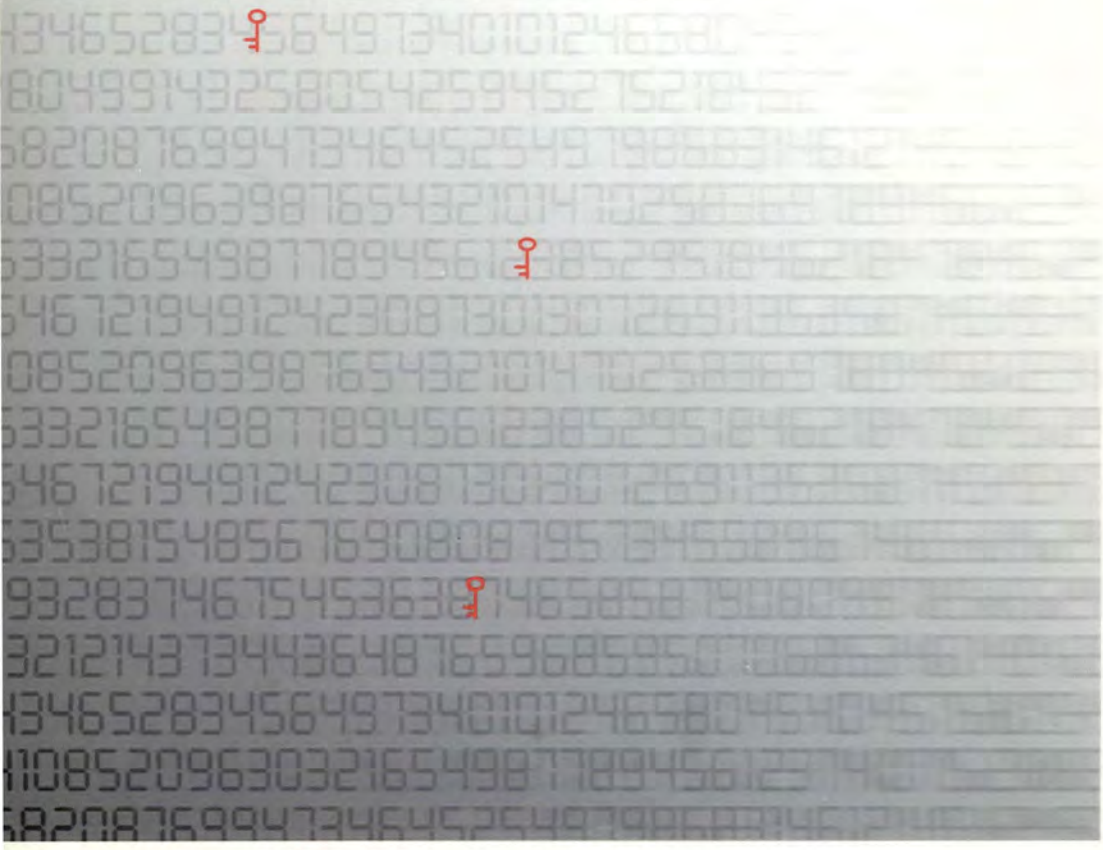
Government of Canada
Gouvernement du Canada

IC

A Cryptography Policy Framework for Electronic Commerce

Building Canada's Information Economy and Society



Canada

A Cryptography Policy Framework for Electronic Commerce

Building Canada's Information Economy and Society

Task Force on Electronic Commerce
Industry Canada
February 1998

A Cryptography Policy Framework for Electronic Commerce — Building Canada's Information Economy and Society is available, in both languages, electronically on the Industry Canada *Strategis* web site at: *http://strategis.ic.gc.ca/crypto*

This document can be made available in alternative formats for persons with disabilities upon request.

Additional print copies of this discussion paper are available from:

Distribution Services
Industry Canada
Room 205D, West Tower
235 Queen Street
Ottawa ON K1A 0H5
Tel.: (613) 947-7466
Fax: (613) 954-6436

For information about the contents of this discussion paper and the consultation process, or to submit your responses to the paper, please contact:

Helen McDonald
Director General, Policy Development
Task Force on Electronic Commerce
Industry Canada
20th Floor, 300 Slater Street
Ottawa ON K1A 0C8
Fax: (613) 957-8837
E-mail: crypto@ic.gc.ca

Submissions must be received on or before April 21, 1998.

Two weeks after the closing date for comments, all submissions will be made available for viewing by the public, for a period of one year, during normal business hours, at:

Industry Canada Library
3rd Floor, West Tower
235 Queen Street
Ottawa ON K1A 0H5

These submissions will also be available for viewing at the regional offices of Industry Canada in Halifax, Montreal, Toronto, Edmonton and Vancouver.

Cat. No. C2-336/1-1998
ISBN 0-662-63406-3
51798B

Contents

Introduction: Building Canada's Information Economy and Society

Connecting Canadians

"We will make the information and knowledge infrastructure accessible to all Canadians by the year 2000, thereby making Canada the most connected nation in the world . . . . A connected nation is more than wires, cables and computers. It is a nation in which citizens have access to the skills and knowledge they need to benefit from Canada's rapidly changing knowledge and information infrastructure. It is also a nation whose people are connected to each other."

Speech from the Throne,
September 23, 1997.

Canada's success in the 21st century depends increasingly on the ability of all Canadians to participate and succeed in the global, knowledge-based economy. And to ensure that success, all of us together — individual citizens, the private sector and governments at all levels — must move quickly to build Canada's information economy and society. For its part, the Government of Canada is committed to helping Canadians access the information and knowledge that will enable them, their communities, their businesses and their institutions to find new opportunities for learning, interacting, transacting and developing their economic and social potential.

That is what connecting Canadians is all about — discovering a world of economic and social opportunities by taking advantage of new technologies, information infrastructure, and multimedia content to spur business growth and development, create new and innovative jobs, improve our capacity to communicate directly with our fellow citizens and our public institutions and services, and extend our reach to other countries.

Electronic commerce, which is at the heart of the information economy, is the conduct of commercial activities and transactions by means of computer-based information and communications technologies. It generally involves the processing and transmission of digitized information. Examples of electronic commerce range from the exchange of vast amounts of financial assets between financial institutions, or electronic data interchange between wholesalers and retailers, to telephone banking and the purchase of products and services on the Internet.

For electronic commerce to flourish in Canada, it requires a clear, predictable and supportive environment where citizens, institutions and businesses can feel comfortable, secure and confident. It also requires an international set of rules where citizens, institutions and businesses can easily exchange

information, products and services across borders and around the world with predictable results and protection. This paper in one of a series related to electronic commerce that seeks your views on how to establish those clear and predictable rules which will make electronic commerce grow and thrive in Canada, and will build Canada's information economy and society.

A Cryptography Policy for Canada

Cryptography is important to the growth of electronic commerce because it allows users to authenticate and safeguard sensitive data such as credit card numbers, electronically signed documents, personal E-mail and other information stored in computers or transmitted over closed or public networks such as the Internet. Cryptography can also be used in a wide range of applications — from the government communicating securely with citizens to ensuring the confidentiality of medical records in hospital databases.

Cryptography has implications both for electronic ways of doing business, and public safety and national security. Cryptography can protect sensitive or personal information, support electronic commerce, prevent theft of sensitive data and protect intellectual property. But the very elements that make cryptography attractive for reasons of privacy, competition, human rights and business security can also conceal activities which pose a threat to the public safety of Canadians. Criminals and terrorists can use cryptography to thwart the legally mandated information-gathering abilities of law-enforcement and security agencies. The inability to access or to decrypt information could well have a significant impact on the prevention, detection, investigation and prosecution of crime, as well as Canada's ability to monitor security threats to Canadians.

The Government of Canada is committed to creating the right climate and conditions for the growth of electronic commerce and to making Canada a world leader in this area by the year 2000. The government is also committed to a vigorous campaign against organized crime and terrorism, and has pledged, in international fora, to do so in cooperation with other nations. Since both electronic commerce and threats to public safety are transnational and global in nature, Canada's actions must be guided by both domestic and international considerations.

