WIPO
OMPI

PCT/EF/PFC 04/001

STATUS AT: July 20, 2004
SITUATION AU : 20 juillet 2004

W O R L D I N T E L L E C T U A L P R O P E R T Y O R G A N I Z A T I O N
O R G A N I S A T I O N M O N D I A L E D E L A P R O P R I É T É I N T E L L E C T U E L L E
GENEVA/GENÈVE

ADMINISTRATIVE INSTRUCTIONS UNDER THE PATENT COOPERATION TREATY (PCT)

STANDARD FOR THE ELECTRONIC FILING AND PROCESSING OF INTERNATIONAL APPLICATIONS

INSTRUCTIONS ADMINISTRATIVES DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

NORME CONCERNANT LE DÉPÔT ET LE TRAITEMENT ÉLECTRONIQUES DES DEMANDES INTERNATIONALES

PROPOSAL FOR CHANGE FILE

DOSSIER RELATIF À LA PROPOSITION DE MODIFICATION

SUBJECT: **SUJET :**	SSL Authentication (Annex F, section 5.1.2.1) Authentification par voie SSL (section 5.1.2.1 de l'annexe F)	**PROPOSED BY:** **PROPOSÉE PAR :**	JP, EP, US
HANDLING: **TRAITEMENT :**	Expedited cycle Cycle accéléré	**PROPOSED DATE OF ENTRY INTO FORCE:** **DATE PROPOSÉE D'ENTRÉE EN VIGUEUR :**	01.01.2005

ANNEX/ ANNEXE	CONTENT/CONTENU	ORIGIN/ ORIGINE	DATE
1	Proposal/Proposition	JP, EP, US	02.04.2004

[Annex 1 follows/
L'annexe 1 suit]

NEXT ACTION: **PROCHAINE ACTION :**	recommendations recommandations	**BY:** **POUR LE :**	31.08.2004

ANNEX 1/ ANNEXE 1

SSL Authentication

1. Proposed Changes

The Annex F-5.1.2.1 should be changed as follows.

5.1.2.1 Use of the SSL Tunnel

These events are all performed within an SSL tunnel that is established before issuing the Begin Transaction event. The SSL tunnel is built using both client and server authentication. The SSL tunnel may be stopped at the end of the transaction or, if a batch of transmission is foreseen, the SSL tunnel can be left open and only stopped when all transmissions are complete. The SSL tunnel uses the SSL protocol version 3.0.

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

(1) Data of the applicant/representative digital certificate(s) obtained beforehand by the RO is stored in the server.
(2) At the time of client authentication by SSL3.0, 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 process (1).
(3) If the check result in the above (2) is a negative one, the server disconnects the SSL tunnel.

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

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

2. Notes for the changes

The following notes should also be added as footnotes in connection with the changes.

(1) By storing the data of applicant/representative's digital certificate in the server, the RO is able to refuse any communication made using a digital certificate whose data has not been stored in the server beforehand. With this function, the server's robustness against Denial of Service (DOS) attack can be enhanced.

(2) The pre-registration should be dealt with using an on-lineprocess . The pre-registration mechanism is analogous to a creation of a new account for numerous existing Internet sites exchanging confidential and/or value-added information with secure network connectivity such as on-line shopping, on-line subscription etc. and therefore has already been generally

accepted by the public. It should not take unduly long time to complete the pre-registration compared to the obtaining procedure for low-level certificate. Thus the mechanism of pre-registration would not cause any delay of obtaining filing date for first time filers or *pro se* applicants with low-level certificates. Therefore, this pre-registration would not negate the Basic Common Standard, which provides for the use of low-level certificates enabling them to file their application as early as possible to avoid loss of rights under first-to-file system.

(3) Considering such cases as when the language used for the digital certificate of the applicant/representative differs from the language used by the RO, it is desirable that the RO may require the applicant/representative to provide the RO with additional information on the applicant/representative.

3. Reasons for proposed changes

Reasons for the changes are described in the above notes.

[End of Annex and of file/
Fin de l’annexe et du dossier]