E

WIPO

SCCR/7/3
ORIGINAL: English
DATE: April 4, 2002

WORLD INTELLECTUAL PROPERTY ORGANIZATION
GENEVA

STANDING COMMITTEE ON COPYRIGHT AND RELATED RIGHTS

Seventh Session
Geneva, May 13 to 17, 2002

STUDY ON THE PROTECTION OF UNORIGINAL DATABASES

Study prepared by Mr. Sherif El-Kassas
Associate Director, Department of Computer Science
American University in Cairo

TABLE OF CONTENTS*

* At the request of its member States, WIPO commissioned, in 2001, five studies on the economic impact of the protection of non-original databases in developing countries and countries in transition. This study, one of those five, contains the research and opinions of only its author and does not in any way reflect the views or position of WIPO.

Page

§

SUMMARY OF THE STUDY

This paper aims at dealing with the impact of the protection of unoriginal databases on developing countries. The paper deals exclusively with databases that are not protected under copyright. It is focused on two main aspects: the possible implications of unoriginal database protection on development, and technical alternatives to legal protection.

The paper presents an overview of the main database protection initiatives: the European Community (EC) model, the United States of America (USA) and international models, and the laws found in Mexico and Scandinavian countries. It then examines the main arguments for and against unoriginal database protection. A review of possible technical measure for protection is presented together with examples from industries with similar concerns. Finally, a number of conclusions are offered. The paper contains appendices that provide a more detailed view of some important technical protection measure.

Arguments supporting database protection initiatives assert that the goals of protection include the need "to rescue database producers from the threat of market-destructive appropriations by free-riding competitors," [1], to encourage investment in the collection of certain types of data, and to maintain and equitable advantage as compared to EC based companies (and other regions) that provide *sui generis* database protection and extend it to foreign companies on a reciprocity treatment basis [3].

However, it is argued that this type of protection, would in reality "create an exclusive property rights regime of virtually unlimited duration […]," and that it would "jeopardize basic scientific research, eliminate competition in the markets for value-added products and services, and convert existing barriers to entry into overwhelming legal barriers to entry."

Hence, the paper concludes that *sui generis* protection of unoriginal databases in the current proposals would have negative effects on developing countries and on the scientific and academic communities worldwide. Moreover, it is asserted that the legitimate concerns of database compilers can either be met within the framework of the existing IP laws and systems and/or by using technical measures for protecting their database systems.

STUDY

I. DISCLAIMER

This study was commissioned by the World Intellectual Property Organization (WIPO) to deal with the impact of the protection of unoriginal databases on developing countries. The study is to be used by the standing committee on Copyright and relate rights in its work on the possible establishment of an international instrument for the protection of databases.

The study deals exclusively with databases that are not protected under copyright (i.e., that do not fulfill the originality criterion of the Berne Convention and the WIPO Copyright Treaty).

As this author is of technical background with experience in the Information Technology (IT) in developing countries, Security of IT systems, and IT applications in the administration of IP rights, this study will be focused on two main aspects: the possible implications of unoriginal database protection on development, and technical alternatives to legal protection.

II. INTRODUCTION

Arguments supporting database protection initiatives assert that the goals of protection include the need "to rescue database producers from the threat of market-destructive appropriations by free-riding competitors," [1], to encourage investment in the collection of certain types of data, and to maintain and equitable advantage as compared to EC based companies (and other regions) that provide *sui generis* database protection and extend it to foreign companies on a reciprocity treatment basis [3].

The database laws seem to offer protection to anyone who invests in the collection of material and the development of a database [1, 6]. The protection does not require that the database contain original content or constitute an original work.

It is argued in [1] that this type of protection, as proposed in EC and USA initiatives "would create an exclusive property rights regime of virtually unlimited duration that would be subject to few, if any, public policy limitations. It would jeopardize basic scientific research, eliminate competition in the markets for value-added products and services, and convert existing barriers to entry into overwhelming legal barriers to entry. The European and United States initiatives could thus lead to relatively high prices for the use of public goods. Economic efficiency, however, calls for very low prices for such use and favors minimum incentives to provide the needed investment and services."