Recent developments in cryptography products and use (including the growth of a Canadian cryptography industry), the growth in Canadian and worldwide electronic business transactions, the increasing trans-border use of electronic communications for criminal and other threatening activities, as well as international discussions on use, control and interoperability of

encryption materials have prompted the Government of Canada to review is policy on cryptography.

This discussion paper raises policy questions regarding the use of cryptography on which the government seeks your views. Questions such as: What can governments do to accelerate the roll-out of the infrastructure which would offer public access to cryptography services and secure electronic commerce? What controls, if any, should apply to product manufacturers and service providers in the domestic sale, import and export of cryptography products and services? What measures, if any, should be introduced with respect to the domestic use of cryptography by businesses or individuals? How can we maintain law enforcement capabilities and safeguard national security interests to protect the social and economic well-being of Canadians? How can we best ensure that Canadian solutions make sense in a global context?

Your comments on the issues discussed in this document and any other related matters are important. They may be sent in writing, by mail, fax or E-mail by April 21, 1998, to:

Chair, Interdepartmental
Cryptography Policy
Working Group
Information Policy and
Planning Branch
Task Force on
Electronic Commerce
Industry Canada
300 Slater Street, Room 2063C
Ottawa, Ontario
Canada K1A 0C8

Tel.: (613) 990-4244
Fax: (613) 957-8837
E-mail: **crypto@ic.gc.ca**

Part 1: Cryptography and its Applications

Cryptography, a science for keeping data secure, has existed for thousands of years. Cryptographic methods can provide both **encryption/decryption** and **digital signatures**.[1] *Encryption* provides for confidentiality: keeping information protected from unauthorized disclosure or viewing by mathematically scrambling the original text. *Digital signatures* — which are analogous to written signatures[2] — provide three other functions:

- *authentication* — proof that users are who they claim to be or that resources (e.g. computer device, software or data) are what they purport to be;
- *non-repudiation* — proof that a transaction occurred, or that a message was sent or received, thus one of the parties to the exchange cannot deny that the exchange occurred; and
- *integrity* — so that data cannot be modified without detection.

Cryptography performs these functions by using digital keys (a unique combination of ones and zeros) that can be employed by an individual user to encrypt, decrypt and verify digital data. With cryptography, any type of digital information — text, data, voice or images — can be encrypted so that only individuals with the correct key can make it comprehensible.

There are two major cryptographic methods. In **secret key cryptography**, the same key (or a copy thereof) is used to encrypt and decrypt the data. In **public key cryptography**, there are two different but related keys, and what is encrypted with one can only be decrypted by the other.

Without access to the correct key, data encrypted to ensure confidentiality can only be decrypted into understandable **plaintext**[3] by using "brute-force" techniques, i.e., trying all possible variations of the key and checking to see if the resulting plaintext is meaningful. All other things

1. Words in boldface are defined in the Glossary of Terms, page 33.
2. A digital signature is an electronic identifier created by a computer and attached to an electronic document. A digital signature has the same properties as a handwritten signature but should not be confused with electronic replicas of a handwritten signature such as when someone signs a letter and sends it by fax.
3. The original information is sometimes referred to as "plaintext" and, when encrypted, it is called "ciphertext." Decryption reverses the process and turns "ciphertext" back into "plaintext." A "cryptographic algorithm" (sometimes called a "cipher") is the mathematical function used for encryption and decryption. Security in cryptography comes from the fact that, even if the algorithm is publicly known, there are millions or trillions of possible "keys" that could have been used for encryption. For example, a bit-length of 56 bits makes possible roughly 72 quadrillion keys.

being equal, cryptographic strength is defined by the length of the cryptographic key (or "bit-length"), which establishes the number of possible permutations. With each bit added to the length of the key, the strength is doubled. In July 1997, it took 78,000 volunteered computers on the Internet 96 days to crack a message encrypted with DES (the Data Encryption Standard), a secret key algorithm that uses a single 56-bit key. It is estimated that it would take the same computer resources 67 years to crack a secret key algorithm using a 64-bit key and well over 13 billion times the age of the universe to crack a 128-bit key. Of course, with expert knowledge, specialized hardware, and substantial funds, one can accelerate the process to some degree. In 1993, a Canadian mathematician proposed the design for a machine he believed could be built for $1 million which would complete a brute-force attack on a 56-bit DES key in an average of three-and-a-half hours.[4] But even with such resources, breaking an 80-bit key will be beyond the realm of possibility for at least a decade.

Secret Key Cryptography

Secret key cryptography can be used to encrypt data and either store it electronically (on a computer disk or hard drive) or transmit it to a close associate; however, on its own, it has significant limitations that make it unsuitable for widespread use over public networks among users who do not know each other. Secret key cryptography requires both parties to pre-arrange the sharing of the single key that is used for both encryption and decryption. If the reason for using encryption is due to the lack of security of the communication channel (e.g. a computer network), it stands to reason that one should not send the secret key along that same channel where anyone could copy it and decrypt all one's encrypted data. It is broadly recognized that the main problems faced by secret key cryptography in open networks pertain to distribution of keys and scalability (i.e. scalability refers not just to the notion of an increasing number of users but also to the notion that open networks include entities of different sizes, from individuals to multinational corporations, as well as transactions escalating in both volume and value).

4. For details see M. J. Wiener, "Efficient DES Key Search," TR-244, School of Computer Science, Carleton University, May 1994; also in *Proceedings*, Crypto '93, Springer-Verlag, 1993.

Public Key Cryptography

Public key cryptography, however, offers a solution to both these challenges since it involves the use of a pair of different yet related keys. Each user has a private key and a public key. The private key is kept secure, known only to the user; the other key can be made public and either sent over the network to each correspondent or, even better, placed in a secure public directory, almost like the electronic equivalent of a telephone book. To use this kind of system, the sender would encrypt a message with the recipient's public key. Only the recipient's private key could decrypt the message. Public key cryptography thus permits the secure transmission of data across open networks such as the Internet without the necessity of previously exchanging a secret key. This allows parties who do not know each other to exchange and authenticate information and conduct business in a secure manner.

In addition to the capability to encrypt for confidentiality, some forms of public key cryptography also enable key holders to make their documents capable of subsequent authentication by using their private key to create a digital signature.[5] This technique also ensures the integrity of documents and enables recipients to determine quickly if a message has been altered in any way during transmission.

While public key cryptography has definite advantages over secret key cryptography for use over open, public networks, secret key cryptography has its own strengths that are essential to a variety of applications.[6] Both secret and public key cryptography will be used together to protect sensitive information stored in computers and distributed over communications networks.

Certification Authorities

If public key cryptography is to work on a large scale for electronic commerce, one of the main problems to be solved is the trustworthy distribution of public keys. Some software programs, such as PGP ("Pretty Good Privacy"), which is widely available on the Internet, require users to distribute their public key to other users — an approach which may work well in small, closed groups.[7] A secure, accessible directory, however, is at the heart of broad scale distribution of public keys — especially when combined

5. The sender "signs" a message with the private key. Signing is accomplished by a cryptographic algorithm applied to the message itself or to a small block of data that is bound in some way to the message (e.g. a "message digest," which is a unique value generated by running the message through a one-way data compression function).
6. Secret key cryptography is generally faster than public key cryptography. It is therefore common to take advantage of this efficiency by employing secret key cryptography to encrypt a document and then using public key cryptography to encrypt only the secret key itself.
7. This approach works well if one can exchange one's public key directly with a friend or close associate. Trust begins to fray when public keys are exchanged through friends of friends. For example, some people attach a copy of their public key to the E-mail messages which they post to public fora, such as USENET newsgroups. This approach breaks down, if, let's say, Mallory, masquerading as Alice, posts a message to a public forum and appends his own public key, then all messages intended for Alice are subsequently encrypted with Mallory's key.

with procedures to ensure that a specific public key genuinely belongs to a particular user.

