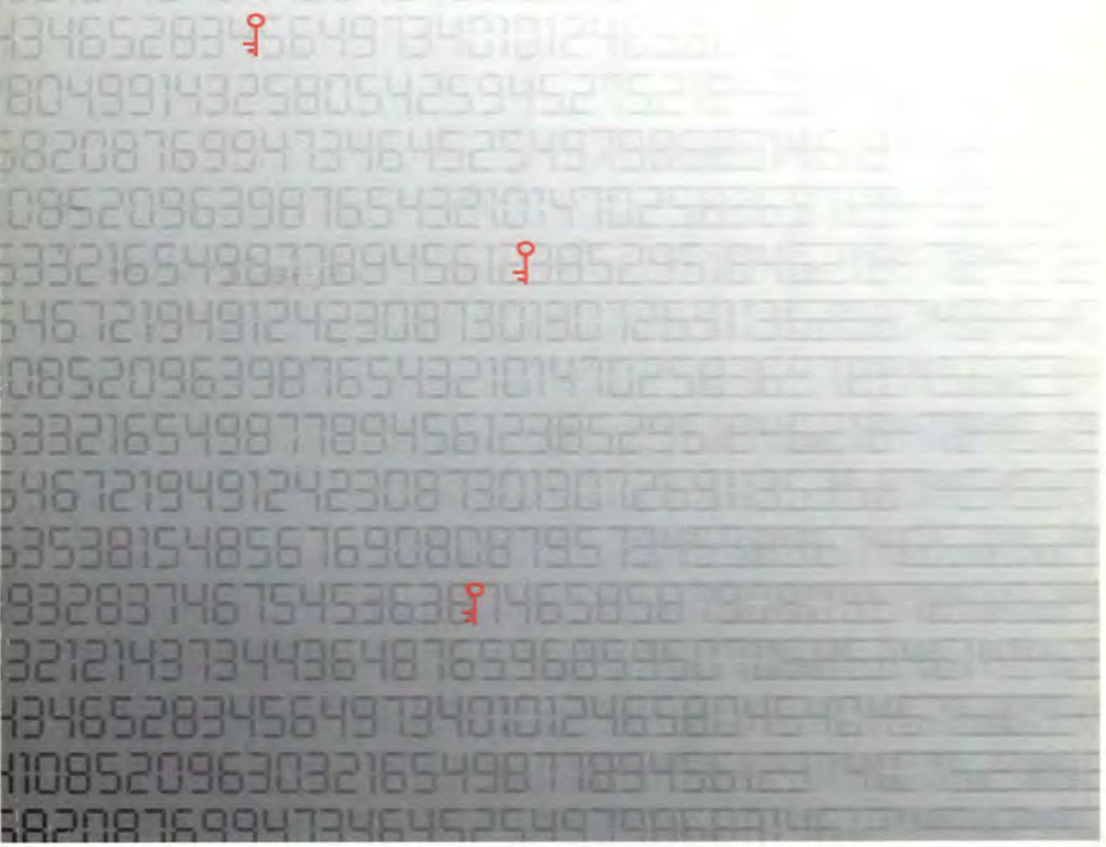
Gouvernement du Canada
Government of Canada

Politique cadre en matière de cryptographie aux fins du commerce électronique

Pour une économie et une société de l'information au Canada



Canada

Politique cadre en matière de cryptographie aux fins du commerce électronique

Pour une économie et une société de l'information au Canada

Groupe de travail sur le commerce électronique
Industrie Canada
Février 1998

Le document ***Politique cadre en matière de cryptographie aux fins du commerce électronique — Pour une économie et une société de l'information au Canada*** est également diffusé, dans les deux langues officielles, en version électronique sur *Strategis*, site Web d'Industrie Canada (*http://strategis.ic.gc.ca/crypto*).

Cette publication est aussi disponible sur demande dans une présentation adaptée a des besoins particuliers. Communiquer avec les Services de distribution aux numéros ci-dessous.

Pour obtenir des exemplaires du présent document de travail, veuillez vous adresser aux :

Services de distribution
Direction générale des communications
Industrie Canada
Bureau 205D, tour Ouest
235, rue Queen
Ottawa (Ontario) K1A 0H5

Téléphone : (613) 947-7466
Télécopieur : (613) 954-6436

Si vous souhaitez avoir des précisions sur le contenu du présent document de travail et sur le processus de consultation, ou soumettre vos commentaires, veuillez communiquer avec :

Helen McDonald
Directrice générale, Développement des politiques
Groupe de travail sur le commerce électronique
Industrie Canada
300, rue Slater, 20e étage
Ottawa (Ontario) K1A 0C8

Télécopieur : (613) 957-8837
Courrier électronique : crypto@ic.gc.ca

Vous avez jusqu'au 21 avril 1998 pour nous faire parvenir vos commentaires.

Deux semaines après cette date limite et durant une période d'un an, le public pourra consulter les commentaires durant les heures d'affaires, à l'adresse suivante :

Bibliothèque d'Industrie Canada
3e étage, tour Ouest
235, rue Queen
Ottawa (Ontario) K1A 0H5

et dans les bureaux régionaux d'Industrie Canada à Halifax, Montréal, Toronto, Edmonton et Vancouver.

