E

WIPO

WORLD INTELLECTUAL PROPERTY ORGANIZATION
GENEVA

PATENT COOPERATION TREATY (PCT)

ADMINISTRATIVE INSTRUCTIONS
UNDER THE PATENT COOPERATION TREATY:

ANNEX F
STANDARD FOR THE FILING AND PROCESSING
IN ELECTRONIC FORM OF INTERNATIONAL APPLICATIONS

as in force from January 1, 2022

1.   This document contains the consolidated text of Annex F of the Administrative Instructions under the Patent Cooperation Treaty (PCT), as in force from January 1, 2022, established under Article 58(4) and Rule 89.2(a), and modified under Rule 89.2(b) and in accordance with the change procedure provided for in section 2.5 of Annex F.

2.   The text of the Administrative Instructions as in force from January 1, 2022, with the exception of Annexes A and F (available separately), is contained in document PCT/AI/22 dated October 26, 2021. The text of Appendix I of Annex F of the Administrative Instructions as in force from July 1, 2021 is contained in document PCT/AI/DTD/15 dated April 21, 2021. This document is to be read, subject to any subsequent additions or revisions, with these texts.

3.   This document is published on WIPO's website at www.wipo.int/pct/en/texts/index.htm; paper copies are available from the International Bureau of WIPO upon request.

ANNEX F
STANDARD FOR THE FILING AND PROCESSING
IN ELECTRONIC FORM OF INTERNATIONAL APPLICATIONS
(as in force from January 1, 2022)

TABLE OF CONTENTS

1.   INTRODUCTION

This Annex has been elaborated so as to provide standardization in relation to the electronic filing, processing, and storage of international applications under the Patent Cooperation Treaty,[1] and in particular, under PCT Rule 89*bis* and AIs Part 7. The standard is intended to allow applicants to file an international application in electronic form which is acceptable to all receiving Offices, International Searching Authorities and International Preliminary Examining Authorities, for the purposes of the international phase, and to all designated Offices, for the purposes of the national phase, that accept the filing or processing of applications in electronic form. It comprises a set of requirements including certain options for applicants and receiving Offices concerning the submission of international applications (and related documents) in electronic form based on the implementations set out in this Annex, including its Appendices.

The application of the standard is subject to certain options for receiving Offices, for example, as to the type of electronic signature and level of digital certificate that they will accept. Receiving Offices are required under AIs Section 710 to communicate their choices to the International Bureau, which will publish them for the benefit of applicants. Designated Offices will be required likewise to notify the International Bureau of the acceptable type of electronic signature and level of digital certificate from among those permitted under the standard. All receiving Offices and designated Offices accepting electronic filing are required, however, to accept international applications which comply with the "basic common standard" referred to in AIs Section 703 and elaborated in Appendix III.

The standard has been formulated to apply to international applications filed under the PCT, both in the international phase and, by virtue of PCT Article 27(1), in the national phase of processing. It is also expected that the standard will become a de facto standard applied to non-PCT applications by national and regional Offices. In addition, the standard may become the subject of wider application by virtue of its possible future adoption, *mutatis mutandis*, as a general WIPO Standard for patent applications filed in electronic form. Upon the future coming into force of the Patent Law Treaty (PLT), and subject to adoption by the PLT Assembly, the standard would become applicable to national and regional Offices which become bound by the provisions of the PLT.

The main body of the Annex contains the basic technical principles to be adopted for electronic filing. Further details, including certain specific implementations, are set out in Appendices.

2.   THE E-PCT STANDARD: OVERVIEW AND VISION

This Annex and its Appendices contain the technical standard, including requirements, format and procedures, relating to the filing and processing, including exchange among PCT

---

[1]   References in this document to "Articles," "Rules" and "Sections" are, respectively, to those of the Patent Cooperation Treaty ("the Treaty" or "PCT"), of the Regulations under the PCT ("the Regulations") and of the Administrative Instructions under the PCT ("the Administrative Instructions" or "AIs"), 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/pct/en/texts/index.htm. See also the Abbreviated expressions, interpretation and glossary in section 9 of this Annex.

Offices and Authorities,[2] of international applications and related documents and data ("E-PCT" standard). The following section presents a brief, high-level overview of the business requirements and long-term vision driving the overall effort.

2.1 Scope

This standard is meant to be applied to the creation and exchange of electronic PCT documents throughout the PCT process. It covers the following technical areas:

(a)   electronic international application (IA) document format, structure and requirements;

(b)   electronic IA submission packaging and transmission; and

(c)   rules and guidelines for the use of this standard throughout the PCT process.

Additional technical information supporting the main body of the Annex can be found in several Appendices. All systems constructed for the purpose of electronic filing and processing of PCT documents and data should be conformant to this standard, unless an exception is specifically mentioned herein.

Matters outside the scope of this document:

(d)   specification of software systems to use this standard; and

(e)   electronic systems used by designated Offices during the national phase, except to the extent that PCT Article 27(1) applies (and noting the broader considerations mentioned in section 1).

2.2 Business case and requirements review

Electronic filing and processing of PCT documents has long been considered as an important and justifiable means of improving the PCT system. There are numerous benefits that can be expected, including the following:

(a)   IAs filed with minimal formal defects, having been prepared by officially designed software;

(b)   avoidance of the manual process of entering data into computer systems;

(c)   documents and data in an agreed format for exchange with other IP Offices;

(d)   applications can be processed faster and at lower cost;

(e)   PCT users can take advantage of current technology such as the Internet; and

(f)   fully electronic document and data sharing and publication is possible.

2.2.1 Business requirements

---

[2]   The term "Office" is often used herein in a generic sense to include RO, ISA, IPEA, DO, EO, IB and/or national or regional industrial property Office, as applicable according to the context.

The detailed functional requirements for E-PCT systems and standards are too numerous to discuss here. However, the primary business requirements can be summarized by the following goals of this standard:

2.2.1.1   Security

Solutions implemented under this standard must satisfy the following four basic criteria for secure electronic data exchange:

(a)   authentication – the process of validating an identity claimed by or for an entity;

(b)   integrity – ability to verify that data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed;

(c)   non-repudiation – ensure that strong and substantial evidence is available to the sender of data that the data has been delivered (with the cooperation of the recipient), and to the recipient of the sender's identity, sufficient to prevent either from successfully denying having possessed the data; this includes the ability of a third party to verify the integrity and origin of the data;

(d)   confidentiality – ensure that information can be read only by authorized entities.

This standard supports, in particular, a solution relying on a public key infrastructure (PKI) for authentication and data security in the Internet environment. However, it also envisages that there may in the future be other solutions which satisfy the above four security criteria.

Any Office with an operational solution that satisfies the four criteria may choose to submit the specification for inclusion in this standard, in which case the proposed modification would be the subject of consultation under PCT Rule 89.2(b).

2.2.1.2   Efficiency

This standard should designate technologies that promote high performance and facilitate instantaneous or on-demand information sharing. E-PCT systems should eventually lower costs to applicants and Offices through reduction of paper and saving of time.

2.2.1.3   Interoperability

Systems conformant to this standard must accept and produce electronic documents and data in a consistent format that permits sharing between applicants and Offices, and among Offices, with no loss of information. Systems should be able to exchange data using a common protocol that allows the reliable transfer of data without special and costly setup procedures for each type of interaction.

2.3   Overview of PCT communication sectors

In Figure 1, the various communications that occur in the PCT business process have been categorized into four sectors that require specific variations of the high-level business requirements above, such as level of confidentiality and/or authentication. These PCT "communication sectors" are described below.
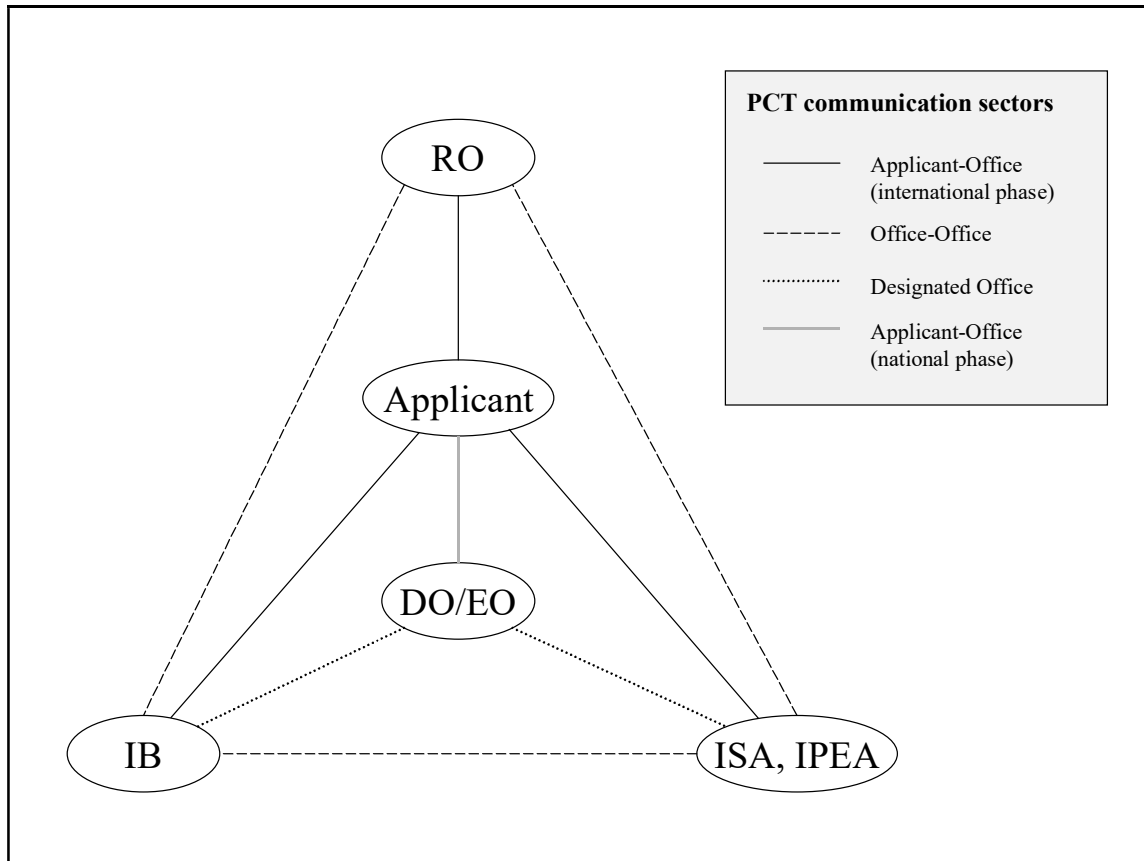
Figure 1 - PCT communication sectors

2.3.1   Applicant-Office (international phase) sector

The Applicant-Office (international phase) sector includes all communications between applicants and Offices in the international phase. The initial filing is included along with subsequent exchanges between the applicant and the receiving Office ("RO"), International Bureau ("IB"), International Searching Authority ("ISA") and International Preliminary Examining Authority ("IPEA").

Some of the PCT workflow transactions included in this sector are:

–   applicant files IA with RO

–   applicant sends amendments to the IB or IPEA

–   applicant sends request for changes to IB (PCT Rule 92*bis*)

–   applicant sends demand to IPEA

–   applicant furnishes power of attorney

–   applicant withdraws IA

–   IB sends copy of pamphlet to applicant

–   IB sends forms to applicant

–   IB sends translation of international preliminary examination report ("IPER") to applicant

–   ISA sends international search report ("ISR") with cited documents to applicant

In addition to meeting the high-level requirements above in section 2.2, systems in this communication sector must be able to interoperate efficiently with very large numbers of applicants and, in the case of applicant systems, with a number of different Offices. National law may contain restrictions on technology[3] and/or systems dealing with the general public. Therefore, systems must be designed to accommodate any such restrictions or special requirements.

2.3.2   Office-Office sector

Document exchanges and communications taking place in the Office-Office sector generally involve one PCT Office sending documents and/or data to another Office during the international phase, including the following PCT workflow transactions:

–   RO sends search copy to ISA

–   RO sends record copy to IB

–   RO sends priority document to IB

–   ISA sends ISR to IB

–   IPEA forwards demand to IB

–   IPEA sends IPER to IB

The high-level requirement of security as described above in section 2.2, in particular authentication and confidentiality, is emphasized for the Office-Office communications in this sector.

---

[3]   In particular, cryptographic technology is subject to various national restrictions.

2.3.3   Designated Office sector

The designated Office sector includes communications between the designated/elected Offices ("DO/EOs"),[4] and the IB . Document exchanges and communications include priority documents and publication data, and include the following PCT workflow transactions:

–   IB sends pamphlet to DO/EO

–   IB sends priority documents to DO/EO

–   IB sends IPER to DO/EO

–   IB sends forms to DO/EO

The levels of interoperability and information security required in this sector varies considerably according to the kind of data exchanged, and may differ from requirements in the Office-Office sector. For example, the communication of applications to DOs after they have been published may involve little or no requirement for confidentiality.

2.3.4   Applicant-Office (national phase) sector

Communications between applicant and Offices in the national phase are required, to the extent that PCT Article 27(1) applies, to adhere to this standard.

2.4   E-PCT vision

The goals stated earlier in this section demand a secure, interoperable group of automated PCT systems capable of quickly and efficiently sharing electronic documents and data between PCT applicants and Offices, improving operations for all. The International Bureau envisions an environment in which any applicant can file an international application with any Office in the world which accepts electronic filing with a cost free and standardized software. The PCT environment of the future will allow faster, more reliable access to information for all PCT Offices and their customers.

This sophisticated level of systems integration will be difficult to achieve in this or any other integrated system. It will require the close cooperation of all parties involved, and take a great deal of time and effort. Many of the necessary technologies, including those used for ensuring data security and even the Internet itself, are continually evolving. This will require systems to undergo numerous developmental changes.

The goal is attainable, especially given the extremely rapid progress of technology and the constant evolution of international standards for data interchange. This standard is designed to take advantage of industry standards where possible, building on the strength of accessible and widely used technologies.

---

[4]   References to designated Offices encompass such Offices in their capacity as elected Offices unless the context otherwise requires. In some cases, the fact that both capacities are meant is emphasized by referring to "designated/elected Offices" ("DO/EOs").

2.5   Change procedure

2.5.1   Scope

It is necessary to modify the standard from time to time in the light of practical experience and of new technical developments. The change procedure outlined in this section constitutes the usual means by which the Director General undertakes consultation pursuant to PCT Rule 89.2(b) concerning proposals to modify the contents of Annex F (including its Appendices) ("proposals for change"), before deciding whether to promulgate such modifications. The procedures outlined in this section shall also be used as an additional means of information when changes are proposed to other parts of the Administrative Instructions which may have consequences for the technical requirements in this Annex.

2.5.2   Web site; information list; Consultative Group

The International Bureau maintains a Web site for the processing of proposals for change. The Web site provides for interested persons to register their e-mail addresses on the e-filing information list of persons who wish to be informed when proposals for change (or other materials relating to PCT electronic filing) are made available on the site.

The national Office of any State, and any PCT Authority, any intergovernmental organization (including any regional Office) and any non-governmental organization, that is invited to participate in meetings of the PCT Assembly may register, via the Web site, to participate in the work of a Consultative Group which considers proposals for change. It is strongly encouraged that the participants nominate as their representatives in the Consultative Group both technical and legal specialists to ensure that proposals for change are fully considered. Participants should preferably register at an early stage in the annual change management cycle outlined in section 2.5.4, below.

National Offices of PCT Contracting States and PCT International Authorities which register to participate in the Consultative Group do so as members, and other participants as observers. All Consultative Group members and observers are also automatically included in the e-filing information list. The International Bureau, as secretariat, coordinates the activities of the Group. Consideration of matters by the Group is informal and takes place via the Web site and e-mail and, where necessary, via other means of telecommunication; meetings of the Group in person are not envisaged.

Consultative Group members and observers are invited to discuss, and make recommendations on, how proposals for change should be handled and, in particular, whether changes should be promulgated and with what effective date, as outlined further below. It is expected that the Group would operate on the basis of consensus.

Consultative Group members and observers shall be informed by the International Bureau of any proposed modifications submitted under the ordinary consultation pursuant to PCT Rule 89.2(b) which include changes to Annex F, or which appear likely to the International Bureau to require consequential changes to Annex F if adopted.

2.5.3   Proposals for change

Proposals for change may be submitted to the International Bureau by any Office or Authority entitled to register as a member of the Consultative Group, and may be initiated by

the International Bureau. An Office or Authority or the International Bureau may, if it wishes, submit a proposal for change that has been suggested to it by a third party. Proposals for change may be submitted, preferably via the Web site, at any time during the year.

A proposal for change may be modified or withdrawn by the Office or Authority that submitted it. Each proposal for change is published by the International Bureau on the Web site as a "Proposal for Change" (PFC) file to which comments, modifications, etc., are annexed. Exchanges of views on a proposal for change, if not annexed to the PFC file concerned, are stored in an archive accessible via the Web site.

Each proposal for change must set forth the requested modifications of the text and/or figures concerned, a list of items that may be impacted, the reason, including processing or policy issues involved, and the proposed date of implementation, including, if appropriate, a request for expedited handling, and should also, if possible, include a draft implementation (for example, a new XML DTD). It shall preferably also indicate if, in the view of the person making the proposal, the proposal is of a mere technical nature, or of a legal and technical nature.

Consideration of proposals for change would ordinarily proceed under the (standard) annual change management cycle in accordance with section 2.5.4. If needed, generally on request by the proposer, the International Bureau may determine, after consultation with the Consultative Group, that consideration of a proposal for change should be expedited in accordance with section 2.5.5. It is to be understood that consideration of any proposal for change resulting from a change to a PCT Contracting State's national law relating to the standards contained in this Annex would be expedited.

2.5.4   Annual change management cycle

1. Each proposal for change received by the International Bureau is published on the Web site, forthwith after its receipt, in a PFC file together with an indication that comments on the proposal may be sent to the International Bureau. That publication is promptly notified by e-mail to the e-filing information list.

2. Any comments received from interested parties following the publication and notification of a proposal for change referred to in section 2.5.3 are promptly published on the Web site in the PFC file and notified by e-mail to the e-filing information list.

3. Further consideration of the proposal does not take place until the following February, unless expedited consideration is accorded to the proposal under section 2.5.5.

4. On or promptly after February 15, the International Bureau publishes on the Web site a list of all pending standard proposals for change and references to the relevant PFC files, with an indication that comments may be sent to the International Bureau by March 31, and sends a notification by e-mail to the e-filing information list. The International Bureau also sends a written circular to all PCT Offices and Authorities, interested intergovernmental organizations and certain non-governmental organizations representing users, referring to the Web site, inviting comments by March 31 and advising that paper copies of the proposals for change are available from the International Bureau.

5. Any further comments received by the International Bureau are published, forthwith after their receipt, in the PFC file on the Web site and notified by e-mail to the e-filing information list.

6. Promptly after March 31, the International Bureau invites the Consultative Group to consider the pending proposals for change and comments, and the Consultative Group makes recommendations to the International Bureau by May 15. The recommendations are published forthwith in the PFC file on the Web site and notified by e-mail to the e-filing information list.

7. Taking into account the comments received and the recommendations of the Consultative Group, and after any necessary revision, the International Bureau publishes on the Web site, by June 30, modifications intended to come into force on January 1 of the following year or, exceptionally, before that date, and sends a notification by e-mail to the e-filing information list.

8. The usual procedures for promulgation of modifications of the Administrative Instructions apply (written circular and publication in the PCT Gazette).

9. If applicable, new or revised requirements of Offices are notified to the International Bureau, as provided for in Section 710 of the Administrative Instructions, for publication in the PCT Gazette.

2.5.5 *Expedited consideration of change proposals*

1. At any time, on request or at its own initiative, the International Bureau may decide that a proposal for change should be accorded expedited consideration, even if the proposal for change has so far been treated as standard.

2. Each proposal for change which is accorded expedited consideration is published on the Web site for comment and notified by e-mail to the e-filing information list, as outlined in section 2.5.4, paragraphs 1 and 2, except that comments are invited within six weeks. At the same time as that publication, the International Bureau sends the written circular referred to in section 2.5.4, paragraph 4, inviting comments within six week. Any comments received within six weeks are published, forthwith after their receipt, in the PFC file on the Web site and notified by e-mail to the e-filing information list.

3. In parallel to the actions referred to in paragraph 2, the International Bureau invites the Consultative Group members and observers to consider the proposal for change and any subsequent comments received during the six week period referred to in paragraph 2, and to make any recommendation before the end of that six week period, including a recommendation, if applicable, as to the appropriate date of entry into force of the proposed modifications. The recommendations are published forthwith in the PFC file on the web site and notified by e-mail to the e-filing information list.

4. Taking into account the comments received and the recommendations of the Consultative Group members and observers, and after any necessary revision, the International Bureau publishes the modifications, and their date of entry into

force, on the Web site, and sends a notification by e-mail to the e-filing information list.

5. The modifications are promulgated, and any new requirements of Offices are notified and published, as outlined in section 2.5.4, paragraphs 8 and 9.

2.5.6 Version handling

Where the practice and the technical systems of the recipient Office so permit, earlier versions of certain aspects of the standard (notably, DTDs and the E-filing interoperability protocol) may operate simultaneously for a limited period of time. Each version should be clearly identified by the appropriate version number.

3. E-PCT SUBMISSION STRUCTURE AND FORMAT

Electronic international application submissions contain many different types of documents and information. Text, images and sequence listings can all be printed on paper, but each of these requires a different electronic representation. For example, text can be stored in "character codes" while images can be stored in grids of picture elements called "bitmaps". The concept is further complicated by the fact that most information can be stored in multiple electronic formats. Sequence listings can be stored as plain text. Printed text can be optically scanned and stored as an image.

In addition to format, the structure (or lack of structure) of information can have a large impact on the ability of automated systems to facilitate processing of the information. Images of typed pages of text have no electronic text structure and must be electronically "recognized" or hand-keyed by a human operator before they can be searched.

On the other hand, text and other information can be structured to enforce business rules and associate information with meaningful business identifiers. The format specified by this standard for such structured text is called XML (eXtensible Markup Language).

Using XML, computer systems can identify specific pieces of information and reach new levels of capability. For example, if an international application has been structured in XML according to the E-PCT standard, a computer system could automatically display the first claim; it could link figure references to the actual figure (within drawings); it could hyperlink patents and other types of citations to the actual patents and documents. Publication and information retrieval systems also gain significant capabilities from structured documents.

In addition to structured information within an electronic format, international application submissions may contain documents that are composed of multiple types of information stored in multiple electronic formats. This collection of documents must have an overall structure that allows computer systems to identify the type of document and each of its components.

When designing automated information systems for document processing, electronic format and structure is critical; it can either enable or inhibit processing. This section describes the format and structure necessary for electronic IA documents to be compliant with the E-PCT standard. It specifies several allowable electronic document formats and the manner in which they must be structured.

