F

OMPI

SCIT/WG/1/6
ORIGINAL : anglais
DATE : 1er octobre 1998

ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE
GENÈVE

COMITÉ PERMANENT DES TECHNIQUES DE L'INFORMATION

GROUPES DE TRAVAIL
Première session
Genève, 16 - 20 novembre 1998

PROBLÈMES TECHNIQUES CONCERNANT L'ÉCHANGE DE DOCUMENTS DE PRIORITÉ PAR LE RÉSEAU (TÂCHE N° 27)

Document établi par le Bureau international

INTRODUCTION

1. L'échange de données non publiées entre offices de propriété intellectuelle par le réseau mondial d'information est prévu dans le cadre du programme relatif au Banc d'essai concernant l'échange à haut débit d'information en matière de propriété intellectuelle (voir la page 6 du document SCIT/1/4). Dans un premier temps, la tâche ci-après a été définie et incorporée dans le programme de travail du SCIT :

Tâche n° 27	"Recenser les problèmes techniques concernant l'échange de données non publiées et exécuter des projets pilotes pour trouver des solutions viables à ces problèmes".

Tout l'éventail des données de propriété intellectuelle susceptibles d'être échangées entre offices de propriété intellectuelle par le réseau relève de l'étude qui doit être menée dans le cadre de la tâche n° 35 du SCIT (voir le document SCIT/WG/1/4). Le présent document est consacré aux problèmes techniques concernant ces échanges.

2. Les documents de priorité constituent l'une des sources principales de données non publiées susceptibles d'être échangées entre offices de propriété intellectuelle. Les documents de priorité (une copie des demandes nationales antérieures sur la base desquelles la priorité est revendiquée) sont délivrés par les offices de propriété intellectuelle qui, à la demande des déposants, en transmettent une copie à d'autres offices. Dans le cadre de la procédure selon le PCT, le document de priorité doit être transmis par l'office récepteur au Bureau international, qui en adresse une copie aux offices qui en font la demande (voir la règle 17 du Règlement d'exécution du PCT).

3. Afin de réduire sensiblement le coût de la production, de la transmission et de la réception de copies de documents de priorité sur papier et les ressources que ces opérations nécessitent, les offices du groupe de coopération trilatérale (l'Office européen des brevets, l'Office japonais des brevets et l'Office des brevets et des marques des États-Unis d'Amérique) ont collaboré à l'instauration d'un système d'échange des documents de priorité sous forme électronique. Les données contenues dans les documents de priorité sur support électronique sont des données non publiées jusqu'à ce que les demandes soient publiées en tant que demandes de brevet non examinées ou en tant que brevets (en général 18 mois après la date de dépôt). Les offices du groupe de coopération trilatérale ont lancé ce projet sous la forme d'un projet pilote destiné à trouver des solutions techniques pour l'échange électronique de données non publiées par le réseau.

4. À la première session plénière du SCIT, l'Office japonais des brevets a présenté un exposé, au nom des offices du groupe de coopération trilatérale, sur les progrès réalisés dans le domaine de l'échange électronique de documents de priorité (voir l'exposé distribué au cours de la session, que l'on peut consulter sur la page consacrée au SCIT du site Web de l'OMPI). Le projet se compose de deux phases :

i) l'échange électronique de documents de priorité sur disque compact ROM et

ii) l'échange électronique de documents de priorité par le "réseau trilatéral", réseau virtuel privé qui relie les offices du groupe de coopération trilatérale.

S'agissant de l'échange de documents de priorité par le réseau, les offices du groupe de coopération trilatérale ont recensé les problèmes techniques ci-après :

1. le mécanisme d'échange
2. le chiffrement
3. les types de données
4. les éléments de données (définition du type de document)
5. l'emballage ou l'enveloppe destiné à regrouper les fichiers électroniques
6. la signature numérique.

5. Compte tenu de l'importance technique que le projet pilote revêt par rapport à la tâche n° 27 et des progrès récents accomplis par les offices du groupe de coopération trilatérale, le Secrétariat a demandé à ces derniers de communiquer les résultats du projet concernant les conditions requises sur le plan technique pour l'échange de documents de priorité par le réseau trilatéral au Bureau international. Une liste de ces conditions requises, telles qu'elles ont été définies par les offices du groupe de coopération trilatérale, figure à l'annexe du présent document.

6. Il semble que la plupart des conditions requises définies par les offices du groupe de coopération trilatérale s'appliquent à l'échange de *toute* donnée non publiée entre offices de propriété intellectuelle par le réseau mondial d'information. C'est pourquoi, il est proposé de faire état de ces conditions requises, telles qu'elles figurent à l'annexe[1] du présent document, dans la demande de propositions relative au réseau mondial d'information.

7. Le Groupe de travail du SCIT est invité à prendre note du contenu du présent document et à faire des recommandations à la session plénière sur les prochaines mesures à prendre.

