E

WIPO

SCIT/WG/1/5
ORIGINAL: English
DATE: November 3, 1998

WORLD INTELLECTUAL PROPERTY ORGANIZATION
GENEVA

STANDING COMMITTEE ON INFORMATION TECHNOLOGIES

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

STUDY THE POTENTIAL OF ELECTRONIC COMMERCE, ITS INFRASTRUCTURE AND THE USAGE OF TOOLS THEREFOR BY INTELLECTUAL PROPERTY OFFICES (TASK NO. 28)

Document prepared by the International Bureau

INTRODUCTION

1. The Plenary session of the Standing Committee on Information Technologies (SCIT) in June 1998 proposed that "the Information Security Working Group (ISWG) should discuss technical issues in relation to the exchange of data, and to undertake pilot projects, associated with the IPDL program and using the WIPONET, in the areas of electronic filing, the exchange of priority documents for the examination of patent applications, and other planned activities of electronic commerce" (see document SCIT/1/7 Prov., paragraph 14(c)). It proposed that the ISWG should also provide an opportunity to intellectual property offices to share the experience of offices advanced in this area and work on the following points of technical cooperation:

- technical cooperation to Member States to assist them in their use of network infrastructure and tools for electronic commerce;
- coordination between the electronic commerce activities of WIPO and the Member States from technical viewpoints (e.g., adoption of the necessary tools, possible adoption of general technical guidelines for electronic commerce in the intellectual property area);

- pilot projects using electronic commerce tools for the provision of intellectual property information.

2. In this connection, the following task was included in the Working Program:

Task No. 28 "Study the Potential of electronic commerce, its infrastructure and the usage of tools therefor by intellectual property offices".

ACTION TAKEN

3. As initial activity on the above task the International Bureau has taken action as follows:

i) As an aid to a common understanding of the security issues involved--which is considered a necessary precursor to the establishment of electronic commerce applications--the International Bureau has produced an overview document on information security related technical issues (see the Annex to this document), and

ii) Outlined a proposed pilot project (see below).

PROPOSED PKI PILOT PROJECT

4. A Pilot Project is proposed for the exchange of messages between offices, applicants, and the International Bureau concerning requests for priority documents. This project will not cover the exchange of documents themselves, and will run from January 1999 through April 1999.

5. Parties to the project would be able to exchange secure, authenticated, messages (using digital certificates and digital signatures) which request or acknowledge requests for priority document exchange. The messaging mechanism could be as simple as secure electronic mail.

6. In detail, two or more intellectual property offices and the International Bureau will exchange secure electronic e-mail containing messages requesting the delivery of priority documents from one office to the International Bureau, then to another office. The priority documents themselves will not actually be exchanged; only the messages.

7. The messages will be authenticated and encrypted through the use of digital certificates and digital signatures. The digital certificates will be issued by each office, under their own security and authentication policies. The actual signing, validation, encryption, and decryption of messages will be performed by commercial electronic mail packages.

8. This pilot project will test the interoperability of PKI (Public Key Infrastructure; for more information see the Annex to this document) environments managed by different offices and organizations, and will permit the identification of problems and issues associated with the issuance of certificates and cross-certification of users within the broader intellectual property community.

9. The Secretariat needs to receive guidance from the ISWG as to how to select two or three intellectual property offices which will participate in the pilot project if it is approved by the ISWG.

10. The SCIT Working Group is invited to approve this proposal.

[Annex follows]

ANNEX

INFORMATION SECURITY – ISSUES OVERVIEW

INTRODUCTION

1. The Plenary session of the Standing Committee on Information Technologies (hereinafter referred to as the "SCIT") has noted outstanding information security issues of importance to the development of the Global Information Network (WIPOnet). These technical issues are related to the exchange of unpublished (confidential) data using WIPOnet, such as priority documents, electronic filing systems and other planned activities. This document provides an overview of some of these technical issues as they relate to information security.

OVERVIEW

2. The general architecture of international communications networks, and the technologies used in the low-level exchange of data lead to a variety of issues related to information security.

3. From the hardware and connectivity perspective, individual data streams across networks can be protected, regardless of the applications software generating the data. Internet-based networks make use of *packet-switching* technologies. In other words, data, such as documents, are divided up into small chunks known as packets. This division is done at a very low level and is invisible to the user. Each of these packets contains, among other things, the address of the originating machine, the address of the receiving, or target, machine, some data, and a checksum of the data. The checksum is used to verify the correctness of the received data by the target machine.

4. For the purposes of this discussion, the two addresses in the packet are of the most interest. Devices known as *routers* are able to read these addresses in each packet and switch, or route, the packet to its correct location, over the designated communications infrastructure. The routers determine the "best path" for a packet to follow, based upon its origin and destination. This "best route" may not be the geographically shortest. These paths are set up by the router maintainers, and can be changed when conditions warrant.

