E

WIPO

SCIT/WG/1/6
ORIGINAL: English
DATE: October 13, 1998

WORLD INTELLECTUAL PROPERTY ORGANIZATION
GENEVA

STANDING COMMITTEE ON INFORMATION TECHNOLOGIES

WORKING GROUPS
First Session
Geneva, November 16 to 20, 1998

TECHNICAL ISSUES IN RELATION TO THE EXCHANGE OF PRIORITY DOCUMENTS THROUGH THE NETWORK (TASK NO. 27)

Document prepared by the International Bureau

INTRODUCTION

1. The exchange of unpublished data between intellectual property offices via the global information network is planned for under the High Performance Intellectual Property Exchange Testbed program (see document SCIT/1/4, page 6). As preparation, the following task was created and included in the SCIT Work Program:

Task No. 27 "Identify technical issues in relation to the exchange of unpublished data and undertake pilot projects to find viable technical solutions".

The full range of intellectual property data to be exchanged between intellectual property offices via the network is being determined as part of the survey being conducted in connection with SCIT Task No. 35 (see document SCIT/WG/1/4). The focus of this paper is on the technical exchange issues.

2. A major source of unpublished data to be exchanged between intellectual property offices relates to priority documents. Priority documents (a copy of earlier filed national applications on the basis of which the priority is claimed) are issued by intellectual property offices which, at the request of applicants, will transmit a copy of the priority document to other offices. Under the PCT procedure, the priority document should be transmitted by the Receiving Office to the International Bureau which further transmits it to offices which request to obtain a copy of the document (see Rule 17 of PCT Regulations).

3. To significantly reduce the cost and resources consumed by the process of producing, transmitting and receiving copies of priority documents in paper form, the Trilateral Offices (the European Patent Office, the Japanese Patent Office and the United States Patent and Trademark Office) have worked together to introduce electronic exchange of priority documents among the Trilateral Offices. The data contained in priority documents in electronic form are unpublished data until such applications are published as unexamined patent applications or granted patents (usually 18 months after the filing date). The Trilateral Offices undertook this project as a pilot project to determine technical solutions for the electronic exchange of unpublished data on the network.

4. At the first plenary session of the SCIT, on behalf of the Trilateral Offices, the Japanese Patent Office gave a presentation on the progress of electronic exchange of priority documents (see the presentation paper distributed during the session which is available in the SCIT area of the WIPO Web site). The project consists of two phases:

i) the electronic exchange of priority documents on CD-R, and

ii) the electronic exchange of priority documents via the “Trilateral Network” which is a virtual private network set up between the Trilateral Offices.

The Trilateral Offices identified the technical issues that needed to be addressed in respect of priority document exchange via the network to be as follows:

1. Exchange mechanism
2. Encryption
3. Data types
4. Data elements (Document Type Definition)
5. Wrapper or Envelope to pack electronic files
6. Digital signature.

5. In light of its technical relevance to Task No. 27 and the recent progress made by the Trilateral Offices, the Secretariat requested the Trilateral Offices to share the results of their pilot project work concerning the technical requirements for the exchange of priority documents on the Trilateral network with the International Bureau. A list of the requirements as determined for use by the Trilateral Offices is given in the Annex to this document.

6. Most of the requirements agreed by the Trilateral Offices appear to be useful and relevant to the exchange of *any* unpublished data among intellectual property offices via the global information network. Therefore, it is proposed that the need for such requirements as described in the Annex[1] to this document should be reflected in the RFP (Request for Proposal) for the Global Information Network.

7. The SCIT Working Group is invited to note the content of this document and to make recommendations on the next action to be taken to the Plenary session.

[Annex follows]

[1] The products named in the Annex are illustrative of the type of product required and are as such not necessarily those that would be implemented in WIPONET.

ANNEX

INTERNATIONAL PRIORITY DOCUMENT EXCHANGE (IPDE)

Technical Requirements as determined by the Trilateral Offices in connection with priority document exchange via the Trilateral Network

Related Standard (where applicable)	Description	Example Product	Comments re use
Frame Relay	Frame Relay is an international standard for high speed access to public wide area data networks (WAN). It is currently priced to offer low cost per unit of capacity compared to other competing technologies. Capacity is packaged in terms of a committed information rate (CIR) which the vendor promises to provide all the time and an excess information rate (EIR typically 2x the CIR) which the vendor will support when capacity is available.	Frame Relay circuits from international telecommunications carriers	

Related Standard (where applicable)	Description	Example Product	Comments re use
IP	Internet Protocol An Internet Standard defining an addressing mechanism and rules for routing data packets between addressed systems.	IP router devices that interconnect networks and IP interface cards in computers attached to a network. Many products.	IP routers will be used to interconnect the Frame Relay Network and patent office networks.
IPSEC	IP Security A set of protocols being developed by the Internet Engineering Task Force (IETF) to support secure exchange of packets at the IP layer. IPSEC uses public/private key technology. IPSEC is intended to be a standard that will be acceptable and attractive to equipment vendors who will incorporate it in their products in order to provide interoperability with equipment from other vendors.	CISCO Systems	The final form of the IPSEC standards is being developed. Consequently, many vendors are taking a wait and see approach before going forward with plans to implement IPSEC in their products.
TCP/IP	Transmission Control Protocol and Internet Protocol An Internet Standard protocol for ensuring reliable end-to-end transfer of data between TCP ports on computers attached to interconnected networks	TCP/IP is implemented in software that is normally supplied by the computer system vendor or networking software vendor.	TCP/IP will be used for communications between software applications on computers that are connected via the TSVPN. Combined together TCP and IP implement the Network and Transport layers of the ISO 7-layer Network Protocol Model.

