GRESHAM

COLLEGE

THE INTERNET AND ELECTRONIC COMMERCE

Lecture 2

THE INTERNET: SECURITY AND CONTRACT AT A DISTANCE

by

PROFESSOR GERALD WAKEFIELD BSc LLB DipLaws DipMet FRSA
Gresham Professor of Law

10 November 1998

Electronic Free Trade: Will This Be Possible?

It has been a dream since the early trade in goods through the various civilisations stretching from the Egyptians to the Babylonians to the Greeks to the Romans and to the Modern for a world where products flow easily and seamlessly over national borders without any tariffs or other barriers standing in their way. Entrenched special interests pose significant challenges to Government negotiators seeking free trade in existing sectors. For example the WTO negotiations in breaking down the barriers to trade in services is but one example.

However, it should be much easier to achieve free trade in cyberspace, a totally new phenomenon. The advantage in free trade between States can be seen in the growth of the United States economy once trade barriers between the States were eliminated, and to a lesser extent in Australia where again growth took place at a much faster pace once the trade barriers between the States had been phased out. Europe is now in this process.

Such a duty free world is what the Clinton administration Information Infrastructure Task Force proposed in 1996 in a wide ranging draft policy for global electronic commerce. The policy (which is available on the task force web site http://iitf.nist.gov), called for a minimum of regulation for electronic commerce. However, it is also recognised that some sort of legal framework for transactions in cyberspace is necessary if business is to thrive.

There have been mixed reactions to the Clinton initiative. Pro-internet interest groups were quick to applaud the policy of minimal regulation, but other observers, fearing privacy invasion and effects of homepages by child pornographers, suicide cults and political extremists, say that the policy does not call for enough regulation. The controversy comes because the stakes are high, particularly for business, in this effort to create a regulatory and legal framework for electronic commerce.

The focus of these lectures will be on the legal aspects and issues raised by the Internet and electronic commerce so let me now turn to what is becoming a new area of law which is being termed Cyberspace Law.

Cyberspace Law

In general, Cyberspace Law typically encompasses all the cases, statutes, and constitutional provisions that impact persons and institutions who:

- control the entry to cyberspace;

- provide access to cyberspace;
- create the hardware and software which enable people to access cyberspace; or
- use their own computers to go online and enter cyberspace.

Some of the key players in cyberspace disputes may thus include phone companies, regulatory agencies, personal computer companies, software companies, major online services, internet service providers, schools, colleges, universities and all persons and companies that have established a presence on the Net, and those who, in increasingly large numbers, are becoming Net Surfers or "Netizens".

Currently, Cyberspace Law is a wide-open area of law with much uncharted territory and many unresolved questions. Only a handful of cases are directly on point and these are mainly from the United States jurisdiction, and major statutory schemes, which are not yet on the books. Barristers, solicitors and policy makers currently look to analogise cases and statutes, with many people questioning the efficacy of applying arguable outmoded law to a new digital environment.

One important feature of Cyberspace Law is its international nature and scope. Cyberspace Law is an international medium, and the Internet is a completely global entity. The worldwide web, for example, enables persons to move seamlessly and effortlessly from a web site in Australia to a web site in Mexico. Net Surfers can literally bounce around from Germany to South Africa, to Chile to the Channel Islands with a click of a mouse. Electronic mail can be sent overseas as easily as it can be sent to the person next door. A further point, of significance to the lawyer, is the path the person takes as he or she travels through cyberspace, which is never predictable. Again for example, the persons Internet connection may take him or her through the UK, on route to San Francisco to New Orleans. Or any email message from London to New York may travel through computers in France and Indian in one direction while the response may bounce up through Denmark down to Egypt across to the Argentine and then back to Docklands.

There is typically no way to predict which international borders will be crossed. Indeed, in cyberspace international borders have been significantly blurred.

As disputes arise and areas of law evolve, eleven distinct components of Cyberspace Law may be distinguished:

- jurisdiction and related issues
- freedom of expression

- intellectual property
- privacy protection
- safety concerns
- equal access
- electronic commerce
- data protection
- choice of law
- security
- contract-at-a-distance.

On the jurisdictional issue, academics and practitioners are now beginning to analyse which laws might be applicable in cyberspace at any particular moment in time. For example, whether a particular communication in cyberspace is controlled by the laws of the country where the transmissionary originated, the laws where the Internet service provider is located, the laws where the item is accessed, or some other law.

A further problem that has emerged as a major area of controversy in Cyberspace Law is freedom of expression. The range of free speech issues that have arisen include anonymity, accountability, defamation, discriminatory harassment, obscenity, pornography, liability of online services and internet providers, and the legal responsibilities of educational institutions.

A further set of problems is raised by intellectual property. Although patent, trademark and trade secret law is occasionally relevant, it is the area of copyright law that receives the most attention.

Privacy in Cyberspace, or lack thereof, is another area that has received a great deal of attention, particularly in the United States. To protect valuable information, persons and companies are commencing to rely on encryption and I intend to deal with this issue in some detail at this lecture. The other issues raised above will be dealt with as the lecture series proceeds.

However before discussing security and encryption, I would like to emphasis the problems that now exist when particular governments take unilateral action, which they foresee, as necessary to protect their own citizens.