The nature of Digital Information systems has also contributed to the motivation to provide legal protection of databases. This is mainly due to the ease of access and copying of published digital information.

Overview of Database Protection Initiatives[1]

It is asserted that copyright laws exclude unoriginal databases. This has motivated the drive to fill the gap between most current intellectual property legal system and the need for database protection. Hence, the proposals to protect "non-copyrightable databases under *ad hoc* or *sui generis* intellectual property systems that deviate from the classical patent and copyright models underlying the Paris and Berne Conventions" [1].

(a) The European Union Initiative

In the context of database protection [1] reports that the Commission of the European Communities pursued two objectives: (1) harmonize the rules of the member states with regard to copyrightable databases; and (2) fill a perceived gap in existing intellectual property regimes with regard to electronic compilations of data.

The European Commission's vision of a strong exclusive property right for database protection governs the EC Directive on Databases [1,6].

The *sui generis* right granted to database makers enables them to obtain an exclusive "right to prevent extraction and/or reutilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database." This exclusive right lasts for an initial period of at least fifteen years. The publisher of such a database may continually renew that right for additional fifteen-year terms if the he has made additional investments in the database.

The EC Directive conditions *sui generis* protection on proving that "there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents or in any substantial change resulting from the accumulation of successive additions, deletions or alterations." It is reported that the EC Directive provides no guidelines for evaluating the requisite level of investment. Hence, the threshold for qualifying for protection remains uncertain. Furthermore, "there are no limits to the number of quantitative or qualitative changes that will qualify for such extensions, and any publisher who continues to make a substantial investment in updating, improving, or expanding an existing database can obtain perpetual protection" [1].

From the above it is asserted that the *sui generis* right depends exclusively on *investment*. However, "the scope of protection that the Final EC Directive affords investors in non-copyrightable databases now appears roughly equivalent to that afforded authors of copyrightable compilations" [1].

Moreover, under the EC directive, "every independent generation of data, however mundane or commonplace, will obtain protection if it costs money, and every regeneration or reutilization of the same data in updates, additions, and extensions that cost money will extend that protection without limit as to time."

---

[1] This section is based on the presentation and material found in [1,6].

As a consequence, third parties will not be able to avoid the expense of regenerating preexisting data, unless the originator of the relevant database has abandoned it or declined to exercise his or her proprietary rights, much as occurs under trademark laws.

Furthermore, regardless of whether it is possible to regenerate the data from publicly available sources, investors in database production can always deny third parties the right to use pre-existing data in value-adding applications.

In [1] it is asserted that the EC Directive harbors no working conception of a public domain. Essentially, this is because each new extension of the database maker's exclusive rights (because of his or her investment in updates, additions, and revisions) will qualify that investor for protection of the database as a whole for an additional fifteen year[2]. This strengthens the originator's ability to deny third parties the right to build upon preexisting scientific and technical knowledge, and it creates a further barrier to entry.

This is especially significant for developing and underdeveloped countries that may lack the necessary funding to purchase access to such information. Without protection this information would be available to them at no charge.

(b) The United States of America (USA) and International Models

The United States of America (USA) and European Union both submitted proposals for worldwide protection of the contents of databases under *sui generis* intellectual property regimes akin to that embodied in the EC Directive.

WIPO hosted a diplomatic conference to consider these proposals in December 1996. Under the USA bill and proposal also extended protection to the compiler of data. The compiler would qualify for exclusive rights to prevent extractions and reuses of the whole or substantial parts of a database on the grounds of having made substantial investments in the collection, assembly, verification, or presentation of the database contents. If the compiler continued to invest in updating or maintaining the database, its twenty-five year initial term of protection could be perpetually renewed without limit.

