S

OMPI

SCIT/WG/1/6
ORIGINAL: Inglés
FECHA: 1 de octubre 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

CUESTIONES TÉCNICAS RELACIONADAS CON EL INTERCAMBIO DE DOCUMENTOS DE PRIORIDAD EN LA RED (TAREA Nº 27)

Documento preparado por la Oficina Internacional

INTRODUCCIÓN

1. El intercambio de datos no publicados entre oficinas de propiedad intelectual a través de la red mundial de información ha sido previsto en el marco del programa del Banco de Pruebas para el intercambio a alta velocidad de grandes volúmenes de información en materia de propiedad intelectual (véase el documento SCIT/1/4, página 6). Como medida preparatoria, se ha creado la siguiente tarea que se ha incluido en el programa de trabajo del SCIT:

> Tarea Nº 27: "Identificar las cuestiones técnicas relativas al intercambio de datos no publicados y emprender proyectos piloto para encontrar soluciones técnicas viables".

Se determinará la gama completa de datos en materia de propiedad intelectual que las oficinas de propiedad intelectual intercambiarían a través de la red, como parte del estudio que se está realizando en relación con la Tarea Nº 35 del SCIT (véase el documento SCIT/WG/1/4). El presente documento trata de las cuestiones técnicas relativas al intercambio.

2. La principal fuente de los datos no publicados que intercambiarían las oficinas de propiedad intelectual consiste en los documentos de prioridad. Estos documentos (una copia de la solicitud nacional presentada anteriormente sobre la base de la cual se reivindica la prioridad) son emitidos por las oficinas de propiedad intelectual las cuales transmiten, a petición de los solicitantes, una copia del documento de prioridad a las demás oficinas. En el marco de los procedimientos del PCT, la Oficina receptora debería transmitir el documento de prioridad a la Oficina Internacional, y ésta a su vez debería transmitirlo a las oficinas que soliciten una copia del documento (véase la Regla 17 del Reglamento del PCT).

3. Con miras a lograr una reducción considerable de los costos y los recursos en que se incurre en el proceso de producción, transmisión y recepción de copias de los documentos de prioridad en papel, las Oficinas de la Cooperación Trilateral (la Oficina Europea de Patentes, la Oficina Japonesa de Patentes y la Oficina de Patentes y Marcas de los Estados Unidos) se han aunado para introducir una modalidad de intercambio electrónico de documentos de prioridad entre esas Oficinas. Los datos contenidos en los documentos de prioridad en forma electrónica constituyen datos no publicados hasta que esas solicitudes sean publicadas como solicitudes de patente no examinadas o como patentes concedidas (generalmente 18 meses después de la fecha de presentación). Las Oficinas de la Cooperación Trilateral emprendieron este proyecto experimental para determinar las soluciones técnicas al intercambio electrónico de datos no publicados a través de la red.

4. En la primera sesión plenaria del SCIT, la Oficina Japonesa de Patentes, en nombre de las Oficinas de la Cooperación Trilateral, efectuó una presentación sobre el progreso alcanzado en el intercambio electrónico de documentos de prioridad (véase el documento distribuido en la sesión y que está disponible en la sección dedicada al SCIT del sitio Web de la OMPI). El proyecto consiste en dos fases:

i) el intercambio electrónico de documentos de prioridad en discos compactos reescribibles (CD-R), y

ii) el intercambio electrónico de documentos de prioridad a través de la “Red Trilateral”, una red virtual privada que conecta a las Oficinas de la Cooperación Trilateral entre sí.

Las Oficinas de la Cooperación Trilateral identificaron las cuestiones técnicas que deberían abordarse en relación con el intercambio de documentos de prioridad en la red:

1. el mecanismo de intercambio;
2. el cifrado;
3. el tipo de datos;
4. los elementos de datos (Definición del Tipo de Documento);
5. el envoltorio o sobre donde archivar los ficheros electrónicos; y
6. la firma digital.

5. Habida cuenta de su relevancia técnica para la Tarea Nº 27 y de los avances logrados recientemente por las Oficinas de la Cooperación Trilateral, la Secretaría solicitó a estas Oficinas que compartiesen los resultados de la labor de su proyecto piloto concerniente a los requisitos técnicos del intercambio de documentos de prioridad en la red trilateral con la

Oficina Internacional. El Anexo del presente documento contiene una lista de los requisitos de utilización fijados por las Oficinas de la Cooperación Trilateral.

6. La mayoría de los requisitos fijados por las Oficinas de la Cooperación Trilateral parecen ser útiles y pertinentes para el intercambio de *cualquier* dato no publicado entre oficinas de propiedad intelectual a través de la red mundial de información. Por consiguiente, se propone que quede reflejada la necesidad de los requisitos descritos en el Anexo[1] del presente documento en la solicitud de ofertas para la Red Mundial de Información.

7. Se invita al Grupo de Trabajo del SCIT a tomar nota del contenido del presente documento y a formular recomendaciones sobre la próxima medida que debería adoptarse en la sesión plenaria.