One of the ways this can be accomplished is through a **certification authority** (CA), a trusted agent who manages the distribution of public keys or **certificates** containing such keys.[8] Sometimes the term **trusted third party** (TTP) is used as a synonym for certification authority, but the two terms are not always used in quite the same way.[9]

A "certificate" is an electronic form (similar to an electronic version of a driver's license, a passport or a video rental card) containing the key holder's public key and some identifying information which confirms that both the key holder and the certificate issuer (the CA) are who they say they are.

One of the main advantages of having a supporting trusted agent is that it relieves individuals of distributing keys and managing large numbers of relationships[10] in a complex, multiple-security environment (the security relationship one establishes with a bank or a hospital will be different than that with an acquaintance or an on-line bookstore). It is not, however, simply an issue of convenience or efficiency. The CA "binds" the specific identity of a key holder to a particular certificate containing the relevant public key by signing the certificate with the CA's key, thereby ensuring authentication[11] and preventing non-repudiation, with the ultimate objective of maintaining confidence in the system.

Given the differences between digital signature functions (authentication, non-repudiation and integrity) and the encryption function (confidentiality), many cryptographic systems now require two pairs of keys: one pair for digital signatures and the other to provide encryption for confidentiality. If there is no supporting infrastructure of certification authorities, the user must generate the private and public key pairs for both digital signatures and confidentiality. If there is a supporting infrastructure, there are options as to where the key pairs are generated.

In the case of key pairs for digital signatures, the key pair should be generated by the user application and the public key should be signed by the CA and distributed for use. In order to limit the possibility of fraud, the

8. The term "certification authority" or "supporting infrastructure" will be used throughout the remainder of this discussion paper. When CAs are established in a hierarchy or linked together with other CAs with whom they have cross-certified, this is referred to as a public key infrastructure (PKI).
9. Some writers argue that "certification authority" is the broader term and that a "trusted third party" is a CA with specific provisions for lawful access. The United Kingdom's public consultation paper defines a "trusted third party" as "an entity trusted by other entities with respect to security-related services and activities" (*Licensing of Trusted Third Parties for the Provision of Encryption Services*, Department of Trade and Industry, United Kingdom; *http://www.dti.gov.uk/pubs/pubs/index.html*). The U.K. definition emphasizes the "third party" aspect of the concept, leading some writers suggest that a CA established by a corporation for its own use is not a "trusted third party."
10. Any user is likely to have hundreds or thousands of relationships varying in their level of security required; therefore, much like a telephone directory, what is required is a list of everyone a user might wish to contact or conduct business with.
11. Given that the certificate as a whole constitutes an electronic document that has been digitally signed by the certification authority (i.e. a message digest of the certificate is encrypted with the CA's private key), no unauthorized change can be made to the certificate without the modification being detected (i.e. any modification would result in a different hash value being generated).

private signing key should never leave the user application.

In the case of key pairs for confidentiality, the key pair is often generated by the CA in order to ensure back-up capability so that the private encryption key can be retrieved, thereby permitting recovery of encrypted data in the event that the private key is lost or compromised.

Making a back-up of the confidentiality key (also known as key archiving)[12] is one of several methods available to provide for lawful access to plaintext. Other methods for such access — often generically referred to as **key recovery** — include **key encapsulation** (where, for example, **a session key** or **long-term encryption key** is itself encrypted by a key recovery agent's public key) and key derivation techniques (for example, the approach proposed at the Royal Holloway College[13] in London, which allows for the confidentiality key to be regenerated from either end of the communication by the trusted third parties who originally provided the mathematical elements used in generating the key).

12. "Key archiving" is a generic term for storing a back-up of the encryption keys (or of key parts in the event that each encryption key is split up and held by more than one entity). One kind of key archiving is called "key escrow," which involves storing keys or key parts directly with one or more escrow agents (i.e. an entity other than the key owner). Depending on the model, the escrow agent could be a private sector service provider or government agency.
13. Nigel Jeffries, Chris Mitchell and Michael Walker, *Combining TTP-based Key Management with Key Escrow*, Information Security Group, Royal Holloway College, University of London, April 19, 1996.

Part 2: Cryptography Policy in Canada Today

Traditionally, cryptography was the almost exclusive preserve of governments. Cryptography was used to protect military or diplomatic secrets and was predominantly embedded in hardware. The current Canadian policy framework was set up in this context and thus consists entirely of controls on the export of cryptography.

Canada is signatory to a 33-nation agreement (the Wassenaar Arrangement)[14] that requires export controls on a long list of "dual-use products,"[15] including cryptography. Canada has reflected this agreement in a domestic regime[16] which restricts the export of customized encryption software or hardware. Canada's export control regulations are designed to prevent the movement of certain goods that may not be in the strategic interest of Canada or its allies.

Until recently, customized encryption software or hardware products with a key length of 40 bits or less were exportable. Banking and financial institutions were permitted to export 56-bit DES products. On December 24, 1996, Canada modified its policy for a twelve-month trial period to allow export of 56-bit customized encryption software or hardware with embedded encryption to most countries. This has been extended for another six months until June 30th, 1998.

Canada does not restrict the export of digital signature products and, like most Wassenaar signatories, permits the export of any strength of *mass market software* (MMS) or *public domain software* (PDS) used for encryption.[17] Canada permits the export to the United States of any strength of customized encryption software or hardware with encryption embedded in it (as does the United States to Canada) and no export permit is required.

There are no constraints on either the import or domestic use of cryptographic products. Canadian individuals and firms are free to use and trade in any strength of encryption throughout Canada. The export of cryptographic

14. Canada's export control guidelines were adopted as a national regime consistent with our international obligations as specified by COCOM (the Coordinating Committee for Multilateral Strategic Export Controls) of which Canada had been a member since 1950. COCOM was originally intended to preserve Western technological superiority by reducing the flow of military, dual-use and nuclear technologies from Western industrial nations to the Soviet bloc and other Communist countries. COCOM was abolished on March 31, 1994, and has been replaced by a modified agreement. Named after the town of Wassenaar, outside The Hague, where five rounds of negotiations took place between 1993 and 1995, the *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies* is intended to provide a framework for addressing the new security threats of the post-Cold War world.
15. Dual-use products have both military and civilian application.
16. Statutory authority derives from the *Export and Import Permits Act* (EIPA) of 1947. Section 3(d), "to implement an intergovernmental arrangement or commitment," is used to add items to the Export Control List (ECL), which is a regulation. The Wassenaar Arrangement, including its sections on cryptography, is the particular "intergovernmental arrangement" which is implemented using the EIPA.
17. The General Software Note (GSN), which was first formulated under COCOM in the 1980s, is part of the Wassenaar Arrangement's control list, although its purpose is to exclude certain items from the agreement (i.e. to exclude items from controls). The effect of the GSN for cryptography is to exclude all mass market and public domain software (MMS/PDS) products from controls, leaving only hardware and customized software applications subject to export controls. Some analysts argue that the GSN was formulated in a time in which few understood the increasingly dominant role that would be played by MMS and PDS cryptography software. Five countries, including the U.S. and U.K., override the GSN and control the export of MMS and PDS.

products for use by Canadian individuals and firms abroad, although controlled, is normally supported.

Why a New Policy on Encryption

Changes in the global supply of and demand for cryptography products require that this policy be reviewed. Today, strong encryption is increasingly being used by businesses and individuals, and strong cryptography is increasingly available in shrink-wrapped mass market software or public domain "free-ware" on the Internet. There is a growing global demand for cryptography products, and design and manufacturing capabilities are emerging in many nations. At the same time, law enforcement agencies and national security agencies are concerned that the widespread use of strong encryption without some capability for lawful access will significantly impact upon their investigative capabilities. Many countries are reviewing their cryptography policies in light of these pressures and the role of these technologies in electronic commerce.

In response to these pressures, the federal government asked Canada's Information Highway Advisory Council (IHAC) for advice on what was needed to address security requirements for electronic commerce.