Furthermore, the USA proposal contained a broader definition of a database. It includes non-copyrightable components of computer programs in its definition of databases, and it provides no apparent criteria for excluding even facts or data compiled for scientific and historical works. Furthermore, the USA proposal to WIPO, would grant database makers a twenty-five year initial term.

The USA proposal reinforces the single most disturbing aspect of the EC Directive, namely, that it precludes formation of an evolving public domain from which third parties can freely draw.

The USA proposal, "by providing a longer period of protection, more powerful exclusive rights, no public interest exceptions or privileges, harsh criminal penalties […], and ancillary rules reinforcing self-help policing of online transmissions, the proposed USA law

---

[2] This extended protection is not limited to the revised or added matter as would occur under the copyright laws.

would grant database owners a more absolute monopoly than that emanating from the EC Directive" [1].

(c) National Legislations

WIPO published a survey of the national legislation of its Member States [6][3]. The survey identified *sui generis* legal protection for databases which do not meet the criterion of originality in the following countries: Denmark, Finland, Iceland, Mexico, Norway and Sweden.

The protection granted under the Nordic laws (Denmark, Finland, Iceland, Norway and Sweden) cover copying (in Iceland, reprint and copying) only. No protection is granted against other use, and the laws do not specify to which extent they are applicable as regards unauthorized extraction and copying of parts of protected compilations.

The term of protection and its calculation differs somewhat in the Nordic laws. In Denmark, it is ten years from the year of first making available to the public, but not longer than 15 years from the year of making; in Finland, ten years from the year of publication, but not longer than 15 years from the year of making; in Iceland, ten years from the year of publication; and in Norway and Sweden, ten years from the year of publication. None of the laws contain explicit provisions regarding the renewal of the term in case the compilation is continuously or occasionally updated, enlarged or revised.

The Federal Law on Copyright of Mexico provides for a *sui generis* protection of databases which extends the protection to non-original databases. The rights granted are exclusive rights to authorize or prohibit the following: (1) permanent or temporary reproduction in whole or in part, in any medium and form; (2) translation, adaptation, rearrangement and any other modification; (3) distribution of the original or copies of the database; (4) communication to the public; and (5) reproduction, distribution, or communication to the public of the results of the operations, mentioned under (2), above. The original owner of the rights is the person who has made the database. There are no explicit provisions regarding transfer of ownership.

The term of protection is five years. There are no explicit provisions regarding the renewal of the term in case the compilation is continuously or occasionally updated, enlarged or revised.

[3] The remainder of this subsection is based on material extracted from [6].

III. THE MAIN ARGUMENTS ON *SUI GENERIS* DATABASE PROTECTION[4]

(a) The Main Arguments in Favor of *Sui Generis* Database Protection

There are three major argument that are presented by supporters of s*ui generis* protection of databases in [2], in addition to those further arguments are opposed for developing and underdeveloped countries. They can be summarized as follows:

1. The large investment in compiling and maintaining databases needs additional protection. Especially in the digital, on-line world which makes copying databases easy.

2. Existing copyright law provides no protection for large comprehensive on-line databases which are used by means of a search engine. The compiler has exercised no selection because the databases are comprehensive. Furthermore, arrangement only occurs when the user conducts a search. Hence, in the absence of selection and arrangement, no copyright protection is available.

3. The EU Database Directive will provide European companies an advantage in the database market. Because the Directive extends *sui generis* protection to non-EU entities on a reciprocity rather than national treatment basis, the Directive will deny non-European companies the new legal protection afforded databases unless their home countries offer comparable protection.

4. In developing counties, protection can constitute motivation for compilation of databases that can have positive effects on development (in the form of information becoming available due the collections and compilation). In other cases, it is argued that protection might help retain foreign investment.

(b) The Main Arguments Against *Sui Generis* Database Protection

A number of argument have been made in [2,3] to oppose *sui generis* database protection.

1. Adequate protection exists within the present intellectual property law framework. For instance, only a small amount of selection or arrangement is necessary to bring a database within the protection of the copyright laws. It is argued that this is sufficient to protect against wholesale copying.