3.1   Allowable electronic document formats

This Annex is based on the principle of establishing an industry standards-based environment for electronic exchange of IA documents. A notable result of this is: the standard for submitting electronic documents emphasizes the use of open standards and will not promote, as far as possible, proprietary vendor formats for electronic documents. The reasons for this policy include avoiding the need to maintain multiple copies of electronic filings in specific versions of proprietary electronic document formats over which Offices have no control.

This standard requires the IA documents to be free from virus or other malicious logic.

Note that this standard also applies to other documents and correspondence relating to international applications filed or processed in electronic form by virtue of Rule 89*bis*.2 and AIs Section 713(b).

Any document in electronic form that is prepared or exchanged in accordance with this standard shall be in one of the electronic document formats listed in sections 3.1.1 to 3.1.3 which are allowed under section 3.4 in the communication sector concerned. Note, however, that section 3.4 permits, in the Office-Office communication sector, the sending Office and the recipient Office to agree on the use of other types of electronic document formats for IA documents filed on paper and converted into electronic form, except for the record copy.

Applicants may present a nucleotide and amino acid sequence listing in any of the electronic document formats listed in sections 3.1.1 to 3.1.3 which are allowed under section 3.4 in the Applicant-Office communication sector. However, where the sequence listing is not presented in the electronic document format specified in paragraph 40 of the Standard for the Presentation of Nucleotide and Amino Acid Sequence Listings in International Patent Applications under the PCT (see Annex C of the Administrative Instructions and WIPO Standard ST.25, and section 3.1.1.2, below; hereinafter referred to as "Annex C/ST.25 text file"), the competent International Searching Authority and the International Preliminary Examining Authority may, for the purposes of the international search and of the international preliminary examination, respectively, invite the applicant to furnish to them a sequence listing in that electronic document format (see Rule 13*ter*) (see also paragraph 42(iv) of Annex C of the Administrative Instructions with regard to the right of designated or elected Offices to invite the applicant to furnish a sequence listing in that electronic document format).

Where a table is contained in an international application, the spatial relationships (e.g., columns and rows) of the table elements shall, irrespective of the electronic document format in which the table is presented, be maintained.

3.1.1   Character coded formats

3.1.1.1   XML

All documents in XML format must conform to their corresponding DTDs (Document Type Definitions) specified in Appendix I.

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

In addition , each receiving Office may specify a character encoding scheme as described in IETF RFC 2277 (Internet Engineering Task Force Policy on Character Sets and Languages) and IETF RFC 2130 (Report of the IAB Character Set Workshop) and shall inform the International Bureau of the specification. In this case, the following must be defined:

(a)   coded character set;

(b)   character encoding scheme;

(c)   translation rules between the coded character set and International Standard ISO/IEC 10646:2000.

Example encoding schemes that conform to the above rules would be native-JIS and shift-JIS.

For the Applicant-Office (international phase) communication sector, receiving Offices must accept this format per the basic common standard. For the Office-Office communication sector, Offices must be able to transmit and receive this format.

3.1.1.1.1   Paragraph Numbering in XML documents (description)

If the description part of an international application is encoded in XML format, the paragraphs of that description part shall be numbered by a four-digit Arabic number, with leading zeros where required, for example, [0099], enclosed in square brackets and placed to the right of the left margin of the document.

If the number of paragraphs exceeds four digits, then the numbering of paragraphs should increase by one digit, and so forth, according to need. For example, paragraph [10000] follows paragraph [9999] and paragraph [100000] follows paragraph [99999].

3.1.1.2   Annex C/ST.25 text file

Any sequence listing presented as an Annex C/ST.25 text file (see paragraph 40 of the Standard for the Presentation of Nucleotide and Amino Acid Sequence Listings in International Patent Applications under the PCT (Annex C of the Administrative Instructions and WIPO Standard ST.25)) must be included as a referenced document.

For the Applicant-Office (international phase) communication sector, receiving Offices must accept this electronic document format in accordance with the basic common standard. For the Office-Office communication sector, Offices must be able to transmit and receive this format.

3.1.1.3   ASCII

Any file in this format, if present, must be included as a referenced document.

For the Applicant-Office (international phase) communication sector, receiving Offices shall notify the International Bureau whether they will accept documents in this format, which documents they will accept in this format, and whether they will accept seven-bit and/or eight-bit ASCII.

For the Office-Office communication sector, this format may not be included in document packages, except when included in the original wrapped application documents (WAD, see section 4.1.1) filed by the applicant, as part of the record copy (Applicant Package, see section 5.2.2).

3.1.2   PDF

Any file in this format, if present, must be included as a referenced document.

All documents in PDF format must meet the following requirements:

(a)   Adobe Portable Document Format Version 1.4 compatible;

(b)   non-compressed text to facilitate searching;

(c)   unencrypted text;

(d)   no embedded OLE objects;

(e)   all fonts must be embedded and licensed for distribution.

For the Applicant-Office (international phase) communication sector, receiving Offices shall notify the International Bureau whether they will accept documents in this format, including, where applicable, details as to the version(s) that are acceptable. In order to accommodate Offices that do not accept documents in PDF format, any Office that chooses to accept documents in this format must also convert the documents (that is, text and drawings) to TIFF images and transmit the documents in both formats to the International Bureau.

For the Office-Office communication sector, Offices shall notify the International Bureau whether they will transmit or accept documents in this format, including details as to the version(s) in use. For documents originally submitted in PDF format, Offices may request transmission of the original documents in PDF format in addition to the converted documents in TIFF format.

3.1.3   Image formats

Images may be used for drawings, figures, equations or other illustrations, or scanned documents. A receiving Office may choose to allow applicants to submit all or part of the description or claims in image format.

3.1.3.1   Tagged Image File Format (TIFF)

Any file in this format, if present, must be included as a referenced document.

TIFF facsimile (black and white) images for use in IA document exchange must meet the following requirements:

(a) TIFF V6.0 with Group 4 compression, single strip, Intel encoded.

(b) Resolution of either 300 or 400 dpi

(c) Maximum size: whole pages should be either A4[5] or Letter[6] size, however the recommended maximum size is 255mm by 170mm.

For the Applicant-Office (international phase) communication sector, receiving Offices must accept this format per the basic common standard. Images may be used for drawings, figures, equations or other illustrations, and for the description and the claims. This format is not intended to be used as a replacement for character-coded document formats.

For the Office-Office communication sector, Offices must be able to transmit and receive this format. Images may be used for drawings, figures, equations or other illustrations, and for the description and the claims. This format may also be used to transmit scanned documents between offices in the form of page images.

3.1.3.2 JPEG File Interchange Format (JFIF)

Any file in this format, if present, must be included as a referenced document.

JFIF images for use in IA document exchange must meet the following requirements:

(a) Resolution of either 300 or 400 dpi

(b) Maximum size of 255mm by 170mm.

For the Applicant-Office (international phase) communication sector, receiving Offices shall notify the International Bureau whether they will accept images in this format. Images may be used for drawings, figures, equations or other illustrations. This format is not intended to be used as a replacement for character-coded document formats.

For the Office-Office communication sector, Offices shall notify the International Bureau whether they will transmit or accept images in this format.

3.1.4 Pre-conversion formats

Documents in pre-conversion format submitted under AIs Section 706(a) or (f) must be included as referenced documents.

For the applicant Office (international phase) communication sector, receiving Offices shall notify the International Bureau whether they will accept the filing, under AIs Section 706(a) and (f), of documents in pre conversion format and, if so, which pre-conversion formats they will accept (see AIs Section 710(a)(iv)).

---

[5] A4 size = 210x297mm, with a maximum of 3307x4677 pixels at 400dpi.
[6] Letter size = 215.9x279.4mm (8.5x11 inches), with a maximum 3400x4400 pixels at 400dpi.

For the purposes of the procedure under AIs Section 706(b), any receiving Office which chooses to accept documents submitted under AIs Section 706(a) or (f) in a pre-conversion format which the International Bureau cannot process must transmit the document concerned to the International Bureau in both an electronic document format which the International Bureau can process and the original pre conversion format.

3.2   E-PCT document and submission structure

An international application submission may contain multiple documents, each with text, drawings and sequence listings stored in multiple electronic document formats. In order to accommodate the need for multiple electronic document formats while preserving a structure that a computer system can understand, an E-PCT submission, including its documents, must conform to the structure specified in this section.

In order to be in compliance with this requirement, each E-PCT submission must contain an XML package data file that explicitly references the submission documents, and must conform to the "package-data" DTD (Document Type Definition) as specified in Appendix I, section 3.1. However, in the Office-Office communication sector, the sending Office and the recipient Office may agree to use other types of structures for IA documents filed on paper and converted into electronic form. In such case, the recipient Office should inform the International Bureau accordingly. The referenced documents (e.g. the request and the patent application) are logically part of the submission as such.

As shown in Figures 2 and 2*bis*, the referenced documents (external entities) are typically the request, the application (description, claims), the priority documents, etc. which in turn may contain images, tables, drawings which are separate but related objects that may be encoded as either XML, PDF, ST.25, ASCII or image formats (TIFF or JFIF). Each document in XML format shall conform to one of the DTDs specified in Appendix I, except for referenced "other-documents", where a receiving Office may choose to accept documents in XML format conforming to DTDs not specified in Appendix I, in which case the Office shall notify those DTDs to the International Bureau. The version of the DTD must be set in the "DTD VERSION" attribute of the document in XML format (as specified by the DTD itself).

XML package data	Referenced documents	
package-data xml	request xml	
	application-body xml	drawing/image tiff, jfif, pdf
	sequence list st-25	
	fee-sheet xml	
	declaration xml	
	power-of-attorney xml	
	amendment-request xml	drawing/image tiff, jfif, pdf
	biological-deposit xml	
	table xml	
	other-documents xml, pdf, tiff, jfif, wad, wsp	

Note: all referenced XML documents may point to other documents formatted in PDF

Figure 2 - Example of E-PCT IA structure where the text of the description, claims and abstract is in character coded format (in XML format)

XML package data	Referenced documents	

Note: all referenced XML documents may point to other documents formatted in PDF
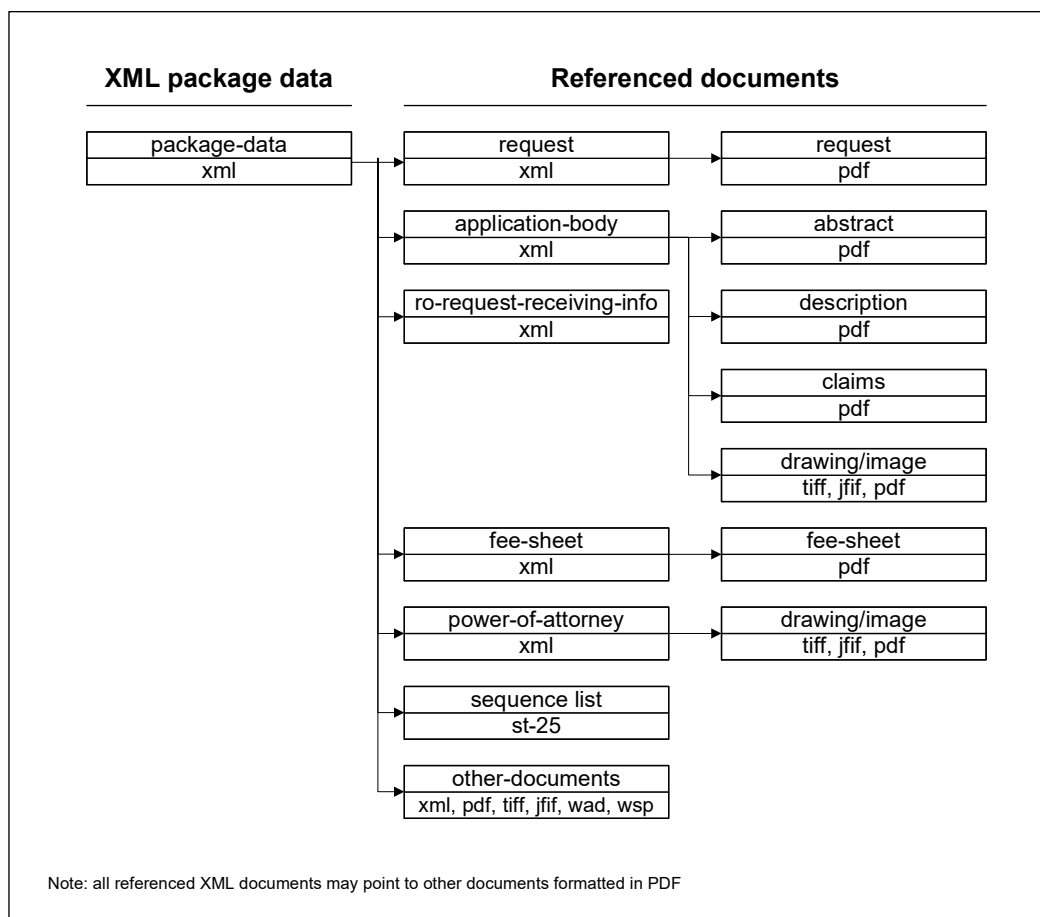
Figure 2*bis* - Example of E-PCT IA structure where the text of the description, claims and abstract is not in character coded format (but in PDF format)

3.3 *Electronic signature*

For IA document exchange, a number of electronic signature types (see AIs Section 701) are permitted by this standard. Each receiving Office shall notify the IB which types of signature it will accept.

The sections below describe these types of signatures, categorized as basic and enhanced electronic signatures.[7] At this time, this standard does not support the use of multiple enhanced electronic signatures but it does support the use of multiple basic electronic signatures.

3.3.1 *Facsimile signature*

To create this type of signature, an XML file (e.g. the request) must include the <fax> element and an external entity reference set in the FILE attribute that points to a TIFF file containing a bitmap of the signature. The TIFF file must meet the requirements as described in section 3.1.3.1.

---

[7] For definitions of "basic electronic signature" and "enhanced electronic signature," see section 9.

3.3.2   Text string signature

To create this type of signature, an XML file 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:

/janedoe/

The text-string must be a string of characters which does not include the forward slash "/" character, and which is chosen by the user as its electronic signature. Valid examples include:

/John Smith/

/Tobeornottobe/

/1345728625235/

/Günter François/

3.3.3   Click wrap signature

To create this type of signature, typically the user clicks on a button, labeled "I accept", in a user interface. This is indicated in an XML file by the presence of a <click-wrap/> empty element.

3.3.4   Enhanced electronic signature
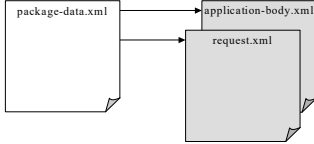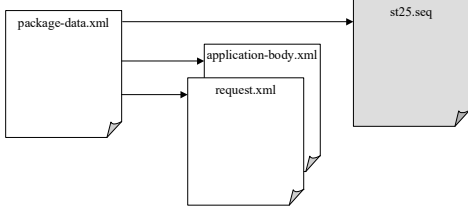
An enhanced electronic signature relies on the use of a PKI and a PKCS #7 digital signature data type. See section 4.2 and Appendix II for additional information on PKCS #7 and PKI.

The PKCS #7 SignedData type is generated from the electronic message by the act of the signer invoking the use of their private signing key to encrypt the message digest. The PKCS #7 SignedData type includes a copy of the digital certificate of the signer.

3.4   Allowable document formats, by PCT communication sector

The document and image formats that are allowable under this standard are contained, listed by PCT communication sectors, in the tables below. For each format, the tables state the options available to Offices and an example of a corresponding valid package contents under this standard.

Any document in electronic form that is prepared or exchanged in accordance with this standard shall be in one of the electronic document formats listed in sections 3.1.1 to 3.1.3 which are allowed under this section in the communication sector concerned. However, in the Office-Office communication sector, the sending Office and the recipient Office may agree to use other types of electronic document formats for IA documents filed on paper and converted into electronic form, except for the record copy. In such case, the recipient Office should inform the International Bureau accordingly.

Applicant-Office (international phase) sector		
Format	*Options allowable*	*Example package contents*
XML See section 3.1.1.1	A receiving Office must accept this format per the basic common standard. A receiving Office shall notify the IB of the character encoding scheme for XML documents (as described in section 3.1.1.1) if it is other than the standard encoding scheme (UTF-8).	
Annex C/ST.25 text file See section 3.1.1.2	A receiving Office must accept this format per the basic common standard.	

Applicant-Office (international phase) sector		
Format	Options allowable	Example package contents
ASCII See section 3.1.1.3	A receiving Office shall notify the IB whether it will accept documents in this format, which documents it will accept in this format, and whether it will accept seven-bit and/or eight-bit ASCII.	
PDF See section 3.1.2	A receiving Office shall notify the IB whether it will accept documents in this format. In order to accommodate Offices that do not accept PDF documents, any Office that chooses to accept documents in this format must also convert the document text and drawings to TIFF images and transmit those documents in both formats to the IB.	
TIFF See section 3.1.3.1	A receiving Office must accept this format per the basic common standard. Images may be used for drawings, figures, equations or other illustrations. This format is not intended to be used as a replacement for character-coded document formats.	

Applicant-Office (international phase) sector		
Format	*Options allowable*	*Example package contents*
JFIF See section 3.1.3.2	A receiving Office shall notify the IB whether it will accept images in this format.	

Office-Office sector		
Format	*Options allowable*	*Example package contents*
XML See section 3.1.1.1	Offices must be able to transmit and receive this format. A receiving Office shall notify the IB of the character encoding scheme for XML documents (as described in section 3.1.1.1) if it is other than the standard encoding scheme (UTF-8).	
Annex C See section 3.1.1.2	Offices must be able to transmit and receive this format.	

Office-Office sector		
Format	*Options allowable*	*Example package contents*
ASCII See section 3.1.1.3	Offices shall notify the IB whether they will transmit and receive documents in this format.	package-data.xml → application-body.xml, request.xml → other-doc.txt
PDF See section 3.1.2	Offices shall notify the IB whether they will transmit or accept documents in this format. For documents originally submitted in PDF format, Offices may request transmission of the original PDF documents in addition to the document converted in TIFF format.	package-data.xml → application-body.xml, application-body.pdf, request.xml → page02tif, page01.tif XML document created to contain references to converted TIFF page image files. Converted TIFF page image files Original PDF document
TIFF See section 3.1.3.1	Offices must be able to transmit and receive this format. Images may be used for drawings, figures, equations or other illustrations, as in the first example to the right.	package-data.xml → application-body.xml, request.xml → fig02.tif, fig01.tif TIFF drawings XML document includes fully-tagged content.

Office-Office sector		
Format	Options allowable	Example package contents
TIFF (cont'd)	This format may also be used to transmit image based or scanned documents between offices in the form of page images, as in the second example to the right.[8]	
JFIF See section 3.1.3.2	An Office shall notify the IB whether it will transmit or accept images in this format.	

4.   IA DOCUMENTS PACKAGING

Because an IA document will generally consist of several files, it is useful to assemble these files together into a single electronic "package" for transmission. Two kinds of packages are included under this standard: non-PKI and PKI based packages. Wrapped Application Documents Files ("WADs") are non-PKI based packages while Wrapped and Signed Packages ("WASPs") are PKI based packages. More detailed information about the implementation of PKI based solutions for the purposes of this standard is set out in Appendix II.

Any document in electronic form that is prepared or exchanged in accordance with this standard shall be packaged as prescribed in sections 4.1 and 4.2. However, in the Office-Office communication sector, the sending Office and the recipient Office may agree not to package IA documents filed on paper and converted into electronic form, or to package

---

[8]   See TIFF in the Applicant-Office sector table for an example of TIFF images used as drawings, etc. The example package contents shown here are not permitted in the Applicant-Office sector.

such documents in a different manner. In such case, the recipient Office should inform the International Bureau accordingly.

All electronic document exchange files under this standard must be first packaged as a WAD. Section 5.2 provides additional information on allowable package/transmission combinations according to the different PCT communication sectors.

4.1   Non-PKI based package

This standard includes only one type of non-PKI based package: the WAD.

4.1.1   Wrapped application documents (WAD)

The IA submission along with any referenced documents are wrapped and treated as one data block. This data block is called the wrapped application documents package (WAD) and is created using the wrapping standard, ZIP.

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: 08/01/1998). All ZIP files must have a flat directory structure.

The ZIP standard allows the compression software to select from among a number of compression algorithms. The compression method must be "deflation" with the normal compression option.

4.2   PKI package types

This standard includes only two types of PKI based packages: the WASP and the C-WASP. See Appendix II for further information on PKI.

4.2.1   Wrapped and signed package (WASP)

When the person who signs the WASP is the applicant (or his representative), the signature of the WASP may also serve as an enhanced electronic signature of the application (see section 3.3) if technical systems in place provide that the application is automatically signed thereby.

A low-level or high-level digital certificate (see definitions in section 9) accompanies the digital signature.

Figure 3 is a simplified anatomy of the WASP. 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 PKZIP wrapping has been left out of the diagram.

In case of a notification sent by the Office to the applicant, the Office prepares, signs and sends the WASP which contains such notification.
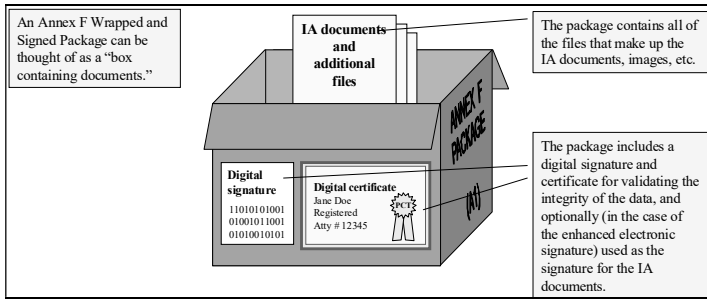
Figure 3 – Wrapped and signed package (WASP)

See Appendix II for additional detail on the WASP technical specification.

4.2.2   Compound WASP (C-WASP)

The one or more WASPs sent to the applicant from the Office are wrapped using the ZIP as shown in the section 4.1.1 and treated as one data block. This data block is called "Compound WASP" (C-WASP).

4.3   File naming convention

The present file naming convention is established in order to enhance server automation, as well as to establish a client side software workflow and a good work practice for user understanding. It shall be applied in respect of any document in electronic form that is prepared or exchanged in accordance with this standard. However, in the Office-Office communication sector, the sending Office and the recipient Office may agree to apply other file naming rules for the purposes of their transactions. In such case, the recipient Office should inform the International Bureau accordingly. The following set of tables constitutes the file naming convention and the client side software should automatically produce the suffixes and extensions accordingly. Each of these tables addresses a level of the standard, followed with tables of examples.