On April the 16th 1997, German prosecutors indicted the general manager of CompuServe in Deutschland. CompuServe, is a commercial online service that is available to subscribers around the world through local telephone access numbers. It is a full Internet service provider (ISP). The controversy in Germany had been brewing for sometime. In December 1995 the police in Munich, the capital of the conservative state of Bravura, raided the CompuServe offices and in response, the online service temporarily barred access to 200 Internet Usenet sites for some 4 million subscribers worldwide. A huge outcry ensued, with many customers and free speech activists protesting the decision in and online discussion forums. Particularly troublesome to many of those online protestors was the fact that some of the prohibited sites focused on issues like breast cancer and AIDS. According to the Munich prosecutor's office, Mr Somm, the general manager of CompuServe, had been accused of trafficking in pornography and neo-Nazi propaganda. The office said he "knowingly allowed images of child pornography, violent sex and sex with animals from news groups "... to be made accessible to customers of CompuServe Germany. CompuServe also said that subscribers were also given access to computer games that contained forbidden images of Hitler and Nazi symbols such as swastikas.

So here we have a situation where authorities in one state of one country can effectively bar access to the Internet on a worldwide basis. CompuServe argued in response that it bears "no responsibility for the contents of thousands of Internet sites via CompuServe, and cannot monitor and sensor cyberspace". Implicit in these comments is the contention already mentioned that German law should not be allowed to restrict international Internet access.

I would now like to make some brief remarks about the jurisdiction issue which is a threshold issue in Cyberspace Law.

Security and the Use of Encryption Algorithms

The Internet is the fastest growing communication channel this century. Inexpensive and efficient, it may in the foreseeable future replace our traditional methods of communication. However, the potential of this communication network operating as a widespread channel for payments and transmissions of secure information will not be achieved until users are confident of its security.

The desire for security voiced by bankers and users are met with equally strong claims from governments and regulators over the need to protect the general population from criminal and other illegal activities. These concerns were recently highlighted by the flow of publicity relating to the transmission of child pornography over the Internet. As governments and regulators come to accept that some degree of freedom to provide secure communication and payment systems is necessary, it is important that in implementing measures for the security of their electronic payments and communications systems bankers and other users are aware of the strict legal and regulatory regimes with which they will be required to comply.

A secure payment system requires the implementation of cryptography theory, including decisions with regard to the type of algorithms used, key management and key storage. Several governments have established strict rules with respect to the commercial use and, in some cases, export of encryption algorithms, whether hardware or software based. The main goal of these rules is to prevent the availability of powerful bulk-encryption processing capabilities, as these could be used for criminal purposes. Some governments are now considering and implementing new policies with regard to the export of algorithms, but others governments stand opposed, classifying robust encryption technology as a defence article which may not be imported or exported without a licence.

The effect of these restrictions in the United States is that US companies are both hampered in providing US citizens with the benefits of encryption and handicapped in completing against industries abroad that have grown up under the protection of US restraints on its own companies. Attempts to reverse this situation have not been welcomed by the Clinton administration and there are efforts to move congress to change the status quo.

However the most promising progress appears to be in the courts. In the Bernstein case, C-950582MHP (ND CAL. April 15 1996) a federal court in San Francisco allowed a suit filed on behalf of a Ph.D candidate in mathematics who was blocked by the State Department from publishing an academic paper describing an encryption system he developed and its source code. In doing so, the court ruled that the source code is protected by the First Amendment (the State Department conceding it erred in restricting publication of the academic paper). The facts of the case are that Bernstein, whilst a graduate student, developed a zero delay public key encryption system. He expressed his mathematical ideas in an academic paper: "the Snuffle Encryption System" and his source code, Snuffle.C and Un-Snuffle.C. In June 1992, Bernstein asked the State Department to determine whether the three items were covered by the International Traffic in Arms Regulation (the ITAR). The ITAR implements the Arms Export Control Act which authorises the President to control the import and export of defence articles and services. Restricted items are placed on the US munitions list. They cannot be exported or imported without a licence. When doubt exists about whether an article or service belongs on the munitions list, an ITAR commodity jurisdiction procedure allows the State Department Office of Defence Trade Controls to determine coverage. The arms export control plainly states the designations of defence articles and services are not subject to judicial review.

Encryption systems, with some domestic exceptions, equipment and software are covered by the munitions list. The office of Defence Trade Controls notified Bernstein all items in his request were restricted defence articles.

Bernstein sued the State Department for relief from enforcement of the Arms Export Control Act and ITAR, on the grounds that they were unconstitutional constraints on speech, vague and overboard, and infringed rights of association and equal protection, among other things. The Government replied with a request that the court dismisses the case on grounds that the claims are non-justifiable. After much argument the court concluded by emphasising that the only substantive holding is that source code is speech for the purpose of the first amendment and that Bernstein's case is justifiable.

As a result of this case, the US Government took encryption from the munitions list and placed it on the commercial list but then passed legislation to limit the length of any algorithm that could be exported from the United States.