Related Standard (where applicable)	Description	Example Product	Comments re use
	Virtual Private Network (VPN) A technology for providing private communications within a public network by using data encryption. The data payload of packets sent through the network is encrypted and only the header information used to route data across the network is sent as clear text. Data that might be intercepted or monitored by parties other than the intended recipient is protected by the cryptographic system.	BorderGuard packet encryption device from StorageTek, Inc.	The BorderGuard is installed between the patent office's firewall and the wide area network port in the patent office. The BorderGuards are managed by a network management system. An export license is required to allow the use of 128 bit cryptographic key lengths.
IDEA	International Data Encryption Algorithm IDEA is similar to DES (Data Encryption Standard). It can be used in software outside of the US to its full 128-bit key length. It is believed to be a strong algorithm and no practical attacks on it have been published.	IDEA is implemented in the BorderGuard router and it will be used for the TSVPN encryption.	
	Intrusion Detection System A system used with the packet encryption devices to detect attempts to penetrate or intrude into the network.	NetRanger Probes and NetRanger Director software licensed by The Wiehl Group.	Intrusion detection involves recognizing packets that fail to match with what the encryption expects to see, traffic patterns that differ from normal, or known intrusion patterns. The vendor periodically updates this software to detect new threats.

Related Standard (where applicable)	Description	Example Product	Comments re use
SGML	Standard Generalized Markup Language An international standard for defining markup used to indicate the structure and content of documents. SGML tags are inserted with document text to indicate structural parts and content elements. For example: <FNI>Thomas A. Edison</FNI> would be a valid SGML tagging of the first named inventor.	Commercial off-the-shelf SGML authoring tools and SGML enabled word processors are available to create SGML documents.	IPDE documents are SGML documents. In the near term, while priority document images are exchanged, small SGML documents are created for descriptive data and the document images are referenced by the SGML document as external entities.
DTD	Document Type Definition A formal description (written in the SGML syntax) of the allowed tags and structure of a particular SGML document type.	Commercial off-the-shelf tools are available for creating DTDs.	USPTO has created four DTDs to be used for IPDE.
SDIF	SGML Document Interchange Format An international standard for packaging a SGML document that might be stored as several component files into a data stream for interchange in a way that permits the recipient to reconstitute the separate files. SDIF is media independent and can be used for interchange over data networks or on transportable media.	There are no commercial products that implement SDIF.	SDIF was selected by the Trilateral Partners for exchange of priority documents largely due to its being an international open standard and to give independence from a vendor. SDIF will be used for packing priority documents on CD-R media and for transmission over the TSVPN.
PKCS#7	Public Key Cryptographic Standard 7 A RSA Laboratories standard for data that may have cryptography applied to it such as digital signatures and digital envelopes.	A number of products from RSA Data Security, Inc. use PKCS#7. BSAFE has been selected.	The Trilateral Partners have agreed to use PCKS#7 as the standard for applying digital signatures to priority documents and use the BSAFE product. The USPTO must obtain an export license for strong encryption.

Related Standard (where applicable)	Description	Example Product	Comments re use
	Digital Signature A technique for certifying the data integrity of a digital document and associating the signer with a digital certificate from a trusted third party. To create a digital signature, the object to be signed is processed by a Secure Hash Algorithm to create a small message digest file that is uniquely associated with the signed object. This means that if the digest is recalculated after any change occurs to the signed object, the digest will be different. The digest is encrypted with the public key of the signer to create a digital signature block which is then packaged with the signed object using PKCS#7 rules.	Digital Signature is provided in products from RSA, Trusted Information Systems, Netscape, Microsoft and others.	Export restrictions on the use of strong encryption do not apply to digital signatures provided it can be shown that the digital signature software is not readily adaptable to encrypting data content.
X.509 Ver. 3	Digital Certificate Standard An international standard for the format and content of digital certificates. A digital certificate enables a trusted third party to certify (vouch for) the relationship between a public key and information identifying the key's owner.	X.509 is implemented in software that runs on the BorderGuard encryption device. X.509 certificates are authenticated by authentication servers on the patent office networks.	Digital Certificates, Digital Signatures, Public Key Cryptography and procedures for verifying certificates form the basis for a Public Key Infrastructure (PKI). Although the X.509 standard is used, certificate systems from different vendors don't inter-operate readily.

[End of Annex and of document]