Nota — Aux fins du présent document, la forme masculine disigne, s'il y a lieu, aussi bien les femmes que les hommes.

N° de catalogue C2-336/1-1998
ISBN 0-662-63406-3
51798B

Table des matières

Introduction : Pour une économie et une société de l'information au Canada

Un Canada branché

« Nous mettrons l'infrastructure de l'information et du savoir à la portée de tous les Canadiens d'ici l'an 2000, ce qui fera du Canada le pays le plus « branché » du monde... Un pays « branché », c'est beaucoup plus qu'un réseau de fils, de câbles et d'ordinateurs. C'est un pays où les citoyens ont accès aux compétences et aux connaissances dont ils ont besoin pour profiter de l'infrastructure du savoir et de l'information qui évolue si rapidement. C'est aussi un pays dont les citoyens sont reliés les uns aux autres. »

Discours du Trône,
23 septembre 1997.

La réussite du Canada au XXIe siècle sera largement fondée sur la capacité des Canadiens de participer pleinement à l'économie mondiale du savoir et d'en tirer parti. Or, nous ne saurions être assurés de cette réussite si nous ne travaillons pas collectivement — particuliers, secteur privé et tous les paliers de gouvernement — à doter le Canada d'une économie et d'une société de l'information. Pour sa part, le gouvernement du Canada s'est engagé à aider les Canadiens à avoir accès à l'information et aux connaissances qui leur permettront, à eux-mêmes, en tant qu'individus, ainsi qu'à leurs collectivités, à leurs entreprises et à leurs institutions de trouver de nouvelles possibilités d'apprendre, de nouer des liens, de faire des transactions et de développer leur potentiel social et économique.

Tel est l'objectif du raccordement des Canadiens à l'inforoute — leur faire découvrir un univers de possibilités économiques et sociales en tirant parti des nouvelles technologies, de l'infrastructure de l'information et du contenu multimédia pour favoriser le développement et la croissance des entreprises, créer des emplois novateurs, améliorer les communications des citoyens entre eux de même qu'avec leurs institutions et leurs services publics, et relier le Canada au monde entier.

Le commerce électronique, qui est au cœur de l'économie de l'information, se définit comme un ensemble de transactions et d'activités commerciales informatiques et électroniques comprenant, en règle générale, le traitement et la transmission de données et de renseignements numérisés. Ainsi, le commerce électronique peut comprendre l'échange de sommes importantes entre institutions financières, l'échange de données informatisées entre grossistes et détaillants, la conclusion de transactions bancaires par téléphone et l'achat de biens et services par Internet.

Pour que le commerce électronique se développe au Canada, il faut un

milieu stable, où les particuliers, les institutions et les entreprises se sentiront à l'aise, et en sécurité, un milieu dans lequel ils auront confiance. Il faut également, à l'échelle internationale, des règles permettant aux particuliers, aux institutions et aux entreprises d'échanger facilement des renseignements, des produits et des services d'un pays à l'autre, en toute sécurité et sans mauvaises surprises. Le présent document fait partie d'une série de documents sur le commerce électronique. Ceux-ci ont été produits dans le but de connaître votre avis sur le moyen d'établir des règles claires qui favoriseront l'essor du commerce électronique au Canada et l'édification, à l'échelle nationale, d'une économie et d'une société de l'information.

Pour une politique en matière de cryptographie au Canada

La cryptographie est importante pour l'essor du commerce électronique, car elle permet aux utilisateurs d'authentifier et de protéger des données de nature délicate comme les numéros de carte de crédit, les documents signés par voie électronique, le courrier électronique personnel et d'autres renseignements stockés dans des ordinateurs ou transmis par des réseaux fermés ou publics, comme Internet. La cryptographie peut également être utilisée dans un large éventail d'applications — depuis les communications protégées du gouvernement avec des particuliers jusqu'aux bases de données confidentielles des hôpitaux.

La cryptographie a des répercussions sur la façon de faire des affaires par voie électronique ainsi que sur la sécurité publique et la sécurité nationale. Elle permet de protéger les renseignements personnels ou de nature délicate ainsi que la propriété intellectuelle, de favoriser le commerce électronique et de prévenir le vol de données de nature délicate. Mais les éléments mêmes qui rendent la cryptographie attrayante pour des raisons de confidentialité, de concurrence, de droits de la personne et de sécurité commerciale peuvent aussi servir à masquer des activités qui constituent une menace pour la sécurité des Canadiens. Les criminels et les terroristes peuvent utiliser la cryptographie pour empêcher les organismes de sécurité et d'application de la loi dûment mandatés de recueillir certaines données. L'impossibilité d'avoir accès à des renseignements ou de les déchiffrer pourrait avoir de graves répercussions sur la prévention et la détection du crime ainsi que sur les enquêtes et les poursuites criminelles. La sécurité du public pourrait même en souffrir.