Crypto Systems

Cryptography deals with the transformation of ordinary text (plain text) into coded form (ciphertext) by encryption and transformation of ciphertext into plain text by decryption. Normally these transformations are parameterised by one or more keys. The motive for encrypting text is security for transmission through insecure channels.

Three of the most important services provided by crypto systems are secrecy, authenticity and integrity. Secrecy refers to denial of access to information by unauthorised individuals. Authenticity refers to validating the source of a message, i.e. that it was transmitted by a properly identified sender and is not a replay of a previously transmitted message. Integrity refers to assurance that a message was not modified accidentally or deliberately in transit, by replacement, insertion or deletion. A fourth service, which may be provided, is non-repudiation or origin, i.e., protection against a sender of a message later denying transmission.

Classical cryptography deals mainly with the secrecy aspect. It also treats keys as secret. However, since the greater use of the Internet and its potential for high-volume message carrying, two new trends have become apparent:

(i) authenticity as a consideration which rivals and sometimes exceeds secrecy in importance; and

(ii) the notion that some key material need not be secret.

The first trend has arisen in connection with applications such as electronic mail systems and electronic funds transfer. In such settings the electronic equivalent of a hand-written signature may be desirable. Also, intruders into a system often gain entry by masquerading as legitimate users; cryptography presents an alternative to password systems for access control.

The second trend addresses the difficulties, which have traditionally accompanied the management of secret keys. This may entail the use of couriers who are rather costly, inefficient and not really secure. In contrast, if keys are public the task of key management may be substantially simplified.

An ideal system might solve all three problems concurrently, i.e., using public keys; providing secrecy; and providing authenticity. Unfortunately, no single technique proposed to date has met all three criteria. Conventional systems, such as DES (Data Encryption Standard), require management of secret keys; systems using public key components may provide authenticity but are inefficient for bulk encryption of data due to low bandwidths.

Fortunately, conventional and public key systems are not mutually exclusive; in fact they can complement each other. Public key systems can be used for signatures and also the distribution for keys using systems such as DES. Thus it is possible to construct hybrids of conventional and public key systems which can meet all the above goals: secrecy, authenticity and ease of key management.

Example of a Conventional Cipher: DES

The most notable example of a conventional crypto system is DES (Data Encryption Standard). It is a block cipher, operating on 64-bit blocks using a 56-bit key. Essentially the same algorithm is used to encipher or decipher. The important characteristics of DES are its one-key feature and the nature of the operations performed during encryption/decryption.

Both permutations and table look-ups are easily implemented, especially in hardware. Thus encryption rates exceeding 40 Mbit/sec. have been obtained. This makes DES an efficient encryptor especially when implemented in hardware.

Digital Signatures and Hash Functions

Digital signatures are the electronic analogue of hand-written signatures. A common feature is that they must provide the following:

(i) a receiver must be able to validate the sender's signature

(ii) a signature must not be forgeable; and

(iii) the sender of a signed message must not be able to repudiate it.

The main difference between hand-written and digital signatures is that a digital signature cannot be constant; it must be a function of the document, which it signs. If this were not the case then the signature, due to its electronic nature, could be attached to any document. Furthermore, the signature must be a function of the entire document; changing even a single bit should produce a different signature.

Thus a signed message cannot be altered.

There are two major variants of implementation:

(i) true signatures; and

(ii) arbitrators' signatures.

In a true signature system, signed messages are forwarded directly from signer to recipient. In an arbitrated system, a witness (human or automated) validates a signature and transmits the message on behalf of the sender. The use of an arbitrator may be helpful in the event of key compromise.

Hash functions are useful ancillaries in this context, i.e., validating the identity of a sender. They can also serve as cryptographic check sums (i.e., error detected codes) thereby validating the contents of a message. Use of signatures and hash functions can thus provide authentication and verifications of message integrity at the same time.

Numerous digital signature schemes have been proposed. A major disadvantage of signature schemes in conventional systems is that they are generally one-time schemes. A signature is generated randomly for a specific message, typically using a large amount of key material, and is not reusable. Furthermore, later resolutions of disputes over signed documents require written agreements and substantial bookkeeping on behalf of the sender and receiver, making it more difficult for a third party adjudicator.

International Organisations-Overview

The Co-ordinating Committee for Multilateral Export Controls

The Co-ordinating Committee for Multilateral Export Controls ("COCOM") was an international organisation for the mutual control of the export of strategic products and technical data from country members to prescribed destinations. In 1991, COCOM decided to allow export of mass-market cryptographic software. Most countries followed the regulations with the exception of the United States. The main purpose of the COCOM regulations was to prevent cryptography from being exported to "dangerous" countries such as Libya, Iraq, Iran and North Korea. Exporting to other countries was normally allowed although states often required a licence to be granted. COCOM was dissolved in March 1994.

The seventeen member states of COCOM were Australia, Belgium, Canada, Denmark, France, Germany, Greece, Italy, Japan, Luxembourg, The Netherlands, Norway, Portugal, Spain, Turkey, United Kingdom and the United States. Co-operating members included Austria, Finland, Hungary, Ireland, New Zealand, Poland, Singapore, Slovakia, South Korea, Sweden, Switzerland and Taiwan.