[L'annexe suit]

[1] Les produits mentionnés à l'annexe sont des exemples du type de produit nécessaire et ne sont pas forcément les produits qui seront utilisés sur le WIPONET.

ANNEXE

ÉCHANGE INTERNATIONAL DE DOCUMENTS DE PRIORITÉ (IPDE)

Conditions requises sur le plan technique définies par les offices du groupe de coopération trilatérale pour l'échange de documents de priorité par le réseau trilatéral

Norme applicable (le cas échéant)	Description	Exemple de produit	Observations sur l'utilisation du produit
Relais de trame	Le relais de trame est une norme internationale pour l'accès haute vitesse à des réseaux étendus (WAN). À l'heure actuelle son coût par unité de capacité est faible par rapport aux autres techniques concurrentes. La capacité est calculée en fonction d'un débit d'informations garanti (CIR) que le distributeur s'engage à assurer à tout moment et d'un débit d'informations supplémentaire (EIR, qui correspond habituellement à 2x le CIR) que le distributeur s'engage à assurer lorsque la capacité est disponible.	Les circuits à relais de trames des entreprises internationales de télécommunications	

Norme applicable (le cas échéant)	Description	Exemple de produit	Observations sur l'utilisation du produit
IP	Protocole Internet Norme de l'Internet définissant un mécanisme d'adressage ainsi que des règles d'acheminement des paquets de données entre systèmes.	Dispositifs du routeur IP reliant les réseaux et les cartes d'interface IP des ordinateurs reliés à un réseau. Nombreux produits.	Les routeurs IP seront utilisés pour relier le réseau à relais de trames et les réseaux des offices de brevet.
IPSEC	Sécurité IP Ensemble de protocoles mis au point par le Groupe de développement Internet (IETF) afin d'assurer la sécurité des échanges de paquets de données sur la couche IP. L'IPSEC utilise des techniques à clés publiques ou secrètes. L'IPSEC est destinée à devenir une norme acceptable et attrayante pour les distributeurs de matériel, qui l'intégreront à leurs produits afin d'offrir une interopérabilité avec les matériels vendus par d'autres professionnels	Systèmes CISCO	La forme définitive des normes IPSEC est en cours d'élaboration. En conséquence, de nombreux distributeurs adoptent une attitude prudente avant de donner leur accord aux projets visant à incorporer l'IPSEC dans leurs produits.
TCP/IP	Protocole de commande de transmission/protocole Internet TCP/IP Protocole normalisé de l'Internet destiné à assurer la fiabilité du transfert de données d'un point à un autre entre des ports TCP d'ordinateurs connectés à des réseaux reliés entre eux.	Le protocole TCP/IP est incorporé dans le logiciel que fournit normalement le distributeurs du système informatique ou du logiciel de gestion de réseau.	Le protocole TCP/IP sera utilisé pour les communications entre les logiciels d'application des ordinateurs reliés par le TSVPN. Associés, le TCP et l'IP activent les couches réseau et transport du modèle de protocole de réseau à 7 couches de l'ISO.

Norme applicable (le cas échéant)	Description	Exemple de produit	Observations sur l'utilisation du produit
	Réseau privé virtuel (VPN) Technique permettant des communications privées sur un réseau public grâce à l'utilisation du chiffrement des données. Les paquets de données envoyés par le réseau sont chiffrés et seules les informations contenues dans l'en-tête utilisé pour acheminer les données à travers le réseau sont envoyées en clair. Les données susceptibles d'être interceptées ou contrôlées par des tiers sont protégées par le système chiffreur.	Dispositif de chiffrement de paquets de données *BorderGuard* de *StorageTeck, Inc.*	Le dispositif *BorderGuard* est installé entre le pare-feu et le port réseau étendu de l'office des brevets. Les dispositifs *BorderGuard* sont gérés par un système de gestion de réseau. Une licence d'exportation est nécessaire pour l'utilisation de longueurs de clé de chiffrement de 128 bit.
IDEA	Algorithme international de chiffrement de données L'IDEA est similaire à la DES (Norme de chiffrement de données). Il peut être utilisé dans les logiciels en dehors des États-Unis jusqu'à une longueur de clé de 128 bit. Il est considéré comme un algorithme solide à propos duquel aucune critique n'a été publiée.	L'algorithme IDEA est utilisé par le routeur *BorderGuard* et sera utilisé pour le chiffrement sur le TSVPN.	