IHAC's September 1995 report[18] identified the need for the technological and legal structure to assure the privacy and confidentiality of financial and other sensitive information, whether stored in databases or in transit over public networks. The Council called for:

- public consultations to determine how best to balance the legitimate use and flow of data, privacy, civil and human rights, law enforcement and national security interests in a national security policy;
- a basic level of security on the Information Highway that provides message integrity and authentication, as well as a reasonable expectation that communications intended to be private and personal will be protected;
- public scrutiny of encryption algorithms and standards, and freedom of choice in their use;

18. *Connection, Community, Content: The Challenge of the Information Highway*, Report of the Information Highway Advisory Council, September 1995. Available at **http://strategis.ic.gc.ca/IHAC**.

- a partnership among the federal government, provinces and territories, the private sector and other stakeholders to develop mutually acceptable security standards and to promote the widest acceptance of these, within Canada and with our international trading partners; and
- a federal leadership role in developing privacy, integrity and authenticity services on the Information Highway, through the creation of a uniform public key infrastructure to meet federal government needs.

The federal government's initial reaction was articulated in May 1996, in a report entitled *Building the Information Society: Moving Canada into the 21st Century.*[19] In this report, the government stressed the importance of electronic commerce as its preferred means to conduct business, internally and with external clients. The government further committed to work closely with the private sector, other levels of government and other stakeholders to develop and implement policies, standards and protocols for a widespread and seamless electronic commerce system.

Government of Canada Public Key Infrastructure

Central to this development would be a Government of Canada Public Key Infrastructure (GOC PKI)[20] to provide a basis for the use of digital signatures and secure internal and external electronic transactions. A number of government departments and agencies are actively engaged in the development of the government PKI and the introduction of its base technologies. Individual departments are using PKI technologies and establishing certification authorities to secure local files and network communications for electronic business applications such as E-mail, data interchange, database access, and Web interactions. The GOC PKI will be fully implemented in late 1998.

The GOC PKI will interface with private sector and institutional PKIs adhering to similar levels of privacy, integrity and security standards, in order to provide the easy and seamless secure electronic transactions demanded by Canadians. This will be best accomplished by working in partnership with industry and other

19. The full contents of this report are available at: *http://strategis.ic.gc.ca/IHAC*
20. Government of Canada Public Key Infrastructure White Paper, Communications Security Establishment, May 1997 (*http://www.cse-cst.gc.ca/cse/english/gov.html*).

levels of government, and through the reliance on internationally recognized standards and practices.

In order for the GOC PKI to fulfill its functions for the federal government and the citizens who choose to access federal services through it, a legal framework for digital signatures must be in place. The government is examining the changes to existing federal legislation which may have to be made to recognize the use of digital signatures and electronic records, and to remove legal barriers to electronic service delivery.

Review of Canada's Encryption Policy

The government is reviewing Canada's existing cryptography policy, with a particular focus on the issue of encryption for confidentiality. The public response to this discussion paper will provide the government with essential input into this policy review.

The government is committed to the development of a balanced policy framework, consistent with the OECD Guidelines for Cryptography Policy,[21] which protects the vital economic and financial information that is held in Canada's private sector, secures individual privacy and freedom of expression, and safeguards law enforcement and national security responsibilities to the public and the government.

More particularly, an updated policy on cryptography must:

- help realize the economic and social benefits that can be derived through the use of cryptography in secure global electronic commerce;
- ensure business and public confidence in the use of certification authorities, other cryptographic service providers, and cryptography product suppliers in Canada;
- respond to the challenges when lawful access to encrypted real-time communications or encrypted stored data is mandated; and
- respond to the challenges posed to national security information-gathering capabilities by the international spread of strong cryptographic products.

21. Canada participated in the development of the 1997 OECD Guidelines on Cryptography Policy (*http://www.oecd.org/dsti/sti/it/secur/index.htm*). These are a set of eight principles that nations should weigh in the development of national policy frameworks.

The following sections of the discussion paper present key factors which must be taken into account in developing a new Canadian policy on cryptography. These considerations are followed by three sets of options for assessment and comment.

Part 3: Considerations in Developing Canada's Cryptography Policy

In developing its policy on encryption, Canada, like many countries, is faced with the challenge of balancing fundamental questions of privacy and individual rights, commercial and business interests, and the obligations of the state in maintaining its ability to protect itself and its citizens from various threats to public safety.

Various options exist which address privacy and electronic commerce requirements and which permit, to differing degrees, lawful access to information or communications for security, law enforcement and regulatory purposes. Every option entails trade-offs borne by all stakeholders and all come at some cost, even though the costs differ for each option.[22] The requirement to balance the commercial, privacy and lawful access needs of society and its members is not new, but has assumed a more acute importance today because of recent technological developments, which impact or may soon impact both legitimate and illegitimate activities. Significant developments include the following:

- the increasing use of strong cryptography itself, as encryption software and computers powerful enough to encrypt and decrypt data easily are becoming commonly available;
- the rapidly increasing use of telecommunications media suitable for encryption (e.g. E-mail and other data conveyed via the Internet or other computer-based media), both as a means of personal communication and a means of conducting many forms of commercial communications;
- the increasing use of wireless cellular telephones, which has created pressure for the development of digital equipment and lead to the encryption of their signals in some cases; and
- the increasing reliance on computers and computer networks for commercial activities and the need to

22. Each option implies a different set of technical and operational elements, legal and cost implications, as well as difficult-to-measure dimensions such as public safety, sovereignty and civil liberties. No option can totally guarantee lawful access, although some may come closer than others.

protect privacy and security, which has led companies to store business records in secure computer facilities or in encrypted form.

In developing a balanced policy, Canada will need to take into account the considerations discussed below. These same factors also confront other developed countries; their assessment of these factors and the policies they ultimately select will also be critical to Canada, since many of the practical applications of cryptography involve transnational communications.

Electronic Commerce Considerations

As more and more transactions shift from closed networks to open networks,[23] cryptography becomes essential for the conduct of electronic commerce. Historically, most electronic commerce, such as electronic data interchange (EDI) or electronic funds transfer (EFT), has been conducted on closed networks. In a global trading environment, the full advantages of electronic commerce can only be achieved through a transition to open networks.

Open networks, however, pose a variety of security challenges including concerns over the authentication of communicating parties, the integrity of data being communicated, the confidentiality of proprietary or personal data, and the assurance that transactions have been authorized by legitimate users. Without cryptography to support dependable digital signatures and strong confidentiality services packaged in a trustworthy, cost-effective and user-friendly way, these challenges may not be met.

In the world of open networks and in an environment which is increasingly characterized by uncertainty and global economic competition, strong encryption enables corporations to protect themselves from competitive intelligence-gathering and criminal threats, and to protect sensitive information and communications, as in the following cases:

- Businesses are beginning to use the Internet for their communications and access to corporate information holdings. Businesspeople on the road as well as teleworkers often need to exchange sensitive information such as business intelligence,

23. A closed network connects users who already have contractual relationships and mutual trust, e.g., banking customers and employees. A closed system is often enforced through various technical means, such as the parties employing end-to-end encryption on leased lines. By contrast, the most obvious example of an open network is the Internet, a vast interconnected network composed of thousands of networks (each of which have their own forms of administration, creating a complex environment ranging from virtual anarchism through cooperative community services to multiple commercial security policies).

bidding information and marketing strategies with the home office. Encryption helps ensure that only authorized users have access to data and protect sensitive data from unauthorized viewing or malicious use.

- Encryption supports the secure communications needed for virtual organizations and strategic partnerships. Many of today's businesses have offices for research and development, production, and sales in different geographic locations in Canada or abroad. In some instances, strategic partners have access to corporate databases for joint ventures and at the same time are competitors in other undertakings. A broad range of intellectual property such as trade secrets, blueprints, designs, and operational records that never before traversed open networks must now be protected.
- It is becoming more common to make information, cultural products and software available directly to consumers over open networks. Satellite television and pay-TV are two examples in which encryption is being used to protect intellectual property from fraudulent or unpaid use.
- If business is to be conducted on-line, consumer confidence is crucial. The willingness of consumers to make purchases over the Internet depends upon the certainty that their transactions are secure. Encryption is one means of maintaining the confidentiality of consumers' credit card numbers and other personal information. Data protection laws, which place obligations on data users to protect confidentiality, will further promote the use of encryption.
- As governments increasingly move to third party and on-line delivery of services, citizens will increasingly demand the assurance that their sensitive medical, employment, revenue, and other information is protected to the greatest extent possible.