4.3.1   Tables

Table 1

Codes used in the descriptions below	
A	One character from the following set: {ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz}
A…	Any combination of at least two characters from the following set: {ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789}
AAA	Any combination of one to three characters from the following set: {ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789}
NNNNNN	Any combination of six characters from the following set: {0123456789}

Table 2

Each instance of a document type		
A…	Applicant's or Office's identifier, not to exceed 50 positions	Mandatory
-	Separator (dash)	

A…	Document type *(see Table 6)* or Subdocument type *(see Table 7)*	
-	Separator (dash)	Optional
A	Entity type *(see Table 8)*, in case of image file	
NNNNNN	Document sequence number, right justified, left padded with zero	
.	Separator (period)	Mandatory
AAA	File type *(see Table 5)*	

Table 3

	External entities referenced from within document instances	
A…	Applicant's or Office's identifier, not to exceed 50 positions	Mandatory
-	Separator (dash)	
A…	Document type *(see Table 6)* or Subdocument type *(see Table 7)*	
-	Separator (dash)	
A	Entity type *(see Table 8)*	
NNNNNN	Entity sequence number, right-justified, left-padded with zero	
-	Separator (dash)	Optional
NNNNNN	Page sequence number, right-justified, left-padded with zero	
.	Separator (period)	Mandatory
AAA	File type *(see Table 5)*	

Table 4

	Files not referenced from within document instances	
A…	Applicant's or Office's identifier, not to exceed 50 positions	Mandatory
-	Separator (dash)	Optional
A…	Document name as provided by applicant, not to exceed 50 positions	
.	Separator (period)	Mandatory
AAA	File type	

Table 5

	File name extensions accepted
Txt	Text file, see section 3.1.1.3.
xml	XML file, see section 3.1.1.1.
Tif	TIFF file, see section 3.1.3.1.
Jpg	JFIF file, see section 3.1.3.2.
pdf	Portable document format (PDF) file, see section 3.1.2.
app	ST.25 file, see section 3.1.1.2.
Zip	Archive file containing one or more files

Table 6

Document and package types currently accepted for initial ePCT filing	
Document type	*Code*
record copy (package)	reco
home copy (package)	hoco
package header	pkgh
package data	pkda
request	requ
receiving office information	rrri
declarations	decl

application body	appb
fee sheet	fees
original separate power of attorney	poat
original general power of attorney	gpoa
copy of general power of attorney	cgpa
statement explaining the lack of signature	lacs
priority documents	pdoc
translation of application	tapp
document in pre-conversion format	dpcf
biological deposit	biod
sequence listing	seql
sequence listing not forming part of the application	seqn
sequence listing table	seqt
table external	tabx
transmission receipt	xmre
application receipt list	aprl
dispatch list	dspl
amendment request	amnd
change of bibliographic material	bibc
ex-officio correction	exoc
correspondence	crsp
notification	noti
demand	dmnd
IPEA demand receiving information	idri
fee-sheet-chapter2	fee2
international search report (ISR)	isre
international preliminary examination report (IPER)	iper
international search opinion (ISO)	isop
translation of international search report	isrt
translation of international preliminary examination report	ipet
translation of international search opinion	isot
published application	papp
office specific document types	[2-position country code]AA
table exceeding fifty printed pages	mtbl

Table 7

Subdocument types currently accepted for initial ePCT filing	
Subdocument type	Code
description	desc
claims	clms
abstract	abst
drawings	draw

Table 8

Entity types	
T	Table
M	Mathematical formula
C	Chemical structure or formula

S	Sequence listing
D	Drawing page (contains one or more figures per image page and one or more image pages)
F	Figure (exactly one figure on exactly one image page)
I	Embedded image (one or more image pages)
P	Document page

4.3.2   Applicant's identifier

The applicant's identifier is determined by the applicant with or without the help of the filing tool. The name of every file that is part of a submission will begin with the same applicant's identifier. Applicant's identifier might be a name or a docket number or some other string that has significance to the applicant. An applicant's identifier is not necessarily unique to each submission, that is, it might be used for another submission associated with prosecution of the same application; it could even be used by the applicant for all submissions for all his applications. The applicant's identifier is placed first so that in a directory listing, all the files for a particular submission or application or applicant will sort together.

Example of Applicant Package containing an international application

File	Contents
dupont0340-pkda.xml	Package data
dupont0340-requ.xml	Request
dupont0340-fees.xml	Fee sheet
dupont0340-biod.xml	Biological deposit
dupont0340-decl-000001.xml	First declaration
dupont0340-decl-000002.xml	Second declaration
dupont0340-poat-000001.xml	First power of attorney
dupont0340-poat-I000001.tif	First image of first power of attorney
dupont0340-poat-I000002.tif	Second image of first power of attorney
dupont0340-poat-000002.xml	Second power of attorney
dupont0340-poat-I000003.tif	First image of second power of attorney
dupont0340-lacs-I000001.tif	First lack of signature
dupont0340-lacs-I000002.tif	Second lack of signature
dupont0340-seql.app	Sequence listing (ST.25)
dupont0340-appb.xml	Application
dupont0340-appb-C000001.tif	First chemical structure, TIFF format
dupont0340-appb-C000001.cdx	First chemical structure, ChemDraw format
dupont0340-appb-C000001.mol	First chemical structure, MOL format
dupont0340-appb-M000001.tif	First mathematical formula, TIFF format
dupont0340-appb-M000002.tif	Second mathematical formula, TIFF format
dupont0340-appb-T000001.tif	First table, TIFF format
dupont0340-appb-T000002-000001.tif	Second table, first page, TIFF format
dupont0340-appb-T000002-000002.tif	Second table, second page, TIFF format

4.3.3   Office's identifier

The office's identifier is determined by each office with or without the help of their system. The name of every file should begin with 'pct | RO-code | IA-number', for example 'pctib2004012345'.

Example of RO Package containing a record copy (pctib2004012345-reco.wsp)

File	Contents
pctib2004012345-pkda.xml	Package data
pctib2004012345-requ.xml	Request
pctib2004012345-rrri.xml	Receiving office information
pctib2004012345-fees.xml	Fee sheet
pctib2004012345-biod.xml	Biological deposit
pctib2004012345-decl-000001.xml	First declaration
pctib2004012345-decl-000002.xml	Second declaration
pctib2004012345-poat-000001.xml	First power of attorney
pctib2004012345-poat-I000001.tif	First image of first power of attorney
pctib2004012345-poat-I000002.tif	Second image of first power of attorney
pctib2004012345-poat-000002.xml	Second power of attorney
pctib2004012345-poat-I000003.tif	First image of second power of attorney
pctib2004012345-lacs-I000001.tif	First lack of signature
pctib2004012345-lacs-I000002.tif	Second lack of signature
pctib2004012345-seql.app	Sequence listing (ST.25)
pctib2004012345-exoc.xml	*Ex-officio* correction
pctib2004012345-appb.xml	Application
pctib2004012345-appb-C000001.tif	First chemical structure, TIFF format
pctib2004012345-appb-M000001.tif	First mathematical formula, TIFF format
pctib2004012345-appb-M000002.tif	Second mathematical formula, TIFF format
pctib2004012345-appb-T000001.tif	First table, TIFF format
pctib2004012345-appb-T000002-000001.tif	Second table, first page, TIFF format
pctib2004012345-appb-T000002-000002.tif	Second table, second page, TIFF format

5.   TRANSMISSION

The IA package can be transmitted over secure or non-secure channels depending on the package type. This section includes the protocol to be followed as well as the package/transmission combinations that are permitted in the Applicant-Office (international phase), Office-Office, and designated Office communication sectors. While additional sectors are referred to in this standard (see section 2.3), permissible transmission/package combinations can be categorized in the three sectors listed above.

5.1   The E-filing interoperability protocol

This section describes both the transmission layer protocol between the clients and the server as well as providing a definition of the behavior required of both the client and the server.

The protocol is designed to support HTTP communication over an SSL (or TLS) Tunnel for all PKI based E-filing solutions and includes the following capabilities:

(a)   Enables large applications to be transmitted via multiple HTTP post actions to address reliability and integrity issues

(b)   Efficient error detection and correction

(c)   Enables offices to control optimal transaction size

Note that this is an evolving protocol, with production systems in development at a number of IP Offices, and further revisions are foreseen.

5.1.1 Principles

The following principles have been adopted for the interoperability protocol:

(a)   All communications between client and server is in the form of HTTP post actions initiated by the client

(b)   All post requests and resulting responses use the same transaction management header followed by an optional data block

(c)   All transmissions use the Division mechanism to divide large blobs of data into manageable chunks with a protocol that allows for retries and pacing.

5.1.2 Application layer protocol for application

At the highest level for application, there are five events that the protocol requires a client and server to support. These events are:

(a)   Begin Transaction

(b)   Send Package Header

(c)   Send Package Data

(d)   Get Receipt

(e)   End Transaction

In between the Begin and End Transactions, there are three types of WASP sent between the client and the server:

(i)   The package header contains essential information for initial processing to identify the submission. It is a WASP containing the package header in XML format.

(ii)   The package data contains the information for submitting application. It is a WASP consisting of various types of files.

(iii)   The receipt is an acknowledgment of the submission. The content of this receipt (XML data plus an optional human readable certificate in PDF or TIFF format), which is signed by the receiving Office, is defined in Appendix I.

5.1.2.1 Use of the SSL (or TLS) tunnel for application

These events are all performed within an SSL (or TLS) tunnel that is established before issuing the Begin Transaction event. The SSL (or TLS) tunnel is built using both client and server authentication. The SSL (or TLS) tunnel may be stopped at the end of the

transaction or, if a batch of transmissions is foreseen, the SSL (or TLS) tunnel can be left open and only stopped when all transmissions are complete. The SSL tunnel uses the SSL protocol version 3.0.

The Receiving Office (RO) has discretion over which protocol to be used, SSL or TLS.

When the client authentication is to be conducted by the server, in addition to the function supported by the SSL protocol version 3.0 (or the TLS protocol) that confirms the fact that the digital certificate transmitted by the client software is actually issued by the recognized CA, disconnection of the SSL (or TLS) tunnel may be controlled by the server based on the following process:

(a) Data of the applicant/representative digital certificate(s) obtained beforehand by the receiving Office is stored in the server.

(b) At the time of client authentication by the SSL protocol version 3.0 (or the TLS protocol), the server checks whether the data of the applicant/representative digital certificate sent by the client software exists in the data previously stored in the server by the above-mentioned step (a).

(c) If the check result in step (b) is negative, the server disconnects the SSL (or TLS) tunnel.

In order to carry out the above function, the receiving Office may conduct a pre-registration process to obtain beforehand the following data, on its own initiative or from the applicant/representative: (i) data (or updated data) of digital certificate(s) used by the applicant/representative; and as the need arises, (ii) additional information on the applicant/representative.

In all cases except where the SSL (or TLS) tunnel is disconnected in the process described above, the current protocol requires each individual transaction to be acknowledged by an individual receipt.

5.1.2.2   Application level events for application

Start SSL (or TLS) session (see Figure 5)

Step 0: Begin Transaction
Client action:
Get transaction Information.
Server response:
Return values in the *transaction_id* and *max_division_size* transaction management header elements.

transaction_id is a unique identifier assigned by the server associating all transactions involved in the submission of an application.

max_division_size is the maximum number of bytes permitted by the server for the size of a division.

Step 1: Send Package Header
  Client action:
    Send package header
  Server response:
    a) OK
    b) Error (Abort, go back to step 0)
    c) Package already received; go to step 3 to get the receipt.

  After receiving the last division of the WASP containing the package header, the server must verify the signature of the WASP. If the signature is invalid (for instance expired), the Application Response Code (ARC) will remain OK, but the server will capture the error and provide a message on the receipt.

Step 2: Send Package Data
  Client action:
    Send package data
  Server response:
    a) OK
    b) Error (Abort, go back to step 0)

  After receiving the last division of the WASP containing the package data, the server must verify the signature of the WASP and compare the message digest of the unsigned package against the message digest provided in the Package Header in Step 1 of the transaction before returning the ARC to the client. If both conditions are met, the server should return an ARC indicating OK. If the hash values in package header and the WAD of the package data do not match, the ARC value should be set to FFF7. If the signature is invalid (for instance expired), the ARC will remain OK, but the server will capture the error and provide a message on the receipt.

Step 3: Request Receipt
  Client action:
    Send request
  Server response:
    a) OK (Receipt object included in response)
    b) Error (Abort, go back to step 0)

Step 4: End Transaction.
  Client action:
    Send acknowledgment of completion including information about any client problem to the server.
  Server response:
    a) OK
    b) Error (Client can ignore this response)

Close SSL (or TLS) session

In all cases of SSL (or TLS) Tunnel, the current protocol requires each individual transaction to be acknowledged by an individual receipt.
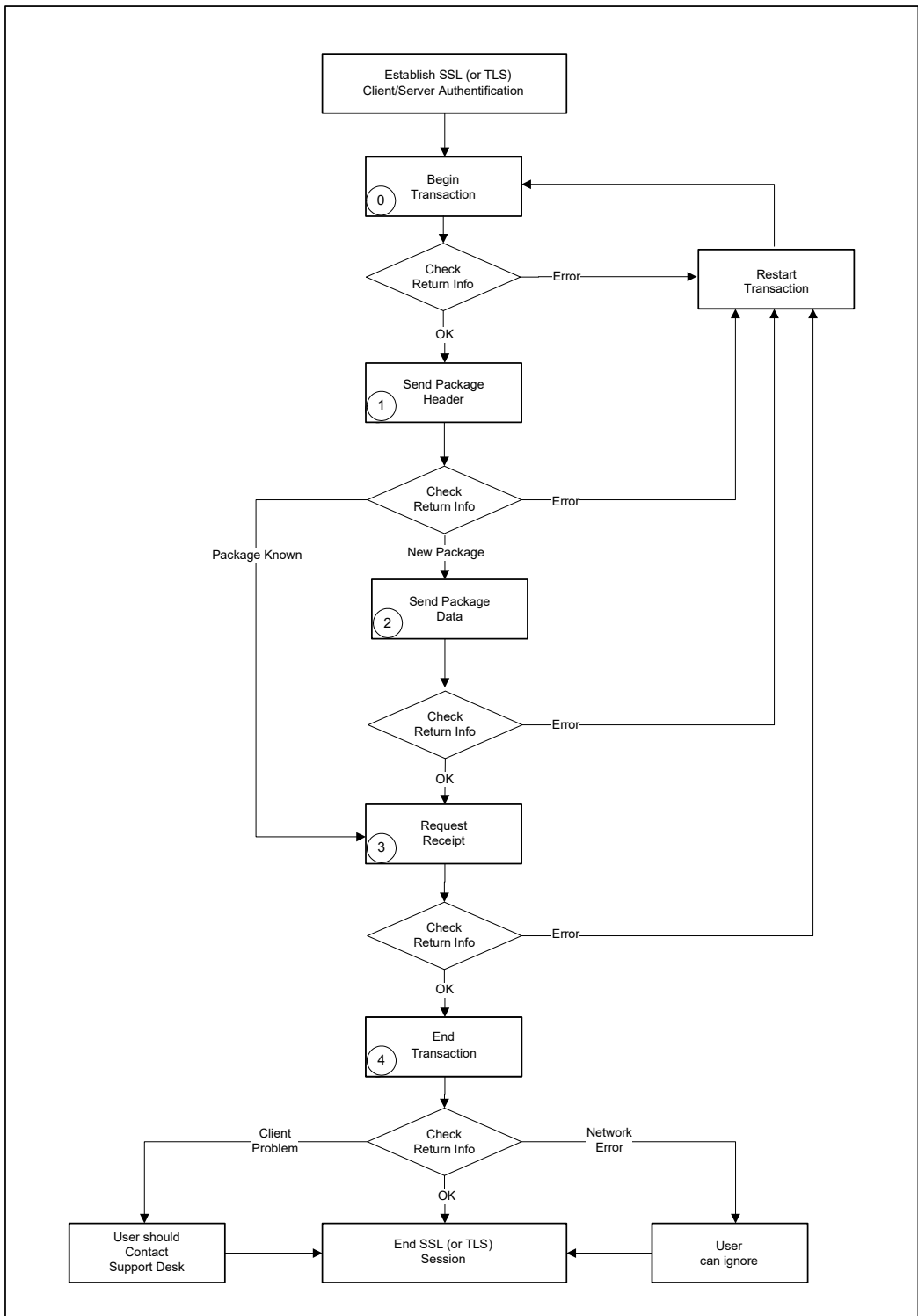
Figure 5 – Application level protocol behavior for application

5.1.3   Application layer protocol for notification

At the highest level for notification, there are five events that the protocol requires a client and server to support[9]. These events are:[10]

    (a)   Begin Transaction

    (b)   Get Package Header (for notification, or dispatch list, or application receipt list)[11]

    (c)   Get Package Data (for notification, or dispatch list, or application receipt list)[12]

    (d)   Send Receipt Check Notice (for notification, or dispatch list, or application receipt list)[12]

    (e)   End Transaction

In between the Begin and End Transactions, there are two types of WASP and one type of C-WASP sent between the client and the server:

    (i)   The client action package header contains essential information for initial processing to identify the request for notification. It is a WASP containing the package header in XML format. (This is applied to request to a server from a client.)

    (ii)   The server response package header contains summary information (such as a dispatch-number and the number of notifications to be sent) on the notification to be notified. It is a WASP containing the package header in XML format. (This is applied to response to a client from server.)

    (iii)   The package data contains the dispatched notification information. It is a C-WASP that consists of one or more WASP(s).

5.1.3.1   Use of the SSL (or TLS) tunnel for notification

Refer to Section 5.1.2.1, "Use of the SSL (or TLS) tunnel for application."

5.1.3.2   Application level events for notification

Start SSL (or TLS) session (see Figure 6)

Step 0: Begin Transaction

---

[9]   The Office may inform the applicant of the existence of notifications before these five events, by other means of communication, such as e-mail.

[10]   This protocol may be used to transmit the dispatch list, the application receipt list, and the notification. Transmission of the dispatch list, the application receipt list, and the notification is supported at the discretion of the Office. The dispatch list contains dispatch numbers corresponding to notifications that the Office has sent to the applicant. The application receipt list contains application numbers corresponding to application documents that the Office has received from the applicant.

[11]   The server uses the value of the"transaction-type" attribute (see section 5.1.4) to identify the type of document requested, e.g. notification, dispatch list, application receipt list.

Client action:

Get transaction Information.

Server response:

Return values in the *transaction_id and max_division_size* transaction management header elements.

transaction_id is a unique identifier assigned by the server associating all transactions involved in sending a notification.

max_division_size is the maximum number of bytes permitted by the server for the size of a division.

Step 1: Get Package Header

Client action:

Send request for package header (The WASP of package header for request of notification is contained.)

Server response:

a) OK (The response contains the WASP of package header containing summary information (such as dispatch-number, number-of-notification) of notifications.)[12]

b) Error (Abort, go back to step 0)

After receiving the last division of the WASP containing the package header, the server must verify the signature of the WASP. If the signature is invalid (for instance, due to a signature verification error or validation data expiration), the application response code (ARC) value is set to FFF6.

If the number of sendable notifications in package header of Server response is "0(zero)" (there is no sendable notifications), then go to Step 4.

Step 2: Get Package Data

Client action:

Send request for Package data

Server response:

a) OK (The response contains the C-WASP consisted of one or more WASP(s))

b) Error (Abort, go back to step 0)

Step 3: Send Receipt Check Notice

Client action:

Send Receipt Check Notice

Server response:

a) OK

b) Error (Abort, go back to step 0)

---

[12]   If the C-WASP contains multiple WASP, the notice-info of each notification is set in the package header.

Step 4: End Transaction.
> *Client action:*
>> Send acknowledgment of completion including information about any client problem to the server.
>
> *Server response:*
>> a) OK
>> b) Error (Client can ignore this response)

Close SSL (or TLS) session

In all cases of SSL (or TLS) Tunnel, the current protocol requires that, for each transaction, the client acknowledge the reception by sending Receipt Check Notice to the server.
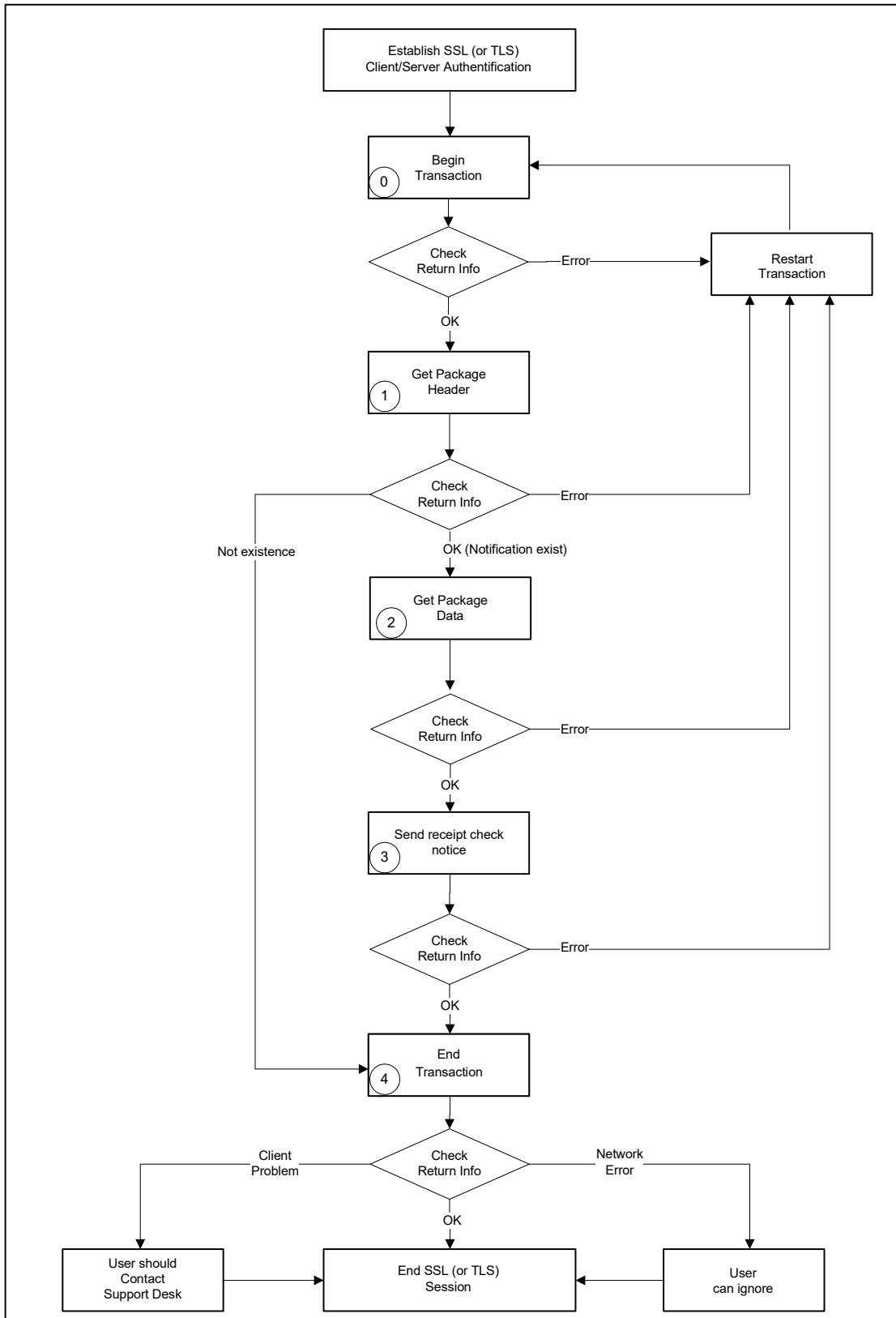
Figure 6 – Application level protocol behavior for notification

5.1.4   Transaction management header elements

The following items, which are all fixed length, are included in all post and response messages. Unused parameters of header elements are set to space (ASCII '20').

