S

OMPI

SCIT/WG/1/5
ORIGINAL: Inglés
FECHA: 3 de noviembre de 1998

ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL

GINEBRA

COMITÉ PERMANENTE DE TECNOLOGÍAS DE LA INFORMACIÓN

GRUPOS DE TRABAJO
Primera sesión
Ginebra, 16 a 20 de noviembre de 1998

ESTUDIAR EL POTENCIAL DEL COMERCIO ELECTRÓNICO, SU INFRAESTRUCTURA Y EL EMPLEO DE HERRAMIENTAS A TAL FIN POR OFICINAS DE PROPIEDAD INTELECTUAL (TAREA Nº 28)

Documento preparado por la Oficina Internacional

INTRODUCCIÓN

1. En junio de 1998, el Plenario del Comité Permanente de Tecnologías de la Información (SCIT) propuso que "el Grupo de Trabajo sobre Seguridad de la Información (ISWG) debería examinar las cuestiones técnicas relacionadas con el intercambio de datos y emprender proyectos piloto, en el marco del programa BDPI y utilizando WIPONET, en materia de presentación electrónica, intercambio de documentos de prioridad para el examen de solicitudes de patentes y otras actividades programadas de comercio electrónico" (véase el párrafo 14.c) del documento SCIT/1/7 Prov.). También propuso que el ISWG brindase a las oficinas de propiedad intelectual la oportunidad de compartir la experiencia de las oficinas avanzadas en esta esfera y se ocupase de los siguientes asuntos de cooperación técnica:

- cooperación técnica con los Estados miembros para asistirles en la utilización de la infraestructura de red y de las herramientas destinadas al comercio electrónico;

- coordinación entre las actividades sobre comercio electrónico de la OMPI y de los Estados miembros desde el punto de vista técnico (por ejemplo, adopción de los instrumentos necesarios, posible adopción de principios técnicos generales para el comercio electrónico en el campo de la propiedad intelectual);

- proyectos piloto que hagan uso de herramientas de comercio electrónico para el suministro de información en materia de propiedad intelectual.

2. A este respecto, se ha incluido la siguiente tarea en el Programa de Trabajo:

Tarea Nº 28: "Estudiar el potencial del comercio electrónico, su infraestructura y el empleo de herramientas a tal fin por oficinas de propiedad intelectual".

LABOR EMPRENDIDA

3. Como medida inicial para la realización de la tarea mencionada anteriormente, la Oficina Internacional ha emprendido los siguientes trabajos:

i) para facilitar un entendimiento común de las cuestiones de seguridad implicadas -que se considera como precursor necesario del establecimiento de aplicaciones para el comercio electrónico- la Oficina Internacional ha redactado un documento de carácter general sobre la seguridad de la información y las cuestiones técnicas conexas (véase el Anexo del presente documento), y

ii) ha esbozado una propuesta de proyecto piloto (véase a continuación).

PROPUESTA DE PROYECTO PILOTO SOBRE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA

4. Se ha propuesto un proyecto piloto para el intercambio de mensajes entre las oficinas, los solicitantes y la Oficina Internacional en lo que atañe a las peticiones de documentos de prioridad. Este proyecto no abarcará el intercambio de los propios documentos, y su ejecución tendrá lugar entre enero y abril de 1999.

5. Los participantes en el proyecto podrán intercambiar mensajes seguros y autentificados (mediante certificados y firmas digitales) en los que pidan o acusen recibo de peticiones de intercambio de documentos de prioridad. El mecanismo de mensajería podría ser tan simple y seguro como el correo electrónico.

6. La operación consistiría en el intercambio de mensajes seguros por correo electrónico, entre dos o más oficinas de propiedad intelectual y la Oficina Internacional, en los que se solicite a una oficina la puesta a disposición de documentos de prioridad a la Oficina Internacional para transmitirlos posteriormente a otra oficina. No se intercambiarían los propios documentos de prioridad sino simplemente los mensajes.