Different kinds of transactions require different kinds of solutions in order to meet these demands. Some enterprises will protect their corporate communications between branches by establishing virtual private networks or by using hardware encryptors to guarantee secure data transmission over the Internet. Other organizations, from multinationals down to medium-sized firms, may set up their own certification authorities to meet the cryptographic requirements for secure E-mail-enabled electronic commerce and a wide range of applications demanding authorization, authentication and integrity services. Among the early adopters in this regard are banks, which are establishing their own CAs in order to provide home banking over the Internet, and financial institutions, which have implemented the Secure Electronic Transaction (SET) protocol for credit

card transactions. Other businesses may choose to out-source to cryptography service providers, which offer a suite of certificate-based services supporting a full range of authentication, non-repudiation, integrity and confidentiality functions. In fact, certification authorities offering services to business are already in operation in Canada and elsewhere.

Each of these different modes of providing cryptography-based security services raises a variety of considerations not only for business but for lawful access as well. Among the considerations are:

- the nature of the keys employed (i.e. whether these are one-off session keys for data in transit which are discarded after use or long-term encapsulation keys);
- the issue of who controls the cryptographic keys at each phase of the keys' life cycle, beginning with key generation through to key archiving or destruction (i.e. is it the data owner or a trusted agent other than the owner); and
- the differences that arise whether one is dealing with the encryption of stored data or the encryption of real-time communications.

Businesses must assess the extent of their information assets, their value to the company, and the firm's information technology capabilities and resources. Given the diverse range of scenarios with which different businesses must cope, there is a vocal demand for freedom of choice in algorithms, selection of standards, and implementation. Trust in the technology and the infrastructure is essential for commercial deployment.

In order to facilitate electronic commerce globally, the supporting infrastructure, including procedures and physical components, should be designed to ensure interoperability between users served by certification authorities in different jurisdictions with different national policies. National cryptography policies are designed to establish a level of trust for a country's users and service providers. Interoperability, however, requires some form of matching between each nation's policies. International business organizations consistently ask that national policy implementation in one jurisdiction neither creates an obstacle to interoperability nor reduces the level of trust in the infrastructure of the other jurisdiction.

Within national boundaries, there are evidently areas where consensus seems achievable and others where challenges remain. There is, for example, a recognized business need for back-up of the private encryption key. Back-up keys would be used when an employee forgets the password to access their private key, when a technology failure occurs, or in circumstances when the key holder is no longer an employee. The decision

to implement key back-up is made by the data owner, i.e., the business rather than the employee. It is important for key back-up mechanisms to be designed in a manner that does not diminish the cryptographic protection available.

While there is a business case for the recovery of stored data, there is not an equivalent commercial need for key recovery for encrypted real-time communication (e.g. telephone calls, real-time sessions between two computers on a network, and remote application or database access). In real-time sessions, the parties in communication already have decrypted voice or data at each end. If an encrypted session somehow goes awry, one simply calls again, setting up a new encrypted session. There is no need for key recovery in this instance.[24] Although some companies may need to generate an audit trail of real-time transactions, these functions would logically be introduced before the encryption is applied rather than after. A variety of financial institutions that routinely employ encryption also require extensive audit functions, yet it appears that few of these institutions have implemented these processes in a manner that involves key recovery for data-in-transit.

Clearly the aims of law enforcement and business coincide when cryptography protects proprietary information, trade secrets and in general helps defend industry and consumers against fraud and other unlawful activities. In addition, cryptography meets national security objectives to the extent that it helps protect sovereignty, national infrastructures and their valuable information.

As an electronic commerce enabler, cryptography increases the competitiveness of businesses and provides opportunities for job creation and industrial growth. Government policies which encourage marketplace innovation and standardization will facilitate the development of cost-effective and user-friendly products and infrastructures and the widespread use of electronic commerce. Regulatory measures risk slowing down the rapid evolution within the information technology products and services market, and creating obstacles to international commerce. Although regulatory control measures have the potential for making it more difficult for criminals to use cryptography, they

24. One might imagine exceptional circumstances (i.e. suspicion of a rogue employee), in which a company may need to intercept its employees' encrypted communications. If this were the case, however, it would be easier for the company to initiate surveillance before the communication has been encrypted rather than tackling the more difficult problem that arises after encryption.

could also introduce significant costs to the government and private sector required to implement the systems. They might also fail to prevent criminals from circumventing the same measures, for example, through the use of double encryption.

The policy challenge is to find solutions that will limit criminal misuse without interfering with legitimate business, institutional or individual interests. Canada has an obvious obligation to protect its citizens from criminal and illegitimate activities. There are both social and competitive economic advantages to having a safe, civil society — a reputation which is enjoyed by Canada.

The supply side of the electronic commerce equation must also be carefully considered. Canada has a well-deserved reputation as a world leader in the telecommunications and software sectors and impressive niche strengths in cryptography products. Our industry is well-positioned to increase its market share in a global market expected to grow from US$600 million in 1996 to US$5 billion by 2000.[25] To ensure that these opportunities are not lost, the Canadian cryptography industry is calling for policies that encourage innovation and enable competion on an equal footing internationally.

Lawful State Access Considerations

Computer networks have created new opportunities for personal and commercial communications, but not without some adverse impacts on the abilities of law enforcement agencies to protect the public. The new technology has also generated new forms of criminal activity, new methods of committing old crimes, and new ways to conceal evidence. The widespread use of strong cryptography raises concerns in this context, because it can create significant obstacles to the detection and investigation of criminal activities and security threats, as well as the inspection of computer records to monitor compliance with commercial, taxation, environmental and other legal and regulatory requirements.

Public safety, crime control, national security and regulatory compliance all require that the agencies involved be rapid and effective in quickly gathering accurate information and evidence about the activities of criminal elements. Agencies that play key roles

25. Dataquest.

include the RCMP, provincial and local police forces, the Canadian Security Intelligence Service, Revenue Canada (Taxation, Customs and Excise), the federal Competition Bureau, as well as federal and provincial environmental enforcement agencies. These agencies are responsible for identifying threats and detecting, investigating and prosecuting matters ranging from terrorism, crimes of violence and property crimes to abuses of domestic and international commercial and financial systems.

The effectiveness of these agencies in monitoring criminal activities, and in investigating and prosecuting offenders often depends on their ability to conduct electronic surveillance of communications and to search or inspect places, including computers, where relevant information may be kept. This is done, as required by the Canadian *Charter of Rights and Freedoms*, the *Criminal Code*, and other statutes, only with the authorization of a court, based on an assessment of the legal justification for invading the privacy of the suspects and those who communicate with them. The necessity for such surveillance is recognized by the Charter [ss. 1, 8 and 24 (2)], which allows seizures and surveillance that are "reasonable" and "justifiable in a free and democratic society," and allows evidence to be used if its admission does not "bring the administration of justice into disrepute."

Historically, as the use of electronic and radio telecommunications and the technical ability to monitor them have evolved, it has been recognized throughout the developed world that there is a legitimate need for agencies of the state to be permitted to monitor communications, provided that adequate legal and judicial safeguards are in place. Similar principles apply to physical searches and inspections, which are now being extended to the search or inspection of computers and networks. In regulating these activities, national constitutions, legislation and court decisions have always balanced the need to protect fundamental privacy interests against equally fundamental interests in public safety and security.