[Sigue el Anexo]

[1] Los productos mencionados en el Anexo son ilustrativos del tipo de producto exigido y, por lo tanto, no son necesariamente los que se aplicarían en la WIPONET.

ANEXO

INTERCAMBIO INTERNACIONAL DE DOCUMENTOS DE PRIORIDAD
(IPDE)

Requisitos técnicos determinados por las Oficinas de la Cooperación Trilateral en relación con el intercambio de documentos de prioridad en la Red Trilateral

Norma relacionada (cuando proceda)	Descripción	Ejemplo de producto	Comentarios sobre el uso
Retransmisión de tramas	La retransmisión de tramas es una norma internacional que permite el acceso a alta velocidad a redes públicas de datos de área amplia (WAN). Tiene actualmente un bajo costo por unidad de capacidad en comparación con otras tecnologías competidoras. Se suele hablar de capacidad en función de una velocidad de información concertada (CIR) que el proveedor se compromete a proporcionar todo el tiempo, y de un exceso de velocidad de información (EIR , que normalmente es el doble de la CIR) que el proveedor asumirá cuando esté disponible la capacidad.	Circuitos de retransmisión de tramas de los servicios de telecomunicaciones internacionales	

Norma relacionada (cuando proceda)	Descripción	Ejemplo de producto	Comentarios sobre el uso
IP	Protocolo Internet (IP) Norma de Internet en la que se define un mecanismo de direccionamiento y reglas para el encaminamiento de paquetes de datos entre sistemas direccionados.	Dispositivos del encaminador IP que conectan entre sí a las redes con tarjetas de interfaz IP en los ordenadores conectados a la red. Muchos productos.	Se utilizarán los encaminadores IP para interconectar la red de transmisión de tramas con las redes de las oficinas de patente
IPSEC	Seguridad de IP Conjunto de protocolos en curso de elaboración por el Grupo de Tareas sobre Ingeniería de Internet (IETF) para abordar el intercambio seguro de paquetes a nivel de la capa IP. La norma de seguridad de protocolo Internet (IPSEC) emplea una tecnología de claves públicas/privadas. IPSEC está destinada a convertirse en la norma que será aceptable e interesante para los distribuidores de equipos puesto que la incorporarán en sus productos a fin de ofrecer una interoperabilidad con los equipos de otros distribuidores.	Sistemas CISCO	Se está desarrollando la forma final de la norma IPSEC. Por consiguiente, muchos proveedores han optado por esperar antes de dar el visto bueno a los planes de aplicación de la norma IPSEC en sus productos.
TCP/IP	Protocolo de control de transmisión y Protocolo Internet (TCP/IP) Protocolo normalizado de Internet que asegura una transferencia fiable de datos de extremo a extremo entre puertos TCP en ordenadores pertenecientes a redes conectadas entre sí.	El TCP/IP está incorporado en el soporte lógico que proporciona normalmente el proveedor de sistemas informáticos o el proveedor de soporte lógico de red.	Se empleará el TCP/IP en las comunicaciones entre aplicaciones de soporte lógico de ordenadores conectados a través de la TSVPN. Combinados, el TCP y el IP conforman las capas de red y transporte del Modelo de 7 capas de Protocolo de Red, de la ISO.

Norma relacionada (cuando proceda)	Descripción	Ejemplo de producto	Comentarios sobre el uso
	Red Virtual Privada (VPN) Tecnología que atiende las comunicaciones privadas en una red pública mediante el cifrado de los datos. Los paquetes de datos que se envían a través de la red están cifrados y solamente aparece como un texto claro la información de encabezamiento que se emplea para encaminar los datos por la red. Los datos que pueden ser interceptados o controlados por terceros están protegidos por el sistema criptográfico.	*BorderGuard* para el cifrado de paquetes de datos, de *StorageTek, Inc.*	El programa *BorderGuard* se instala entre el cortafuegos de la oficina de patentes y el puerto de red de área amplia de la oficina de patentes. Un sistema de gestión de red administra los programas *BorderGuard*. Se necesita una licencia de exportación para poder utilizar longitudes de la clave criptográfica de 128 bits.
IDEA	Algoritmo Internacional de Cifrado de Datos (IDEA) IDEA es similar a DES (Norma de Cifrado de Datos). Puede utilizarse en soportes lógicos fuera de los EE.UU. hasta una longitud máxima de clave de 128 bits. Se cree que se trata de un algoritmo sólido sobre el que no se han publicado críticas.	El algoritmo IDEA es empleado por el encaminador *BorderGuard* y se utilizará en el cifrado de redes TSVPN.	

