F

OMPI

PCT/AI/1 Add.9
ORIGINAL : français
DATE : 29 juin 2000

ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE
GENÈVE

TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

INSTRUCTIONS ADMINISTRATIVES DU
TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS

PROPOSITIONS DE MODIFICATION RELATIVES AU DÉPÔT, AU TRAITEMENT ET À L'ARCHIVAGE ÉLECTRONIQUES DES DEMANDES INTERNATIONALES ET À LA GESTION DES DOSSIERS ÉLECTRONIQUES RELATIFS À CES DEMANDES

COMMENTAIRES
DE L'OFFICE ALLEMAND DES BREVETS ET DES MARQUES

pour examen
lors d'une réunion consultative informelle du PCT relative au dépôt électronique, Genève, 11-14 juillet 2000

OBSERVATIONS RELATIVES AUX INSTRUCTIONS ADMINISTRATIVES
DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS
(Document PCT/AI/1/Add.2 Prov., en date du 10 mai 2000)

Il conviendrait d'ajouter l'alinéa suivant à l'instruction 704 :

c) Tout office récepteur peut exiger que le déposant s'inscrive pour participer au dépôt électronique des demandes internationales. Lorsque la demande internationale est déposée sans que le déposant soit inscrit, l'office récepteur n'est pas tenu d'accepter ou de traiter la demande. Si l'office récepteur décide de recevoir cette demande, celle-ci est considérée comme ne remplissant pas les conditions matérielles visées à l'article 14.1)a)v) et l'office récepteur agit en conséquence.

[COMMENTAIRE : En inscrivant le déposant, il est possible d'empêcher des déposants non identifiables de bloquer l'accès à l'office récepteur en déposant des demandes en grand nombre. La création de comptes d'utilisateurs permet d'identifier l'expéditeur des données déposées, indépendamment de la "signature numérique renforcée".

Lors de l'inscription des déposants auprès de l'office récepteur, qui peut aussi s'effectuer électroniquement, l'office récepteur crée un compte d'utilisateur contenant les données d'accès (identification et mot de passe du déposant) nécessaires pour participer au dépôt électronique des demandes. Ces données peuvent également être utilisées comme certificat ad hoc (PCT/AI/1 Add. 3 Prov.). L'office récepteur doit transmettre l'identification et le mot de passe au déposant en toute sécurité. La transmission de ces données peut s'effectuer électroniquement, si des mécanismes de transmission fiables entre le déposant et l'office ont déjà été établis. Le service postal peut aussi être utilisé pour une transmission en toute sécurité. Les modalités techniques correspondantes devraient être précisées dans l'annexe F.]

L'instruction 706.b) devrait être modifiée de la manière suivante :

b) Tout office récepteur qui accepte les demandes internationales déposées sous forme électronique conformément à l'instruction 703.a) vérifie si les demandes ne sont pas contaminées par des virus ou d'autres éléments malveillants. S'il constate qu'une demande électronique est contaminée par un virus ou par un autre élément malveillant, il ~~notifie ce fait à bref délai au déposant, peut exiger que le déposant lui envoie un nouvel exemplaire de la demande et utilise tous les moyens qui lui sont normalement disponibles pour la lire (aux fins de la vérification visée à l'article 11) tels que notamment, mais pas uniquement, l'impression. L'office récepteur n'est pas tenu de nettoyer les fichiers contaminés, mais il prend toutes les mesures nécessaires pour préserver, lorsque cela est possible, la date de dépôt international~~ peut considérer que la demande est illisible en vertu de l'alinéa a). Dans ce cas, l'office

récepteur notifie ce fait à bref délai au déposant et l'invite à lui envoyer un nouvel exemplaire de la demande.

[COMMENTAIRE : L'office récepteur ne devrait pas être tenu d'accepter des données infectées et de traiter, stocker, archiver ou transmettre ces données sous quelque forme que ce soit, y compris sous forme imprimée, car l'acceptation de telles données implique toujours un risque de propagation des virus et d'altération des données et des systèmes. L'office récepteur devrait néanmoins avoir la possibilité d'accepter la demande si, pour une raison ou une autre, cela ne présente aucun risque. En tout état de cause, l'utilisation de pare-feux et d'antivirus empêchera les données infectées de pénétrer au sein de l'office. Dans le cadre de ces techniques, il conviendrait de choisir des procédés informant automatiquement l'expéditeur du type de virus contaminant ses données.]

OBSERVATIONS RELATIVES AUX INSTRUCTIONS ADMINISTRATIVES DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (ANNEXE F) (Document PCT/AI/1 Add. 4 Prov., en date du 9 juin 2000)

Le document n'indique pas clairement si la norme PCKS#7 est utilisée pour la signature ou le codage.

5.1 Préparation des documents, paragraphe 4

Il conviendrait de supprimer ce paragraphe, car la norme ne devrait pas faire état d'"avantages" ni de systèmes exclusifs.

5.3 Signature des documents constitutifs de la demande compactés

Il y a une contradiction. Alors que le point 4 ("Mécanismes de signature") prévoit différentes options pour les signatures (signatures électroniques simples ou renforcées), le point 5.3 exige que les documents compactés soient exclusivement signés au moyen d'une signature électronique renforcée (voir le paragraphe 2 : "Les spécifications PKCS#7 sont appliquées pour la production d'un type "données signées" pour la signature.").

Légende du tableau A4

"Facultatif : Si l'algorithme de chiffrement, qui est utilisé dans les certificats numériques en adjonction à une signature numérique, diffère de l'algorithme décrit dans cette spécification, l'office récepteur doit notifier cet algorithme au Bureau international."

Cette prescription doit être obligatoire et non facultative, ainsi que l'indique le terme doit dans le texte reproduit ci-dessus.

[Fin du document]