Attrib. Name	division_hash
Values	ASCII upper case Hexadecimal representation of 160-bit hash value
Length	40 bytes (40 x 8bit characters)
Description	SHA-1 Hash of the current division (will be "white space" or blank when SHA-1 is not used).

Attrib. Name	protocol_version
Values	Unique
Length	4 bytes (4 x 8bit ASCII char)
Description	A unique identifier for the version of the protocol used to create the transaction data (e.g. 0100 for Version 1.0) First two bytes are for the major version number and last two for the release within this version.

Attrib. Name	transaction_type	
Values	pbeg, ebeg,	
	pend, eend	
	ehdr, phdr,	
	edat, pdat,	
	erct, prct,	
	ephn, pphn	Get package header for notification
	epdn, ppdn	Get package data for notification
	ercn, prcn	Send receipt check notice for notification
	ephd, pphd	Get package header for dispatch list
	epdd, ppdd	Get package data for dispatch list
	ercd, prcd	Send receipt check notice for dispatch list
	epha, ppha	Get package header for application receipt list
	epda, ppda	Get package data for application receipt list
	erca, prca	Send receipt check notice for application receipt list
	ASCII lower case 7-bit ISO 646 e-stands for encrypted, p-plain text	
Length	4 bytes	
Description	Attrib. of the transaction header that identifies the nature of the data transmitted. The value beginning with letter d or z is not available.	

Note that the value beginning with the letter d or z is reserved for domestic application or the other transmission.

Attrib. Name	transaction_id
Values	Unique
Length	36 bytes
Description	A unique identifier assigned by the server associating all transactions involved in the submission of an application. For Begin Transaction this is blank (ASCII x'20').

Attrib. Name	reserved_use
Values	Reserved for domestic use (e.g. Server date and time YYYYMMDDHHMMSS)
Length	32 bytes
Description	This data area is available for the option by each RO. (e.g. To inform a client of the machine time of the RO server).

Attrib. Name	total_bytes
Values	Numeric ASCII with left-hand zero padding (e.g. 0000000123456789)
Length	16 bytes (16 x 8bit chars)
Description	The total size in bytes of the object being sent (WASP containing the Package Header, WASP containing the package data, and the WASP containing the receipt).

Attrib. Name	division_size
Values	Numeric ASCII with left-hand zero padding (e.g. 0000000123456789)
Length	16 bytes (16 x 8bit chars)
Description	The size in bytes of the data component (chunk) of the object being transferred.

Attrib. Name	division_offset
Values	Numeric ASCII with left-hand zero padding (e.g. 0000000123456789)
Length	16 bytes (16 x 8bit chars)
Description	Value representing the starting position of the data within the object being transferred. Division_offset starts at 0.

Attrib. Name	division_response_code	
Values	**Division RCs** / **Meaning**	
	0000	OK
	FFFF	General Error
	FFFE	Resend Last
	FFFD	Wait
	FFFC	Protocol Sequence Error
	ASCII 4 x 8bit char	
Length	4 bytes	
Description	Server or client return code used to manage the division mechanism	

Attrib. Name	application_response_code		
Values		*Application RCs*	*Meaning*
		0000	OK
		FFFF	General Error
		0001	OK, Package Known
		0002	OK, New Package
		0003	OK, Not Existence
		1000	Pending
		FFFB	Client Problem
		FFFA	Network Error
		FFF9	Protocol Version Error
		FFF8	Hash Value of "division hash" in the Transaction Management Header is erroneous.
		FFF7	The hash values in package header and the WAD of package data do not match.
		FFF6	The signature is invalid (for instance, due to a signature verification error or validation data expiration).[13]
	ASCII 4 x 8bit char		
Length	4 bytes		
Description	Server or client return code used to manage the application level events		

Attrib. Name	encoding_method		
Values		*Application RCs*	*Meaning*
		UTF8	UNICODE UTF8
		SJIS	UNICODE Shift-JIS
		KS X	UNICODE KS X 1001
	ASCII 4 x 8bit char		
Length	4 bytes		
Description	Encoding scheme for error message translation.		

Attrib. Name	error_message
Values	UNICODE UTF8, UNICODE Shift-JIS, UNICODE KS X 1001
Length	256 bytes (256 x 8bits)
Description	Optional text explaining the reason for error response codes. If an error message is needed for both division and application response codes, these should be concatenated. Each server will choose one of the specified encoding schemes to translate the error message into human readable format.

---

[13] This code is applied when the server cannot verify the authentication in Get package header.

Attrib. Name	Algorithm_name
Values	ASCII with right-hand space padding
Length	10 bytes (10 x 8bit chars)
Description	the name of algorithm used, example: SHA-256

Attrib. Name	division_hash2_length
Values	ASCII with left-hand zero padding
Length	4 bytes (4 x 8bit chars)
Description	length of division_hash2.

Attrib. Name	division_hash2
Values	ASCII upper case Hexadecimal representation
Length	variable length (length specified by division_hash2_length)
Description	hash value computed with the algorithm specified by algorithm name

5.1.5   Transaction management data elements

Attrib. Name	max_division_size
Values	Numeric ASCII with left-hand zero padding
Length	16 bytes (16 x 8bit chars)
Description	Maximum bytes allowed for a division.
Example	0000000000008192 (8Kbytes)

5.1.6   Server parameters

Attrib. Name	server_timeout
Values	Numeric ASCII with left-hand zero padding (e.g. 0000000123456789)
Length	16 bytes (16 x 8bit chars)
Description	Time in seconds before the server can assume that a client has lost its network connection and the transaction can be abandoned.
Example	0000000000000120 (2 minutes)

Note that the value for the server_timeout at the protocol level is set at the discretion of the individual Office.

5.1.7   Client parameters

Attrib. Name	client_preferred_division_size
Values	Numeric ASCII with left-hand zero padding
Length	16 bytes (16 x 8bit chars)
Description	Preferred number of bytes to be used for a division.
Example	0000000000004096 (8k)

Attrib. Name	client_retry_limit
Values	Numeric ASCII with left-hand zero padding
Length	16 bytes (16 x 8bit chars)
Description	Number of times the client should resend a division before abandoning the transaction
Example	0000000000000005 (5 retries)

Note that the maximum number of Attrib. Client_retry_limit is NN (16 times). When a server retries more than 16 times, the transmission may be terminated.

Attrib. Name	client_retry_wait
Values	Numeric ASCII with left-hand zero padding (e.g. 0000000123456789)
Length	16 bytes (16 x 8bit chars)
Description	The time in seconds the client should wait before issuing a retry
Example	0000000000000005 (5 secs)

Note that the value for the client_retry_wait at the protocol level is set at the application level.

5.1.8 Division mechanism

When sending data between the client and server, this data is divided into manageable chunks which, together with a transaction management header, are called divisions. Under the control of the client, the size of these divisions can vary during the life of the transactions. This provides a pacing mechanism that can be used to overcome Internet transmission problems.

The initial size of the division data message is set to the smallest of either:

(a)   max_division_size returned by the server as a response to the Begin Transaction Request

(b)   client_preferred_division_size set in the startup parameters of the client

The client builds one or more divisions made up of the transmission management header and a data message. As each division is sent in the divided order to the server, the server checks for completeness of the transmission by calculating the hash value of the division.

5.1.8.1 Calculating the division hash value

The hash is calculated on the basis of all fields in the header as well as any data message. The hash, which is calculated using the SHA-1 algorithm, is placed as the first element of each division. However, if the algorithm used is other than SHA-1, all space is set to division_hash and the hash value computed with the algorithm specified by algorithm_name is set to division_hash2.

Before the server rejects a package as invalid, it should check the version of the protocol before checking the hash value in case a future version of the protocol should adopt a different hash algorithm.

The following fields of the HTTP Post or response message are therefore included in the hash calculation:

Name	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application rc	Encoding method	Error message	Data message
Length	4	4	36	32	16	16	16	4	4	4	256	???

5.1.9 Event level protocol

Transactions described in this section are further illustrated in Figure 7 to 12 below.

5.1.9.1 Begin transaction

The Begin Transaction post message submitted by the client contains the highest protocol version supported by the client. If the server supports the version provided by the client, it should communicate with the client in accordance with the rules for that version of the protocol and use that version number in all response messages. If the server cannot support the protocol version specified by the client, the application response code should indicate protocol version error, and the version number specified in the response message should be the highest protocol version supported by the server. The client should support earlier versions.

Post Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	0
Value	X	0100	pbeg	blank	???	0	0	0	0	0	???	blank	none

Response Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	16
Value	X	0100	pbeg	new id	???	16	16	0	0	0	???	???	???

Data Message: max_division_size (16 bytes)

Post Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	pbeg	blank	???	0	0	0	0	0	???	blank	none	???	???	x

Response Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	pbeg	new id	???	16	16	0	0	0	???	???	???	???	???	x

Data Message: max_division_size (16 bytes)

5.1.9.2   Send package header

Post Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	???
Value	X	0100	phdr	tranid	???	X	Y	Z	0	0	???	blank	pkghdr

Data Message: WASP containing package header

Response Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	0
Value	X	0100	phdr	tranid	???	0	0	0	a	b	???	blank	none

Post Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	phdr	tranid	???	x	y	z	0	0	???	blank	pkghdr	???	???	x

Data Message: WASP containing package header

Response Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	phdr	tranid	???	16	16	0	a	b	???	blank	none	???	???	x

5.1.9.3   Send package data

Post Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	???
Value	X	0100	pdat	tranid	???	x	y	z	0	0	???	blank	pkgdata

Data Message: WASP containing package data

Response Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	0
Value	X	0100	pdat	tranid	???	0	0	0	a	b	???	blank	none

Post Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	pdat	tranid	???	x	y	z	0	0	???	blank	pkgdata	???	???	x

Data Message: WASP containing package data

Response Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	pdat	tranid	???	0	0	0	a	b	???	blank	none	???	???	x

5.1.9.4   Get receipt

Post Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	0
Value	x	0100	prct	tranid	???	0	0	0	???	0	???	blank	none

Response Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	???
Value	x	0100	prct	tranid	???	x	y	z	???	0	???	blank	receipt

Data Message: WASP containing receipt

Post Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	prct	tranid	???	0	0	0	???	0	???	blank	none	???	???	x

Response Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	prct	tranid	???	x	y	z	???	0	???	blank	receipt	???	???	x

Data Message: WASP containing receipt

5.1.9.5   End transaction

Post Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	0
Value	x	0100	pend	tranid	???	0	0	0	0	0	???	blank	none

Response Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	0
Value	x	0100	pend	tranid	???	0	0	0	a	b	???	???	none

Post Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	pend	tranid	???	0	0	0	0	0	???	blank	none	???	???	x

Response Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	pend	tranid	???	0	0	0	a	b	???	???	none	???	???	x

5.1.9.6 *Get package header for notification*

Post Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	???
Value	x	0100	pphn	tranid	???	x	y	z	a	b	???	blank	pkghdr

Data Message: WASP containing package header

Response Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	0
Value	X	0100	pphn	tranid	???	x	y	z	a	b	???	blank	pkghdr

Data Message: WASP containing package header

Post Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	pphn	tranid	???	x	y	z	a	b	???	blank	pkghdr	???	???	x

Data Message: WASP containing package header

Response Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	pphn	tranid	???	x	y	z	a	b	???	blank	pkghdr	???	???	x

Data Message: WASP containing package header

5.1.9.7 *Get package data for notification*

Post Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	0
Value	x	0100	ppdn	tranid	???	0	0	0	a	b	???	blank	none

Response Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	???
Value	x	0100	ppdn	tranid	???	x	y	Z	0	0	???	blank	pkgdata

Data Message: C-WASP containing WASP

Post Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	ppdn	tranid	???	0	0	0	a	b	???	blank	none	???	???	x

Response Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	ppdn	tranid	???	x	y	z	0	0	???	blank	pkgdata	???	???	x

Data Message: C-WASP containing WASP

5.1.9.8 *Send receipt check notice for notification*

Post Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	0
Value	x	0100	prcn	tranid	???	0	0	0	0	0	???	blank	none

Response Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	0
Value	x	0100	prcn	tranid	???	0	0	0	a	b	???	blank	none

Post Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	prcn	tranid	???	0	0	0	0	0	???	blank	none	???	???	x

Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	prcn	tranid	???	0	0	0	a	b	???	blank	none	???	???	x

5.1.9.9 Get package header for dispatch list

Post Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	???
Value	x	0100	pphd	tranid	???	x	y	z	a	b	???	blank	pkghdr

Data Message: WASP containing package header

Response Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	0
Value	x	0100	pphd	tranid	???	x	y	z	a	b	???	blank	pkghdr

Data Message: WASP containing package header

Post Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	pphd	tranid	???	x	y	z	a	b	???	blank	pkghdr	???	???	x

Data Message: WASP containing package header

Response Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	pphd	tranid	???	x	y	z	a	b	???	blank	pkghdr	???	???	x

Data Message: WASP containing package header

5.1.9.10   Get package data for dispatch list

Post Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	0
Value	x	0100	ppdd	tranid	???	0	0	0	a	b	???	blank	none

Response Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	???
Value	x	0100	ppdd	tranid	???	x	y	z	0	0	???	blank	pkgdata

Data Message: C-WASP containing WASP

Post Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	ppdd	tranid	???	0	0	0	a	b	???	blank	none	???	???	x

Response Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	ppdd	tranid	???	x	y	z	0	0	???	blank	pkgdata	???	???	x

Data Message: C-WASP containing WASP

5.1.9.11   Send receipt check notice for dispatch list

Post Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	0
Value	x	0100	prcd	tranid	???	0	0	0	0	0	???	blank	none

Response Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	0
Value	x	0100	prcd	tranid	???	0	0	0	a	b	???	blank	none

Post Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	prcd	tranid	???	0	0	0	0	0	???	blank	none	???	???	x

Response Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	prcd	tranid	???	0	0	0	a	b	???	blank	none	???	???	x

5.1.9.12   Get Package header for application receipt list

Post Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	???
Value	x	0100	ppha	tranid	???	x	y	z	a	b	???	blank	pkghdr

Data Message: WASP containing package header

Response Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	0
Value	x	0100	ppha	tranid	???	x	y	z	a	b	???	blank	pkghdr

Data Message: WASP containing package header

Post Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	ppha	tranid	???	x	y	z	a	b	???	blank	pkghdr	???	???	x

Data Message: WASP containing package header

Response Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	ppha	tranid	???	x	y	z	a	b	???	blank	pkghdr	???	???	x

Data Message: WASP containing package header

5.1.9.13   Get package data for application receipt list

Post Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	0
Value	x	0100	ppda	tranid	???	0	0	0	a	b	???	blank	none

Response Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	???
Value	x	0100	ppda	tranid	???	x	y	z	0	0	???	blank	pkgdata

Data Message: C-WASP containing WASP

Post Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	ppda	tranid	???	0	0	0	a	b	???	blank	none	???	???	x

Response Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	ppda	tranid	???	x	y	z	0	0	???	blank	pkgdata	???	???	x

Data Message: C-WASP containing WASP

5.1.9.14   Send receipt check notice for application receipt list

Post Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	0
Value	x	0100	prca	tranid	???	0	0	0	0	0	???	blank	none

Response Message

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message
Length	40	4	4	36	32	16	16	16	4	4	4	256	0
Value	x	0100	prca	tranid	???	0	0	0	a	b	???	blank	none

Post Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	prca	tranid	???	0	0	0	0	0	???	blank	none	???	???	x

Response Message, protocol 2.0

Name	Division hash	Protocol version	Transaction type	Transaction id	Reserved use	Total bytes	Division size	Division offset	Division RC	Application RC	Encoding method	Error message	Data message	Algorithm name	Division hash 2 length	Division hash 2
Length	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Value	**blank**	**0200**	prca	tranid	???	0	0	0	a	b	???	blank	none	???	???	x

Fatal
Error
(FFFF)

Start

Fatal
Error
(FFFF)

Event
End
OK

Build
Transmission
Header

No

Yes

Yes

Is there
any more
data?

Add up to division_size
bytes as message_data

Is
client_retry_limit
exceeded?

Client

No

Client
sends HTTP
POST Request

Server sets
Application
Response Code

"Pending"
(1000)

Server checks
Completeness of
Division

Server sets
Application
Response Code

"Hash Error"
(FFF8)

Server

Server sets
Application
Response Code

"New Package"
(0002)
"Package Known"
(0001)

Is division
OK?

No

No

Yes

Yes

Is Application
Event complete?

Server sets
Division
Response Code

"Resend Last Division"
(FFFE)

Server sets
Division
Response Code

"OK"
(0000)

