WIPO
OMPI

PCT/EF/PFC 09/004

STATUS AT: February 17, 2010
SITUATION AU : 17 février 2010

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 :**	Changes to Annex F, Appendix I, section 3.6 (Addition of TLS alongside SSL as encryption communication protocol) Modifications de la section 3.6 de l'appendice I de l'annexe F (Addition of TLS alongside SSL as encryption communication protocol)	**PROPOSED BY:** **PROPOSÉE PAR :**	EP,JP,US
HANDLING: **TRAITEMENT :**	Expedited cycle Cycle accéléré	**PROPOSED DATE OF ENTRY INTO FORCE:** **DATE PROPOSÉE D'ENTRÉE EN VIGUEUR :**	1.07.2010

ANNEX/ ANNEXE	CONTENT/CONTENU	ORIGIN/ ORIGINE	DATE
1	Addition of TLS alongside SSL as encryption communication protocol	EP,JP,US	15.10.2009
2	Comment	IB	2.11.2009
3	Comment	SK	16.12.2009
4	Comment	UZ	18.12.2009
5	Comment	RU	22.12.2009
6	Comment	US	14.01.2010
7	Comment	IB	5.02.2010

[Annex I follows/
L'annexe I suit]

NEXT ACTION: **PROCHAINE ACTION :**	Entry in to force Entrée en vigueur	**BY:** **POUR LE :**	1.7.2010

ANNEX I /ANNEXE I

ADDITION OF TLS ALONGSIDE SSL FOR USE AS ENCRYPTION COMMUNICATION PROTOCOL

1. Introduction

At present, SSL is the only protocol which is accepted as encryption communication protocol compliant with PCT technology standard. SSL is the de facto standard developed by Netscape Communications Corp., and has been upgraded to version 3.0. In the meantime, another protocol, TLS, is developed, which is regarded as successor to SSL. TSL is developed by ITEF (Internet Engineering Task Force), aiming at standardization of communication via the Internet, and releasing its specifications on the RFC. Furthermore, currently it is more common that both SSL and TLS are permitted in the universal browser.

Taking all into considerations, the JPO supposes that TLS should be permitted in addition to SSL. Currently, there is not a recognized urgent need to do so. However, given an opportunity to present a proposal on revising cryptographic algorithm (SHA-1) of Annex F, the JPO has captured this moment as the best timing to propose on addition of TLS.

2. Revised Contents

The followings are the revised contents accompanied by addition of TLS.

Where “SSL” is referred, “TLS” is added behind it.
Specifically, “SSL is replaced with “SSL (or TLS)”

The statement of “The Receiving Office (RO) has discretion over which protocol to be used, SSL or TLS." is inserted.

The definition of “TLS” is added.

3. Others (for reference)

The definitions of “SSL” and “TLS” are as follows.

- SSL□Secure Socket Layer□
  SSL is a protocol to provide security for communication developed by Netscape Communications Corp. Given client/server authentications and encrypted communication between them, transmitting private documents via the Internet is possible. SSL has been upgraded to version 3, and its specifications are revealed as “The SSL Protocol Version 3.0.”

- TLS□Transport Layer Security□
  TLS is a protocol to provide security for communication between client and server. In communicating, mutual authentication using the certificate is

performed, and then encrypted communication starts. In order to generalize SSL developed by Netscape Communications Corp, IETF has been presenting TSL as subsequent to SSL.

- The latest version of TLS is version 1.2 (as of May 8, 2009)
  - RFC 2246 January 1999 The TLS Protocol Version 1.0
  - RFC 4346 April 2006 The Transport Layer Security (TLS) Protocol Version 1.1
  - RFC 5246 August 2008 The Transport Layer Security (TLS) Protocol Version 1.2

4. Proposed Changes to Annnex F of the PCT Administrative Instructions

Submitted by	EPO, JPO, USPTO	Date:	2009-10-15
Requested Modification	Addition of TLS		
PFC TO-09/01	**<Modified Section>** page 33 5.1.4 Transaction management header elements *Changed from:* The protocol is designed to support HTTP communication over an SSL Tunnel for all PKI based E-filing solutions and includes the following capabilities: *To:* 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:		
Items Impacted			
Reason	To make TLS available		

