapping
(d) Transfer mechanism including return of a confirmation Certificate

These are available in source as well as object code.

In addition, standard test data sets are available to verify third-party implementations.

9 Access to Electronic Forms of Documents

A receiving Office may optionally provide means of access by applicants or members of the general public to documents stored by that Office in electronic form.

A receiving Office may allow access to confidential data. To ensure that confidential data is available to authorized viewers only, the Office will use Recognized Certificates with PKI techniques to authenticate the identity of the person seeking access.

It is envisaged that the applicant will access these receiving Office database services over the Internet using freely available web browser software. Current versions of web browsers support 128-bit SSL sessions, which can be used to provide secure encrypted communication between the applicant and the receiving Office.

The receiving Office may provide electronic documents to the applicant on request, in the standard document formats supported by that Office, by means of e-mail or secure e-mail, or on standard physical media specified in Appendix III and supported by that Office (floppy disk, CD-Recordable, etc.).

Attachment 1 - Acronyms

DTD	Document Type Definition
EPCT	Electronic PCT Application
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
IP Sec	IP Security
PCT	Patent Cooperation Treaty
PKCS	Public Key Cryptographic Standard
PKI	Public Key Infrastructure
RFC	Request For Comments
SGML	Standardized Generic Mark-up Language
SSL	Secure Sockets Layer
WAD	Wrapped Application Documents
WIPO	World Intellectual Property Organization
XML	Extensible Mark-up Language

[End of document]