7. Los mensajes se autentificarán y codificarán mediante el empleo de certificados y firmas digitales. Cada oficina emitirá los certificados digitales con arreglo a sus propias políticas en materia de seguridad y autenticación. La firma, validación, codificación y descodificación de los mensajes se efectuaría mediante programas comerciales de correo electrónico.

8. Este proyecto piloto tiene por objetivo comprobar el funcionamiento de entornos de infraestructura de clave pública (PKI - *Public Key Infrastructure*; para más informaciones véase el Anexo del presente documento) que administren diferentes oficinas y organizaciones, y permitirá la identificación de problemas y cuestiones asociadas con la emisión de certificados y la certificación cruzada de usuarios en el contexto más amplio de la comunidad de la propiedad intelectual.

9. La Secretaría necesita recibir el asesoramiento del ISWG para determinar la forma de seleccionar a dos o tres oficinas de propiedad intelectual a fin de que participen en el proyecto piloto, siempre que éste sea aprobado por el ISWG.

10. Se invita al Grupo de Trabajo del SCIT a aprobar esta propuesta.

[Sigue el Anexo]

ANEXO

PANORAMA DE LAS CONSIDERACIONES ASOCIADAS CON LA SEGURIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

1. El Plenario del Comité Permanente de Tecnologías de la Información (denominado en adelante "el SCIT") ha observado que existen cuestiones pendientes en materia de seguridad de la información que son importantes para el desarrollo de la Red Mundial de Información (WIPONET). Esas consideraciones técnicas guardan relación con el intercambio de datos no publicados (confidenciales) a través de la WIPONET, tales como los documentos de prioridad, con los sistemas de presentación electrónica y otras actividades previstas. En este documento se ofrece un panorama de las consideraciones técnicas relacionadas con la seguridad de la información.

PANORAMA

2. La estructura general de las redes internacionales de comunicaciones y las tecnologías empleadas en el intercambio de bajo nivel de datos, tienen como denominador común una variedad de consideraciones relacionadas con la seguridad de la información.

3. Desde el punto de vista del soporte lógico y de la conectividad, se pueden proteger los flujos individuales de datos que recorren las redes con independencia de las aplicaciones del soporte lógico que genera los datos. Las redes basadas en Internet emplean tecnologías de *conmutación de paquetes*. Dicho de otro modo, los datos, como por ejemplo los documentos, se dividen en pequeñas porciones que se denominan paquetes. Esta división opera a un nivel muy bajo y es invisible para el usuario. Cada uno de esos paquetes contiene, entre otras cosas, la dirección de la máquina de origen, la dirección de la máquina receptora o destinataria, algunos datos y una suma de control (o verificación) de los datos. La suma de control sirve para verificar la exactitud de los datos recibidos por la máquina destinataria.

4. A los efectos de este examen, las dos direcciones contenidas en el paquete revisten de un gran interés. Los dispositivos conocidos como *encaminadores* pueden leer estas direcciones en cada paquete y conmutar, o encaminar, el paquete al lugar exacto mediante la infraestructura de comunicaciones designada. Los encaminadores determinan el "mejor itinerario" para un paquete, sobre la base de su origen y destino. Este "mejor itinerario" puede no corresponder con el más corto desde un punto de vista geográfico. Los operadores de encaminadores establecen esos itinerarios, que pueden cambiarse siempre y cuando lo permitan las condiciones.

5. Las cuestiones planteadas por esas consideraciones estructurales son:

- la actualización y gestión de los encaminadores de la WIPONET en un entorno seguro;
- la codificación de bajo nivel de los datos;

- la exclusión de entidades no autorizadas de las redes de las oficinas de propiedad intelectual.

6. Las consideraciones de seguridad física también son importantes para una red segura, puesto que el acceso físico no autorizado a las máquinas puede plantear problemas de seguridad. Estas consideraciones abarcan:

- el control físico de las máquinas;

- el reprocesado de discos duros y disquetes;

- la seguridad del nombre del usuario y de la contraseña;

- el acceso no autorizado a redes internas y externas.