2. Contract, trade secret and unfair competition laws provide an additional layer of protection for databases irrespective of whether the compilation is copyrightable.

3. Even without legal protection, the database compiler can still protect its investment through technological means that prevent copying of the database. These technological means are discussed in more detail in section 4 and the appendices.

4. To date no evidence or concrete examples have been presented where a database publisher decided not to develop a product out of fear that the product would receive

[4] This section draws on material presented in [2] and [3].

insufficient intellectual property protection. It is argued that no evidence has been produced because none exists [2].

5. The broad scope of protection (provided by the USA proposal) is one of the more problematic points. The USA proposal defines a database to include a collection of work, data or other materials this all-inclusive definition would go beyond what is commonly thought of as a database.

6. The term of protection is also problematic. The EU directive offers 15 years of protection, while the USA proposal offers a 25 year term. However, both models would allow many databases to receive perpetual protection because any significant change or updating of the database would result in the creation of a new database with a new term of protection. This perpetual protection, when combined with the possibility of the protection applying to works now covered by copyright, may have permitted database publishers to circumvent the term limits in the Copyright law, leading to a drastic diminution of the public domain.

7. Objections by Scientists and Researchers. Most forms of research require the use of large amounts of data. Some forms of research require the use of entire databases. If databases which are now freely available fall under *sui generis* protection, the cost of research will inevitably increase. Moreover, *sui generis* protection will motivate institutions to treat their own databases as profit centers and hence will have adverse effects on scientific data sharing. *Sui generis* protection will raise the cost of research and in all likelihood will make it even more prohibitive for developing counties.

8. Objections by Software Developers. The USA proposal implies that databases contained within computer programs would receive protection. Thus, look-up tables, command sets, character sets, and similar data structures and program elements would receive protection as databases. This will hamper software development and increase its cost. Another element that is especially important for developing countries that might be prevented from realizing the benefits of open-source and free software because of this form of protection.

9. Objections by Internet Companies[5]. Routing tables and directories necessary to the functioning of the Internet fall within the definition of a database in the USA proposal. *Sui generis* database protection, therefore, could lead to the concentration of market power in the Internet. Additionally, the unauthorized transmission of a database could lead to vicarious liability for the on-line service company which unknowingly provided the hardware and software facilities by which the transmission occurred. Another important concern for developing countries as it such effects will increase the cost of and hamper the development of the Internet in local communities.

10. Objections by Value Added Database Publishers. There are many legitimate firms which take data from existing databases and add value to them by inserting new information or arranging the information in a different way. *Sui generis* protection could put this entire industry out of business.

---

[5] A more detailed treatment of this item can be found in [5].

11. In developing counties, companies that take initiatives to compile databases about local resources, and heritage can effectively obtain a destructive monopoly and is likely to have adverse effects on development and information access.

IV. TECHNICAL ALTERNATIVES TO LEGAL PROTECTION

The sections above outline major issues surrounding s*ui generis* protection of databases. This author believes that such protection would have adverse effect on development. However, it important not to dismiss the valid right of compilers of databases to protect their investment. It is argued that in most cases protection beyond that offered by the more traditional intellectual property rights is not necessary, and that in those areas where it might be desirable to offer extra protection technical means can be deployed to bridge this gap.

(a) Copy protection schemes

Many copy protection schemes have been proposed by the computer industry. They are mainly used to protect various electronic, multimedia and data content. These include software, Music, videos and books. The copy protection schemes can operate at the information level or device level and may use software or hardware means to accomplish its goal. For example, the DVD industry implements the so-called Content Scrambling System (CSS) to protect the contents of DVD media. Similarly the music industry is pursuing copy protected CDs that cannot be easily copied. And in the electronic publishing world. Adobe (*www.adobe.com*), creator of the industry-standard Acrobat program. This is basically a tool for creating e-books; it offers publishers wishing to protect their content the ability to configure Acrobat to restrict the ability of users to reproduce or pass on their copies of e-books. Database publishes can utilize the same schemes when appropriate. For example, a publisher of a CD containing a phone directory can deploy one of the copy protection schemes outlined above. This will grant the publisher control over the use of the database, however, it will not enable him or her to turn the database into a perpetual monopoly. Appendix A, provides a summary of some of the main schemes that can be directly applied to the database world.