Wassenaar Arrangement

In 1995 the Wassenaar Arrangement on Export Controls for conventional arms and dual-use goods and technologies was established as a follow-up to COCOM. Negotiations on the treaty were completed in July 1996 and signed by 31 countries. (*Argentina, Australia, Austria, Belgium, Canada, The Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, The Netherlands, New Zealand, Norway, Poland, Portugal, The Republic of Korea, Romania, the Russian Federation, Slovakia Republic, Spain, Sweden, Switzerland, Turkey, United Kingdom and the United States. Later Bulgaria and Ukraine also signed the treaty.)*

The Wassenaar Agreement controls the export of weapons and of dual-use goods, that is, goods that can be used both for military and for civil purposes. Cryptography is a dual-use good. The provisions are largely the same as the COCOM regulations.

Membership is open on a global and non-discriminatory basis to all countries meeting the established criteria, under which a country is to:

- be a producer/exporter of arms or associated duel-use goods and technology;
- have appropriate national policies, such as not selling arms or sensitive dual-use items to countries whose behaviour is a cause for concern;
- adhere to international non-proliferation norms and guidelines; and
- implement fully effective export controls. (see http://jwa.com/wawsenr3.htm)

Organisation for Economic Co-operation and Development (OECD)
Policy Developments

On 27th March 1997 the OECD released its recommendation of the counsel concerning guidelines for cryptography policy. These are non-binding guidelines to member governments but provide principles which states should take into account when developing national cryptography policy. The principles are:

1. trust in cryptographic methods;
2. choice of cryptographic methods;
3. market driven development of cryptographic methods;
4. standards for cryptographic methods;
5. protection of privacy and personal data;
6. lawful access;
7. liability;
8. international co-operation.

The OECD Recommendation also pinpoints the five key elements required to achieve the secure use of information technology. These are as follows:

1. confidentiality (ensuring that data is not disclosed to unauthorised individuals, entities or processes);
2. integrity (ensuring that the data has not been modified or altered in an unauthorised manner);
3. availability (ensuring that the data and communications systems are as accessible as required);

4. authentication (establishing the validity of a claimed identity of a user or entity);
5. non-repudiation (preventing an individual or entity from denying having performed a particular action related to data).

These guidelines are sufficiently vague to allow a broad range of interpretation and states are able to choose a privacy-oriented or a law-enforcement-driven policy line as they see fit.

The full text of these guidelines is reproduced in Annexure 1.

International Chamber of Commerce (ICC)
Policy Developments

At a meeting held on 19th/20th December 1995 "the meeting agreed that encryption controls should be kept to a minimum consistent with the requirements of law enforcement and national policy."

It was agreed that independent trusted third parties could hold deposited keys, to which governments are allowed access under proper judicial warrant, provided sufficient safeguards are in place.

Regional Organisations – Overview
Council of Europe

The Council of Europe in its recommendation of September 1995 (*Recommendation R(95)13 concerning problems with criminal procedure law connected with information technology, 11th September 1995*), stated that "measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offences, without affecting its legitimate use more than is strictly necessary".

European Union
Import/Export Restrictions

The export of dual-use goods (*Cryptography is a subset of dual-use goods*) including cryptography is regulated by Council Regulation (EC) No. 3381/94 and European Council Decision No. 94/1942/PESC 96/613/FUSP of July 1995. In general, a licence is needed for the export of cryptographic hardware and software outside of the EU. Exceptions are granted for most market and public domain software.

Legislation and Regulations

The European Council Resolution of 17th January 1995 on the lawful interception of telecommunications (96/C329/01) contains a requirement for network operators and service providers, if they use encryption, to provide intercepted communications to law enforcement agencies.

Policy Developments

The European Commission is preparing a draft proposal on the establishment of a Europe-wide network of trusted third party services. The network would be established for providing certification services by private TTPs. Although primarily meant for establishing infrastructure for the use of public key encryption, the proposal will also try to address the legal interception problem: law enforcement authorities could, with a court order or warrant, apply to the TTPs for assessing suspect keys. The TTPs would probably need accreditation to operate. The proposal would not entail harmonisation of national rules. The European Union has adopted a green paper on legal protection of encrypted services on a single market. This is a discussion proposal on protecting services, which are encrypted to ensure payment of a fee. The green paper considers proposing a harmonisation of national laws to prohibit the manufacture, sale, importation, possession, and promotion of illicit decoders, as well as unauthorised decoding.

Annex 1
OECD Guidelines for Cryptography Policy

I. Aims

The Guidelines are intended:

- to promote the use of cryptography;
- to foster confidence in information and communications infrastructures, networks and systems and the manner in which they are used;
- to help ensure the security of data, and to protect privacy, in national and global information and communications infrastructures, networks and systems;
- to promote the use of cryptography without unduly jeopardising public safety, law enforcement and national security;
- to raise awareness of the need for compatible cryptography policies and laws, as well as the need for interoperable, portable and mobile cryptographic methods in national and global information and communications networks;
- to assist decision-makers in the public and private sectors in developing and implementing coherent national and international policies, methods, measures, practices and procedures for the effective use of cryptography;
- to promote co-operation between the public and private sectors in the development and implementation of national and international cryptography policies, methods, measures, practices and procedures;
- to facilitate international trade by promoting cost-effective, interoperable, portable and mobile cryptographic systems;
- to promote international co-operation among governments, business and research communities, and standards-making bodies in achieving co-ordinated use of cryptographic methods.