7. Además de las cuestiones básicas de estructura de redes, esos sistemas que operan a nivel de aplicaciones (los clientes de comercio electrónico, los navegadores Internet, etc.) plantean otro conjunto de consideraciones en materia de seguridad de la información. La mayoría del soporte lógico seguro emplea actualmente sistemas de clave pública para codificar y autenticar la información que intercambian los usuarios. Por ello, es fundamental en este campo la observancia de normas internacionales bien definidas puesto que los fabricantes de soporte lógico y otros deben interactuar en forma segura. Algunas de esas consideraciones abarcan:

- la creación, utilización y verificación de certificados digitales;

- las normas de codificación;

- los protocolos de intercambio de clave;

- la recuperación de la clave cuando se extravíen o dañen claves de seguridad;

- la firma digital y la no repudiación.

8. Es importante comprender la distinción entre el carácter confidencial de los datos y la autenticidad de los mismos. Si, por ejemplo, una oficina desea hacer públicos ciertos datos, es igualmente importante disponer de un mecanismo que permita asegurar la autenticidad de la información pública como la de los datos confidenciales.

9. Es evidente que la mayor parte de estas cuestiones está relacionada entre sí. Los sistemas de información y la industria de la seguridad han acuñado el término “infraestructura de clave pública” (PKI) para describir las políticas, el soporte físico y el soporte lógico utilizado para garantizar el intercambio seguro y la autenticación de la información y los datos de seguridad a través de las redes. Algunas de estas cuestiones también son comunes a la categoría amplia de “comercio electrónico”.

10. Con independencia de preocupaciones terminológicas, las consideraciones asociadas con la PKI y el “comercio electrónico” revisten de importancia para las actividades diarias de las oficinas de propiedad intelectual, y la aptitud para utilizar métodos electrónicos facilitaría la interacción eficiente de las oficinas y los solicitantes.

Relación entre las actividades de intercambio de información de las oficinas de propiedad intelectual y las consideraciones en materia de seguridad de la información

11. Las actividades de intercambio de información girarán en torno al intercambio de información confidencial y no publicada. Por ejemplo, todo intercambio entre solicitantes y examinadores exige excelentes niveles de seguridad y confidencialidad de los datos. Además, la mayoría de esas actividades también exige un cierto grado de seguridad en cuanto a la identidad de una u otra parte. Por ejemplo, si un solicitante intercambia información con un examinador, el examinador necesitará saber que el individuo está autorizado a proporcionar la información (por ejemplo, prueba de identidad), y el solicitante necesita asegurarse de que ha entrado en contacto con un examinador de patente y no con un pirata informático inteligente. Esas transacciones también deben revestir de un carácter de no repudiación (por ejemplo, si un individuo envía una nueva reivindicación al examinador, ese individuo no debería ser capaz de repudiar la transacción ulteriormente).

12. El intercambio de documentos de prioridad constituye otro ejemplo interesante. Si se debe intercambiar un documento de prioridad en forma electrónica, la parte que lo envía debe validarlo. Dicho de otro modo, el documento debe estar firmado para que quede demostrada su autenticidad, debe contar con la garantía impresa de la hora de la transacción, emitida de preferencia por un tercero (para evitar la falsificación supuesta o real de fechas y horas), y debe ofrecer una cierta garantía de precisión para que la parte que recibe el documento pueda ver si ha sido alterado.

13. Todas las cuestiones que acaban de mencionarse pueden ser consideradas como problemas de seguridad de la información y todas pueden ser resueltas mediante una infraestructura de clave pública bien organizada y planificada con detenimiento.

Infraestructura de clave pública

14. La Infraestructura de Clave Pública (PKI) es el sustrato de la utilización segura y autentificada de los recursos en la estructura de una red. Toda PKI completa establece los mecanismos, las especificaciones y las políticas para la utilización de certificados de clave pública a los fines de la seguridad de los sistemas de información, del comercio electrónico y las comunicaciones seguras, con inclusión del correo electrónico y las conferencias a distancia.