Figure 7 – Send package header behavior
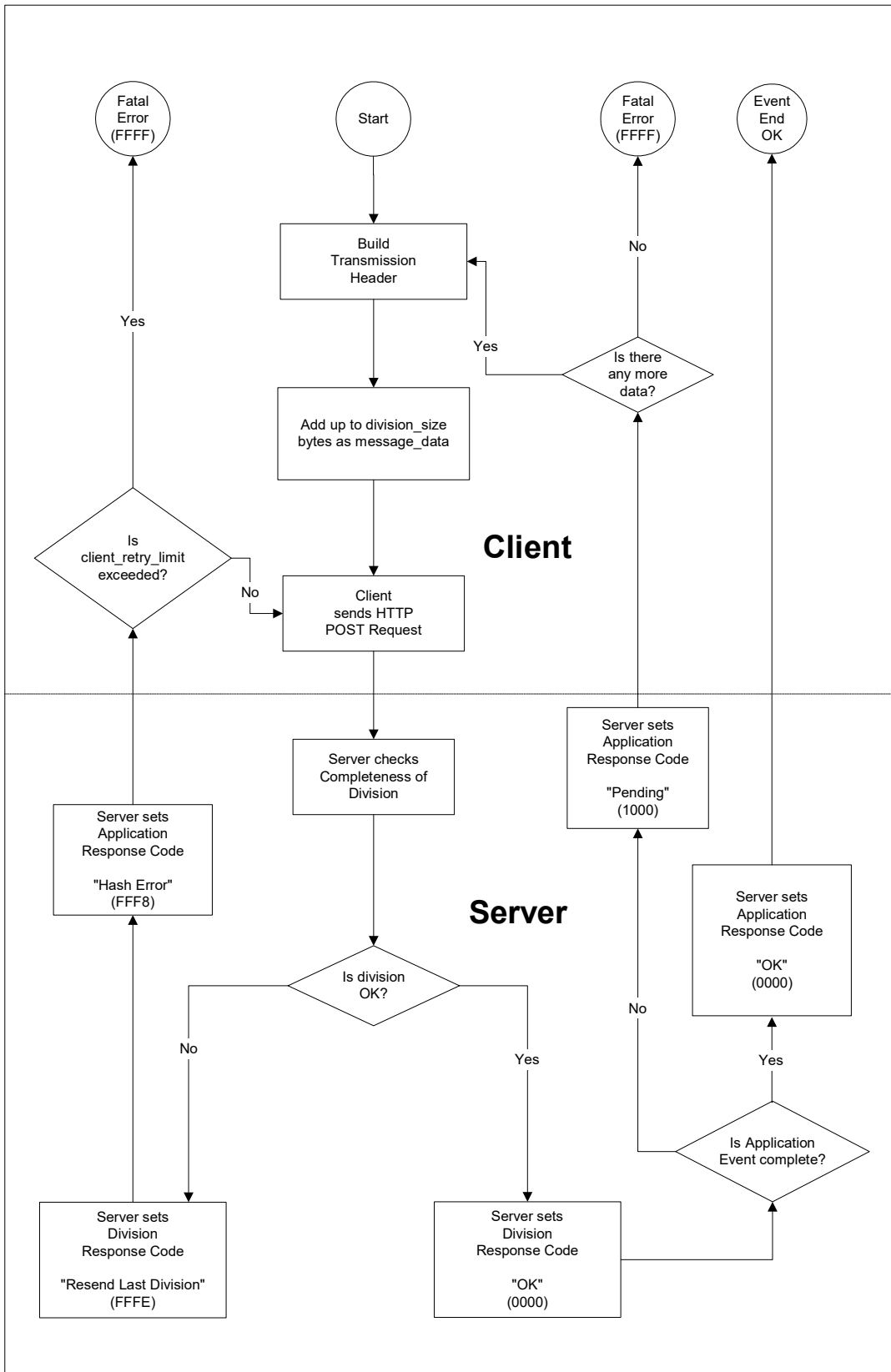
Figure 8 – Send package data behavior
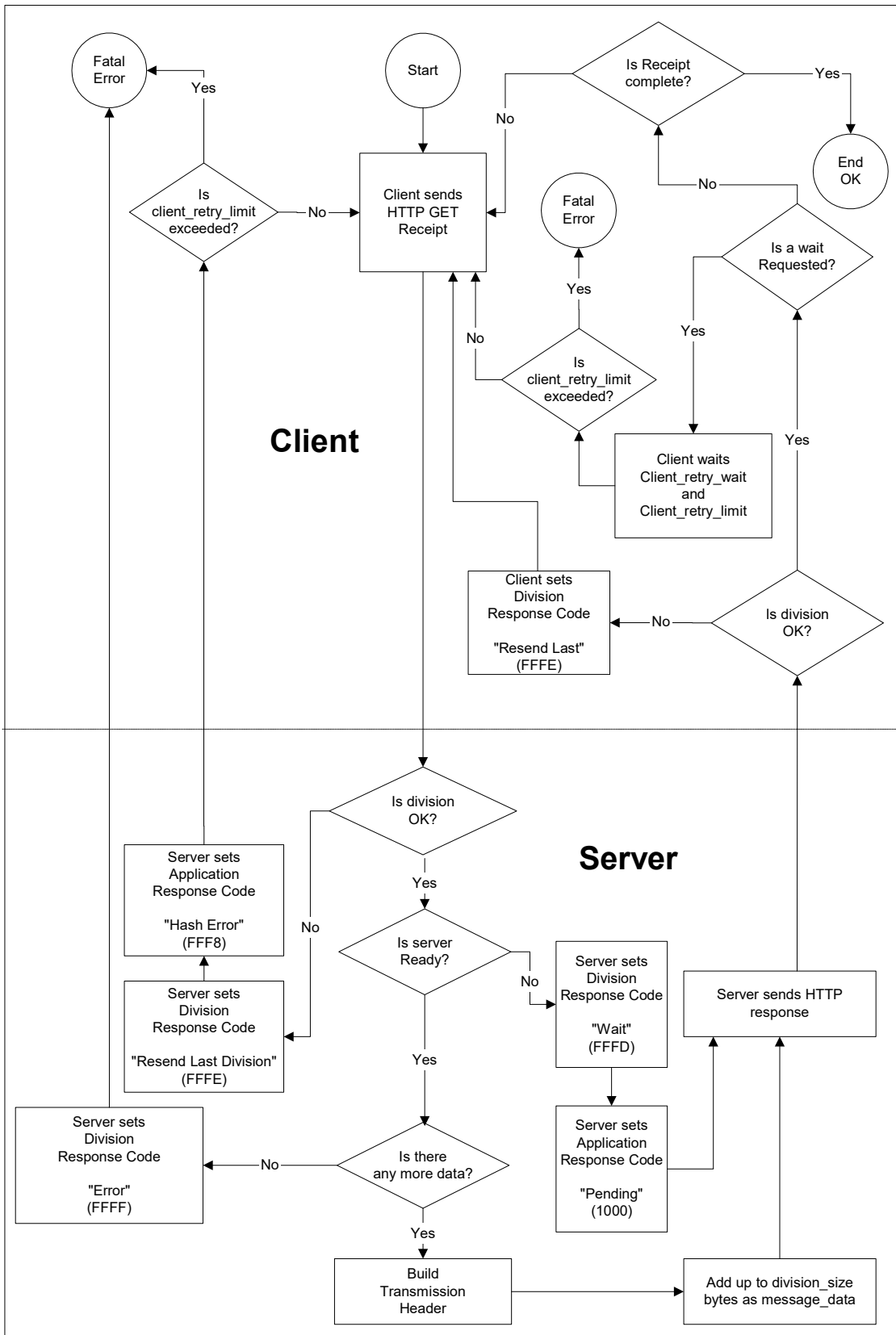
Figure 9 – Get receipt behavior
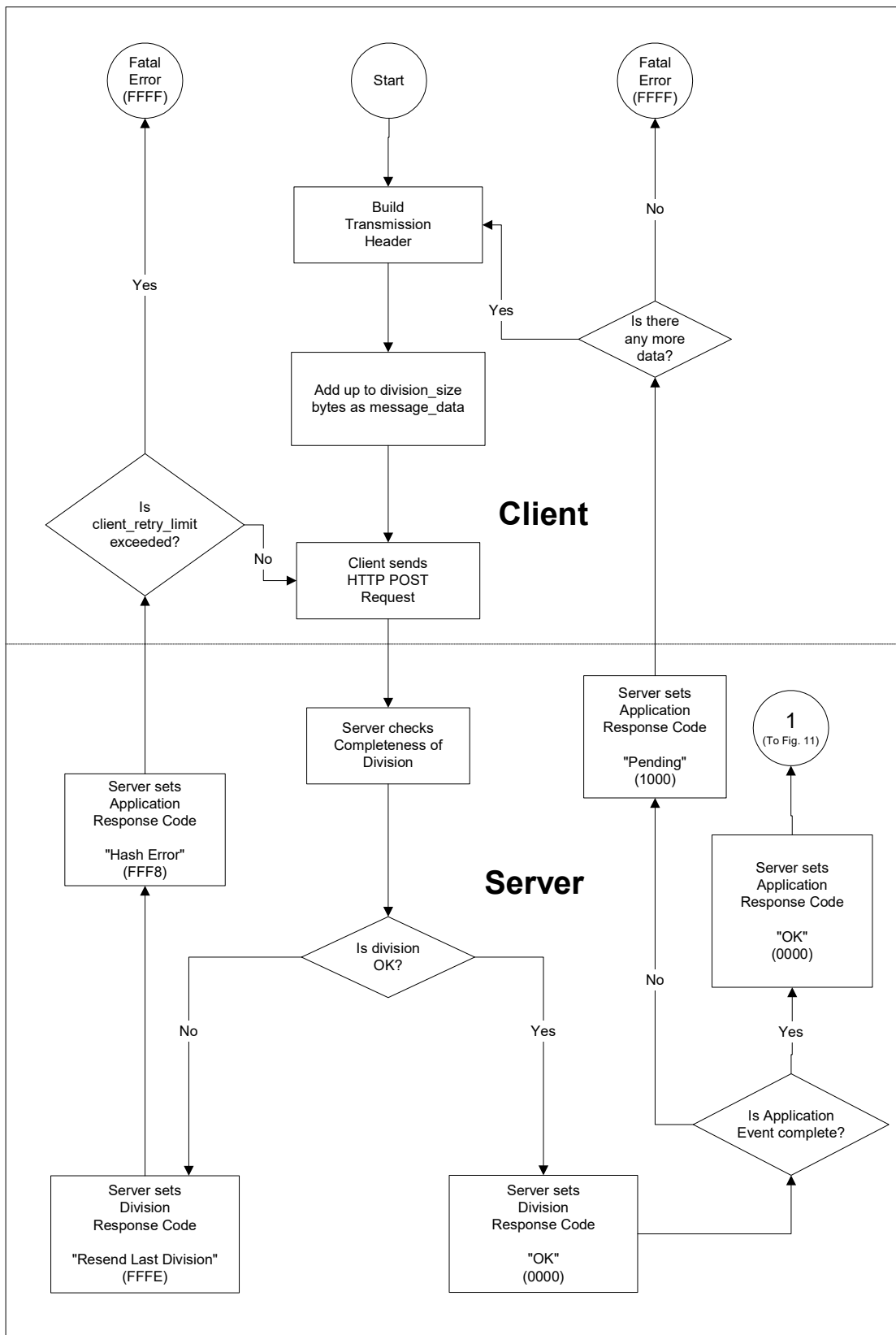
Figure 10 – Get package header behavior <upstream>
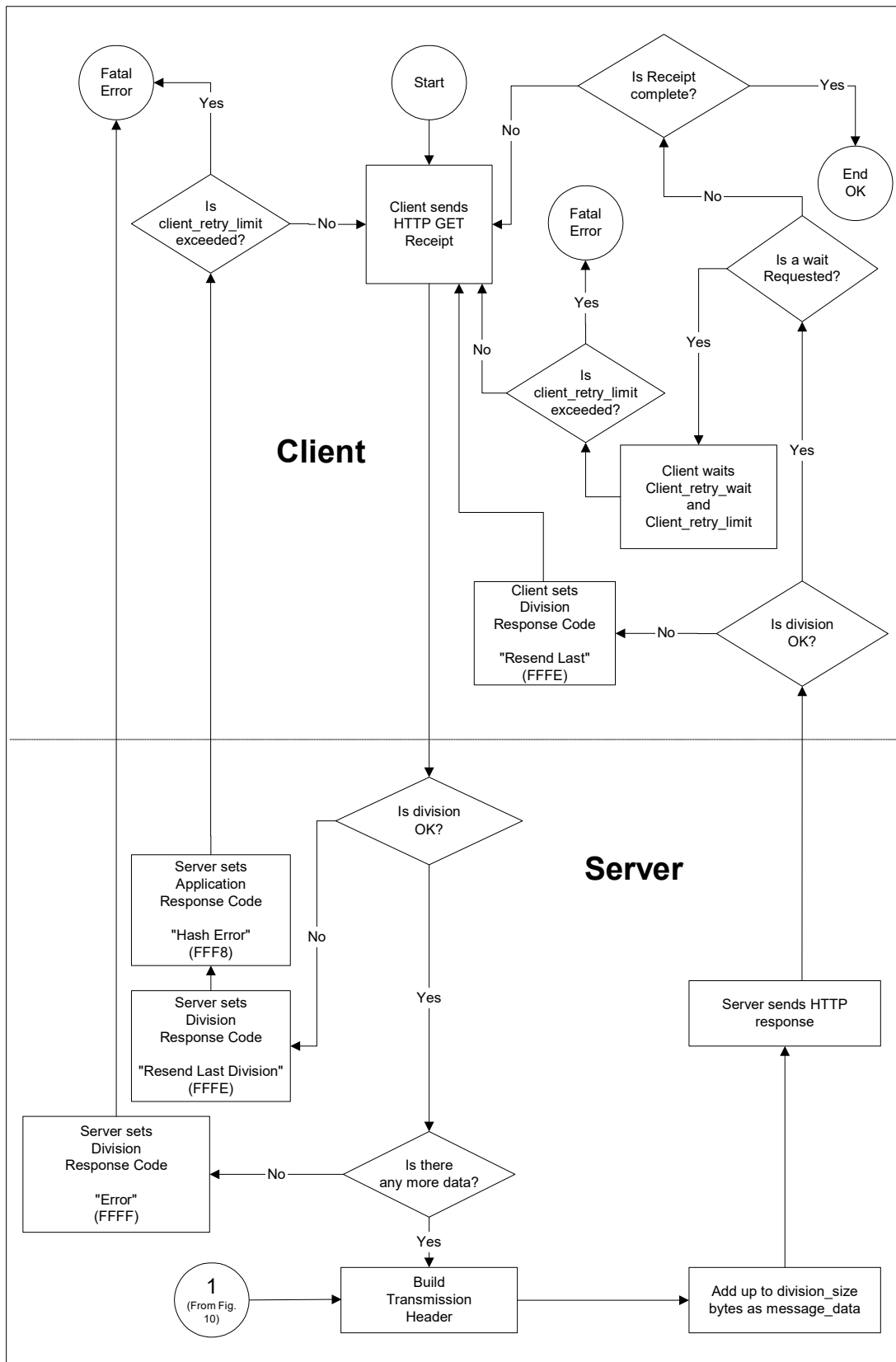
Figure 11 – Get package header behavior <downstream>
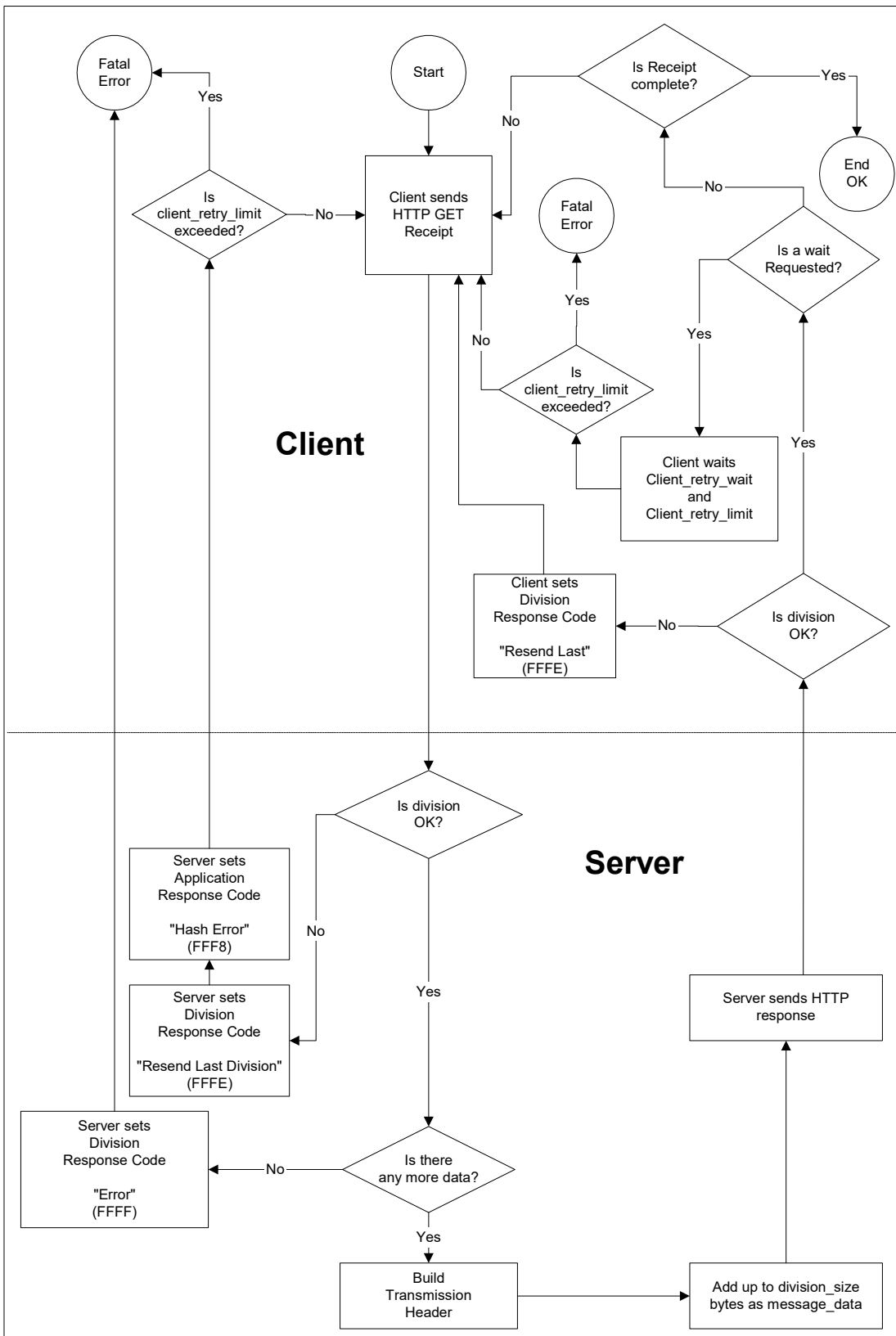
Figure 12 – Get package data behavior

5.1bis   Alternative means of online transmission

Alternative means of online transmission may be used, in agreement with the International Bureau, by Offices which do not use the E-filing interoperability protocol, provided that:

(a) interoperability between the existing PCT E-filing client and server software is maintained without needing further technical intervention; and

(b) the outcome of the transmission is equivalent to the outcome of the E-filing interoperability protocol (in particular in terms of receipt and level of security provided).

5.1ter   Alternative means of secure online transmission by recipient retrieval

Offices offering electronic transmission of documents through online retrieval by a recipient (either the applicant or Office processing the application) should use a secure protocol. Unless the applicant has explicitly requested an alternative arrangement (such as transmission of documents directly by email), transmission should use a connection protected by a modern, secure version of TLS or an alternative protocol of similar security mandated by national law, and a means appropriate to the sensitivity of the documents concerned to ensure that the documents can be retrieved only by authorized persons.

A preferred implementation involves:

(a) the international application being associated with one or more accounts with the Office, secured by two-factor authentication;

(b) notifications being sent to the recipient when a document becomes available, either using email to the recipient or, where so agreed with the recipient, by the recipient regularly accessing a secure list of newly available documents provided through an associated account, either manually through a secure browser connection or automatically through a RESTful secure web service;

(c) the recipient downloading such documents from an associated account, either manually through a secure browser connection or automatically through a RESTful secure web service.

The association between the international application and any applicant account should preferably be set up using information provided by the applicant at the time of filing using compatible online filing software. Offices should also provide secure means for adding, removing or modifying such associations after filing.

5.2   Package/transmission combinations

This section describes the permissible package/transmission combinations, for each of the PCT communication sectors. This standard does not preclude provision of publicly available information by means other than those covered in the standard. Further packaging types (e.g., web-based document delivery) and package/transmission options may become available in the future.

5.2.1   Applicant-Office communication (international phase) sector

In this sector, IA documents may be filed by online means (using PKI) over a secure channel or transmitted off-line (using PKI or non-PKI) on physical media. The option of online filing of an international application utilizing a non-PKI method is not presently permitted, except under transitional reservations notified under AIs Section 703(f).

Figure 13 shows a matrix of the package/transmission combinations that are permissible in this sector:

(a)   Online/over a secure channel: a WASP or C-WASP must be used. This is defined as a telecommunication connection established to exchange data over a network which includes: (i) a private network; (ii) the Internet using channel level encryption (e.g. SSL (or TLS)); (iii) a Virtual Private Network (VPN) connection over the Internet.

(b)   Off-line/on a physical medium: a WASP, C-WASP or WAD package must be used. Physical media (e.g., diskette, CD-ROM, DVD, etc.) are used to store IA data with no real-time data exchange.

Figure 13 - Package/transmission combinations permitted in
the Applicant-Office communication (international phase)
sector

5.2.2   Office-Office communication sector

In this sector, IA documents may be exchanged by online means over a secure channel or off-line on a physical medium. Note that, in this sector, where the sending Office and the recipient Office have agreed, in accordance with section 4, not to package IA documents filed on paper and converted into electronic form, or to package such documents in a different manner, different types of combinations for IA documents filed on paper and converted into electronic form may be applicable.

Figure 14 shows a matrix of the package/transmission combinations that are permissible in this sector:

(a)   Online/over a secure channel: a WASP or WAD must be used. This is defined as a telecommunication connection established to exchange data, over a network

which includes: (i) a private network; (ii) the Internet using channel level encryption (e.g. SSL (or TLS)); (iii) a Virtual Private Network (VPN) connection over the Internet.

(b)   Off-line/physical media: a WASP or WAD must be used. Physical media (e.g. diskette, CD-ROM, DVD, etc.) is used to store IA data with no real-time data exchange.

Figure 14 - Package/transmission combinations permitted in the Office-Office communication sector

The electronic package prepared by the sending Office which contains all relevant documents and data (see Figures 2 and 2*bis* in section 3.2, and Figures 14*bis* and 14*ter*, below) and is sent to the recipient Office is identified by an indication of the capacity in which the Office acts (RO, IB, ISA or IPEA), as follows:

- "RO Package" for any package prepared by the receiving Office,

- "IB Package" for any package prepared by the International Bureau,

- "ISA Package" for any package prepared by the ISA, and

- "IPEA Package" for any package prepared by the IPEA.

The figures below show examples of RO Packages containing record copies as they should be sent to the International Bureau. Figure 14*bis* shows a record copy of an international application which was filed in PDF format; in this case, the working copy should contain converted TIFF images (see section 3.1.2, last paragraph, above). Figure 14*ter* shows a record copy of an international application which was filed in XML format; in this case, there is no need for the working copy to contain converted TIFF images. The working copy referred to in this paragraph shall be construed as the part of the RO Package that is produced by the RO, in addition to the electronic package received from the applicant ("Applicant Package"), by copying, converting or modifying the documents contained in the Applicant Package (for example, request.xml) or by generating new documents (for example, ex-officio-corrections.xml).
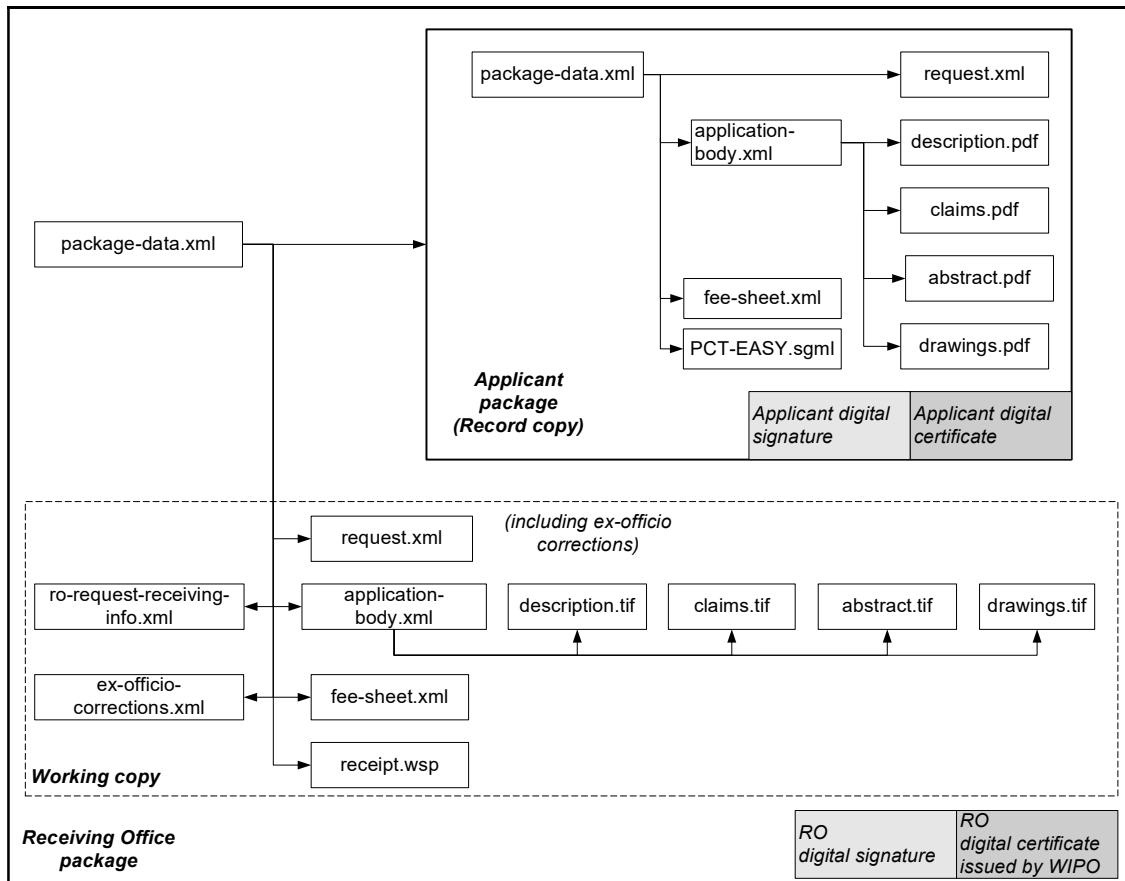
Figure 14*bis* - Example of RO Package containing a record copy where the text of the description, claims and abstract is not in character coded format (but in PDF format)
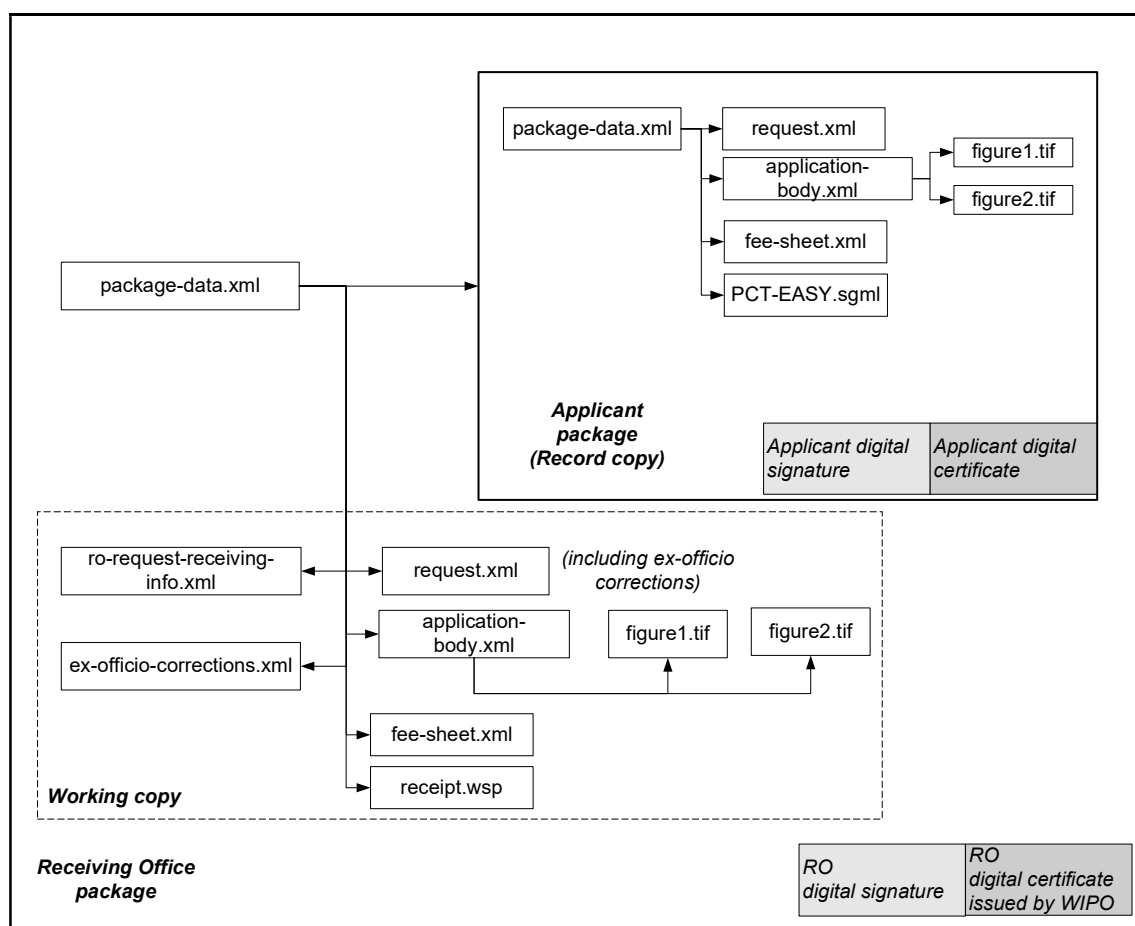
Figure 14*ter* - Example of RO Package containing a record copy where the text of the description, claims and abstract is in character coded format (in XML format)

5.2.3 *Designated Office communication sector*

In this sector, IA documents may be exchanged by online means over a secure channel, off-line on a physical medium or, as regards documents of a non-confidential nature, over the Internet.