NEXT ACTION:	Entry into force	**BY:**	1.07.2010
PROCHAINE ACTION :	Entrée en vigueur	**POUR LE :**	

Submitted by	EPO, JPO, USPTO	Date: 2009-10-15
Requested Modification	Addition of TLS	
PFC TO-09/02	**<Modified Section>** page 34□5.1.2.1 Use of the SSL tunnel for application *Changed from:* 5.1.2.1 Use of the SSL tunnel for application 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 transmissions 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 supported by the SSL protocol version 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: (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, 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 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 tunnel is disconnected in the process described above, the current protocol requires each individual transaction to be acknowledged by an individual receipt. *To:* 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.
Items Impacted	
Reason	To make TLS available

Submitted by	EPO, JPO, USPTO	Date: 2009-10-15
Requested Modification	Addition of TLS	

PFC TO-09/03	**<Modified Section>**
	page 34□5.1.2.2 Application level events for application
	
	Changed from:
	`Start SSL session (See Figure 5)`
	
	To:
	`Start SSL(or TLS) session (See Figure 5)`	

Items Impacted		
Reason	To make TLS available	

NEXT ACTION:	Entry into force	**BY:**	1.07.2010
PROCHAINE ACTION :	Entrée en vigueur	**POUR LE :**	

Submitted by	EPO, JPO, USPTO	Date: 2009-10-15
Requested Modification	Addition of TLS	
PFC TO-09/04	**<Modified Section>** page 36□5.1.2.2 Application level events for application *Changed from:* Close SSL session In all cases of SSL Tunnel, the current protocol requires each individual transaction to be acknowledged by an individual receipt. *To:* 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.	
Items Impacted		
Reason	To make TLS available	

NEXT ACTION:	Entry into force	**BY:**	1.07.2010
PROCHAINE ACTION :	Entrée en vigueur	**POUR LE :**	

Submitted by	EPO, JPO, USPTO	Date: 2009-10-15
Requested Modification	Addition of TLS	
PFC TO-09/05	**<Modified Section>** page 37 Figure 5 – Application level protocol behavior for application *Changed from:* Establish SSL Client/Server Authentication End SSL Session *To:* Establish SSL(or TLS) Client/Server Authentication End SSL(or TLS) Session	
Items Impacted		
Reason	To make TLS available	

NEXT ACTION:	Entry into force	**BY:**	1.07.2010
PROCHAINE ACTION :	Entrée en vigueur	**POUR LE :**	

Submitted by	EPO, JPO, USPTO	Date: 2009-10-15
Requested Modification	Addition of TLS	
PFC TO-09/06	**<Modified Section>** page 38□5.1.3.1 Use of the SSL tunnel for notification *Changed from:* 5.1.3.1 Use of the SSL tunnel for notification Refer to Section 5.1.2.1, "Use of the SSL tunnel for application." *To:* 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."	
Items Impacted		
Reason	To make TLS available	

NEXT ACTION:	Entry into force	**BY:**	1.07.2010
PROCHAINE ACTION :	Entrée en vigueur	**POUR LE :**	

Submitted by	EPO, JPO, USPTO	Date: 2009-10-15
Requested Modification	Addition of TLS	
PFC TO-09/07	**<Modified Section>** page 39□5.1.3.2 Application level events for notification *Changed from:* Start SSL session (See Figure 6) *To:* Start SSL(or TLS) session (See Figure 6)	
Items Impacted		
Reason	To make TLS available	

NEXT ACTION:	Entry into force	**BY:**	1.07.2010
PROCHAINE ACTION :	Entrée en vigueur	**POUR LE :**	

