E

WIPO

PCT/AI/1 Add.7
ORIGINAL: French
DATE: June 28, 2000

WORLD INTELLECTUAL PROPERTY ORGANIZATION

GENEVA

PATENT COOPERATION TREATY (PCT)

ADMINISTRATIVE INSTRUCTIONS
UNDER THE PATENT COOPERATION TREATY:

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

COMMENTS BY THE
NATIONAL INSTITUTE OF INDUSTRIAL PROPERTY OF FRANCE

for consideration at a
PCT informal consultation meeting on electronic filing,
Geneva, July 11 to 14, 2000

COMMENTS BY THE
NATIONAL INSTITUTE OF INDUSTRIAL PROPERTY OF FRANCE

1. At its twenty-eighth session (Geneva, March 13-17), the PCT Union Assembly requested the International Bureau to redraft the Administrative Instructions on electronic filing in the light of a certain number of principles,[1] including the introduction of an electronic filing system based on an environment of PKI (Public Key Infrastructure) type. It was decided that the national experts (both lawyers and computer specialists) would meet around mid-July for informal consultations to discuss more thoroughly the redraft of the Administrative Instructions, the aim being to submit a final text to the Offices gathered for the WIPO/PCT Assemblies in September 2000.

2. The French Delegation is pleased with the new draft Administrative Instructions presented by the International Bureau (document PCT/AI/1 Add.2 Prov.) and the new draft Annex F as written by the International Bureau, the EPO and the USPTO (documents PCT/AI/1 Add.3 to 6 Prov.), which very extensively reflect the comments expressed by delegations at the Assembly meeting in March. There are however certain points that require clarification; above all *the crucial question of cross-certification is not dealt with*, which has the makings of a definite problem when electronic filing is actually implemented at the international level.

I – COMMENTS ON THE DRAFT ADMINISTRATIVE INSTRUCTIONS
(document PCT/AI/1 Add.2 Prov.)

1. *IA 702*: Paragraph (b)(i) states that any copy of the package may be considered the record copy for the purpose of the filing of the international application. Should there not be a mention of the record copy on a write-once medium, on reception of the said international application (cf. the comments on IA 708(c)(i))? How is paragraph (c) to be understood in conjunction with §2(f) of Annex F, Appendix III ("the specification must contain an incorporation-by-reference of the material on the physical medium …")?

Paragraph (d) states that the electronic form of an application filed on paper may be considered the record copy within the meaning of PCT Article 12. If however the scanning of the application produces an error (a page, line or date of receipt, for instance, that is not digitized), that putative record copy would not be consistent with the copy filed with the receiving Office. In order to avoid such a risk, a systematic check would have to be made to ensure that the paper copy and the electronic copy are identical. That amounts to a considerable burden for which receiving Offices will have to prepare themselves if they choose to forward to the International Bureau scanned record copies of applications filed on paper.

2. *AI 703*: Paragraph (b) could be redrafted to make it clearer ("(b) where the international application is not in an electronic document format accepted by the receiving Office, the receiving Office may consider that the application does not meet the physical requirements referred to in Article 14(1)(a)(v), in which case the receiving Office shall proceed

[1] See the report, PCT/A/28/5, page 7.

accordingly.”). How is the word “*sinon*” to be understood? In what case can the receiving Office actually determine the date of entry into force of an amendment?

Is paragraph (h) really of any use? After all, it probably concerns only those cases in which applications are filed electronically but on a physical medium (such as a diskette). If ever applicants feel there is a risk of contamination with a virus, they will file their applications on paper only. Conversely, if filing in diskette form is considered safe, applicants will not bother to send their applications in paper form as well. In any event, the words “where such a paper copy is received on the same day as the application in electronic form” could be removed without the meaning of the paragraph being altered. The following sentence could be redrafted as follows: “In that case the receiving Office would choose the paper copy rather than the application in electronic form where the latter is unusable. The receiving Office shall inform the applicant accordingly.”

3. *IA 706*: In paragraph (a), the words “to the extent that it is illegible [has been distorted in meaning], or that the attempted transmission failed …” could be deleted. Apart from that, how is the expression “[or appears to be distorted in meaning]” to be interpreted? In the Receiving Office Guidelines (paragraph 16) there is no mention of any requirement that a verification of the contents of the application be made by receiving Offices. The comment refers to a “central virus scanning system” included within WIPOnet. What is that?

4. *IA 707*: Paragraph (a) says that international applications in electronic form are to be processed in accordance with Annex F, without any reference to the Treaty, to the Regulations or indeed to the Administrative Instructions. Annex F deals only with the technical requirements to which Offices have to conform. Paragraph (d) says that records management has to conform to Annex F, in addition to Instruction 708(c). However, the former Appendix 5 on electronic file management was (quite rightly) removed from Annex F so that it could where necessary serve as a subsidiary document having the value of a mere recommendation (guideline). Paragraph (d) should not therefore refer to Annex F, which no longer deals with filing, but only to paragraph (c) of Instruction 708.