Norme applicable (le cas échéant)	Description	Exemple de produit	Observations sur l'utilisation du produit
	Système de détection des intrusions Système utilisé avec les dispositifs de chiffrement des paquets de données afin de détecter toute tentative de pénétration du réseau.	Les logiciels *NetRanger Probes* et *NetRanger Director* dont la licence appartient au *Wiehl Group*.	La détection des intrusions implique l'identification des paquets de données ne correspondant pas à ce que le dispositif de chiffrement s'attend à rencontrer, des configurations de trafic qui diffèrent de la normale ou des configurations d'intrusion connues. Le distributeur met régulièrement à jour ce logiciel afin qu'il puisse détecter les nouvelles menaces.
SGML	Langage normalisé de balisage généralisé Norme internationale visant à définir le balisage utilisé pour indiquer la structure et le contenu des documents. Des marqueurs SGML sont insérés dans le texte du document pour indiquer les parties structurelles et les éléments de contenu. Ainsi, <FNI>Thomas A. Edison</FNI> serait un marqueur SGML valable pour le premier inventeur désigné.	Des systèmes auteurs SGML et des traitements de texte compatibles SGML, qui permettent de créer des documents SGML, sont disponibles dans le commerce.	Les documents IPDE sont des documents de format SGML. À cour terme, des images de documents de priorité seront échangées et de petits documents SGML seront créés pour les données descriptives, les images de documents étant mentionnées par le document SGML comme des entités externes.
DTD	Définition de type de document Description formelle (rédigée en syntaxe SGML) des marqueurs autorisés et de la structure d'un type de document SGML donné.	Des outils sont disponibles dans le commerce pour la création de DTD.	L'USPTO a créé quatre DTD destinés à être utilisés pour l'IPDE.

Norme applicable (le cas échéant)	Description	Exemple de produit	Observations sur l'utilisation du produit
SDIF	Format d'échange de documents SGML Norme internationale d'emballage d'un document SGML susceptible d'être stocké sous la forme de plusieurs fichiers dans un train de données, afin qu'il puisse être échangé de façon à permettre aux destinataires de reconstituer les différents fichiers. Le SDIF est indépendant du support et peut être utilisé pour l'échange de données par le biais de réseaux ou de supports transportables.	Aucun produit commercial n'utilise le SDIF.	Le SDIF a été choisi par les partenaires de la coopération trilatérale pour l'échange de documents de priorité, essentiellement parce qu'il constitue une norme internationale ouverte et qu'il permet de garder une certaine indépendance par rapport aux distributeurs. Le SDIF sera utilisé pour enregistrer les documents de priorité sur disques compacts ROM et pour les transmettre par le TSVPN.
PKCS#7	Norme 7 de clé publique de chiffrement Norme des laboratoires *RSA* applicable aux données qui peuvent être chiffrées et qui supportent par exemple les signatures et les enveloppes numériques.	Un certain nombre de produits de *RSA Data Security, Inc.* utilisent la norme PKCS#7. La norme *BSAFE* a été choisie.	Les partenaires de la coopération trilatérale ont convenu d'utiliser la norme PCKS#7 pour apposer des signatures numériques sur les documents de priorité et d'utiliser le produit *BSAFE*. L'USPTO doit obtenir une licence d'exportation pour le chiffrement poussé.

Norme applicable (le cas échéant)	Description	Exemple de produit	Observations sur l'utilisation du produit
	Signature numérique Technique de certification de l'intégrité des données d'un document numérique, qui consiste à associer le nom d'un signataire à un certificat numérique émis par un tiers reconnu. Pour créer une signature numérique, il faut traiter l'objet à signer à l'aide d'un algorithme de condensation sécurisé afin de créer un petit fichier message condensé qui ne peut être associé qu'à l'objet signé. Il en résulte que si un condensé est recalculé après qu'un changement est intervenu dans l'objet signé, il sera lui aussi différent. Le résumé est chiffré à l'aide de la clé publique du signataire afin de créer un bloc de signature numérique, qui est alors ajouté à l'objet signé selon les règles de la norme PKCS#7.	La possibilité d'utiliser une signature numérique existe dans les produits de *RSA, Trusted Information Systems, Netscape, Microsoft* et d'autres.	Les restrictions à l'exportation appliquées à l'utilisation du chiffrement poussé ne sont pas applicables aux signatures numériques à condition qu'il puisse être prouvé que le logiciel de signature numérique ne peut être immédiatement adapté pour chiffrer le contenu des données.

Norme applicable (le cas échéant)	Description	Exemple de produit	Observations sur l'utilisation du produit
X.509 Ver. 3	Norme de certification numérique Norme internationale applicable au format et au contenu des certificats numériques. Un certificat numérique permet à un tiers reconnu d'authentifier (de se porter garant pour) le lien entre une clé publique et des renseignements permettant d'identifier le titulaire de la clé.	La norme X.509 est appliquée dans le logiciel utilisé par le dispositif de chiffrement *BorderGuard*. Les certificats X.509 sont authentifiés par des serveurs d'authentification situés sur les réseaux des offices de brevets.	Les certificats numériques, les signatures numériques, le chiffrement à l'aide de clés publiques et les procédures de vérification des certificats constituent la base d'une infrastructure à clés publiques (PKI). Même si la norme X.509 est largement utilisée, l'interopérabilité des systèmes d'authentification des différents distributeurs n'est pas satisfaisante.

[Fin de l'annexe et du document]