Submitted by	EPO, JPO, USPTO	Date: 2009-10-15
Requested Modification	Addition of TLS	
PFC TO-09/08	**<Modified Section>** page 40□5.1.3.2 Application level events for notification *Changed from:* Close SSL session In all cases of SSL Tunnel, the current protocol requires that, for each transaction, the client acknowledge the reception by sending Receipt Check Notice to the server. *To:* 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.	
Items Impacted		
Reason	To make TLS available	

Submitted by	EPO, JPO, USPTO	Date: 2009-10-15
Requested Modification	Addition of TLS	
PFC TO-09/09	**<Modified Section>** page 41 Figure 6 – Application level protocol behavior for notification *Changed from:* Establish SSL Client/Server Authentication End SSL Session *To:* Establish SSL(or TLS) Client/Server Authentication End SSL(or TLS) Session	
Items Impacted		
Reason	To make TLS available	

NEXT ACTION:	Entry into force	**BY:**	1.07.2010
PROCHAINE ACTION :	Entrée en vigueur	**POUR LE :**	

Submitted by	EPO, JPO, USPTO	Date: 2009-10-15
Requested Modification	Addition of TLS	
PFC TO-09/10	**<Modified Section>** page 58□5.2.1 Applicant-Office communication (international phase) sector *Changed from:* (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); (iii) a Virtual Private Network (VPN) connection over the Internet. *To:* (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.	
Items Impacted		
Reason	To make TLS available	

NEXT ACTION:	Entry into force	**BY:**	1.07.2010
PROCHAINE ACTION :	Entrée en vigueur	**POUR LE :**	

Submitted by	EPO, JPO, USPTO	Date: 2009-10-15
Requested Modification	Addition of TLS	
PFC TO-09/11	**<Modified Section>** page 59□5.2.2 Office-Office communication sector *Changed from:* (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); (iii) a Virtual Private Network (VPN) connection over the Internet. *To:* (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.	
Items Impacted		
Reason	To make TLS available	

NEXT ACTION:	Entry into force	**BY:**	1.07.2010
PROCHAINE ACTION :	Entrée en vigueur	**POUR LE :**	

Submitted by	EPO, JPO, USPTO	Date: 2009-10-15
Requested Modification	Addition of TLS	
PFC TO-09/12	**<Modified Section>** page 62□5.2.3 Designated Office communication sector *Changed from:* (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); (iii) a Virtual Private Network (VPN) connection over the Internet. *To:* (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.	
Items Impacted		
Reason	To make TLS available	

NEXT ACTION:	Entry into force	**BY:**	1.07.2010
PROCHAINE ACTION :	Entrée en vigueur	**POUR LE :**	

Submitted by	EPO, JPO, USPTO	Date: 2009-10-15
Requested Modification	Addition of TLS	
PFC TO-09/13	**<Modified Section>** page 67□9. ABBREVIATED EXPRESSIONS, INTERPRETATION AND GLOSSARY *To be added* Add an explanation of TLS to the table on page 67 (between "TIFF" and "WAD"), as presented below. Abbreviation□ TLS Explanation□ transport layer security	
Items Impacted		
Reason	To make TLS available	

Submitted by	EPO, JPO, USPTO	Date: 2009-10-15
Requested Modification	Addition of TLS	
PFC TO-09/14	**<Modified Section>** page 72□4.2 Encryption within the PCT trust model *Changed from:* Encryption of packages made under this standard will be provided by SSL (see the E-filing interoperability protocol, Annex F, section 5.1). For packages sent using SSL, 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. *To:* 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.	
Items Impacted		
Reason	To make TLS available	

NEXT ACTION:	Entry into force	**BY:**	1.07.2010
PROCHAINE ACTION :	Entrée en vigueur	**POUR LE :**	

Submitted by	EPO, JPO, USPTO	Date:	2009-10-15
Requested Modification	Addition of TLS		
PFC TO-09/15	**<Modified Section>** page 72□4.3 Certification authority *Changed from:* 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. *To:* 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).		
Items Impacted			
Reason	To make TLS available		

NEXT ACTION:	Entry into force	**BY:**	1.07.2010
PROCHAINE ACTION :	Entrée en vigueur	**POUR LE :**	