The increasing use of strong cryptography will generate some crime-control benefits by providing technical protection for confidential information, such as the information used to conduct financial transactions electronically, but it also represents a significant threat to the ability to conduct lawful and authorized electronic surveillance. While judicial authorizations could still be obtained, those who intercept encrypted information would not be able to read it. This creates two major difficulties:

- it would become difficult or impossible to determine whether the information being intercepted fell within the scope of the legal authorization to intercept it; and

- it would become difficult for the authorities to decipher the information, or to do so in time to use it effectively or take action to prevent harm from occurring.

In many cases, rapid access to information is essential to successful investigations because subsequent steps depend on the information and cannot be taken until it is too late. This is particularly true with respect to computer systems, which can be used to move, conceal or erase large quantities of information at the touch of a button. In some cases, timely access may be necessary in order to permit steps to be taken to prevent a crime or a terrorist act from being committed.

The increase in global telecommunications has created new opportunities for domestic and transnational crime and new obstacles to effective controls. Any form of illegal activity which requires the co-ordinated or concerted efforts of many people in different places will be facilitated by the availability of secure telecommunications, and governments have an obligation to respond. Common examples facing Canadian agencies include:

- protecting Canadians and Canadian sovereignty against terrorism, political or economic destabilisation or similar threats from foreign states or organized groups;
- detecting and prosecuting the use of computers and telecommunications for illegal transfer or trafficking in narcotics, weapons and other dangerous or illegal goods;
- detecting and prosecuting the use of computers and telecommunications to launder the proceeds of crime; and
- detecting and prosecuting the use of computers and telecommunications to transfer information illegally (such as child pornography, hate propaganda, intellectual property and commercial or national secrets).

Offenders can use computers and network technology as a tool to commit old crimes in new ways, such as the distribution of child pornography on the Internet. The availability of easily accessible, secure telecommunications is likely to provide assistance to the business of criminal as well as legitimate enterprises. Examples include the use of computers and telecommunications to move crime proceeds while concealing their origins and the use of such communications by criminal and terrorist groups to organize and co-ordinate their activities.

Gaining lawful access to encrypted, stored data is in some cases not as time-sensitive as the interception of ongoing communications, but it represents a more broad-ranging problem. A large number of federal and provincial laws allow for the inspection of routine business records to check for compliance with taxation laws, import-export controls, environmental or health standards, competition or

trade regulations, and numerous other matters. These legitimate enforcement and inspection activities may be threatened by the widespread use of strong cryptography, even for legitimate commercial security reasons.

The law enforcement, regulatory and security communities clearly recognize the substantial commercial and legitimate privacy advantages which will accrue from the use of encrypted telecommunications for personal and commercial applications. Equally, they recognize that these very advantages bring with them new criminal opportunities and security threats. To effectively discharge their responsibilities to protect Canada and Canadians from these threats, the agencies involved require some means whereby encrypted data can be decrypted and read within a reasonable time and at a reasonable expenditure of resources. This will require striking a policy, legal and technological balance between the interests of personal privacy and the development of efficient commercial communications on one hand, and the protection of society on the other.

Human Rights and Civil Liberties Considerations

On the grounds set out above, there are legitimate reasons for providing lawful state access to encrypted information in some circumstances. In practice, options for ensuring that access generally involve either limiting the use of cryptography products to those which can be decrypted and read when necessary or requiring those who have the keys to decrypt messages on demand. The basic policy options and the practical means of implementing them raise human rights concerns, chiefly with respect to privacy and the freedom of expression.

Ultimately, cryptography policy options must be assessed on their respective costs and benefits in terms of basic human rights, commercial interests, public security and crime-control. This in turn requires an assessment of what crime-control and security benefits might result from limiting encryption, and how this would compare with the harms that might result from unregulated encryption. To make matters even more challenging, the overall impact of cryptography and the feasibility of regulating it are both largely unknown quantities at this stage. For example, even if some form of lawful state access to plaintext were provided, it is not clear whether the ability of security and law-enforcement agencies to fulfill their responsibilities would be maintained at roughly existing levels.

Whether all of this maintains a security and law enforcement capability which is acceptable to Canadians is difficult to establish because any meaningful frame of reference is also changing. The technical ability to conduct various forms of lawful access has been significantly increased by new

technologies in recent decades. Systems for data storage, transmission and retrieval make it possible for large quantities of personal information to be stored and retrieved quickly, and searched automatically. This assists law enforcement, but has also created new criminal activities and new ways for those who wish to avoid detection to conceal their activities. The prospect that information will be obtained by those who should not have access to it also greatly increases the concerns about basic privacy rights and the need for effective safeguards as the quantity of information which can be accessed has increased.

As in many democratic countries, the rights of Canadians to some degree of privacy and to express themselves freely are constitutionally protected. Section 8 of the Charter guarantees Canadians the right to be free from "unreasonable search or seizure" and paragraph 2(b) guarantees the right of free expression. Privacy rights will likely prohibit the state from decrypting data without some fairly compelling justification, and the right to freedom of expression may extend to both the production of cryptographic products and their use to protect the messages being expressed or data being stored.

These guarantees are important, but not absolute. Invasions of privacy, including the seizure of data or interception of communications, must be justified and authorized by the courts. The freedom of expression may protect one's right to create or use cryptography, but could be limited by law, provided that the limits are reasonable and demonstrably justified in a free and democratic society (s.1). How these provisions would apply to the regulation of cryptography in Canada would depend to a large degree on exactly what requirements are set and how they are applied. They will certainly operate as a constraint on the policies and laws which may be adopted, however, and as a safeguard of individual rights once they are in place.

Historically, state intrusions on privacy in the form of search, seizure or electronic surveillance have been based on the justification that there are grounds to believe that the individual whose privacy the state seeks to invade is either involved in some form of wrongdoing, or has some concrete evidence of wrongdoing. These are the criteria applied by the courts in balancing individual privacy against state interests.

The same principles would apply to encrypted information, but decrypting information is not identical to either of the existing precedents — seizing evidence with a search warrant or intercepting communications with a judicial authorization. If decryption requires access to the keys, seizing them with a conventional warrant would alert the recipient of the message that he or she was under investigation.

Setting up a system in which the keys must be held and accessed by a third party would not alert the sender and recipient that they are targets of surveillance. This system, however, requires the sender and recipient to provide the keys even in cases where there was no surveillance, suspicion or judicial scrutiny based on wrongdoing. In such models, the safeguard of judicial scrutiny would have to be conducted at the time encryption keys were actually used. This would only occur with respect to the small minority of messages and keys where lawful state access was actually sought, and other protections would have to be found for the majority of keys.

Internationally, computer networks and other communications media have been combined with encryption to report on human rights abuses and to protect the safety of persons promoting democracy and human rights in oppressive countries. Governments concerned about human rights and democracy should preserve and protect these human rights efforts as much as possible,[26] and should consider the impact their internal and export control policies could have on human rights workers.

For example, by controlling the domestic use or export of encription products that do not have a state access encription feature, countries would likely discourage companies from producing such technologies. As a result, human rights and democracy workers would likely find it difficult to obtain technologies that cannot be accessed by repressive governments.

Technical Security Considerations

The application of the Canadian Charter and legislative requirements imposed by the courts (e.g. on the scope of a warrant) addresses some of the fundamental privacy and freedom of expression issues raised by lawful state access, but does not provide assurance that the creation of mechanisms for giving such access will not inadvertently create gaps in security that might be exploited by illicit interests.[27] From a technical standpoint, strong cryptography products are difficult to "break" short of a "brute force" attack by powerful computers. If commercial products prove deficient in some way, the problem would presumably be identified and corrected quickly by the

26. Some of the arguments being marshaled on behalf of human rights have been presented by the American Association for the Advancement of Science at: *http://www.aaas.org/spp/dspp/cstc/briefings/crypto/*
27. See the 1997 report of leading private sector cryptography experts in the U.S., *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption* (*http://www.crypto.com/key_study/report.shtml*).

marketplace. The possibility that access mechanisms built into the systems for legitimate government purposes might be used by illicit interests would not be so easily prevented or corrected. The exact vulnerabilities, if any, would depend on the nature of the access mechanisms. If keys were kept by CAs or TTPs, for example, precautions against theft would be needed. If some alternate form of access was embedded in encryption software, there would be the possibility that someone other than those authorized by the courts might discover how to use it.