5. *IA 708*: The above comment applies also to this Instruction, in the sense that no reference should be made to Annex F. In the comment on paragraph (a), the International Bureau rightly raises the question of the audits necessary to ensure that Instruction 708 is properly applied, yet it is not very explicit on the subject, which inclines our Delegation to ask itself the following questions: how is the verification system thought out, what authority would be in control, with what frequency would audits be undertaken, and what would be the cost of such a policy?

Paragraph (b) does not seem necessary to our Delegation, inasmuch as Offices are already committed, by virtue of the provisions of paragraph (a), to keeping and storing electronic records in accordance with Rule 93, and in any case according to the principles set forth in paragraph (c). It is therefore unnecessary to ask Offices to issue certificates attesting that they actually do meet the conditions set forth in the PCT Administrative Instructions, unless one were to require those Offices to allow external audits to be undertaken, which would draw strong reservations from our Delegation on account of still-latent uncertainties (cf. the previous paragraph). The French Delegation wonders how the certificates issued by those Offices could have greater evidentiary value before national or foreign courts than the assurance that the Office is bound by the PCT Administrative Instructions. In paragraph (c), item (i) should add that the application has to be stored on a write-once medium (of CD-Rom

or CD-Worm type) for the purpose of the preservation of the file (document of evidentiary value).

6. *IA 709*: Annex F gives nothing specific on access to the international application via electronic media, as Chapter 9 of Appendix 1 does no more than make general statements.

7. *IA 711*: Paragraph (c) could reverse the present approach as follows: "Where the designated Office does not inform the International Bureau that it accepts the electronic filing of electronic international applications in accordance with paragraph (b), the International Bureau or, where appropriate, the receiving Office shall provide it with a paper copy of any document that has been filed or is stored in electronic form." Our Delegation also wonders in what cases the designated Office could actually see fit to ask the receiving Office for a copy of an international application.

8. *General comments*: it would be more logical to reverse the order of Instructions 702 and 703, in order to consider the acceptance of applications by receiving Offices before dealing with their effects. Instruction 701 could be placed at the end of Part 7 of the Administrative Instructions inasmuch as it concerns the whole Part, including the processing of international applications by designated Offices.

II. COMMENTS ON DRAFT ANNEX F
(documents PCT/AI/1 Add.3 Prov. to Add. 6 Prov.)

APPENDIX I

5.1

There is news of a move towards the use of open software for document processing in order to justify the abandonment of .doc, .wps and other formats as acceptable formats.

In the same spirit it would be wise to mention at this stage already that the PDF format is an owner format, the use of which is subject to payment for licenses, and that it should be abandoned in favor of XML as soon as possible, on the understanding that PDF is a fact of life nowadays.

5.1.3

At first sight XML documents created with the aid of proprietary software (such as Microsoft's Word 2000 word processing software, or a drawing tool) will not conform to Appendix II in so far as it provides only for DTDs specific to IP documents.

It should therefore be made clear what XML documents Appendix II should apply to; if it applies to all XML documents without distinction, that should bear out the suggestion that applicants will be in a position to create documents (descriptions, drawings and so on) that conform to Appendix II with the tools obtainable from classical sources.

APPENDIX III

1

No problem with what is said there. In any event INPI will not be in a position to accept *en bloc* the carrier formats specified.

2(g)

Should the expression "labelled" be understood in the sense of physical labelling on the actual medium (with a sticker, for instance)? If the labelling can be done in a logical way (that is, by the addition of data on the physical medium), which seems somewhat unlikely, this idea should be made clearer (inclusion of an additional file, definition of the file format, etc.).

III. QUESTIONS THAT HAVE YET TO BE CLARIFIED CONCERNING CERTIFICATION AUTHORITIES AND CROSS-CERTIFICATION

1. In the course of the discussions on certification, it was mentioned that the International Bureau of WIPO might serve as Certification Authority. However, it does seem that a number of national Offices are also prepared to approve Certification Authorities.[2] *The redraft of the Administrative Instructions moreover reflects this fact by providing in draft Instruction 703(c)(i) that Offices shall convey to the International Bureau a list of acceptable Certification Authorities and the acceptable classes of digital certificates.*[3]

Question 1: How does the International Bureau intend to implement its Certification Authority plan? In what legal framework and with what financing? Is it acceptable for a body involved in transmittal, even if it is a public body, to serve also as Certification Authority? Should certification not be done by independent third parties in order to avoid any risk of a conflict of interest?[4]

Question 2: In the interest of uniformization, is there any plan for guidelines for the accreditation of Certification Authorities to national Offices?

Comments: National Offices should be able to choose freely the Certification Authorities acceptable to them, with the possibility of accepting two or more in order that a degree of competition may be allowed to develop, and so that the costs associated with certification may be the lowest possible. What still remains to be decided is who is going to have to defray those costs. The Certification Authorities should meet a certain number of conditions specific to the electronic filing of patent applications, and Offices should undertake to ensure

[2] For instance, the Finnish and Spanish Offices seem already to have approved Certification Authorities for the exchange of electronic documents.

[3] cf. document PCT/AI/1 Add.2 Prov, p. 9.