Submitted by	EPO, JPO, USPTO	Date: 2009-10-15
Requested Modification	Addition of TLS	
PFC TO-09/16	**<Modified Section>** page 75□4.4.5.1 Low-level certificate *Changed from:* 7. The applicant retrieves the new certificate (via secure channel, e.g. SSL) after the authorization code and challenge phrase is validated. *To:* 7. The applicant retrieves the new certificate (via secure channel, e.g. SSL(or TLS)) after the authorization code and challenge phrase is validated.	
Items Impacted		
Reason	To make TLS available	

Submitted by	EPO, JPO, USPTO	Date: 2009-10-15
Requested Modification	Addition of TLS	
PFC TO-09/17	**<Modifed Section>** page 76□4.4.6.2 Encryption *Changed from:* Subscribers encrypt international application packages using the SSL protocol (see Protocol in section 5.1 of Annex F) or optionally, the destination party's public encryption key. See section 4.2 for additional information on encrypting international application packages. *To:* 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.	
Items Impacted		
Reason	To make TLS available	

[Annex II follows /
L'annexe II suit]

NEXT ACTION:	Entry into force	**BY:**	1.07.2010
PROCHAINE ACTION :	Entrée en vigueur	**POUR LE :**	

ANNEX II /ANNEXE II

Comment by the International Bureau

For administrative reasons the International Bureau has proposed an entry into force date of July 1, 2010; the International Bureau welcomes indications as to whether this is a realistic date for implementation.

[Annex III follows /
L'annexe III suit]

NEXT ACTION:	Entry in to force	**BY:**	1.7.2010
PROCHAINE ACTION :	Entrée en vigueur	**POUR LE :**	

ANNEX III /ANNEXE III

Comment by the Industrial Property Office of the Slovak Republic

The Industrial Property Office of the Slovak Republic in its capacity as a receiving Office under the Patent Cooperation Treaty has no comments concerning the proposals for change to the Standard for the Electronic Filing and Processing of International Applications under PCT which are mentioned in the Circular C.PCT 1194.

[Annex IV follows /
L'annexe IV suit]

ANNEX IV /ANNEXE IV

Comment by the Republic of Uzbekistan State Patent Office

The State patent Office of the Republic of Uzbekistan has no comments or proposals regarding this circular.

[Annex V follows /
L'annexe V suit]

NEXT ACTION:	Entry in to force	**BY:**	1.7.2010
PROCHAINE ACTION :	Entrée en vigueur	**POUR LE :**	

ANNEX V /ANNEXE V

Comment by the Federal Service for Intellectual Property, Patents and Trademarks (ROSPATENT)

Referring to the Circular letter C.PCT 1194 of November 5, 2009 we would like to communicate that the specialists of the Federal Service fir Intellectual Property, Patents and Trademarks (ROSPATENT) have carefully considered the proposed modifications to Annex F of the Administrative Instructions under the PCT and have no objections to them.

[Annex VI follows /
L'annexe VI suit]

ANNEX VI /ANNEXE VI

Comment by the United States Patent and Trademark Office

In PCT/EF/PFC 09/004, Annex I page 2, item 4 mentions Requested Modification PFC TO-09/01 <Modified Section> page 33: *5.1.4 Transaction management header elements*. Based on the modification to the text that is presented, it appears that the reference to page 33 should instead be to page 32: *5.1 The E-filing interoperability protocol*.

[Annex VII follows /
L'annexe VII suit]

ANNEX VII /ANNEXE VII

Comment by the International Bureau

Following review of the comments received the International Bureau agrees with the suggested modification of the proposal from the United States Patent and Trademark Office to modify the reference from 'page 33: *5.1.4 Transaction management header elements'* to 'page 32: *5.1 The E-filing interoperability protocol'*, and will modify Annex F of the administrative instructions as described in the proposal above, with this modification, ready for entry into force on July 1, 2010.

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

NEXT ACTION:	Entry in to force	**BY:**	1.7.2010
PROCHAINE ACTION :	Entrée en vigueur	**POUR LE :**	