II. Scope

The Guidelines are primarily aimed at governments, in terms of the policy recommendations herein, but with anticipation that they will be widely read and followed by both the private and public sectors.

It is recognised that governments have separable and distinct responsibilities for the protection of information which requires security in the national interest; the Guidelines are not intended for application in these matters.

III. Definitions

For the purposes of the Guidelines:

- "Authentication" means a function for establishing the validity of a claimed identity of a user, device or another entity in an information or communications system.
- "Availability" means the property that data, information and information and communications systems are accessible and usable on a timely basis in the required manner.
- "Confidentiality" means the property that data or information is not made available or disclosed to unauthorised individuals, entities or processes.
- "Cryptography" means the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation and/or prevent its unauthorised use.
- "Cryptographic key" means a parameter used with a cryptographic algorithm to transform, validate, authenticate, encrypt or decrypt data.
- "Cryptographic methods" means cryptographic techniques, services, systems, products and key management systems.

- "Data" means the representation of information in a manner suitable for communication, interpretation, storage or processing.
- "Decryption" means the inverse function of encryption.
- "Encryption" means the transformation of data by the use of cryptography to produce unintelligible data (encrypted data) to ensure its confidentiality.
- "Integrity" means the property that data or information has not been modified or altered in an unauthorised manner.
- "Interoperability" of cryptographic methods means the technical ability of multiple cryptographic methods to function together.
- "Key management system" means a system for generation, storage, distribution, revocation, deletion, archiving, certification or application of cryptographic keys.
- "Keyholder" means an individual or entity in possession or control of cryptographic keys. A keyholder is not necessarily a user of the key.
- "Law enforcement" or "enforcement of laws" refers to the enforcement of all laws, without regard to subject matter.
- "Lawful access" means access by third party individuals or entities, including governments, to plaintext, or cryptographic keys, of encrypted data, in accordance with law.
- "Mobility" of cryptographic methods only means the technical ability to function in multiple countries or information and communications infrastructures.

- "Non-repudiation" means a property achieved through cryptographic methods, which prevents an individual or entity from denying having performed a particular action related to data (such as mechanisms for non-rejection of authority (origin); for proof of obligation, intent, or commitment; or for proof of ownership).
- "Personal data" means any information relating to an identified or identifiable individual.
- "Plaintext" means intelligible data.
- "Portability" of cryptographic methods means the technical ability to be adapted and function in multiple systems.

Annex 2

The Quadripartite "Principles of Global Cryptographic Policy"

1. Businesses and individuals must have the right to obtain confidentiality in all information they send, receive or retain.

2. Businesses and individuals must be able to prove the source and integrity of information and to establish the ownership and timeliness of information.

3. In order to comply with data protection laws, businesses must be able to protect personal information while in storage or in transit in whatever form it is stored or transmitted.

4. Businesses must be able to protect their assets and therefore must be able to protect sensitive information while in storage or in transit in whatever form it is stored or transmitted.

5. Businesses and individuals have the right, responsibility and need to determine the level of protection needed for specific information, and to select adequately strong encryption methods.

6. The rights and safeguards concerning the confidentiality and integrity of information should not be applied more restrictively to information created and/or communicated electronically and currently apply to paper-based information.

7. Actions permitted under the existing legal framework should be exhausted before creating new laws to address issues related to electronic information.

8. Governments need to be able to protect themselves, businesses and citizens against the action of criminals.

9. Instantly recognises that governments need to be able to access information, for law enforcement and national security purposes. These activities must be carried out consistent with applicable national and international laws and due process requirements.

10. For the use of confidentiality, in order to establish a proper balance between the duties of national authorities and the needs of the industry and individual users, it is mandatory that governments define first a common statement of the problems that need to be solved before attempting to find any solution allowing legal interceptions. Requirements corresponding to this statement have to be developed by industry and governments working together.

11. Industry must lead the development of the requirements for cryptographic standards, involving governments (including regulators and auditors as necessary) and individuals as important participants in that process.

12. The IT industry will learn the development of voluntary, consensus, international standards consistent with the requirements and which provide for adequately strong confidentiality and integrity of information in the global information infrastructure.

13. Any standards developed must include solutions suitable for use by mass market products as well as for internal business and private use. They must also allow businesses and individuals to conform to national and international laws and regulations on personal privacy and data protection.

14. The mechanism implementing such standards must be published unclassified, so that the effectiveness can be open to public scrutiny.

15. Any patented mechanisms must be available under fair and reasonable conditions on a non-discriminatory basis.

16. The standards must include a procedure for verifying that their products conform. Suppliers may provide a statement or self declaration of conformity to the standards.

17. Businesses developing or using products conforming to such standards must have the right to make technical and economic choices about modes of implementation and operation, including the choice between implementation and hardware, software or firmware where relevant.

18. Cryptographic products that conform to the agreed standards should not be subject to import controls, restriction on use within the law, or restrictive licensing; furthermore, these products should be exportable to all countries except those which are subject to UN embargo.