Figure 15 shows a matrix of the package/transmission combinations that are permissible in this sector:

(a) Online/Internet: a WASP or WAD must be used. This package/transmission combination is permissible only for the transmittal of documents of a non-confidential nature.

(b) Online/over a secure channel: a WASP or WAD must be used. This is defined as a telecommunication connection established to exchange data, over a network which includes: (i) a private network; (ii) the Internet using channel level encryption (e.g., SSL (or TLS)); (iii) a Virtual Private Network (VPN) connection over the Internet.

(c) Off-line/on a physical medium: a WASP or WAD must be used. Physical media (e.g., diskette, CD-ROM, DVD, etc.) are used to store IA data with no real-time data exchange.
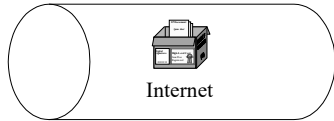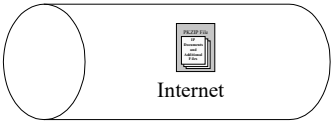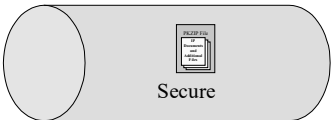
Figure 15 - Package/transmission combinations permitted in designated Office communication sector[14]

6. ELECTRONIC FILING SOFTWARE

The International Bureau provides software[15] that supports all of the requirements of the basic common standard and certain alternatives available under Annex F. Use of this software is not mandatory but any applicant may choose to use it, in which case the receiving Office must accept the international application concerned (except where it has notified a transitional reservation under AIs Section 703(f) in that respect). Any receiving Office may also specify other filing software acceptable to it.

7. *[Deleted]*

8. PRINCIPLES OF ELECTRONIC RECORDS MANAGEMENT

The change to electronic filing and processing of IA documents will have a great impact on records management practices. Since many of the conventions used with paper documents do not apply to electronic documents, new guidelines must be created to deal with the evolving issues of electronic information. This section sets out principles designed to support the requirements of authentication, integrity, confidentiality and non-repudiation for electronic records management of IA documents:

---

[14]   See section 5.2.3(a): only documents of a non-confidential nature may be exchanged over the Internet.

[15]   The current software provided by the International Bureau for this purpose is ePCT. However, for as long as the PCT-SAFE software is still available, any receiving Office may continue to accept PCT-SAFE or both ePCT and PCT-SAFE for this purpose.

(i)   all documents filed in electronic form shall be capable of being printed on paper, and transferred to an electronic records management system, without loss of content or material alteration;

(ii)   information that is routinely collected by the automated systems of an Office concerning the record's origin and destination, its context, and the date and time it was generated, sent or received, often called the document's "metadata," is to be considered part of the electronic records and is to be maintained by the automated systems; however, the requirement to maintain this data does not apply to any information whose sole purpose is to enable the record to be sent or received;

(iii)   electronic records shall be retained either in the electronic document format in which they are generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received;

(iv)   a mechanism shall be provided to ensure the authentication and integrity of the electronically filed document; this requires the ability to verify the identity of the submitter (the applicant or authorized representative responsible for the content of the document) or author of an Office document, as well as the ability to verify that a document has remained complete and unaltered within the system, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display;

(v)   electronic filing, processing and storage systems shall provide backup and recovery mechanisms to protect electronic records against system failures;

(vi)   electronic records shall be maintained for long-term access and retention in a manner that assures the accessibility of the information in a usable form for the required retention period;

(vii)   electronic records management systems shall provide mechanisms and procedures for quality assurance and quality control of the equipment and procedures used for receipt, processing and storage of the stored and managed documents;

(viii) electronic record management systems shall maintain an audit trail of all relevant information concerning additions, deletions or alterations to the electronic records management system and its records.

9.   ABBREVIATED EXPRESSIONS, INTERPRETATION AND GLOSSARY

In general, words and expressions used in the PCT, the Regulations and the Administrative Instructions have the same meaning in this Annex and are used without further explanation (for example, "international application," "request," "receiving Office," etc.).[16] Other terminology has the same meaning that it bears in the field of information technology. Certain terms of specific importance in this Annex are defined in the following paragraph.

---

[16]   See also footnotes 1, 2 and 4.

For the purposes of this Annex:

(a)   "basic electronic signature" means an electronic signature[17] which can be:

    (i)   a particular string of text entered by a user;

    (ii)   a facsimile image of the hand-written signature;

    (iii)   a "click-wrap" signature;

(b)   "enhanced electronic signature" means an electronic signature in respect of which it can be shown, through the use of a security procedure, that the signature:

    (i)   is unique to the signature holder within the context in which it is used;

    (ii)   was created, and attached to or logically associated with, the electronic document by the signature holder or using a means under the sole control of the signature holder and not by any other person;

    (iii)   was created and is linked to the electronic document to which it relates in a manner which provides reliable assurance as to the integrity of the document;

one implementation of an enhanced electronic signature is a "digital signature" which is produced using a PKI-generated certificate and corresponding private key;

(c)   "digital certificate" means a record issued by a certification authority and which identifies a person or entity who holds a particular key pair, in the context of public key infrastructure; for example, a digital certificate shall, amongst other requirements, identify the certification authority issuing it, identify its subscriber, contain the subscriber's public key, identify its period of validity, and be digitally signed by the certification authority issuing it;[18]

(d)   "certification authority" means an entity which issues digital certificates and provides other services related to electronic signatures, such as managing digital certificates and keys and maintaining a register of them;[19]

(e)   "low-level certificate" means a digital certificate which has been issued to the applicant, for example as part of the registration of the on-line filing client or obtained from a certification authority, and which identifies the applicant without prior verification of the applicant's identity;

(f)   "high-level certificate" means a digital certificate which has been issued to the applicant by a trusted party and which identifies the applicant with prior verification of the applicant's identity.

---

[17]   See AIs Section 701(iv).
[18]   See 'Certificate' in Appendix II, Glossary, for a list of minimum requirements for a digital certificate.
[19]   See 'Certification authority' in Appendix II, Glossary.

Fuller explanations of some of the following expressions and abbreviations appear in the main text of this Annex. See also Appendix II for terminology used in the context of PKI.

AIs	Administrative Instructions under the PCT
Applicant-Office communication (international phase) sector	see section 2.3.1 above
Applicant-Office communication (national phase) sector	see section 2.3.4 above
C-WASP	Compound WASP
designated Office communication sector	see section 2.3.3 above
DTD	document type definition
DO	designated Office
DO/EO	designated/elected Office
EO	elected Office
E-PCT	electronic PCT application standard
IA	international application
IB	International Bureau of WIPO
IETF	Internet Engineering Task Force
IPEA	International Preliminary Examining Authority
IPER	international preliminary examination report
ISA	International Searching Authority
ISR	international search report
ISDN	integrated services digital network
JFIF	JPEG file interchange format
JPEG	Joint Photograph Experts Group
Office	when used in a generic context: RO, ISA, IPEA, DO, EO, IB and/or national or regional industrial property Office
Office-Office communication sector	see section 2.3.2 above
PCT	Patent Cooperation Treaty
PKCS	public key cryptographic standard

PKI	public key infrastructure
Referenced document	file contained in the WAD package that is referred to (by means of its file name) in one or more documents in XML format contained in the same package
RFC	request for comments
RO	receiving Office
SSL	secure sockets layer
TCP/IP	Transmission Control Protocol / Internet Protocol
TIFF	tagged image file format
TLS	transport layer security
WAD	wrapped application documents
WASP	wrapped and signed package
WIPO	World Intellectual Property Organization
XML	eXtensible Mark-up Language

[Annex F, Appendix I, follows]

APPENDIX I
XML DTDS FOR THE E-PCT STANDARD

The contents of this Appendix are reproduced in document PCT/AI/DTD/6Rev. dated June 26, 2009, which is published, together with this document, on WIPO's web site at www.wipo.int/pct/en/texts/index.htm; paper copies are available from the International Bureau of WIPO upon request.

APPENDIX II
PKI ARCHITECTURE FOR THE E-PCT STANDARD

1.   INTRODUCTION

This document presents technical information on the public key infrastructure (PKI) components required under Annex F.[20]

2.   SCOPE

Matters outside the scope of this document:

(a)   Specification of the public key infrastructure – Annex F and this Appendix refers to services of a PKI environment. However, it is expected that the specification of PKI certificate policy, technical design and operations documents, etc. will be described in documents external to this standard.

(b)   Cross-certification in a PKI environment is not fully covered.

3.   PUBLIC KEY INFRASTRUCTURE (PKI) REQUIREMENTS

Annex F specifies the use of a PKI as the method of providing secure on-line document exchange. The objectives for the use of PKI are as follows:

(a)   Ensure that PCT Offices provide adequate security for sensitive information throughout the PCT process.

(b)   Provide the necessary services to enable the business processes of the PCT to become part of a system of secure electronic records

(c)   Provide, through cryptographic mechanisms, four basic security services for PCT Offices and authorities and for PCT applicants which include:

(i)   authentication – the process of validating an identity claimed by or for an entity;

(ii)   integrity – ability to verify that data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed;

(iii)   non-repudiation – ensure that strong and substantial evidence is available to the sender of data that the data has been delivered (with the cooperation of the recipient), and to the recipient of the sender's identity, sufficient to prevent either from successfully denying having possessed the data; this includes the ability of a third party to verify the integrity and origin of the data;

(iv)   confidentiality – ensure that information can be read only by authorized entities.

---

[20]   Words and expressions used in this Appendix have the same meanings as in the main body of Annex F; see the Glossary and abbreviations section at the end of that main body. See also the Glossary in this Appendix.

4.   PCT PKI STANDARDS

This section includes a description of an interoperable PKI environment capable of providing applicants and Offices with the security services required for the secure exchange of international application documents.

The E-PCT trust model will be based on a root repository model. The model relies on the software itself (for example, PCT E-filing software) to utilize a trust list of CAs. PKI client software will process certificates (including CRL or OCSP lookup) issued by one of the trusted CAs to determine whether the public key certificate of a user in another community should be trusted.

The root repository trust model is technically a distributed trust architecture but does not require cross-certification for operation. The trust model is used today in the web browser community but the model can be implemented in software other than web browsers (e.g. PCT E-filing software).

This model uses a file to store the public key certificate (PKC) of many CAs (e.g. Intellectual Property Office CA). The relying party then trusts any PKC included in the file. The PKC included in the root repository may be a root CA for some other domain or a subordinate CA, but when included in the trust file, it becomes a root CA for the relying party.

In the E-PCT environment, each Office will maintain a trust list of recognized CAs. Under this architecture, all entities in the trust list and their subordinates would be trusted equally by E-PCT software.

To further illustrate how the root repository model will be applied to the E-PCT PKI trust model, refer to Figure 1 below.
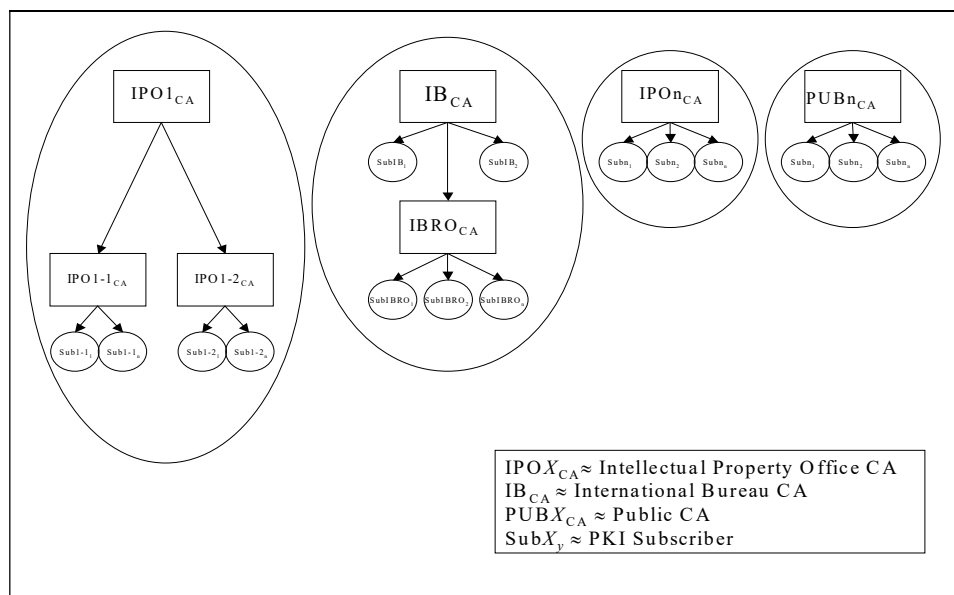

Figure 1 – E-PCT PKI trust model

Each enclosed area in Figure 1 represents an independent PKI domain that provides CA services. There are two types of recognized CAs, an Office CA (e.g. IPO1$_{CA}$) and a public

CA (e.g. PUBn$_{CA}$). The trust list used by E-PCT software will be referenced in order to provide a trust path between PKI domains. For example, in Figure 1, the trust list would include root CA certificates from IPO1$_{CA}$, IB$_{CA}$, IPOn$_{CA}$, and PUBn$_{CA}$. In some cases, Offices may choose not to include the certificates of public CAs (e.g. PUBn$_{CA}$) when they opt not to accept certificates from public CAs during the international and/or national phases.

4.1 *Certificate/signature validation within the E-PCT PKI trust model*

This section addresses the use of a digital certificate used for digital signature. Section 4.2 addresses the use of the certificate used for encryption purposes.

The E-PCT PKI trust model allows for digital certificates issued by a CA in one PKI domain to be validated by entities in other PKI domains. For example, in Figure 1, IPO1$_{CA}$, IB$_{CA}$, and n domains (IPOn$_{CA}$, PUBn$_{CA}$) can issue high-level and low-level certificates to their subscriber community.[21] For purposes of certificate and signature validation, it is not mandatory that a common certificate repository (or another inter-domain directory mechanism) be established/maintained. Instead, certificate validation is accomplished through the trusted root certificate using On-line Certificate Status Protocol (OCSP) or a foreign directory lookup of the applicable CRL.

For example, when subscriber SubIB$_1$ performs certificate validation on a certificate received from Sub1-1$_1$ (as part of the signature validation process), the following steps would occur:

1.   Each certificate in the trust path would be evaluated[22]. In this example, the first certificate Sub1-1$_1$ would be validated by verifying that the certificate was signed using the private key maintained by the holder of the certificate IPO1-1$_{CA}$. In addition, the validity period would be checked as well as revocation status using OCSP or a CRL lookup.

2.   Next, the IPO1-1$_{CA}$ would be validated by verifying that the certificate was signed using the private key maintained by the holder of the certificate IPO1$_{CA}$. In addition, the validity period would be checked as well as revocation status using OCSP or a CRL lookup.

3.   Finally, the last certificate found in the trust path (also know as the anchor certificate) would be validated against the trusted root certificates utilized by the E-PCT software. In this example, the IPO1$_{CA}$ certificate found in the certificate being evaluated would be compared against the IPO1$_{CA}$ certificate in the trust list. In addition, the validity period and ARL (Authority Revocation List) would be checked.

In the example presented above, all validation could be completed locally except CRL and ARL checking. CRLs and the ARL can be maintained independently as long as they are accessible by the relying party.

The process described above provides Offices the ability to validate low-level certificates in the national phase as well. That is, if a designated Office allows low-level certificates to be used in the national phase, the mechanism would allow the applicant to transition into the national phase with his existing low-level certificate.

---

[21]   It is envisioned that the International Bureau CA will issue high-level certificates only to PCT Offices and Authorities. The International Bureau CA will issue low-level certificates to applicants and agents.

[22]   This requires that certificates include the complete certificate chain to the root authority.

For example, if subscriber Sub1-1$_1$ (designated Office subscriber) needed to perform certificate validation on a certificate received from Subn$_1$ (applicant that received a certificate from a public CA), the following steps would occur:

(a)   The applicant would sign the appropriate national phase entry documents with his low-level certificate.

(b)   Each certificate in the certificate trust path would be evaluated. In this example, the first certificate Subn1 would be validated by verifying that the certificate was signed using the private key maintained by the PUBnCA CA. In addition, the validity period would be checked as well as the revocation status using OCSP or a CRL lookup.

(c)   Next, the anchor certificate would be validated against the trusted root certificates utilized by the E-PCT software. In this example, the PUBnCA certificate found in the certificate being evaluated would be compared against the PUBnCA certificate in the trust list. In addition, the validity period and ARL (authority revocation list) would be checked.

In order to tie the international application received from the International Bureau to the applicant, name and e-mail address included on the international application documents would be compared to the name and e-mail address included in the certificate received from the applicant. The designated Office could also obtain authentication through conventional (paper-based) means if they deemed it necessary.

If the designated Office does not provide for the use of a low-level certificate or a certificate (whether high-level or low-level) that was issued by a public CA in the national phase, the applicant would be required to obtain a certificate acceptable by that office.

4.2   Encryption within the PCT trust model

Encryption of packages made under this standard will be provided by SSL (or TLS) (see the E-filing interoperability protocol, Annex F, section 5.1). For packages sent using SSL (or TLS), client-side authentication will include the use of the client's digital certificate. The certificate will be validated using the same method described in section 4.1.

4.3   Certification authority

Each receiving Office will specify the certification authorities that are recognized by that Office to issue certificates for purposes of the E-PCT. The list may include Office CAs or public CAs. This list of recognized CAs will be published by the International Bureau including a link to the published policy of those certification authorities.

The Offices 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 along with the trusted CA root certificates which would be available for download via SSL (or TLS).

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

stores certificate information for all certificates it issues 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 IETF Network Working Group RFC 1777 dated March 1995. In addition, the certification authority publishes certificate revocation information in accordance with the X.509 recommendation.

Each Office needs access to certificate revocation information, in accordance with the X.509 recommendation, for all certification authorities that it accepts. Whenever a certificate is used to authenticate an individual, the certification authority that maintains certificate revocation information is consulted by the Office to ensure that the certificate has not been revoked.

In order to support non-repudiation, Offices and certification authorities should include processes that ensure that the subscriber generates his or her signing key pair on that subscriber's own system and only transferring his or her public verification key to others (e.g. public verification key is sent to the CA during the registration process).

4.4 Digital certificates

Digital certificates must comply with the International Telecommunication Union (ITU) X.509 version 3 recommendation for certificate format.

Two classes of certificates have been defined, low-level and high-level certificates.

4.4.1 E-PCT Certificate Profile

E-PCT certificate profiles, based on RFC 2459 (Basic Certificate Fields) and X.509 version 3, will be included in this standard once they become available. At a minimum, the standard will include profiles for CA Signature and End Entity (subscriber) certificates and the CRL.

4.4.2 Low-level certificate

The low-level certification process does not, in general, require pre-registration. However, the subscriber states, at a minimum, his name and a verifiable e-mail address (see glossary). Additional proof of identity is not required. The subscriber uses an online facility to promptly obtain a low-level certificate from the International Bureau (WIPO customer CA) or the subscriber goes through a similar subscription process with any other recognized CA that provides for such service.

4.4.3 High-level certificate

A high-level certificate means a digital certificate which has been issued to the subscriber by a trusted party and which identifies the subscriber with prior verification of the subscriber's identity. A high-level certificate can be used to authenticate the identity of the subscriber.

Each certification authority will issue certificates in compliance with its published identity proofing standards. The International Bureau will publish a list of recognized certification authorities for high-level certificates.

4.4.4 Certificate lifecycle

This section provides an overview of the certificate life cycle processes. This section only addresses the life cycle within a PKI environment for both applicants and PCT Offices.

Each certificate has a set life span before it expires and needs to be renewed. A subscriber's certificate may be revoked for several reasons by the subscriber, the Registration Authority (RA) or Local Registration Authority (LRA), and authorized management.

4.4.5 Obtaining certificates

Offices and Authorities within the PCT system are required to obtain and utilize high-level certificates issued by the International Bureau for Office-to-Office data exchange. Applicants may obtain and utilize a low-level certificate for E-filing purposes. However, Offices may require that applicants obtain and use a high-level certificate after the initial filing.

4.4.5.1 Low-level certificate

The subscribers to low-level certificates will only include PCT applicants, assignees, and their representatives.

The certification process may vary due to implementation details and certificate policy, but generally will involve the following steps:

1.   In the software provided by the International Bureau or receiving Office, the applicant/agent selects the option to request a low-level certificate.

2.   The applicant/agent enters the following information: name, e-mail address, challenge phrase, selected recognized certification authority (CA).[23]

3.   The applicant/agent's computer generates public/private key pairs for a signing certificate and encryption certificate.

4.   The applicant/agent's computer generates a PKCS #10 certification request and sends it to the selected CA.

5.   The CA performs basic validation on the data submitted (Name given must be unique, challenge phrase must meet security policy criteria, etc.) and either generates the certificate or an error response.

6.   In the case of an error response, the applicant/agent is prompted to correct information and retry. Otherwise, the applicant/agent is sent a message (e-mail address indicated during the application process) to retrieve the new certificate. The message will include an authorization code that is generated by the CA.

---

[23]   It is expected that if the software is capable of interacting with multiple CAs, it will provide the user with a list of applicable CAs from which to choose.

7.   The applicant retrieves the new certificate (via secure channel, e.g. SSL (or TLS)) after the authorization code and challenge phrase is validated.

4.4.5.2 High-level certificate

High-level digital certificates will be issued by the International Bureau to facilitate Office-to-Office data exchange. The International Bureau will handle applications for and issuance of certificates on an individual basis.