(b) Deploying Special Viewing Devices or Programs

Various encryption schemes have been proposed to protect various types of data. For example, the broadcast industry has long deployed encryptions schemes (with mixed success) to control access to Pay-TV services. In this scheme, the viewer deployed a special device that enables him or her to view Pay-TV programming. The program broadcaster can essentially control the device's ability to display Pay-TV programs. Hence, the broadcaster can protect his or her rights by only allowing paying customers to view the programs.

Furthermore, the electronic commerce and on-line trading communities face many similar challenges to those faced by the database community. This is particularly true for access authentication. Alternative schemes have been deployed by those communities. They depend on strong authentication techniques to ensure the identity of systems users and use various cryptographic technologies (deploying both hardware and software solutions) to maintain the integrity and security of their systems. Appendix B outlines the main concerns,

requirements, and technical means of protection in electronic commerce. Much of this experience is directly reusable for database protection.

Similar schemes can be deployed with online databases. The special devise used to display the information could be implement in hardware or software (or a combination of both) and would enable database publishers to protect their rights without having to resort to excessive perpetual protection.

V. CONCLUSIONS

It appears that *sui generis* protection of databases is motivated by the perception that there is a need within the database industry to protect the effort and investment in their business and products. However, this author believes that the protection of databases will have important negative effects on development and on the free flow of information in the scientific communities.

The main concerns echoed in this paper are that *sui generis* protection of data bases:

1. will detract from the public domain and thus significantly reduce the availability of free information and data;

2. may create counter productive perpetual monopolies by allowing owners of databases to indefinitely extend the period of protection;

3. will be harmful for the free flow of information in the scientific communities of the world;

4. will be harmful for the development of the Internet and the software industry because many component of software systems will become protected and hence will no longer be available for free use and utilization; and

5. will hamper many aspects of development in the developing and under developed world.

Moreover, it is asserted that the legitimate concerns of database compilers can either be met within the framework of the existing IP laws and systems and/or by using technical measures similar those outlined in the appendices.

REFERENCES

[1] J.H. Reichman and Pamela Samuelson, *Intellectual Property Rights in Data?*, http://eon.law.harvard.edu/h2o/property/alternatives/reichman.html

[2] Alan D. Sugarman, *Database Protection–Tilting The Copyright Balance*, *http://www.hyperlaw.com/dbprot1.htm*

[3] Jonathan Band and Jonathan S. Gowdy, *Sui Generis Database Protection: Has Its Time Come?*, D-Lib Magazine, June 1997, *http://www.dlib.org/dlib/june97/06band.html*

[4] Anne Linn, History of Database Protection: Legal Issues of Concern to the Scientific Community, *http://www.codata.org/data_access/linn.html*

[5] Gordon Irlam and others, *Software Developers Comments on the WIPO Database Treaty*, *http://www.base.com/gordoni/thoughts/wipo-db.html*

[6] Existing National and regional legislation concerning intellectual property in databases, Information meeting on intellectual property in databases, Geneva, September 17 to 19, 1997, WIPO db/im/2. *http://www.wipo.org/eng/meetings/infdat97/db_im_2.htm*

[7] Information Meeting on Intellectual Property in Databases, Geneva, September 17 to 19, 1997, *http://www.wipo.org/eng/meetings/infdat97/*

[8] *http://www.wipo.org/eng/meetings/infdat97/db_im_3.htm*

[9] Ross Anderson, *Security Engineering: A guide to building dependable distributed systems*, Wiley, 2001.

