world summit
on the information society
Geneva 2003 - Tunis 2005

Document WSIS/PC-2/CONTR/79-E
5 February 2003
English and French only

WISEKEY

Contribution of the International Organization for the Security of Electronic Transactions (IOSET) and the company WISeKey S.A. to the Second meeting of the committee of preparation of the World Summit on Information Society Geneva, February 17-28, 2003

The objective of this document is to propose the transfer of control and management of technologies related to the fundamental security of the Internet to neutral authorities working in the public interest.

The International Organization for the Security of Electronic Transactions (IOSET) and WISeKey SA, member of sector D of ITU, by way of contribution to the Second Meeting of the Global Preparatory Committee of the WSIS have the honor to propose a discussion paper on aspects essential to the construction of a more universal, open and secure information society.

Our proposition adopts a conceptual approach so that its content and objectives are comprehensible.

Concepts

The (DNS) is a technical platform essential for the operation of the Internet. This system of nomenclature is a hierarchical structure whose functions begin from a single central root (the "root servers" authority) which contain the list of the top level domains (generic: com net org biz... and national: de fr jp ca...). The concept of "multiple roots" (or "alternate roots", "open root", "inclusive roots"...) is an overall response to the management of the roots. ICANN "Internet Corporation for Assigned Names and Numbers" is the organization with the exclusive right to the centralized management of the resources of the Internet.

Public key infrastructures (PKI) are hierarchical systems of trust. A "Root CA" is a certification authority which can be trusted by a browser or system; and through which subordinate authorities, and entities are trusted via "inheritance of trust". Currently, several defacto "root CAs" exist, the majority of which are privately owned. The choice of which root certification authorities a browser or operating system vendor accepts by default as trusted, through pre-installation or certified updates, is up to the choice, or goodwill, of that vendor.

The objective of our proposal is to create a more universal, open, reliable and secure Information Society.

Proposals

To transfer to international organizations, the infrastructure essential to the operation and security of the Internet, in particular:

The management of the domain names system, in order to allow a more democratic management of the allocation of domain names. Starting with new extensions to the generic Top Level Domain (gTLD) name space that is currently controlled by ICANN. From inception ICANN´s monopoly of this has been, and continues to be, increasingly disputed by economic, and government entities who accuse them of organizing a shortage, despite there being no true technical obstacle to the creation of an infinite number of gTLDs. In the absence of being able to use this common root, companies are starting to create "alternate roots", i.e. a tree structure on a particular Alternate Root DNS, off-line to the Root DNS on which the public Internet is based.

The management of Public Key Infrastructures and the automatic recognition by Web browsers of digital certificates issued by certification authorities, in order to allow a more democratic management of the recognition of certification authorities. This would necessitate sharing the management and authority for deciding the automatic recognition of PKIs between the private sector and the public sector in order to be able to guarantee its technological and political independence and consequently, to avoid monopoly situations. Internet users wish to work in security, transparency and confidence, and need a universal service of nomenclature managed in the public interest.

To establish and adopt, at the national and regional level, standards applicable to information security products and services. To promote security by large companies and SMEs. Alternatively, to reinforce the installation of regional Internet roots in order to decentralize the universal system of nomenclature. It is also recommended that the following be transfered to an organization able to guarantee the neutrality of the model: the responsibility for, and definition of TLDs, as well as the coordination of the establishment of the rules of operation to ensure global communication.

To study the possibility of combining the governance of the Internet (DNS) with public key infrastructures (PKI). The complementarily of these hierarchical structures could allow the management of the roots of the two structures by a single neutral authority.

Concerning the Information Security, to implement by concrete actions:

- The interoperability, compatibility and international recognition of suppliers of Digital Certification Services;
- Increased cooperation between the various regulatory authorities;
- Co-operation between various consumer protection institutions;
- International recognition of the legal validity of electronic signatures;
- Standardization of rules for data protection and privacy;
- The management of digital identities in an electronic environment (individuals, organizations and equipment;). Services for citizens enabling electronic government (e-government;)
- Information exchange between governments.

All these sectors of economic activity, technical, political, administrative and legal, require standards such that the benefits of ICT become a reality.