Proponents of relaxed controls on the use of encryption point out that in Australia (the Walsh report),[28] the United States (the National Research Council report),[29] and Europe (the European Commission),[30] independent studies by experts in cryptography have identified a number of benefits from encryption, but also a variety of problems with proposals to limit choice of encryption products — primarily the technical challenge, effectiveness and cost associated with fully comprehensive key recovery schemes. They have not recommended that governments require key escrow or key recovery features at this time. At the same time, Canadian policy must respect Canada's international committments.

International Considerations

Canada is a global trading nation and an active member of numerous international bodies. Other countries are examining their encryption policy options at the same time as we are. Canada will need to closely examine the evolving direction of key exporting nations, as well as trading blocks such as NAFTA, the EU and others, in order to ensure that our industrial and economic interests are not disadvantaged and discourage unnecessary obstacles to global trade and commerce.

At present, it is unclear how most countries will come to grips with the issue of export and domestic controls. Some countries have domestic import and use controls in place and others are studying the problems. Some favour export controls as a means of indirectly influencing the types of products available domestically, and others appear reluctant to impose any constraints on the market for encryption. What is clear is that the international context will have a bearing on Canadian policy.

---

28. Walsh, Gerard, *Review of Policy Relating to Encryption Technologies*, Report completed October 10, 1996, for Security Division, Attorney General's Department, Government of Australia, and released under *Freedom of Information Act*, June 1997. (See *http://www.efa.org.au/Issues/Crypto/Walsh/*)
29. Dam, Kenneth and Herbert Lin (editors), *Cryptography's Role in Securing the Information Society*, Committee to Study National Cryptography Policy, National Research Council, Washington, D.C., National Academy Press, 1996.
30. *Towards A European Framework for Digital Signatures and Encryption* (*http://www.ispo.cec.be/eif/policy/970503.html*).

Canada is signatory to a number of international treaties and conventions that protect freedom of expression, media and communications, and privacy and human rights generally. Canada is also signatory not only to the Wassenaar Arrangement, but also to a number of international conventions promoting effective law enforcement measures to counter drug trafficking, money laundering and terrorism. Commitments to our allies, the international community and our international obligations are factors that circumscribe our policy options.

A national policy stance completely at odds with those of our allies could damage long-standing security relationships. A policy at odds with the positions of other producer nations risks being ineffective. If, for example, controls were applied in Canada but not elsewhere, it would be difficult to prevent non-complying software from being physically or electronically smuggled into the country. Cryptography policy has become an important issue because computer software capable of strong encryption and portable computers powerful enough to run such software have become commonplace. As with any other data, strong encryption software is easily transferred from one place or jurisdiction to another using the Internet, making import and export controls difficult to enforce.

Part 4: Policy Options

In setting a future cryptography policy for Canada to support the growth of electronic commerce in a manner which addresses human rights, civil liberties, law enforcement and national security requirements, the government is seeking public comment in the three following areas: encryption of stored data, encryption of real-time communications, and export controls for encryption products. A number of options for each are described below. In order to achieve the optimal balance, a creative combination or variations of elements from the three areas may ultimately prove to be the solution.

Encryption of Stored Data

Market-driven

One option would be to continue with current practices and impose no new laws or licensing conditions on individuals, certification authorities, cryptography service providers or producers. The marketplace would determine outcomes and businesses and individuals would be free to decide what level of security they require from a service provider or what cryptography they choose to own and deploy.

This approach relies on companies and individuals to take precautions against permanently losing important information by creating their own back-up keys. They would be free to determine where these keys would be stored — in a safe, with their lawyer, a firm's security group, or with a third party offering these specialized services. Lawful access to plaintext (i.e. stored data that has been decrypted) would be met only to the degree that individuals and firms adopt data recovery techniques (such as back-ups of decryption keys).

The lack of back-up would pose problems for law enforcement agencies that need to investigate crimes through search-and-seizure provisions under lawful warrant. While large businesses believe back-up of stored data to be a good business practice that minimizes the risks of loss, theft or misuse of keys by employees, not all businesses are likely to provide for back-up. As a result, a model that is essentially market-driven may be insufficient to provide for all forms of lawful access.

A laissez-faire model leaves it up to the consumer to judge what is adequate security. Given the complexity of cryptography products, consumers may have difficulty making the right choices, thus causing uncertainty in the market.

Minimum Standards

Another approach would be for government to actively encourage the back-up of encryption keys or the explicit provision for business data

recovery. Essentially, the government would define a minimum standard or set of practices for data or key recovery capabilities of certification authorities and other businesses offering key management services. This standard or set of minimal practices would be promoted through awareness efforts aimed at businesses and collaboration with service providers on industry codes and self-accreditation. Industry, suppliers and users could be given the task of coming up with a set of responsible practices or codes incorporating key back-up, which could be implemented through industry self-regulation.

The federal government's public key infrastructure (GOC PKI) could also be used to promote such a standard, by cross-certifying only with private sector service providers that meet these back-up and recovery standards. This would create a "white list" of companies and CAs which the federal government believes to be following good business practices. These kinds of actions would provide an incentive for individuals and businesses to build in voluntary provisions for data recovery and better meet the needs of law enforcement and national security.

The existence of a list of federally sanctioned certification authorities might also help consumers in making difficult choices. A set of minimum standards may reduce uncertainty and, given cryptography's enabling role, accelerate the adoption of electronic commerce.

Mandatory Access

Another approach would be for the government to pass legislation to mandate law enforcement access by prohibiting the use of encryption products without key recovery capabilities. This could be done by prohibiting the operation of certification authorities in Canada unless they provide for law enforcement access to plaintext when served with a court order. This would essentially reduce the products available for use in Canada to those with a key archiving or key encapsulation capability.

In order to ensure that individual end-users would not circumvent this solution by applying additional non-key recovery encryption or using foreign CAs that would not escrow or archive keys, the government could prohibit the manufacture, import and use of non-key recovery products in Canada.

Encryption of Real-time Communications

Assistance Orders and Selective Conditions of Licence

One approach would be to maintain the status quo. When served with a court order, telecommunications carriers are currently obliged to assist in the decryption of encrypted communications traveling over their facilities, to the extent that they are capable of doing so. Carriers would presumably be capable of decrypting that which they encrypt to begin with, but there may be difficulties. Their

systems may not be configured to maintain back-up copies of encryption keys for individual communications sessions.

At present, encryption technologies are primarily used by some carriers to ensure the confidentiality of digital wireless communications. The only communications service providers that are required to provide law enforcement and national security access to communications "en claire" are the new wireless providers of personal communications services (PCS) and local multipoint communications services (LMCS). This is a condition for obtaining operating licences and applies only to any encryption that these wireless providers themselves employ.[31]

In the ongoing transition from a monopoly to a competitive environment for telecommunications, there will be an increasing number of players and technologies in this field. A patchwork of approaches could result in an uneven playing field amongst communications service providers. If the use of encryption increases as expected, the patchwork effect may also exacerbate the problem of lawful access to plaintext.

Obligations on all Carriers

Another approach would be for the federal government to impose requirements by legislation that all federally regulated communications carriers that provide encryption services retain the ability to decrypt messages for law enforcement and national security agencies on receipt of a court order. The federal government would need to collaborate with the provinces and territories to extend these same requirements to provincially-regulated service providers. Such an approach would safeguard existing police powers to use court-sanctioned interception as a means of preventing and investigating crime. This approach would prevent the development of an uneven playing field between wireless and wireline service providers. On the other hand, it may impose additional infrastructure costs that would be borne by users. An approach that focuses on communications carriers would not affect Internet service providers (ISPs), which may decide to offer encryption services for real-time communications such as Internet telephone, nor would it prevent employment of encryption by end-users.