Offices (other than the International Bureau) that issue high-level certificates to applicants will typically begin with a registration process. The registration process may vary depending on the Office or on the chosen CA, but generally includes the following steps:

1.   The applicant/agent completes and signs a paper application.

2.   The applicant/agent sends the paper application to the Registration Authority (RA) for review.

3.   If approved, the applicant is typically sent a confirmation of registration via physical mail containing information required to proceed with the certification process.

4.   The RA may require that the applicant/agent appear in person with identifying documents.

The certification process may vary due to implementation details, but generally will involve a similar process as described for the low-level certificate. The major differences in the high-level certification process are:

(a)   The applicant provides information from the confirmation of registration (rather than name, e-mail address, etc.)

(b)   The generation and storage of private keys may vary depending on the chosen CA's policy. For example, smart cards may be used to generate and/or store the key pairs.

(c)   The CA may require that the private key used for encryption be backed up.

4.4.6 Certificate use

Certificates issued by a recognized CA may be used for digital signature and data encryption purposes. All certificates must be validated prior to use[24]. The public key certificate and current certification revocation list are obtained by the relying party's PKI client software. The PKI client software then verifies the CA's signature on the certificate and, using the CRL (or through OCSP), verifies that the certificate has not been revoked. It is envisioned that these activities will be accomplished automatically by client software or back-end systems.

4.4.6.1   PKCS # 7 digital signature (enhanced electronic signature)

---

[24] Generic web browsers do not implement certificate validation and additional means must be provided to implement this function.

Subscribers digitally sign international application packages using their private keys. Relying parties can verify the signatures of subscribers and the integrity of the signed package by obtaining the signer's public verification key from their verification certificate, which is provided with the signed package.

Digital signatures used to sign international application packages must conform to the format and practice specified in RSA Laboratories, PKCS #7 – Cryptographic Message Syntax Standard Version 1.5 definition of SignedData content type.

To build these signatures, a certificate meeting the requirements set out in section 4.4 above must be used.

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

4.4.6.2 Encryption

Subscribers encrypt international application packages using the SSL (or TLS) protocol (see Protocol, Annex F, section 5.1) or optionally, the destination party's public encryption key. See section 4.2 for additional information on encrypting international application packages.

4.4.7 Certificate expiration and renewal

Each certificate has a set life span before it expires and needs to be renewed. The life span is set to avoid vulnerabilities that may occur if an attacker has a large collection of messages signed or encrypted with the same key and sets about breaking the key, a time intensive process. Normally, subscribers' certificates are renewed automatically before they expire, with new key pairs generated, and certificates issued. Subscribers may be required to request renewal. E-PCT software should notify the end user of the certificate's pending expiration.

When key pairs are updated, they are replaced with new key pairs, and new public key certificates are created. If a subscriber's certificate requires an update for other than normal time expiration reasons, the subscriber and RA will need to be involved. Such reasons include the need to modify subscriber identification information, policy that requires periodic confirmation of subscriber information, or to resolve suspected misuse or key compromise.

4.4.8 Certificate revocation

A subscriber's certificate may be revoked for several reasons. Certificate revocation may be initiated by the subscriber, the RA or LRA, and authorized management. Subscribers should advise the cognizant RA or LRA if they:

(a)   no longer require use of the certificate (e.g., termination of employment, change of job responsibilities),

(b)   know of or suspect a compromise of their private key,

(c)   have changed their name. In the absence of a request by the subscriber, the cognizant RA or LRA should request revocation of a subscriber's certificate for any of the

above reasons. The cognizant RA or LRA should also initiate revocation of a subscriber's certificate if there is a material breach of the subscriber agreement.

4.4.9 Key recovery

CAs may optionally provide the capability for key recovery of subscriber decryption keys.   However, if key recovery is made available, it will only apply to decryption keys. Non-repudiation is supported by having the subscriber generate his or her signing key pair on that subscriber's own system and only transferring his or her public verification key to the CA during the registration process.

4.5   Cryptographic 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 must not be used for international application document exchange from that country. Algorithms implemented in hardware or software must 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 intellectual property Offices must be disclosed to both parties.

Where possible, the rsaEncryption algorithm is to be used for asymmetric encryption and the dES-EDE3-CBC algorithm is to be used for symmetric encryption. The same asymmetric encryption algorithm should be used to create digital certificates, digital signatures and envelopes. Other encryption algorithms (e.g. Advanced Encryption Standard) will be included in this section as they become available and gain mutual agreement by Offices.

4.6   Message digest algorithms

The message stream must be input to the strong one-way message digest algorithm SHA-1 or SHA-2 group to create a message digest. Other encryption algorithms will be included in this section after consultation and agreed upon by Offices.
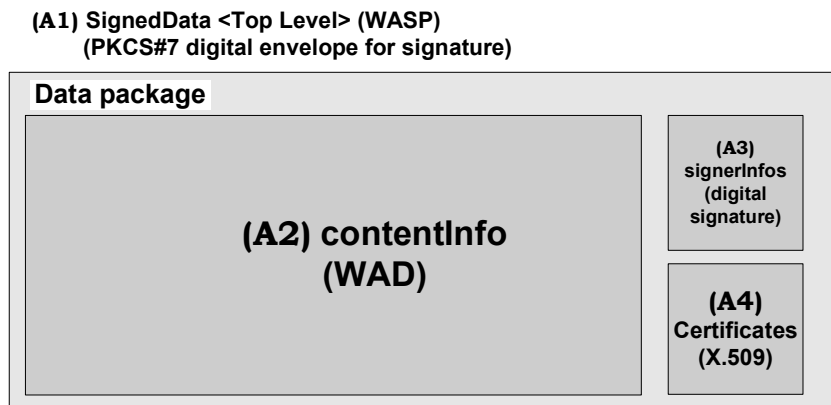
4.7   Data enveloping

Electronic document data that is encrypted to ensure confidentiality for international application document exchange must conform to the format and practice specified in RSA Laboratories, PKCS #7 – Cryptographic Message Syntax Standard Version 1.5 definition of SignedAndEnvelopedData content type

5.   E-PCT PKI PACKAGE TYPES

5.1   *Wrapped and signed package (WASP)*

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

(A1) SignedData <Top Level> (WASP)
(PKCS#7 digital envelope for signature)

```
Data package
  ┌─────────────────────────┐  ┌──────────────┐
  │                         │  │   (A3)       │
  │                         │  │  signerInfos │
  │                         │  │   (digital   │
  │    (A2) contentInfo     │  │  signature)  │
  │         (WAD)           │  └──────────────┘
  │                         │  ┌──────────────┐
  │                         │  │   (A4)       │
  │                         │  │ Certificates │
  │                         │  │   (X.509)    │
  └─────────────────────────┘  └──────────────┘
```

Rules for producing the PKCS #7 SignedData for certification
(Although SHA-2 group is also used besides SHA-1, SHA-1 is shown as an example below.)

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 (WASP) top level

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

Table A2 contentInfo (WAD) top level

Item name	PKCS #7 item	Content
Content type	ContentType	Set object identifier {pkcs-7 1}
Content	Content	Set user data (binary)

Table A3 signerInfos top level

Item name	PKCS #7 item	Content
Version	Version	Set integer value '1'
Issuer and serial number	IssuerAndSerialNumber	Issuer of certificate and its serial number defined in X.509 spec. (for signer's certificate)
Set of digest algorithms	DigestAlgorithm	
Algorithm identifier	AlgorithmIdentifier	Set ONLY ONE **set of** algorithm identifiers {sha-1} for making digest of digital signature.
Authenticated attributes	AuthenticatedAttributes	Not used (Set no data)
Digest encryption algorithm	DigestEncryptionAlgoritm	Algorithm OBJECT identifier of digest encryption (recommended algorithm : rsaEncryption[2])
Encrypted digest	EncryptedDigest	Message digested data; content is encrypted with signer's private key.
Unauthenticated attributes	UnauthenticatedAttributes	Not used (Set no data)

Table A4 certificates top level

Item name	PKCS #7 item	Content
Set of certificates	ExtendedCertificatesAndCertificates	
The X.509 certificate	Certificate (defined in X.509 spec.)	Set ONLY ONE **set of** X.509 certificate data

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 the International Bureau of the algorithm.

6.   PACKAGE CERTIFICATE/SIGNATURE TYPES

Figure 2 through Figure 6 are intended to focus on the difference between the types of "digital certificate" and "electronic signature" options. Each diagram shows a "box" that represents the wrapped and signed package. The diagrams are intentionally simplified to obscure technical detail that may distract the reader from the key issues. For example, the signed and encrypted package details are not shown.
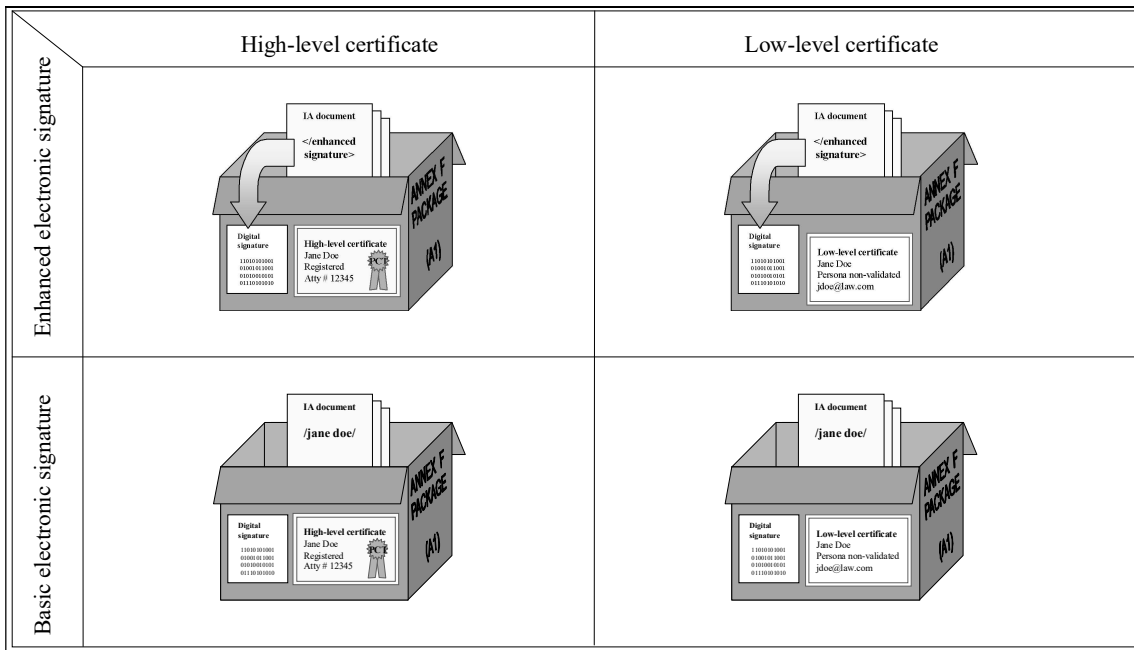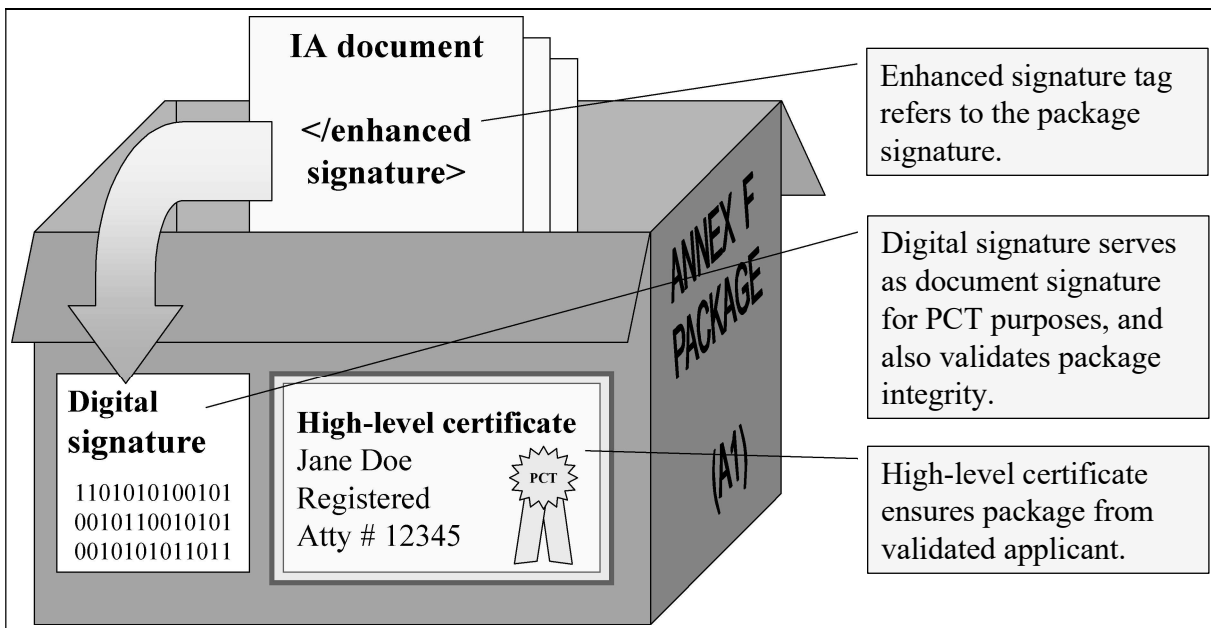
	High-level certificate	Low-level certificate
Enhanced electronic signature	IA document `</enhanced signature>` · Digital signature 11010101001 01001010101 0010010001 01110101010 · High-level certificate Jane Doe Registered Atty # 12345 · ANNEX F PACKAGE (A1)	IA document `</enhanced signature>` · Digital signature 11010101001 01001010101 0010010001 01110101010 · Low-level certificate Jane Doe Persona non-validated jdoe@law.com · ANNEX F PACKAGE (A1)
Basic electronic signature	IA document /jane doe/ · Digital signature 11010101001 01001010101 0010010001 01110101010 · High-level certificate Jane Doe Registered Atty # 12345 · ANNEX F PACKAGE (A1)	IA document /jane doe/ · Digital signature 11010101001 01001010101 0010010001 01110101010 · Low-level certificate Jane Doe Persona non-validated jdoe@law.com · ANNEX F PACKAGE (A1)

Figure 2 – Certificate/signature types

IA document

</enhanced signature>

Digital signature
1101010100101
0010110010101
0010101011011

High-level certificate
Jane Doe
Registered
Atty # 12345

PCT

ANNEX F PACKAGE

(A1)

Enhanced signature tag refers to the package signature.

Digital signature serves as document signature for PCT purposes, and also validates package integrity.

High-level certificate ensures package from validated applicant.

Figure 3 – Enhanced electronic signature / high-level certificate

IA document

</enhanced signature>

Enhanced signature tag refers to the package signature.

ANNEX F PACKAGE

(A1)

Digital signature serves as document signature for PCT purposes, and also validates package integrity.

Digital signature

1101010100101
0010110010101
0010101011011

Low-level certificate
Jane Doe
Persona non-validated
jdoe@law.com

Low-level certificate used to validate digital signature.
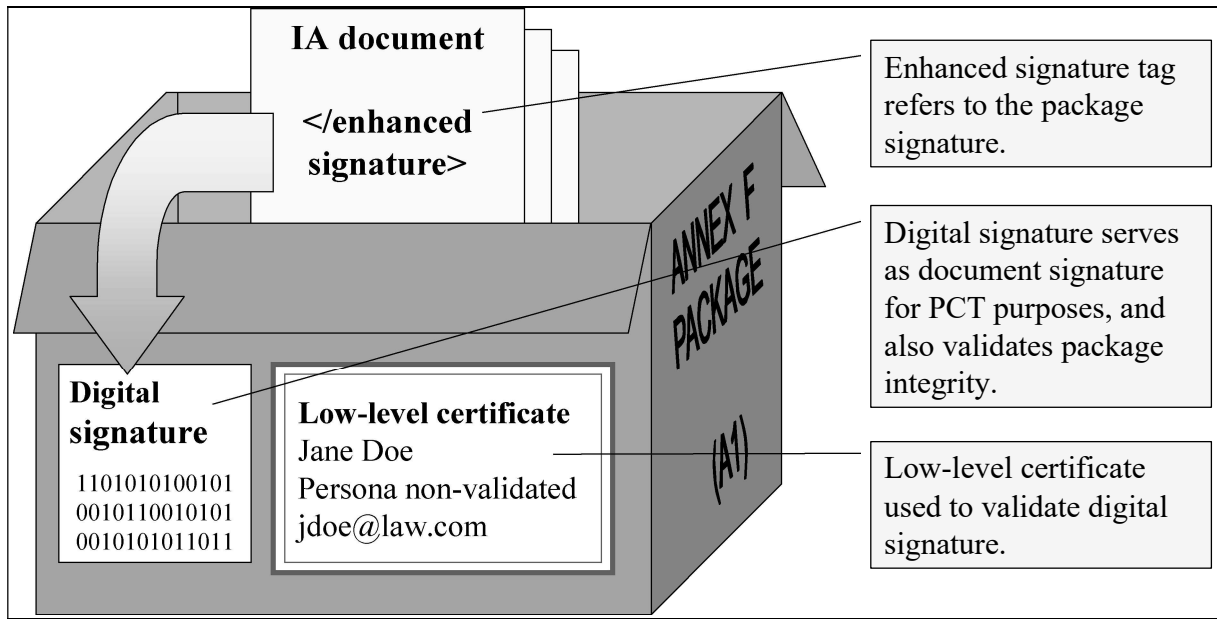
Figure 4 – Enhanced electronic signature / low-level certificate

IA document

/jane doe/

Basic signature indicates signer of the document or click-wrap acknowledgement.

ANNEX F PACKAGE

(A1)

Digital signature only validates integrity of the package.

Digital signature

1101010100101
0010110010101
0010101011011

High-level certificate
Jane Doe
Registered
Atty # 12345

PCT

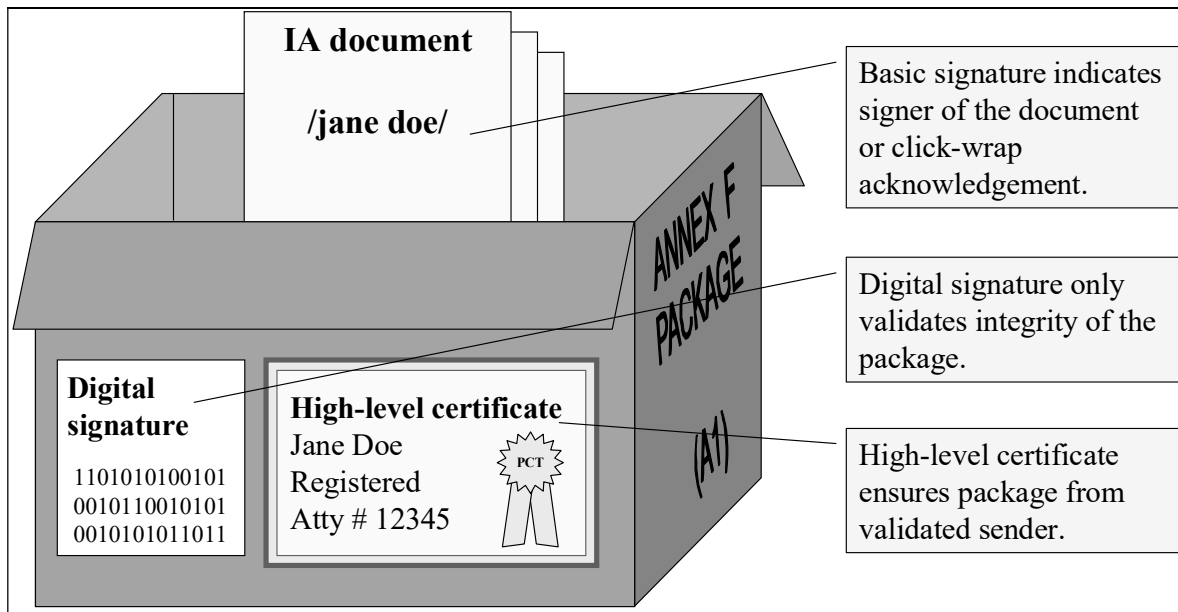High-level certificate ensures package from validated sender.

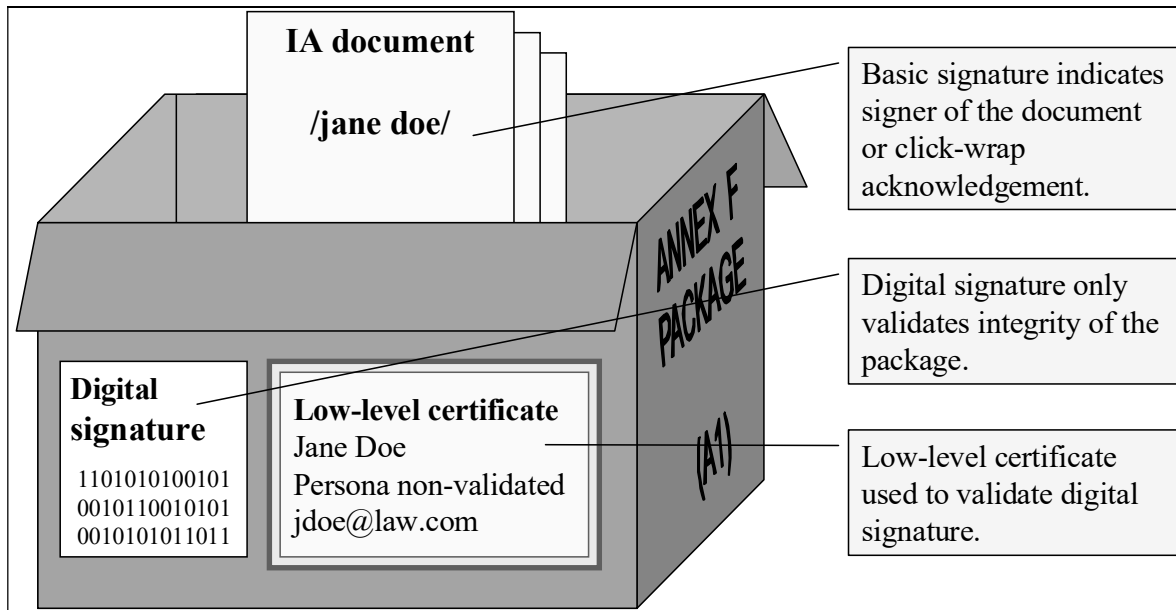Figure 5 – Basic electronic signature / high-level certificate

Figure 6 – Basic electronic signature / low-level certificate

7. GLOSSARY

Authority Revocation List

A type of Certificate Revocation List (see below) that contains revocation information on Certification Authorities.