Norma relacionada (cuando proceda)	Descripción	Ejemplo de producto	Comentarios sobre el uso
	Sistema de detección de intrusión Sistema utilizado con el paquete de programas de cifrado para detectar todo intento de penetración o intrusión en la red.	*NetRanger Probes* y *NetRanger Director*, programas bajo licencia del *Wiehl Group*.	La detección de intrusión implica reconocer los paquetes que no concuerdan con las expectativas del cifrado: esquemas de tráfico que difieren de lo normal o esquemas de intrusión conocidos. El proveedor actualiza periódicamente este soporte lógico con el fin de detectar nuevas amenazas.
SGML	Lenguaje de marcado general normalizado (SGML) Norma internacional que define el marcado que debe emplearse para indicar la estructura del contenido de documentos. Los rótulos SGML se insertan en el texto del documento para indicar las partes estructurales y los elementos de contenido. Por ejemplo: <FNI>Thomas A. Edison</FNI> sería el rótulo SGML válido correspondiente al primer inventor designado.	Se han puesto a la venta herramientas de composición en SGML y procesadores de texto con capacidad SGML, que permiten crear documentos SGML.	Los documentos IPDE tienen un formato SGML. A corto plazo, se intercambiarán imágenes de documentos de prioridad y se crearán pequeños documentos SGML para los datos de la descripción, y los documentos SGML harán referencia a las imágenes de los documentos como si fuesen entidades externas.
DTD	Definición de tipo de documento (DTD) Descripción formal (escrita en sintaxis de SGML) de los rótulos y estructura permitidos de un tipo de documento SGML determinado.	Existen herramientas disponibles comercialmente para crear DTD.	La USPTO ha credo cuatro DTD para su utilización en el IPDE.

Norma relacionada (cuando proceda)	Descripción	Ejemplo de producto	Comentarios sobre el uso
SDIF	Formato de intercambio de documentos SGML Norma internacional para el embalaje de un documento SGML de forma que pueda almacenarse en diversos ficheros dentro de una corriente de datos a los fines del intercambio, y que permita al destinatario reconstituir los distintos ficheros. El SDIF no se limita a un soporte determinado y puede utilizarse para el intercambio en redes de datos o en soportes transportables.	No existen productos comerciales que apliquen el SDIF.	Las Oficinas de la Cooperación Trilateral han seleccionado el SDIF para el intercambio de documentos de prioridad debido, en gran parte, a que se trata de una norma abierta internacional y al hecho de que no está vinculado a un único proveedor. Se empleará el SDIF para grabar documentos de prioridad en discos compactos reescribibles y para su transmisión en la red TSVPN.
PKCS#7	Norma 7 de criptografía de claves públicas (PKCS#7) Norma de *RSA Laboratories* para los datos que pueden cifrarse, como las firmas y los sobres digitales.	Varios productos de *RSA Data Security, Inc.* utilizan PKCS#7. Se ha seleccionado el producto BSAFE.	Las Oficinas de la Cooperación Trilateral han elegido la PKCS#7 como norma para la utilización de firmas digitales en los documentos de prioridad, y han decidido utilizar el producto BSAFE. La USPTO debe obtener una licencia de exportación para el cifrado fuerte.

Norma relacionada (cuando proceda)	Descripción	Ejemplo de producto	Comentarios sobre el uso
	Firma digital Técnica de certificación de la integridad de los datos contenidos en el documento digital y que asocia al firmante con un certificado digital emitido por un tercero reconocido. Para crear una firma digital, se debe procesar el objeto a firmar mediante un Algoritmo de Condensación Segura con el fin de crear un pequeño fichero de mensaje resumido que va asociado en forma única con el objeto firmado. Ello significa que si se vuelve a calcular el resumen tras un cambio en el objeto firmado, el resumen será diferente. Se cifra el resumen con la clave pública del firmante a fin de crear un bloque de firma digital que se añade al objeto firmado según las reglas de la PKCS#7.	*Digital Signature* ha sido incorporado en productos de *RSA, Trusted Information Systems, Nestcape, Microsoft* y otros.	Las limitaciones en materia de exportación en lo que respecta a la utilización del cifrado fuerte no son aplicables a las firmas digitales siempre que se pueda demostrar que el soporte lógico de firma digital no pueda adaptarse inmediatamente para cifrar el contenido de los datos.

Norma relacionada (cuando proceda)	Descripción	Ejemplo de producto	Comentarios sobre el uso
X.509 Ver. 3	Norma sobre certificados digitales Norma internacional sobre el formato y el contenido de los certificados digitales. Un certificado digital permite que un tercero reconocido certifique (avale) la relación entre una llave o clave pública y la información que identifica al titular de la llave.	La Norma X.509 se emplea en el soporte lógico que funciona en el dispositivo de cifrado *BorderGuard*. Los certificados X.509 son autenticados por servidores de autenticación instalados en las redes de las oficinas de patente.	Los certificados digitales, las firmas digitales y la criptografía de clave pública, así como los procedimientos de verificación de los certificados, constituyen la base de la infraestructura de claves públicas (PKI). Aunque la norma X.509 es ampliamente utilizada, los sistemas de certificación de los diferentes proveedores no ofrecen una buena interacción.

[Fin del Anexo y del documento]