19. All parties involved, including users, providers and governments, must agree on the liability for encryption use.

20. Governments should agree that certain enterprises are so trustworthy that their access to cryptographic products and technology should be expanding.

21. Governments are encouraged to inspire confidence in cryptography standards by using standardised mechanisms for all purposes other than the most sensitive diplomatic and defence purposes.

Annex 3

Decree of the President of the Russian Federation No. 334 dated 3rd April 1995

The following is the text of the decree:

1. The conferring of the status of a presidential programme with the specific purpose of creating and developing a programme of telecommunications and information systems in the interests of the organs of state authority. The Administration of the President of the Russian Federation in co-operation with FAPSI (The Federal Agency of Government Communications and Information) will ensure its review and implementation.

2. Prohibiting within the telecommunications and information systems of government organisations and enterprises the use of encoding devices, including encryption methods for ensuring the authenticity of information (electronic signature) and secure means for storing, treating and transmitting information which are not certified by FAPSI, and also the imposition of state law on enterprises and in organisations using the aforementioned technical land encoding devices without certification by FAPSI.

3. Proposing that the Central Bank of the Russian Federation and FAPSI take extraordinary measures with regard to commercial banks of the Russian Federation which avoid the obligatory FAPSI certification in technical methods for securing the storage, treatment and transmission of information under the information subdivision of the Central Bank.

4. In the interests of the information security of the Russian Federation and intensification of the fight against organised crime, prohibiting legal and physical persons from designing, manufacturing, selling and using information media, and also secure means of storing, treating and transmitting information and rendering services in the area of information encoding, without licence from FAPSI in accordance with the Russian Federation law "Concerning the Federal Organs of Government Communications and Information".

5. That the state customs commission of the Russian Federation take measures to bar entry into Russian Federation territory encoding devices of foreign manufacture without licensing by the MVES (Ministry of Foreign Economic Relations) issued in co-operation with FAPSI.

6. That the FSK (Federal Security Service) of the Russian Federation and the MVD (Ministry of Internal Affairs) of the Russian Federation, in co-operation with FAPSI, and the State Tax Service of the Russian Federation and the Department of the Tax Inspector, reveal any legal and physical persons who do not comply with the present Decree.

7. Recommending that the General Prosecutor of the Russian Federation increase procuratory oversight of observance of the Law of the Russian Federation "Concerning the Federal Organs of Government Communications and Information" in the areas of design, production, sale and use of encoding devices, and also services in the area of information encoding in the Russian Federation, subject to licensing by FAPSI.

8. Creating a Federal centre for the safeguarding of economic information under FAPSI (within the bounds of the Agency) entrusting to it the design and implementation of programmes for safeguarding the security of economic information of the Russian credit and financial and other significant economic structures in the country.

9. The present decree takes effect from the day of its publication.

Annex 4

Glossary of Terms and Acronyms[64]

The following terms are described for information only and are not intended to be interpreted as legal definitions:

Anonymous Credential: A credential which asserts a right or privilege or fact without revealing the identity of the holder.

Asymmetric Cipher: Same as public key cryptosystem.

Authentication: The process of verifying an identity or credential.

Biometric Security: A type of authentication using physical/biological signature of an individual.

BlackNet: An experimental scheme devised by T. May to underscore the nature of anonymous information markets. "Any and all" secrets can be offered for sale via anonymous mailers and message pools.

Blinding, Blinded Signatures: A blind signature is a co-operative protocol whereby the receiver of the signature provides the signer with the blinding information.

Blob: The crypto equivalent of a locked box. A cryptographic primitive for bit commitment,- with the properties that a blob can represent a 0 or a 1, that others cannot tell by looking whether it is a 0 or a 1, that the creator of the blob can "open" the blob to reveal the contents, and that no blob can be both a 1 and a 0. An example of this is a flipped coin covered by a hand.

[64] These definitions are compiled from several sources. For further definitions of terms used in electronic commerce/banking and the Internet see: (1) http://tech.ukerna.ac.uk.; (2) http://mailgate.ukshops.co.uk; (3) http://www.oberlin.edu/~brchkind/cypermomicon/chepter19/19.4.htm.

Central Repository: Government department or agency set up by Government to act as a point of contact for interfacing between a TTP and the appropriate law enforcement agency.

Cipher: A secret form of writing, using substitution or transposition of characters or symbols. (From Arabic "sifr," meaning "nothing".)

Ciphertext: The plaintext after it has been encrypted.

Clipper: A chip developed by the United States Government that was to be used as the standard chip in all encrypted communications. Details of how the Clipper chip works remain classified. However it has an acknowledged trapdoor to allow the government to eavesdrop on anyone using Clipper provided they first obtain a wiretap warrant. [Clipper uses an 80 bit key to perform a series of nonlinear transformation on a 64 bit data block.]

Coin Flipping: An important crypto primitive, or protocol, in which the equivalent of flipping a fair coin is possible. Implemented with blobs.

Computationally Secure: Where a cipher cannot be broken with available computer resources, but in theory can be broken with enough computer resources. Contrast with unconditionally secure.