[10] Bruce Schneier, *Applied Cryptography*, 2nd edition, Wiley, 1996.

[11] Towards Electronic Commerce in Egypt: A Certificate Authority for Egypt, The Electronic Commerce Committee, The Internet Society of Egypt, CAINET'1998.

APPENDIX A: COPY PROTECTION SCHEMES

At a technical system level, both copyright and censorship are access control issues, concerned with limiting access to information to people in certain groups [9]. Much of the schemes commonly used in the copy protection world are directly usable for database protection.

(a) Copy Protection of Software

The main software protection schemes include:

– Hardware protection, or dongole devices, are attached to the systems. The software can be copied, but without the dongole (which is a copy and tamer resistant device) the software wouldn't work.

– Installation of software using methods that are resistant to native copying. For example, by deploying a hard-disk sector modification technique that would mark a particular hard disk sector as bad and the program would need to check for this sector to ensure proper operation of the software.

– Detecting the hardware profile and usage patterns of the software can also be used to determine if the software is being copied or used by its lawful owner.

(b) Copy Protection of Audio

Copyright protection for audio is an old concern it can be traced back to the 1960s when the audio cassette recorder was introduced [9]. In the digital world of the Internet copy protection of Audio became a large concern when the MP3 format for compressing Audio become popular. MP3 enabled users to compress megabytes of CD tracks into Kilobytes of MP3 files that could then be sent around the Internet. The music industry tried to make copying difficult by introducing alternative audio formats that supported copyright (by using digital watermarking and similar techniques).

(c) Video and Pay-TV

Video cassettes and video players have a long history of introducing copy protection schemes to make it difficult to copy or pirate video content. Some of the schemes where *software* specific, i.e., relied on how the recording was done, while others depend on support from the video player itself. The Pay-TV industry has a long history in protection of its video content. Protection typically takes the form of set top boxes that are necessary to decipher the incoming TV broadcast. The industry has constantly updated its deciphering devices as the cost of technology dropper. In the early 1970s crude devices were used to implement simple schemes that involved simple manipulations of the TV signals. In the 1980s more sophisticated systems (such as VideoCrypt and EuroCrypt) became available. Those schemes typically involved three components: (1) Subscribed management services; (2) Set-top box; and (3) Smart card which contains the subscribers credentials and program list.

(d) Digital Versatile Disk (DVD)

The DVD (originally named Digital Video Disk) standards supports the so-called content scrambling system (CSS). The DVD players use a build in implementation of CSS to support the copy protection scheme. However, it should be noted that the DVD scheme was not particularly successful in resisting copying. The point made here, however, is that schemes that are similar in nature, but more robust, can be used for database protection.

APPENDIX B: E-COMMERCE SAFEGUARDS AND THEIR APPLICATION IN DATABASE PROTECTION

Electronic commerce systems share much of the goals of the (on-line) database community in terms of the protection of their investment and the integrity of their systems. This appendix is provided here to highlight some of the major technological schemes used to achieve those goals.[6] It is argued that similar means can be used to achieve adequate technological protection of database systems.

(a) Requirements and Safeguards for Electronic Commerce

Security is an essential requirement for electronic commerce. This is especially true for electronic commerce over an open and distrusted network such as the Internet. This section outlines important aspects of security: requirements and safeguards.

(i) Requirements

In general we can identify five main security requirements for electronic commerce: (1) entity authentication; (2) message integrity; (3) non-repudiation; (4) effective audit mechanism; and (5) privacy.

(ii) Entity Authentication

Entity authentication is necessary to ensure confidence in electronic transactions. Its goal is to ensure that each party involved in a transaction is who it claims to be. That is, to prevent fraud that may occur as a result of an impostor posing as a financial institution or authorized merchant and

(iii) Message Integrity

Ensuring message integrity is necessary to prevent errors that may occur due to message change while in transient. Such changes my occur due to fraud or error in the transmission system.