---

31. For details see: *http://spectrum.ic.gc.ca/pcs/engdoc/lic-cond.html*

Mandatory Controls

A third approach would require, in addition to the legislated requirements on carriers described above, legislation to compel any certification authority that furnishes keys for the purpose of encrypting real-time communications (e.g. encrypted Internet telephone, encrypted telnet, or source Web transactions) to provide mandatory assistance for decryption on receipt of a court order. Completeness for law enforcement purposes would require prohibiting users who encrypt their own messages from using non-key recovery products or requiring them to provide the carrier or a CA with the necessary key prior to transmission. Cryptographic software or hardware would be required to either generate a third message key for lawful decryption, or to incorporate some general key accessible only on court orders. Carriers would be prohibited from transmitting messages unless in plaintext or encrypted by key recovery hardware or software.

Export Controls

Relax Controls

One option would be for the government to relax the current export controls on cryptographic hardware products and custom software. Two types of liberalization are possible: either matching the most liberal export policies of those countries exporting cryptography products, or relaxing controls through recognition of the availability of similar-strength cryptography products in foreign markets. Both would support the growth of the Canadian cryptography industry.

Canada is obliged to adhere to the terms of an international agreement with 32 other nations (the 1996 *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies*) that stipulates which products require export permits and which do not, but does not prescribe approval or denial of permits. Making changes to match the most liberal policies elsewhere would set Canada apart from the majority of other nations (particularly the United States and our other national security allies), would be seen as an aggressive move within the Wassenaar Arrangement, and may potentially trigger international pressure to adopt a more restrictive policy. Recognizing foreign availability is, in contrast, a common practice employed with other controlled products and by other Wassenaar signatories.

Maintain Existing Policy

As another option, the government could continue with its current policy, based on Wassenaar lists of controlled goods, and under current approval/denial policies would allow the export of any strength of digital signature product, the export of any strength of mass market software (MMS) or public domain software

(PDS) used for encryption, the export to the United States of any strength of customized encryption software or hardware with encryption embedded in it (because no such export to the U.S. requires a permit), and the export of customized encryption software or hardware with encryption embedded into it up to a 56-bit strength. Canada could continue to show no preference for key recovery products or, on the other hand, foreign availability could be used to give key recovery products some preferential export treatment.

Extend Controls

Another option would have the government extend export controls to MMS and PDS, either in cooperation with other Wassenaar partners or unilaterally. This could be coupled with the decontrol of weaker forms of encryption or other measures to minimize the impact on business. The government could also couple the extension of controls with relaxation for key recovery products. The export of strong cryptography would only be permitted if the products had approved key recovery provisions. Unless these measures were matched by all other cryptography-producing nations, Canadian manufacturers would be on an unequal footing with manufacturers located in countries having a more liberal policy. Different interpretations by various jurisdictions as to what is acceptable key recovery could also unbalance the playing field.

Questions for Public Response

The Government of Canada is updating its cryptography policy so as to protect the vital economic and financial information that is held in Canada's private sector, secure individual privacy and freedom of expression, and safeguard law enforcement and national security responsibilities. The government seeks your view on the following:

- How do you assess the feasibility, cost and international compatibility of the policy options described above, and which option do you favour for:
  - stored data?
  - real-time communications?
  - export controls?

We would also welcome your views on the following, broader questions:

- What can governments do to accelerate the roll-out of the infrastructure which would offer public access to cryptography services and secure electronic commerce?
- How can the government best balance the needs of electronic commerce, privacy and law enforcement? Should conditions be set on private sector cryptography service providers and individual citizens? Would a voluntary approach be effective?
- What controls, if any, should be placed on the activities of common communications carriers, value-added network operators, resellers, Internet service providers and other companies providing encryption of real-time communications? Who should bear the costs of any controls?
- What changes in the export regime would help the government provide an appropriate balance between our national security interests and the needs of Canada's business community, including the cryptography industry?

Glossary of Terms

Certificate: an electronic document that contains credentials bound to an entity and is signed by a certification authority which has verified these credentials.

Certification authority (CA): a third party that verifies an entity's credentials, generates certificates which can be used by these entities to prove their attributes to others, and maintains adequate records to demonstrate the binding between the entity and the credentials which have been certified. Certification authorities also manage, distribute, and store certificates and certificate revocation lists.

Ciphertext: data in its enciphered form.

Digital signature: a cryptographic transformation of data which, when associated with a data unit (such as an electronic file), provides the services of origin authentication, data integrity, and signer non-repudiation.

Encryption: to change plaintext into ciphertext. The word encryption is often used to mean specifically the transformation of data by the use of cryptography to produce unintelligible data (encrypted data) to ensure its confidentiality.

Decryption: the inverse function of encryption; to change ciphertext into plaintext.

Hash: a mathematical function which maps from a large (possibly very large) domain into a smaller range. It may be used to reduce a potentially long message into a "hash value" or "message digest" which is sufficiently compact to be used as an input into a digital signature algorithm.

Hash function: a function which maps a bit string of arbitrary length to a fixed-length bit string and satisifies the following properties: (1) It is computationally infeasible to find any input that maps to any pre-specified output. (2) It is computationally infeasible to find any two distinct inputs that map to the same output.

Key encapsulation: a technique by which a session key is "wrapped" (i.e. the session key is encrypted) by another key belonging to a third party (such as a key recovery agent). In E-mail applications, the "wrapped" key is typically stored in a message's header. In real-time communications, the "wrapped" key may be transmitted in the initial "handshake" that establishes the secure connection.

Key recovery: a broad range of techniques permitting the recovery of plaintext from encrypted data when the decryption key is not in the posession of the decrypting party (e.g. the key is lost; the password encrypting the key has been forgotten; court-authorized agents who otherwise would not have access to the cryptographic key). This could include: (1) retrieving an entity's long-term encryption key, which had been stored in a

secondary location (sometimes called "commercial key back-up" or "key escrow" depending on who controls the backed-up keys); (2) key encapsulation; or (3) key derivation techniques which allow for the confidential key to be regenerated from either end of the communication by the trusted third parties who provided the original mathematical elements used in generating the key.

Long-term encryption key: in public key cryptography, a long-term encryption key would be associated with an entity (e.g. an individual, agent, or automated process) for an extended period of time, perhaps one or two years. Posession of such a key enables access to all data encrypted with that key for the lifetime of its use. A long-term encryption key can be contrasted with a session key.

Plaintext: intelligible data.

Public key cryptography: a form of cryptography that utilizes a cryptographic algorithm which uses two related keys: a public key and a private key. The two keys have the property that, given the public key, it is computationally infeasible to derive the private key. Public key cryptography is also called "asymmetric cryptography." There are three broad functions of public key cryptography systems: (1) encryption/decryption; (2) digital signatures; and (3) key exchange. Some algorithms can perform all three functions and some can perform only one.

Public key infrastructure: a structure of hardware, software, people, processes and policies that employs digital signature technology to facilitate a verifiable association between the public component of an asymmetric public key and a specific end entity. The public key may be provided for digital signature use and/or for message encryption key exchange or negotiation.

Secret key cryptography: a form of cryptography which uses the same key to encrypt and decrypt. Also called "symmetric cryptography."

Session key: an encryption key which may be used for only a single session and then destroyed; sometimes called a "transaction key." For connection-oriented protocols (such as those in real-time communications), a session key is generally used only for the length that the connection is open (unless the connection time is long enough to warrant more than one session key). A new session key is generated for each new session (for example, each time one made a secure telephone call, a different session key would be generated). In many E-mail implementations which employ both public key cryptography and secret key cryptography, the term "session key" is sometimes used to describe the symmetric key that has been generated to encrypt that specific document. In this instance, the symmetric key would likely be encrypted with the recipient's public key to facilitate key exchange.

Trusted third parties (TTPs): security authorities or agents that are trusted with respect to some security-related activities; often the term is used to refer to a certification authority operated by someone other than the data owner.

References and Resources

Government of Canada Public Key Infrastructure
http://www.cse-cst.gc.ca/cse/english/gov.html

1997 OECD Guidelines on Cryptography Policy
http://www.oecd.org/dsti/sti/it/secur/index.htm