Confidentiality: The prevention of the unauthorised disclosure of information.

Credential: Facts or assertions about some entity. For example, credit ratings, passports, reputations, tax status, insurance records, etc.

Credential Clearinghouse: Banks, credit agencies, insurance companies, police departments, etc., that correlate records and decide the status of records.

Cryptanalysis: Methods for attaching and breaking ciphers and related cryptographic systems.

Crypto Anarchy: The economic and political system after the deployment of encryption, untraceable e-mail, digital pseudonyms, cryptographic voting, and digital cash.

Cryptographic Key: A parameter used with a cryptographic algorithm to transform, validate, authenticate, encrypt or decrypt data.

Cryptography: The science and study of writing, sending, receiving and deciphering secret messages. Includes authentication, digital signatures, the hiding of messages (steganography).

Cyberspace: The electronic domain, the Nets, and computer-generated spaces.

Data Encryption Key (DEK): Used for the encryption of message text and for the computation of message integrity checks (signatures).

Datagram: A self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network.

Data Encryption Standard (DES): A data encryption standard developed by IBM under the auspices of the United States Government. DES uses a 56 bit key to perform a series of nonlinear transformation on a 64 bit data block. With the increasing speed of hardware and its falling cost, it would be feasible to build a machine that could crack a 56 bit key in under a day.

Differential Cryptanalysis: The Shamir-Biham technique for cryptanalysing DES Keys that must be tried from about 2^56 to about 2^47 or less.

Digital Cash, Digital Money: Protocols for transferring value, monetary or otherwise, electronically. Digital cash usually refers to systems that are anonymous. Digital money systems can be used to implement any quantity that is conserved, such as points, mass, dollars, etc. There are many variations of digital money systems. A topic too large for a single glossary entry.

Digital Pseudonym: Basically, a "crypto identity". A way for individuals to set up accounts with various organisations without revealing more information than they wish.

Digital Signature: Data appended to a message that allows a recipient of the message to prove the source and integrity of the message. Analogous to a written signature on a document. A modification to a message that only the signer can make but that everyone can recognise. Can be used legally to contract at a distance.

Digital Signature Standard (DSS): The latest NIST (National Institute of Standards and Technology, successor to NBS) standard for digital signatures.

Digital Timestamping: One function of a digital notary public, in which some message (a song, screenplay, lab notebook, contract, etc.) is stamped with a time that cannot (easily) be forged.

Dual Legality: A legal request from a foreign agency which must satisfy legal access conditions in both the requesting country and the country being asked.

Electronic Frontier Foundation (EFF): The Electronic Frontier Foundation (EFF), founded in July, 1990, to assure freedom of expression in digital media, with a particular emphasis on applying the principles embodied in the US Constitution and the Bill of Rights to computer-based communication.

Encryption Algorithm: A mathematical function used to change plaintext into ciphertext (encryption) or vice versa (decryption).

Escrowed Encryption Standard (EES): Current name for the key escrow system known variously as Clipper, Capstone, Skipjack, etc.

International Data Encryption Algorithm (IDEA): Developed in Switzerland and licensed for non-commercial use in PGP. IDEA uses a 128 bit user supplied key to perform a series of nonlinear mathematical transformations on a 64 bit data block.

Information Theoretic Security: "Unbreakable" security, in which no amount of cryptanalysis can break a cipher or system. One time pads are an example (providing the pads are not lost nor stolen nor used more than once, of course). Same as unconditionally secure.

Integrity: Prevention of the unauthorised modification of information.

Key: A piece of information needed to encipher or decipher a message. Keys may be stolen, bought, lost, etc., just as with physical keys.

Key Exchange or Key Distribution: The process of sharing a key with some other party, in the case of symmetric ciphers, or of distributing a public key in an asymmetric cipher.

Key escrow/recovery: A capability that allows authorised persons, under certain prescribed conditions, to decrypt ciphertext with the help of information supplied by one or more trusted parties.

Key management: The process of generating, storing, distributing, changing, and destroying cryptographic keys.

Key revocation: Notification that a public cryptographic key is no longer valid.

Key Escrow: Key escrow means that a copy of the secret key needed to decrypt something is stored with a third party.

Known Plain Text Attack: A method of attack on a crypto system where the cryptanalysis has matching copies of plaintext, and its encrypted version. With weaker encryption systems, this can improve the chances of cracking the code and getting at the plaintext of other messages where the plaintext is not known.

Message Digest Algorithm#5 (MD5): The message digest algorithm used in PGP is the MD5 Message Digest Algorithm, placed in the public domain by RSA Data Security, Inc. The level of security provided by MD5 should be sufficient for implementing very high security hybrid digital signature schemes based on MD5 and the RSA public-key cryptosystem.

MIPS: Million Instructions Per Second.

National Security Agency (NSA): The official communications security body of the US government. It was given its charter by President Truman in the early 50s, and has continued research in cryptology till the present. The NSA is known to be the largest employer of mathematicians in the world, and is also the largest purchaser of computer hardware in the world. Governments in general have always been prime employers of cryptologists. The NSA probably possesses cryptographic expertise many years ahead of the public state of the art, and can undoubtedly break many of the systems used in practice; but for reasons of national security almost all information about the NSA is classified.