(iv) Non-Repudiation

Refers to the systems ability to support undeniable signatures. That is, once a certain party has given its consent to a transaction, the required proof makes it impossible for this party to deny its involvement in this transaction.

---

[6] The material in this appendix in based on the presentation and material of [11].

(v) Effective Audit

Effective audit mechanism must be in place to be used in case analysis and settling disputes that may occur.

(vi) Privacy

Privacy is a common requirement for most financial transactions whether they are electronic or not. The electronic systems must posses the capability of ensuring that all parties involved in transactions remain anonymous and the transaction contents remain confidential.

(vii) Common Safeguards And Security Mechanisms

To ensure that the security requirements outlined above are met, we must deploy appropriate safeguards and mechanisms. In the virtual world of computer systems and networks the solutions lie in the realm of cryptography.

(viii) Cryptography

Cryptography is the science of creating cryptosystems (also called cipher system). Cryptosystems are methods of transforming message in such a way that only certain people can undo the transformation and retrieve the original message. The transformations are typically done using what is commonly called a *key*. Keys are the basic tools for locking and unlocking messages.

(ix) Public-Key Cryptography

When considering cryptosystems that will be used to secure communications over an insecure network, such as the Internet, we often rely on the so-called public-key cryptosystems. Public-key cryptosystems use two keys to solve the key transport problem. One of the keys, called the public-key, is used to lock or encrypt the message, while the other key, called the private key, is used to unlock or decrypt the message. To establish secure communications using such a scheme, the two parties wishing to communicate must send their public-keys to each other. Once the keys are exchanged, the sender would use the recipient's public-key to lock the message to be sent, and the recipient would use the corresponding private-key to unlock the message and retrieve the original text.

Public-key cryptosystems can also be used to create cryptographic signatures. A cryptographic signature is a digital code that is generated using a private-key and the message to be signed. The methods used to generate the signature are designed in such a way to ensure that each signature is unique to the given key and message combination. A signature can be checked and verified using the corresponding public-key.

(x) Cryptographic Certificates

Public-key cryptography and signature systems cater for most of the security requirements outlined earlier. The remaining issue is that of public-key authenticity. This is because the simple use of public-key systems doesn't ensure the identity of the key holder. In an uncontrolled system, anyone could publish a new public-key and assume a new identity. This would be like allowing anyone to issue his or her own passport or driving licenses. This is clearly unacceptable for any application that, like electronic commerce, requires authentication and non-repudiation.

To resolve this problem (essentially a problem of trust) participants in electronic commerce are not allowed to use any public-private key pair. Instead, they must use keys that are certified by a commonly trusted third party. Such a trusted third party is commonly referred to as a *Certificate Authority* (CA).

(b) Certificate Authorities

The Certificate Authority[7] (CA) would be seen as a provider of necessary authentication and security infrastructure to enable more secure communications over the Internet, thus making it more suitable for electronic commerce. The CA creates and issues certificates, which hold the necessary information to fully identify a certain party. This is accomplished by including a person's identification information and public key in a package, which is signed by the CA.

The fact that the CA signs the package enables participants in electronic commerce to verify its validity. This is possible because all participants are assumed to know and trust the CA.

Authentication Protocols

Most modern authentication protocols are based on public-key cryptography and depend on the existence of a CA. A number of such protocols are being used on the Internet, both for general-purpose secure messaging and for electronic commerce.

Examples of general-purpose secure messaging protocols include:

– SSL, short for Secure Socket Layer, was originally developed by Netscape. SSL can be used to secure any application communications that uses TCP/IP. It is most commonly used to establish secure Web connections between Web browsers and servers. SSL, and its more recent descendant TLS, are now part of the Internet standard protocols.

[7] Now commonly deployed within a more elaborate Public Key Infrastructure (PKI) framework.

– S/MIME, Sort for Secure/Multipurpose Internet Mail Extensions. As the name suggests S/MIME comprises a set of specifications that allow users to securely exchange electronic mail over the Internet.

[End of document]