5. The issues that arise from these architectural considerations include:

- Updating and management of WIPOnet routers in a secure environment
- Low-level encryption of data
- Exclusion of unauthorized entities from Intellectual property office networks

6. Physical security issues are also important for a secure network, as unauthorized physical access to machines can result in security problems. These issues include:

- Physical control of machines
- Reprocessing of hard drives and diskettes
- Username and password security
- Unauthorized access to internal and external networks

7. Beyond basic network architectural issues, those of applications-level systems (such as e-mail clients, web browsers, etc) presents another set of information security issues. Most secure software currently makes use of public key systems to encrypt and authenticate information exchanged between users. Adherence to well-defined international standards is critical in this area, as software from different manufacturers must interoperate in a secure manner. Some of these issues include:

- Creation, use, and verification of digital certificates
- Encryption standards
- Key-exchange protocols
- Key recovery, in case of lost or damaged security keys
- Digital signature and nonrepudiation

8. It is important to understand the distinction between data secrecy, and data authenticity. If, for example, an office wishes to make certain public data available, it is equally important to have a mechanism to insure the authenticity of the public information as it would be in the case of secret data.

9. Clearly, many of these issues are related. In the information systems and security industry, the term "public key infrastructure" (PKI) has been coined to describe the policies, hardware, and software used to ensure the secure exchange and authentication of information and security data through networks. Some of these issues also fall into the loose category of "electronic commerce".

10. Regardless of issues of terminology, the issues associated with PKI and "electronic commerce" are of significance to the day to day activities of Intellectual property offices, and the ability to utilize electronic methods would facilitate efficient interactions between offices and applicants.

Relationship between information exchange activities by Intellectual property offices and Information security issues

11. Information exchange activities will include the exchange of confidential, unpublished information. For example, any exchange between applicants and examiners requires excellent levels of security and data privacy. Furthermore, many of these activities require some assurance of the identity of one party or another. For example, if an applicant is exchanging information with an examiner, the examiner needs to know that the individual is indeed authorized to provide information, (e.g., proof of identity), and the applicant needs to be confident that he or she is indeed in contact with a patent examiner and not a clever hacker.

These transactions also need to posses non-repudability, (e.g., if an individual sends an examiner a new claim, the individual should not be able to repudiate the transaction at a later date).

12. The exchange of priority documents provides another interesting example. If a priority document is to be exchanged in electronic form, it needs to be validated by the originating party. In other words, the document needs to be signed to demonstrate its authenticity, it needs to have a guaranteed time stamp associated with the transaction, preferably by a third party (to prevent presumed or actual forgery of dates and times), and it needs to have some guarantee of accuracy, so that a party obtaining the document can tell if tampering occurred.

13. All of the above issues can be thought of as information security problems, and all can be solved through a well-organized, carefully considered public key infrastructure.

Public Key Infrastructure

14. Public Key Infrastructure (PKI) supports the secure, authenticated use of resources within a network framework. A comprehensive PKI establishes facilities, specifications, and policies for the use of public-key based certificates for information systems security, electronic commerce, and secure communications, including e-mail and conferencing.

15. A comprehensive PKI will be required for WIPOnet to permit the secure utilization and exchange of confidential information, as well as the identification of authoritative sources of non-confidential information and services.

16. It is important to realize that WIPOnet is more than just a closed community of Intellectual property offices, and that applications used on WIPOnet will mature over time. Therefore, we should not view WIPOnet PKI as a monolithic, top-down structure. Instead, it will provide a framework for the interoperability of both off-the-shelf and customized applications within the WIPOnet environment, and on the public Internet at large.

17. One of the most obvious challenges will be to craft a PKI that interoperates cleanly with other similar efforts underway within WIPO member states, and within the Internet and information systems industries in general.

International Cooperation

18. Each participating Office in the WIPOnet project (including the International Bureau of WIPO) would have to take responsibility for implementing a suitable information security policy with respect to its network-connected information systems. International cooperation is essential to reduce risk and improve interoperability between information systems and network components. The table below outlines those roles, and demonstrates the level of international cooperation desired and required for an effective information security infrastructure between WIPO, the national Offices of its member states, and interested regional offices.

Issues/items	Parties involved	Solution	Action
Network Security	WIPO (IB) and participating Intellectual property offices	Encryption, physical design	Careful pre-deployment design, public key infrastructure (PKI)
Access Control	WIPO (IB) and participating Intellectual property offices	strict policy controls, policy implementation through unforgeable tokens of identity	guidelines and agreement, PKI support
Identity Confirmation	WIPO (IB) and local participating Intellectual property offices	Local Office as Registration Authority	User registration inputs into PKI
Digital Certificates	WIPO (IB) and participating Intellectual property offices	WIPO/Local/Regional offices as Certification Authorities	pilot project aiming to set up IP community PKI
Data Security	data exchanging Offices	good choice and proper use of COTS	coordination between exchange partners and SCIT recommendation, PKI

Current Technical Solutions

19. Currently, several commercial and freely available products provide digital certificate issuance, validation and management schemes. It will be necessary for various combinations of these products to be evaluated in a representative setting, e.g., a pilot project. A well-designed PKI should be based on multiple-source commercial products, which utilize both industry-wide and international standards. As the commercial market for these services matures, more advanced products will become available, and will indeed be used by Intellectual Property offices and their audiences in industry. The WIPOnet PKI should recognize this and adapt to changing market, industry and networking conditions while providing robust security.

[End of Annex and of document]