F

OMPI

SCIT/WG/1/5
ORIGINAL : anglais
DATE : 3 novembre 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

ÉTUDE DES POSSIBILITÉS OFFERTES PAR LE COMMERCE ÉLECTRONIQUE, DE SON INFRASTRUCTURE ET DU RECOURS PAR LES OFFICES DE PROPRIÉTÉ INTELLECTUELLE À DES OUTILS APPROPRIÉS
(TÂCHE N° 28)

Document établi par le Bureau international

INTRODUCTION

1. À sa session plénière tenue en juin 1998, le Comité permanent des techniques de l'information (SCIT) a proposé que le Groupe de travail sur la sécurité de l'information (ISWG) traite "de questions techniques touchant à l'échange de données et exécute des projets pilotes, en relation avec le programme concernant les BNPI et au moyen du WIPONET, dans les domaines du dépôt électronique et de l'échange de documents de priorité pour l'examen des demandes de brevet, et en ce qui concerne d'autres activités prévues dans le domaine du commerce électronique" (paragraphe 14.c) du document SCIT/1/7 Prov). Il a proposé que "l'ISWG donne aussi aux offices de propriété intellectuelle la possibilité de partager l'expérience des offices ayant atteint un stade avancé dans ce domaine et se concentre sur les points suivants en matière de coopération technique :

- coopération technique au profit des États membres pour les aider à utiliser l'infrastructure et les outils disponibles dans le cadre du réseau aux fins du commerce électronique;

- coordination, d'un point de vue technique, entre les activités de l'OMPI et celles des États membres dans le domaine du commerce électronique (par exemple, adoption des outils nécessaires, adoption éventuelle de principes directeurs techniques généraux pour le commerce électronique dans le domaine de la propriété intellectuelle);
- projets pilotes utilisant les outils du commerce électronique pour la fourniture de l'information en matière de propriété intellectuelle.

2. À cet égard, la tâche suivante a été inscrite au programme de travail du SCIT :

Tâche n° 28 "Étudier les possibilités offertes par le commerce électronique, son infrastructure et le recours par les offices de propriété intellectuelle à des outils appropriés."

MESURES PRISES

3. Dans un premier temps en ce qui concerne la tâche susmentionnée, le Bureau international a pris les mesures suivantes :

i) afin d'aider à la compréhension générale des questions de sécurité qui se posent – et comme préalable à la mise en place d'applications du commerce électronique – il a établi un document général donnant un aperçu des questions techniques relatives à la sécurité de l'information (voir l'annexe du présent document), et

ii) il a donné les grandes lignes d'un projet pilote qu'il propose (voir ci-après).

PROJET PILOTE PROPOSÉ EN CE QUI CONCERNE L'INFRASTRUCTURE À CLÉ PUBLIQUE

4. Il est proposé d'exécuter un projet pilote pour l'échange de messages entre les offices, les déposants et le Bureau international au sujet des demandes de documents de priorité. Ce projet, qui ne porterait pas sur l'échange des documents proprement dits, durerait de janvier à avril 1999.

5. Les parties au projet devraient être en mesure d'échanger des messages sécurisés et authentifiés (faisant appel au certificat numérique et à la signature numérique) par lesquels elles demanderaient l'échange de documents de priorité ou accuseraient réception de telles demandes. Le mécanisme de messagerie pourrait être aussi simple qu'un courrier électronique sécurisé.

6. Concrètement, deux offices de propriété intellectuelle ou plus et le Bureau international échangeraient du courrier électronique sécurisé demandant l'envoi de documents de priorité d'un office au Bureau international, puis à un autre office. Les documents de priorité proprement dits ne seraient pas effectivement échangés; seuls les messages le seraient.

7. Les messages seraient authentifiés et chiffrés à l'aide de certificats numériques et de signatures numériques. Les certificats numériques seraient délivrés par chaque office, en fonction de sa propre politique en matière de sécurité et d'authentification. La signature, la validation, le chiffrement et le déchiffrement proprement dits des messages seraient réalisés par des logiciels commerciaux de courrier électronique.

8. Ce projet pilote permettrait de vérifier l'interopérabilité des environnements d'infrastructure à clé publique (voir l'annexe du présent document) gérés par différents offices et organisations, tout en permettant de recenser les problèmes liés à la délivrance de certificats et à la certification croisée des utilisateurs au sein de la communauté de la propriété intellectuelle en général.

9. Le secrétariat a besoin de directives de la part de l'ISWG quant à la manière de choisir deux ou trois offices de propriété intellectuelle qui participeront au projet pilote, si celui-ci est approuvé par le groupe de travail.

10. Le Groupe de travail du SCIT est invité à approuver cette proposition.

[L'annexe suit]

ANNEXE

SÉCURITÉ DE L'INFORMATION – APERÇU DES QUESTIONS À EXAMINER

INTRODUCTION

1. À sa première session plénière, le Comité permanent des techniques de l'information (ci-après dénommé "SCIT") a pris note d'un certain nombre de questions relatives à la sécurité de l'information qui sont importantes pour le développement du réseau mondial d'information (WIPONET). Ces questions techniques ont trait à l'échange, sur le WIPONET, de données non publiées (confidentielles) comme les documents de priorité, aux systèmes de dépôt électronique et à d'autres activités prévues. Le présent document donne un aperçu de quelques-unes de ces questions techniques.