Negative Credential: A credential that you possess that you do not want anyone else to know, for example, a bankruptcy filing. A formal version of a negative reputation.

One Time Pad: The one time pad is the only encryption scheme that can be proven to be absolutely unbreakable! This algorithm requires the generation of many sets of matching encryption keys pads. Each pad consists of a number of random key characters. These key characters are chosen completely at random using some truly random process. They are not generated by any kind of cryptographic key generator. Each party involved receives matching sets of pads. Each key character in the pad is used to encrypt one and only one plaintext character, then the key character is never used again. Any violation of these conditions negates the perfect security available in the one time pad.

One Way Function: A function which is easy to compute in one direction but hard to find any inverse for, e.g. modular exponentiation, where the inverse problem is known as the discrete logarithm problem.

Privacy Enhanced Mail (PEM): There is a de jure Internet standard called PEM (Privacy Enhanced Mail). To join the PEM mailing list, contact pem-dev-request@tis.com.

PGP: Phillip Zimmerman's implementation of RSA, recently to version 2.0, with more robust components and several new features. RSA Data Security has threatened PZ so he no longer works on it. Version 2.0 was written by a consortium of non-U.S. hackers.

Private key: The private (secret) part of a cryptographic key pair, knowledge of which should be strictly limited.

Proof of Identity: Proving who you are, either your true name, or your digital identity. Generally, possession of the right key is sufficient proof.

Public Key: The key distributed publicly to potential message-senders. It may be published in a phonebook-like directory or otherwise sent. A major concern is the validity of this public key to guard against spoofing or impersonation.

Public Key Cryptosystem: The modern breakthrough in cryptology, designed by Diffie and Hellman, with contributions from several others. Uses trapdoor one-way functions so that encryption may be performed by anyone with access to the "public key" but decryption may be performed only by the holder of the private key. Encompasses public key encryption, digital signatures, digital cash, and many other protocols and applications.

Public Key Encryption: The use of modern cryptologic methods to provide message security and authentication. The RSA algorithm is the most widely used form of public key encryption, although other systems exist. A public key may be freely published, e.g. in phonebook-like directories, while the corresponding private key is closely guarded.

Quantum Cryptography: A system based on quantum-mechanical principles. Eavesdroppers alter the quantum state of the system and so are detected. Developed by Brassard and Bennet, only small laboratory demonstrations have been made.

Rivest-Shamir-Adleman (RSA): The public key encryption method used in PGP. RSA are the initials of the developers of the algorithm which was done at taxpayer expense. The basic security in RSA comes from the fact that, while it is relatively easy to multiply two huge prime numbers together to obtain their product, it is computationally difficult to go the reverse direction: to find the two prime factors of a given composite number. It is this one-way nature of RSA that allows an encryption key to be generated and disclosed to the world, and yet does not allow a message to be decrypted.

First invented in 1978, it remains the core of modern public key systems. It is usually much slower than DES, but special purpose modular exponentiation chips will likely speed it up. A popular scheme for speed is to use RSA to transmit session keys and then a high-speed cipher like DES for the actual message text.

RSAREF: The free library RSA Data Security, Inc., made available for the purpose of implementing freeware PEM applications.

Secret Key Cryptosystem

A system which uses the same key to encrypt and decrypt traffic at each end of a communication link. Also called a symmetric or one-key system. Contrast with public key cryptosystem.

Smart Cards:

A computer chip embedded in a credit card. This can hold small cash, credentials, cryptographic keys, etc. Usually these are built with some degree of tamper-resistance. Smart cards may perform part of a crypto transaction, or all of it.

Steganography:

A part of cryptology dealing with hiding messages and obscuring who is sending and receiving messages. Message traffic is often padded to reduce the signals that would otherwise come from a sudden beginning of messages. "Covered Writing".

TEMPEST:

A standard for electromagnetic shielding for computer equipment. It was created in response to the fact that information can be read from computer radiation (e.g., from a CRT) at quite a distance and with little effort.

The typical home computer would fail all of the TEMPEST standards.

Trapdoor: In cryptography, a piece of secret information that allows the holder of a private key to invert a normally hard to invert function.

Trapdoor One Way Functions: Functions which are easy to compute in both the forward and reverse directions but for which the disclosure of an algorithm to compute the function in the forward direction does not provide information on how to compute the function in the reverse direction. The RSA algorithm is the best-known example of such a function.

GRESHAM COLLEGE

Policy & Objectives

An independently funded educational institution, Gresham College exists

- to continue the free public lectures which have been given for 400 years, and to reinterpret the 'new learning' of Sir Thomas Gresham's day in contemporary terms;

- to engage in study, teaching and research, particularly in those disciplines represented by the Gresham Professors;

- to foster academic consideration of contemporary problems;

- to challenge those who live or work in the City of London to engage in intellectual debate on those subjects in which the City has a proper concern; and to provide a window on the City for learned societies, both national and international.

Gresham College, Barnard's Inn Hall, Holborn, London EC1N 2HH
Tel: 0171 831 0575 Fax: 0171 831 5208
e-mail: enquiries@gresham.ac.uk