15. La WIPONET deberá contar con una PKI que permita la utilización e intercambio seguros de información confidencial, así como la identificación de las fuentes autorizadas de información y servicios no confidenciales.

16. Es importante tomar conciencia de que la WIPONET es algo más que una comunidad cerrada de oficinas de propiedad intelectual, y que las aplicaciones que se utilicen en la WIPONET evolucionarán con el tiempo. Por consiguiente, no debería considerarse la infraestructura de clave pública de la WIPONET como una estructura monolítica y verticalista. En cambio, sí proporcionará el marco en el que interactuarán las aplicaciones comerciales e individualizadas en el entorno de la WIPONET y en el ámbito más amplio y público de Internet.

17. Uno de los desafíos más importantes y evidentes que se plantearán será elaborar una infraestructura de clave pública que pueda funcionar sin problemas con otros esfuerzos similares emprendidos en los Estados miembros de la OMPI, y dentro de Internet y la industria de sistemas de información en general.

Cooperación internacional

18. Cada oficina participante en el proyecto WIPONET (incluida la Oficina Internacional de la OMPI) tendrá que asumir responsabilidad por la puesta en aplicación de una política adecuada en materia de seguridad de la información respecto de sus sistemas de información conectados en red. La cooperación internacional es fundamental para reducir los riesgos y mejorar el funcionamiento entre los sistemas de información y los componentes de red. El cuadro que figura a continuación esboza esas funciones y pone en evidencia el nivel de cooperación internacional que se pretende lograr y que será necesario para que sea eficaz la infraestructura de seguridad de la información que se forje entre la OMPI, las Oficinas nacionales de sus Estados miembros y las oficinas regionales interesadas.

Consideraciones/ temas	Participantes	Solución	Medidas a tomar
Seguridad de la red	OMPI (IB) y oficinas de propiedad intelectual participantes	Codificación, diseño físico	Diseño detallado previo al lanzamiento, infraestructura de clave pública (PKI)
Control del acceso	OMPI (IB) y oficinas de propiedad intelectual participantes	Controles estrictos de política, aplicación de las políticas mediante prueba infalsificable de identidad	Pautas y acuerdo, apoyo a la PKI
Confirmación de la identidad	OMPI (IB) y oficinas de propiedad intelectual locales participantes	Oficina local que actúe como autoridad de registro	Incorporación en la PKI de los datos de registro del usuario
Certificados digitales	OMPI (IB) y oficinas de propiedad intelectual participantes	La OMPI y las oficinas locales y regionales actúan como autoridades de certificación	Proyecto piloto para establecer una PKI destinada a la comunidad de la prop. intelectual
Seguridad de los datos	Oficinas que intercambian datos	Elección y utilización correctas de soporte lógico disponible comercialmente	Coordinación entre los agentes del intercambio y la recomendación del SCIT, PKI

Soluciones técnicas actuales

19. Actualmente, varios productos comerciales y disponibles libremente permiten la emisión, validación y administración de certificados digitales. Será preciso evaluar diferentes combinaciones de esos productos en un conjunto representativo, por ejemplo, en un proyecto piloto. Una infraestructura de clave pública bien diseñada debería estar basada en productos comerciales procedentes de múltiples fuentes que tengan en cuenta tanto las normas internacionales como las que se aplican en el sector industrial. Paralelamente a la evolución del mercado comercial de estos servicios, irá aumentando el número de productos avanzados que estarán disponibles y que serán ciertamente utilizados por las oficinas de propiedad intelectual y sus interlocutores de la industria. La infraestructura de clave pública de la WIPONET debería reconocer este hecho y adaptarse a la situación cambiante de las condiciones del mercado, la industria y la conexión en red, y proporcionar al mismo tiempo una seguridad inquebrantable.

[Fin del Anexo y del documento]