APERÇU DES QUESTIONS

2. L'architecture générale des réseaux internationaux de communication et les techniques utilisées dans l'échange de données à bas niveau posent toute une série de questions relatives à la sécurité de l'information.

3. Du point de vue du matériel et de la connectivité, il est possible de protéger les différents trains de données sur les réseaux, quel que soit le logiciel qui les génère. Les réseaux fondés sur l'Internet font appel à la *commutation par paquets*, technique par laquelle les documents sont divisés en courts fragments dénommés "paquets". Cette division, qui s'effectue à un très bas niveau, est invisible pour l'utilisateur. Chacun des paquets contient, entre autres, l'adresse de la machine expéditrice, celle de la machine réceptrice ("machine cible"), certaines données et un "total de contrôle" qui sert à vérifier l'exactitude des données reçues par la machine cible.

4. En l'espèce, ce sont les deux adresses du paquet qui présentent le plus d'intérêt. Des dispositifs dénommés *routeurs* ont été conçus pour lire ces adresses dans chaque paquet et les "commuter", ou les acheminer, vers leur destination précise dans l'infrastructure de communication spécifiée. Ce sont les routeurs qui déterminent le meilleur trajet que le paquet doit suivre, en fonction de son origine et de sa destination. Cette "meilleure route" n'est pas nécessairement la plus courte géographiquement. Les itinéraires sont fixés par des "mainteneurs de routeurs" et peuvent être changés lorsque les conditions de trafic le justifient.

5. Les questions qui découlent de ces considérations d'architecture de réseau ont trait aux éléments suivants :

- mise à jour et gestion des routeurs du WIPONET dans un environnement sécurisé
- chiffrement à bas niveau des données
- exclusion des entités non autorisées sur les réseaux d'offices de propriété intellectuelle.

6. Les questions de sécurité des installations occupent aussi une place importante dans tout réseau sécurisé, l'accès physique non autorisé aux machines pouvant poser des problèmes. Les points à traiter sont notamment les suivants :

- surveillance des machines
- retraitement des disques durs et disquettes
- protection par nom d'utilisateur et mot de passe
- accès non autorisé aux réseaux interne et externe.

7. Au-delà des questions fondamentales d'architecture de réseau, les systèmes d'application (services de messagerie électronique, navigateurs sur le Web, etc.) posent une autre série de problèmes relatifs à la sécurité de l'information. Actuellement, les logiciels les plus sécurisés font appel à des systèmes à clé publique pour chiffrer et authentifier l'information échangée entre les utilisateurs. L'adhésion à des normes internationales bien définies est donc fondamentale dans ce secteur où les logiciels de fabricants différents doivent interopérer en toute sécurité. Quelques-unes des questions à traiter sont à cet égard les suivantes :

- création, utilisation et vérification de certificats numériques
- normes de chiffrement
- protocoles d'échange de clés
- réattribution de clés en cas de perte ou de dommage
- signature numérique et non-répudiation.

8. Il importe, à cet égard, de bien saisir la différence entre la notion de secret des données et celle d'authenticité des données. Si, par exemple, un office souhaite mettre certaines données publiques à disposition, il lui est tout aussi important de disposer d'un mécanisme assurant l'authenticité de cette information publique que de garantir le secret d'autres types de données.

9. Il est évident que bon nombre de ces questions sont interdépendantes. Dans l'industrie des systèmes informatiques et de la sécurité de l'information, le terme "infrastructure à clé publique" a été forgé pour décrire les politiques, le matériel et le logiciel utilisés afin d'assurer l'échange sécurisé et l'authentification des informations et des données de sécurité sur les réseaux. Certaines de ces questions relèvent aussi de la catégorie plus générale "commerce électronique".

10. Problèmes de terminologie mis à part, les questions qui se posent en relation avec l'infrastructure à clé publique et le "commerce électronique" sont importantes pour les activités au jour le jour des offices de propriété intellectuelle, et la capacité de recourir à des méthodes électroniques faciliterait une interaction efficace des offices et des déposants.

Rapports entre les activités d'échange d'information des offices de propriété intellectuelle et les questions de sécurité de l'information

11. L'échange d'information portera notamment sur des données confidentielles non publiées. Aussi toute communication de ce type entre déposant et examinateur nécessitera-t-elle d'excellents niveaux de sécurité et de secret. Une grande partie de ces activités d'échange exigera, qui plus est, une certaine assurance quant à l'identité de l'autre partie. Par exemple, si un déposant échange de l'information avec un examinateur, celui-ci aura besoin de savoir que la personne qui lui envoie l'information est bien autorisée à le faire (preuve de l'identité) et le déposant devra, pour sa part, avoir la certitude qu'il est bien en contact avec un examinateur de brevets et non avec un pirate futé. Ces transactions devront aussi présenter un caractère de non-répudiabilité en ce sens que, si un déposant envoie une nouvelle revendication à un examinateur, il ne devra pas pouvoir dénier cette transaction par la suite.