CA – See Certification Authority

Certificate

A certificate binds an entity's name (and other additional attributes) with the corresponding public key. For purposes of Annex F, a certificate must comply with ITU Recommendation X.509 version 3 and at a minimum must meet the following:

(a)   Contains a public key that corresponds to a private key under the sole control of the subject

(b)   Names or otherwise identifies its subject

(c)   Identifies the CA issuing it

(d)   Identifies its validity period

(e)   Contains a certificate serial number

(f)   Includes end-entities e-mail address.

(g)   Is digitally signed by the CA issuing it.

Certification authority

A CA is a trusted party that issues and revokes public key certificates for a user community. The CA is responsible for verifying the information appearing on the public key certificates. A CA is supported by CA servers, or computer systems, and the policies and procedures surrounding the operation of these servers. The term "server" refers specifically to the hardware and software that actually generates certificates and CRLs.

The E-PCT permits two types of CAs, an Office CA and a Public CA. An Office CA is defined as a CA that issues certificates bearing the name of that Office (whether internal or outsourced). A public CA is defined as a CA that issues certificates that do not bear the Office's name, but that CA is recognized by certain Offices as being suitable for issuing certificates for E-PCT transactions.

Certificate Revocation List

A time-stamped list of revoked certificates that has been digitally signed by a Certification Authority.

Compromise

The unauthorized disclosure, modification, substitution, or use of sensitive data (including plain text cryptographic keys and other critical security parameters).

Confidentiality

The property by which sensitive information is not disclosed to unauthorized individuals, entities, or processes.

Critical Security Parameters

Security-related information (e.g., cryptographic keys and authentication data such as passwords and personal identification numbers [PIN]) appearing in plain text or another unprotected form whose disclosure or modification could compromise the security of a cryptographic module or the security of the information protected by the module.

CRL – See *Certificate Revocation List*

Cryptographic Key (key)

A parameter used in conjunction with a cryptographic algorithm, that determines the transformation of plain text data into cipher text data, the transformation of cipher text data into plain text data, a digital signature computed from data, the verification of a digital signature computed from data, or a data authentication code computed from data.

Cryptographic module

The set of hardware, software, and firmware, or some combination thereof, that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.

Digital signature

A non-forgeable transformation of data that allows the proof of the source (with non-repudiation) and the verification of the integrity of that data. A transformation of a message using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's public key can accurately determine: a) whether the transformation was created using the private key that corresponds to the signer's public key, and b) whether the initial message has been altered since the transformation was made.

Distinguished name

The unique name of each certificate holder or subscriber. Each entity in the PKI domain must have a clearly distinguishable and unique distinguished name, or DN, in the certificate subject name field.

Encryption

In Public Key Cryptography, privacy protection of data is achieved by encrypting the data using the intended recipient's public key. Because the intended recipient is the only person who has access to the corresponding private key, only the intended recipient can decrypt the data.

Firmware

Programs and data (i.e., software) permanently stored in hardware (e.g., read only memory [ROM], programmable read only memory [PROM], or erasable programmable read only memory [EPROM]) in such a way that the programs and data cannot be dynamically written or modified during execution. (Programs and data stored in electronically erasable programmable read only memory [EEPROM] are considered software not firmware.)

Hardware

The physical equipment used to process programs and data in a cryptographic module.

Integrity

The property that means that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

Interface

A logical section of a cryptographic module that defines a set of entry or exit points that provide access to the module, including information flow or physical access.

Issuer name

A unique identifier of the authority signing the certificate. The syntax of the issuer name is an X.500-distinguished name.

Key – See *Cryptographic key*

Key pair

Two mathematically related keys, having the properties that:

(a)   Either key can be used to encrypt data, but only the other key in the pair can decrypt the data

(b)   It is computationally infeasible [impractical] to determine one of the keys, given knowledge of the other key

Typically, one key pair is generated for the purpose of encryption only and one pair for signing only.

Key recovery

Access to sufficient information to recover encrypted data.

Local registration authority

The authority who acts on behalf of the registration authority in vouching for (i.e., validating via some form of identity proofing) the identity of subscribers. The local registration authority is also involved with other certificate life cycle elements on behalf of its subscribers, such as renewal, key recovery, and general assistance support for PKI functions.

LRA – See *Local registration authority*

Manual key distribution

The distribution of cryptographic keys, often in a plain text form requiring physical protection, by a non-electronic means, such as a bonded courier.

Manual key entry

The entry of cryptographic keys into a cryptographic module from a printed form, using devices such as buttons, thumb wheels, or a keyboard.

Message

A digital representation of information, including text, graphics, images, and sounds.

Message integrity

The assurance of unaltered transmission and receipt of a message from the sender to the intended recipient.

Non-repudiation

Strong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission, or delivery of the message and the integrity of its contents.

Object identifier

A specially formatted number that is registered with an internationally recognized standards organization. It can, and should, be used to identify an organization's suite of PKI policy and practices documents.

Office Certification Authority – See *Certification Authority*

On-line Certificate Status Protocol (OCSP)

As defined in RFC 2560, OCSP enables applications to determine the (revocation) state of an identified certificate. OCSP may be used to satisfy some of the operational requirements of providing more timely revocation information than is possible with CRLs and may also be used to obtain additional status information. An OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificate in question until the responder provides a response.

OID – See *Object identifier*

Operational period of a certificate

The period of a certificate's validity. This period would typically begin on the date when the certificate was issued (or on a later date specified in the certificate) and end (or expire) on the date and time noted in the certificate (unless the certificate was previously revoked).

Operator

An individual accessing a cryptographic module, either directly or indirectly via a process operating on his or her behalf, regardless of the specific role the individual assumes.

Password (or passphrase)

A string of characters used to authenticate an identity or to verify access authorization.

Personal identification number (PIN)

A string of alphanumeric characters used to authenticate an identity (commonly used in banking applications).

Physical protection

The safeguarding of a cryptographic module or of cryptographic keys or other critical security parameters by physical means.

PIN – See *Personal identification number*

PKI – See *Public key infrastructure*

PKI domain – See *Public key infrastructure domain*

Port

A functional unit of a cryptographic module through which data or signals can enter or exit the module. Physically separate ports do not share the same physical pin or wire.

Private key

In public key cryptography, the private key is the portion of a public–private key pair owned by a user that is known only to that user. A user's private key is used to digitally sign data and to decrypt data that was encrypted with the user's public key.

Public Certification Authority – See Certification Authority

Public key

In public key cryptography, the public key is the portion of a public–private key pair owned by a user that is made known to others in the user community via a public key certificate. A user's public key is used by others to encrypt data for that user or to verify the user's digital signature.

Public key certificate

A set of data that unambiguously identifies an entity, contains the entity's public key, and is digitally signed by a trusted party.

Public key (asymmetric) cryptographic algorithm

A cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that, given the public key, it is computationally infeasible to derive the private key.

Public Key Cryptography

Public key cryptography is a cryptographic technique in which pairs of keys are used to encrypt and decrypt data. Each user is assigned a key pair. One of the user's keys is a public key that is made known to anyone who needs it. The other key is a private key which is mathematically related to the public key and known only by that user. Data encrypted by either of the keys in the pair can be decrypted only by the other key of the pair

Public key infrastructure

A PKI includes at least the following services:

(a) CA

(b) RA

(c) Certificate and CRL repository

(d) User PKI client software

(e)   Governing policy, practices, procedures, and standards

(f)   Public key infrastructure operational support plan

(g)   All supporting facilities and services

Public key infrastructure domain

An independent entity consisting of one or more certification authorities where subscribers hold the same anchor or root certificate.

RA – See *Registration authority*

Registration authority

An entity responsible for identification and authentication of certificate subjects, but not for signing or issuing certificates (i.e., a registration authority, or RA is delegated certain tasks related to identity-proofing on behalf of a certification authority). The RA may delegate functions and corresponding authority to local registration authorities (see *Local registration authority*).

Repository

A system for storing and retrieving certificates and other information relating to the certificates.

Responsible individual

A person designated by the registration authority to authenticate individual applicants seeking certificates on the basis of their affiliation with a local registration authority.

Revocation of a certificate

Prematurely ending the operational period of a certificate from a specified time forward.

Secret key

A cryptographic key used with a secret key cryptographic algorithm, uniquely associated with one or more entities, and which will not be made public. The term "secret" in this context does not imply a classification level, rather it implies the need to protect the key from disclosure or substitution.

Secret key (symmetric) cryptographic algorithm

A cryptographic algorithm that uses a single, secret key for both encryption and decryption.

Split knowledge

A condition under which two or more entities separately have key components that individually convey no knowledge of the plain text key that will be produced when the key components are combined in the cryptographic module.

Sponsor

An organization with which a subscriber is affiliated (as an employee, user of a service, business partner customer, etc.). A sponsor performs identity-proofing on behalf of a local registration authority or registration authority for an affiliated individual.

Status information

Information that is output from a cryptographic module to indicate certain operational characteristics or states of the module.

Subject

A person whose public key is certified in a certificate. Also referred to as "subscriber."

Subscriber

The entity who (1) is the subject named or otherwise identified in a certificate issued to that person, (2) holds a private key that corresponds to a public key listed in the certificate, and (3) is the person to whom digitally signed messages verified by reference to the certificate are to be attributed. Also referred to as "subject."

System software

Special software (e.g., operating system, compilers, or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, programs, and data.

Time-stamp

A notation that indicates, at least, the correct date and time of an action and the identity of the person that created the notation.

Trustworthy system

A set of computer hardware, software, and procedures that (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.

Valid certificate

A certificate that (1) a certification authority has issued, (2) has been accepted by the subscriber listed therein; (3) has not expired; and (d) has not been revoked. Thus, a certificate is not valid unless it has been both issued by a certification authority and accepted by the Subscriber.

Verifiable e-mail address

An e-mail address that can be verified as belonging to the subscriber of a digital certificate. Verification would be accomplished, for example, by sending an e-mail containing

information required for certificate pickup to the subscriber. If the e-mail address were incorrect, the subscriber would not receive the necessary information to obtain their certificate from the CA.

[Annex F, Appendix III, follows]

APPENDIX III
BASIC COMMON STANDARD FOR ELECTRONIC FILING

1.   INTRODUCTION

(a)   This Appendix sets out the "basic common standard" for electronic filing of international applications which is referred to in Sections 701(v) and 703(b) and (c) of the Administrative Instructions (AIs).

(b)   Each receiving Office which accepts the filing of international applications in electronic form specifies its requirements for such applications, in accordance with Annex F and pursuant to AIs Section 703(b) (in relation to physical requirements) and (c) (in relation to signature). The receiving Office must accept an international application filed with it if the application meets those requirements.

(c)   By virtue of AIs Section 703(b) and (c), each receiving Office which accepts the filing of international applications in electronic form must accept, in addition to any international application complying with the requirements mentioned in paragraph (b), above, any international application which complies with the requirements of the basic common standard, subject to any transitional reservation made under AIs Section 703(f). Note that the basic common standard itself contains certain options for receiving Offices to specify.

(d)   The provisions of Part 7 and Annex F relating to the form or contents of the international application, including the basic common standard, would automatically, by virtue of Article 27(1), be applicable to international applications so far as designated Offices are concerned. Communications between applicants and designated Offices would not, however, be governed in general by Annex F.

2.   BASIC COMMON STANDARD REQUIREMENTS

An international application complies with the basic common standard

–   *as to electronic document format, if it meets the following requirements:*[25]

(a)   the international application documents are encoded in XML format (see Annex F, section 3.1.1.1), using either of the following, as specified by the receiving Office:

(i)   the Unicode 3.0 (International Standard ISO/IEC 10646:2000) coded character set with UTF-8 character encoding scheme; or

(ii)   a coded character set confined within the repertoire of Unicode 3.0 with encoding scheme specified by the receiving Office as described in Internet Engineering Task Force documents IETF RFC 2277 and 2130 (see Annex F, section 3.1.1.1), provided that the character encoding scheme is registered in the Internet Assigned Numbers Authority (IANA) Charset

---

[25]   See AIs Section 703(b)(i) and (d).

registry and that the use of that scheme is supported by the electronic filing software mentioned in paragraph (g);[26]

(b)   any sequence listing is presented in the electronic document format specified in paragraph 40 of the Standard for the Presentation of Nucleotide and Amino Acid Sequence Listings in International Patent Applications under the PCT ("Annex C/ST.25 text file"; see paragraph 40 of Annex C of the Administrative Instructions and WIPO Standard ST.25; see also Annex F, section 3.1.1.2);

(c)   any drawings are in TIFF format, as specified by the receiving Office (see Annex F, section 3.1.3.1);

–   *as to means of transmittal, if it meets the following requirements:*[27]

(d)   if the receiving Office accepts the filing of international applications on-line and the international application is so filed: the international application is transmitted using the E-Filing Interoperability Protocol (see Annex F, section 5.1);

(e)   if the receiving Office accepts the filing of applications by physical means and the international application is so filed: the international application is stored on 3.5 inch diskette or CD-Recordable disk, as specified by the receiving Office (see Annex F, Appendix IV);

–   *as to electronic packaging, if it meets the following requirements:*[28]

(f)   the international application is packaged as a wrapped and signed package (WASP) prepared using a low-level digital certificate issued by the receiving Office or the International Bureau (see Annex F, sections 4.2.1);

–   *as to electronic filing software, if it meets the following requirements:*[29]

(g)   the international application is prepared and filed using software made available for that purpose by the International Bureau[30] (see Annex F, section 6);

–   *as to viruses, etc, if it meets the following requirements:*[31]

(h)   the international application is free of viruses and other forms of malicious logic (see Annex F, section 3.1);

–   *as to signature, if it meets the following requirements:*[32]

---

[26]   The introduction of other schemes by a receiving Office must therefore be the subject of prior agreement between the receiving Office and the International Bureau (which produces the software mentioned in paragraph (g)).

[27]   See AIs Section 703(b)(ii) and (d).

[28]   See AIs Section 703(b)(iii) and (d).

[29]   See AIs Section 703(b)(iv) and (d).

[30]   The International Bureau provides software that supports all of the requirements of the basic common standard and certain alternatives available under Annex F. Use of that software is not mandatory but any applicant may choose to use it, in which case the receiving Office must accept the international application concerned under Section 703(b)(iv) (unless it has made a reservation under Section 703(f) in that respect) (see Annex F, section 6).

[31]   See AIs Section 703(b)(v) and (d).

(i)   the international application is signed with any basic electronic signature acceptable under Annex F (see Annex F, section 3.3).

[Annex F, Appendix IV, follows]

---

[32]   See AIs Section 703(c) and (d). Note that while signature in compliance with the basic common standard is sufficient for the purposes of filing, compliance with the receiving Office's specified requirements may be required subsequently pursuant to AIs Section 704(g).

APPENDIX IV
USE OF PHYSICAL MEDIA FOR THE E-PCT STANDARD

1.   INTRODUCTION

(a)   This Appendix[33] defines the requirements for applicants for the submission of documents in electronic form using physical media where the receiving Office has notified the International Bureau under AIs Section 710(a) that it is prepared to accept the filing in electronic form on physical media of:

(i)   international applications under AIs Section 703 (see AIs Section 710(a)(i)); or

(ii) other kinds of documents under AIs Section 703 (see AIs Section 710(a)(iii)).

(a-*bis*) This Appendix also defines the requirements for applicants for the submission of sequence listings in electronic form using physical media where the International Searching Authority or the International Preliminary Examining Authority ("Authority") has notified the International Bureau under AIs Section 513(f) and 610(e), respectively, that it is requiring the furnishing of such listings, for the purposes of international search and preliminary examination, respectively, in electronic form on physical media.

(b)   A receiving Office which has notified the International Bureau under AIs Section 710(a) that it is prepared to accept the filing of documents in electronic form on physical media and an Authority which has notified the International Bureau under AIs Section 513(f) or 610(e) that it is requiring the furnishing of sequence listings in electronic form on physical media shall, in addition to the indications required under those Sections, indicate the physical media types and the number of copies of the physical media that are required.

(c)   The acceptable physical media types and formats shall be limited to those described in section 4 of this Appendix, below, provided that any receiving Office referred to in paragraph (a) shall, where the International Searching Authority or, if applicable, at least one of the International Searching Authorities competent for the international searching of international applications filed with that receiving Office has notified the International Bureau under Section 513(f) that it requires the furnishing of sequence listings in electronic form on physical media for the purposes of the international search, accept at least one physical media type that is accepted by that Authority, or, if applicable, by at least one of those Authorities.

(d)   Electronic document formats are limited to those described in the main body of this Annex.

---

[33]   Words and expressions used in this Appendix have the same meanings as in the main body of Annex F; see the Glossary and abbreviations section at the end of that main body.

2.	REQUIREMENTS FOR ELECTRONIC FILING USING PHYSICAL MEDIA

(a)	Each physical medium shall conform to the relevant standards indicated in section 4 of this Appendix, below, and the contents of each physical medium shall be encoded in an electronic document format as specified in the main body of this Annex.

(b)	The contents of each physical medium shall:

(i)	subject to paragraph (b-*bis*), be packaged in accordance with section 4.1 or 4.2 of the main body of this Annex; and

(ii)	subject to paragraph (c), be contained in a single file and be located in the root directory of the physical medium.

(b-*bis*)	Where the physical medium contains a sequence listing furnished under Rule 13*ter*, the contents of the physical medium need not be packaged, unless the file containing such listing is compressed in accordance with paragraph (c-*bis*).

(c)	A receiving Office or an Authority may limit the size of the files written on the physical medium. If, to comply with this requirement, a single document needs to be split into multiple files written on a single physical medium, or if a single document needs to be split into multiple files to be written on multiple physical media, such splitting shall be done such that the files can be rejoined to form one single contiguous file without any repeated or missing contents in accordance with either the ZIP file splitting standard or the Unix/Linux "split" command. In either case, the file names shall be in accordance with the defaults in those standards for splitting and recreating a file with a particular original name, for example, for "sequence-list.txt" in the case of ZIP split files: "sequence-list.z01", "sequence-list.z02", "sequence-list.zip"; or, in the case of Unix split files: "sequence-listaa.txt", "sequence-listab.txt", etc.

(c-*bis*)	File compression is acceptable if done, in accordance with section 4.1.1 of the main body of this Annex, according to the ZIP standard (that standard allows the compression software to select from among a number of compression algorithms; the compression method must be "deflation" with the normal compression option).

(d)	Each physical medium shall be enclosed in a hard case within an unsealed padded and protective mailing envelope and accompanied by a transmittal letter on paper. The transmittal letter shall state the contents of the physical medium (for example: "international application filed under Section 703" or "[*name of other kind of document*] filed under Section 703"). The transmittal letter shall also list for each physical medium the machine format (e.g., IBM-PC), the operating system compatibility (e.g., MS-DOS, MS-Windows, Unix), a list of the files contained on the physical medium including their names, sizes in bytes, and dates of creation, plus any other special information that is necessary to identify, maintain, and interpret the information on the physical medium. Physical media submitted to the Office will not be returned to the applicant.

(e)	Where the receiving Office requires under Rule 11.1(b) that an international application filed in electronic form on a physical medium be submitted in two or three copies, or where an Authority so requires in respect of the furnishing of a sequence listing for the purposes of the international search or international preliminary examination, the transmittal letter that accompanies the physical media must include a statement that the copies of the physical media are identical. In the event that the copies of the physical media are not

identical, the Office or Authority will use the physical medium labeled "COPY 1" (see paragraph (f)(vi), below) for further processing.

(f)   A physical medium must also be physically labeled with the following information:

(i)   the name of the applicant(s) (see also AIs Section 105);

(ii)   the title of the invention;

(iii)   the international application number and the international filing date or, where such number and date is not known to the applicant, the name of the receiving Office with which the application was filed and the file reference used by the person filing the application to identify the application;

(iv)   the date on which the files contained in the physical medium were created or last modified;

(v)   where the document is contained on more than one physical medium, the numbering of each such physical medium, as follows (example: the document is contained on three physical media): "DISK 1/3", "DISK 2/3", "DISK 3/3";

(vi)   where more than one copy of the physical medium is required by the receiving Office or by the Authority, the numbering of each copy submitted, as follows (example: three copies of the physical media are submitted): "COPY 1", "COPY 2", "COPY 3" (see also paragraph (e), above); and

(vii)   an indication of the content of the physical medium (for example: "INTERNATIONAL APPLICATION – SECTION 703"; "ARTICLE 19 AMENDMENTS"; "ARTICLE 34 AMENDMENTS"; "SEQUENCE LISTING – RULE 13*ter*"; "SEQUENCE LISTING – CORRECTION – Rule 13*ter*"; "SEQUENCE LISTING – RECTIFICATION – Rule 13*ter*"; "SEQUENCE LISTING – AMENDEMENT – Rule 13*ter*".

3.   REFERENCES

ISO/IEC 9529-1:1989 Information processing systems – Data interchange on 90 mm (3,5 in) flexible disk cartridges using modified frequency modulation recording at 15 916 ftprad, on 80 tracks on each side – Part 1: Dimensional, physical and magnetic characteristics

ISO/IEC 9529-2:1989 Information processing systems – Data interchange on 90 mm (3,5 in) flexible disk cartridges using modified frequency modulation recording at 15 916 ftprad, on 80 tracks on each side – Part 2: Track format

ISO 9660:1988 Information processing – Volume and file structure of CD-ROM for information interchange

Standard ECMA-119, Volume and File Structure of CDROM for Information Interchange

ISO/IEC 13346 Information technology – Volume and file structure of write-once and rewritable media using non-sequential recording for information interchange

Standard ECMA-167, Volume and File Structure for Write-Once and Rewritable Media using Non-Sequential Recording for Information Interchange

Optical Storage Technology Association Universal Disk Format Specification (OSTA UDF)

ISO/IEC 10149:1995 Information technology – Data interchange on read-only 120 mm optical data disks (CD-ROM)

Standard ECMA-130, Data Interchange on Read-only 120 mm Optical Data Disks (CD-ROM)

ISO/IEC 16448:1999 Information technology – 120 mm DVD – Read-only disk

Standard ECMA-267, 120 mm DVD - Read-Only Disk

Standard ECMA-279, 80 mm (1,23 Gbytes per side) and 120 mm (3,95 Gbytes per side) DVD-Recordable Disk (DVD-R)

4.   ACCEPTED MEDIA TYPES AND FORMATS

4.1   3.5 Inch Diskette

Type

ISO/IEC 9529 Double-sided, high density, 135 TPI, 80 track, 3.5 inch diskette.

Format specification

1.44MB IBM PC Compatible DOS Format.

4.2   CD-ROM

Type

ISO/IEC 10149:1995, 120mm CD-ROM

Format specification

ISO 9660, 650MB

4.3   CD-R

Type

120mm CD-Recordable Disk

Format specification

ISO 9660, 650MB

4.4   DVD

Type

ISO/IEC 16448:1999, 120 mm DVD - Read-Only Disk

Format specification

4.7GB, conforming to either ISO 9660 or OSTA UDF(1.02 and higher)

4.5   DVD-R

Type

Standard ECMA-279, 120 mm (3,95 Gbytes per side) DVD-Recordable Disk (DVD-R)

Format specification

3.95GB, conforming to either ISO 9660 or OSTA UDF(1.02 and higher)

[End of Appendix, Annex and document]