[4] cf. Chapter III of the draft Uniform Rules on Electronic Signatures, 32nd session of UNCITRAL, Vienna, January 1998.

observance of those conditions. Then the question to be answered would be what the legal consequences of failure to meet the conditions would be.[5]

2. *There is still a grey area with regard to cross-certification.*[6] *There has been no document to explain this important question, which is completely left out of the draft PCT Administrative Instructions.*

Question 3: To what extent are certificates recognized by the receiving Office also recognized by designated offices and competent legal authorities? In other words, is recognition of an electronic signature certified by a Certification Authority acceptable to the receiving Office assured in the designated State, notably in terms of the legislation of that State?

Question 4: What body would be responsible for ensuring that the Certification Authorities implemented procedures consistent with the PCT Administrative Instructions? Would it be the International Bureau of WIPO, a separate international body or the national offices themselves?

Comments: clear rules should be laid down at the outset so that users may have faith in this system, which is legally recognized. One could usefully refer to texts at both Community[7] and international[8] level which recognized the need to introduce legal recognition of electronic certificates issued in other countries.

3. With regard to all these questions, it is the view of our Delegation that *substantive work has yet to be done on the subject of certification* in order to devise a system of cross-certification with the aim that the mutual recognition of Certification Authorities may be technically efficient and also fully effective in law.

4. The need to introduce electronic filing is acknowledged, and our Delegation does not by any means wish to slow the process that has now started. However, *the challenge to be met is all the greater for its success depending, to a large extent, on the credibility of the system to applicants, and therefore on the legal security provided.* By the time electronic filing is actually operational, all the legal difficulties that might affect electronic filing must have been overcome.

---

[5] As far as Certification Authorities are concerned, European Directive 99/93/EC on electronic signatures provides for instance that "As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate (…)" (Article 6). Cf. also Articles 9 ("responsibilities of the signature device holder") and 10 ("responsibilities of a supplier of certification services") of the latest version of the draft Uniform Rules on Electronic Signatures, 36th session of UNCITRAL, New York, February 2000.

[6] cf. item 3.5 of the final document of the seventh Trilateral Conference (Berlin, November 8 to 12, 1999).

[7] At Community level, solutions have been found in Directive 1999/93/EC on electronic signatures, which sets out the conditions that have to be met for the mutual legal recognition of electronic signatures issued by certification authorities that meet the conditions referred to in the Directive (Article 7.1). The Directive also provides that the Commission could initiate bilateral or multilateral negotiations to settle the difficulties at the international level (Article 7.2).

[8] cf. Annex.

ANNEX

Nothing has yet been planned at the international level with respect to cross-certification, even though the problem has been acknowledged (cf. Article 7 of the Community Directive). For information, the latest version of the draft Uniform Rules on Electronic Signatures, drawn up at the thirty-sixth session of UNCITRAL (New York, February 2000), contains an Article 13 on the "Recognition of Foreign Certificates and Electronic Signatures," which provides as follows:

[(1) In determining whether, or the extent to which, a certificate [or an electronic signature] is legally effective, no regard shall be had to the place where the certificate [or the electronic signature] was issued, nor to the State in which the issuer had his place of business.]

(2) Certificates issued by a foreign supplier of certification services are recognized as legally equivalent to certificates issued by suppliers of certification services operating under [the law of the enacting State] if the practices of the foreign suppliers of certification services provide a level of reliability at least equivalent to that required of suppliers of certification services under [the law of the enacting State]. [Such recognition may be made by a published determination of the State or through bilateral or multilateral agreement between or among the States concerned.]

(3) Signatures complying with the laws of another State relating to electronic signatures are recognized as legally equivalent to signatures under … [the law of the enacting State] if the laws of the other State require a level of reliability at least equivalent to that required for such signatures under … [the law of the enacting State]. [Such recognition may be made by a published determination of the State or through bilateral or multilateral agreement with other States.]

(4) In determining equivalence, regard shall be had, if appropriate, [to the factors in paragraph (2) of Article 10] [to the following factors:

(a) financial and human resources, including existence of assets within the jurisdiction;

(b) trustworthiness of hardware and software systems;

(c) procedures for processing of certificates and applications for certificates and retention of records;

(d) availability of information to the [signers] [subjects] identified in certificates and to potential relying parties;

(e) regularity and extent of audits by an independent body;

(f) the existence of a declaration by the State, an accreditation body or the certification authority regarding compliance with or existence of the foregoing;

(g) susceptibility to the jurisdiction of courts of the enacting State; and

(h) the degree of discrepancy between the law applicable to the conduct of the certification authority and the law of the enacting State].

(5) Notwithstanding paragraphs (2) and (3), parties to commercial and other transactions may specify that a particular supplier of certification services, class of suppliers of certification services or class of certificates must be used in connection with messages or signatures submitted to them.

(6) Where, notwithstanding paragraphs (2) and (3), the parties agree, as between themselves, to the use of certain types of electronic signatures and certificates, [that agreement shall be recognized as sufficient for the purpose of cross-border recognition]. [In determining whether, or the extent to which, an electronic signature or certificate is legally effective, regard shall be had to any agreement between the parties to the transaction in which that signature or certificate is used].

[End of document]