12. L'échange de documents de priorité offre aussi un exemple intéressant : si un tel document doit être échangé sous forme électronique, il faudra qu'il soit validé par l'expéditeur. Autrement dit, le document de priorité devra porter une signature prouvant son authenticité, un timbre horodateur garanti concernant la transaction, apposé de préférence par un tiers (pour empêcher toute falsification présumée ou effective des date et heure), ainsi qu'une certaine garantie d'exactitude, afin que le récepteur puisse dire s'il y a eu altération ou non.

13. Toutes les questions ci-dessus peuvent être considérées comme des problèmes de sécurité de l'information, et toutes peuvent être résolues dans le cadre d'une infrastructure à clé publique bien organisée et soigneusement pensée.

Infrastructure à clé publique

14. L'infrastructure à clé publique apporte la garantie d'une utilisation sécurisée et authentifiée des ressources sur un réseau. Toute infrastructure complète de ce type suppose la mise en place d'installations et l'élaboration de spécifications et de politiques relatives à l'utilisation des certificats fondés sur les clés publiques pour la sécurité des systèmes informatiques, le commerce électronique et les communications sécurisées, notamment la messagerie électronique et les téléconférences.

15. Le WIPONET nécessitera une infrastructure à clé publique complète pour permettre l'utilisation et l'échange sécurisé d'informations confidentielles, ainsi que l'identification des sources autorisées d'information et de services non confidentiels.

16. Il faut également se faire à l'idée que le WIPONET sera plus qu'une simple communauté fermée d'offices de propriété intellectuelle, et que les applications utilisées sur ce réseau mûriront avec le temps. On ne doit donc pas voir dans l'infrastructure à clé publique pour ce réseau un système monolithique à structure descendante. Cette infrastructure servira, au contraire, de cadre à l'interopérabilité des applications standard et personnalisées dans l'environnement du WIPONET et sur l'Internet public en général.

17. Indéniablement, l'un des défis à relever consistera à mettre en place une infrastructure à clé publique qui interopère sans difficulté avec des dispositifs analogues en cours d'élaboration au sein des États membres de l'OMPI, dans le cadre de l'Internet et dans l'industrie des systèmes d'information en général.

Coopération internationale

18. Il incombera à chaque office (y compris le Bureau international de l'OMPI) participant au projet WIPONET de mettre en œuvre une politique adaptée en matière de sécurité des données pour ses systèmes d'information reliés au réseau. La coopération internationale sera, à cet égard, essentielle pour réduire le risque et accroître l'interopérabilité des systèmes d'information et des composantes du réseau. Le tableau ci-après décompose les différents rôles dans leurs grandes lignes et indique le niveau de coopération internationale voulu pour la mise en place d'une infrastructure efficace, en matière de sécurité de l'information, entre l'OMPI, les offices nationaux de ses États membres et les offices régionaux intéressés.

Questions ou éléments	Parties intéressées	Solution	Mesures à prendre
Sécurité du réseau	OMPI (BI) et offices de propriété intellectuelle participants	Chiffrement, conception matérielle	Conception minutieuse du prédéploiement, infrastructure à clé publique
Contrôle d'accès	OMPI (BI) et offices de propriété intellectuelle participants	Contrôles stricts des politiques, mise en œuvre de ces politiques au moyen de preuves d'identité infalsifiables	Principes directeurs et accord, logistique d'infrastructure à clé publique
Confirmation d'identité	OMPI (BI) et offices locaux de propriété intellectuelle participants	Office local agissant en tant qu'autorité d'enregistrement	Saisie des données d'enregistrement d'utilisateur dans l'infrastructure à clé publique
Certificats numériques	OMPI (BI) et offices de propriété intellectuelle participants	OMPI/offices locaux/offices régionaux agissant en tant qu'autorités de certification	Projet pilote visant à mettre en place l'infrastructure à clé publique pour la communauté de la propriété intellectuelle
Sécurité des données	Offices échangeant des données	Choix judicieux et utilisation adéquate des produits commerciaux standard	Coordination entre les différents partenaires et recommandation du SCIT, infrastructure à clé publique

Solutions techniques actuelles

19. Actuellement, plusieurs produits commerciaux librement accessibles permettent la délivrance de certificats numériques, la validation et la gestion des échanges d'information. Il faudra que diverses combinaisons de ces produits soient évaluées dans un environnement représentatif, par exemple dans le cadre d'un projet pilote. Pour une infrastructure à clé publique bien conçue, on devra se fonder sur des produits commerciaux d'origine diverse, utilisant à la fois des normes industrielles et des normes internationales. À mesure que le marché dans ce secteur évoluera, des produits plus perfectionnés seront proposés, auxquels les offices de propriété intellectuelle et leurs "clients" dans l'industrie feront appel. L'infrastructure du WIPONET devra en tenir compte et s'adapter à l'évolution du marché, de l'industrie et des réseaux en général, tout en offrant un niveau de sécurité élevé.

[Fin de l'annexe et du document]