Le gouvernement du Canada s'est engagé à instaurer un climat et des conditions propices à l'essor du commerce électronique et à faire du Canada un chef de file mondial dans ce domaine d'ici l'an 2000. Il s'est également engagé à mener une campagne vigoureuse contre le crime organisé et le terrorisme et il a promis devant des tribunes internationales de le faire en collaboration avec d'autres

pays. Étant donné la nature mondiale et transnationale du commerce électronique et des menaces qui pèsent sur la sécurité publique, le Canada doit agir en tenant compte de facteurs nationaux et internationaux.

Les récents progrès relatifs aux produits cryptographiques et à leur utilisation (telle la croissance d'une industrie canadienne de la cryptographie) ainsi que les discussions internationales sur l'utilisation, le contrôle et l'interopérabilité du matériel de chiffrement ont incité le gouvernement du Canada à revoir sa politique en matière de cryptographie. Y ont aussi contribué le fait que l'on assiste à l'heure actuelle à la multiplication des transactions commerciales électroniques au Canada et dans le monde entier et à l'accroissement des communications électroniques transnationales dans le milieu criminel ou dans d'autres milieux dangereux.

Le présent document de discussion soulève une série de questions d'orientation relatives à l'utilisation de la cryptographie, questions sur lesquelles le gouvernement aimerait connaître votre avis. Que peuvent faire les pouvoirs publics pour accélérer la mise en place d'une infrastructure facilitant l'accès public à des services de cryptographie et à un commerce électronique sûr? Quels contrôles, le cas échéant, devrait-on mettre en place à l'intention des fabricants de produits de cryptographie et des fournisseurs de services qui vendent au Canada même, qui y importent ou qui y exportent ce type de produits? Quelles mesures, le cas échéant, devraient être adoptées relativement à l'utilisation de la cryptographie par les entreprises ou les particuliers au Canada? Comment maintenir la capacité d'appliquer la loi et de sauvegarder les intérêts en matière de sécurité nationale en vue de protéger le bien-être social et économique des Canadiens? Comment s'assurer que les solutions adoptées par le Canada correspondent au contexte mondial?

Vos commentaires sur les questions abordées dans ce document et sur toute autre question connexe sont importants. Vous pouvez les transmettre par écrit par courrier postal ou électronique ou par télécopieur avant le 21 avril 1998 au :

Président, Groupe de
travail interministériel sur la
politique en matière de
cryptographie
Élaboration des politiques
Groupe de travail sur le
commerce électronique
Industrie Canada
300, rue Slater, bureau 2063C
Ottawa (Ontario) K1A 0C8
Canada

Tél. : (613) 990-4244
Téléc. : (613) 957-8837
Courriel : **crypto@ic.gc.ca**

Partie 1 : La cryptographie et ses applications

La cryptographie, science qui a pour but de protéger le caractère confidentiel d'une information donnée, existe depuis des milliers d'années. Les méthodes cryptographiques modernes permettent le **chiffrement**, le **déchiffrement** et la **signature numérique**[1]. Le **chiffrement** garantit la confidentialité. Autrement dit, il protège l'information contre toute divulgation non autorisée ou toute visualisation par le brouillage mathématique du texte original. Les **signatures numériques**, analogues aux signatures manuscrites[2], remplissent trois autres fonctions :

- *authentification* — preuve que l'utilisateur est bien qui il prétend être ou que les ressources (p. ex., dispositif informatique, logiciel ou donnée) sont ce qu'elles sont censées être;
- *non-répudiation* — preuve que la transaction a eu lieu ou que le message a bien été envoyé ou reçu; ni l'émetteur ni le destinataire ne peuvent donc nier l'échange;
- *intégrité* — les données ne peuvent être modifiées sans que ce soit décelable.

La cryptographie assure ces fonctions à l'aide de clés numériques (combinaison unique de uns et de zéros) qu'un utilisateur peut employer pour chiffrer, déchiffrer et vérifier les données numériques. Grâce à la cryptographie, tout type d'information numérique — texte, données, voix ou images — peut être chiffré de sorte que seules les personnes détenant la bonne clé puissent le déchiffrer.

Il existe principalement deux méthodes cryptographiques. Dans le cas de la **cryptographie à clé secrète**, la même clé (ou une copie de cette clé) est utilisée pour chiffrer et déchiffrer les données. Dans le cas de la **cryptographie à clé publique**, il existe deux clés différentes, quoique connexes, et ce qui a été chiffré à l'aide de l'une ne peut être déchiffré qu'à l'aide de l'autre.

Sans la clé, les données codées pour des raisons de confidentialité ne

1. Les termes en caractères gras sont définis dans le glossaire, à la page 36.
2. Une signature numérique est un identifiant électronique créé par ordinateur et annexé à un document électronique. La signature numérique possède les mêmes propriétés que la signature manuscrite, mais il ne faudrait pas la confondre avec les reproductions électroniques d'une signature manuscrite comme celle qu'une personne appose au bas d'une lettre qu'elle envoie par télécopieur.

peuvent être transformées en un **texte clair**[3] compréhensible qu'en utilisant des techniques de « force brute », c'est-à-dire en essayant toutes les variantes possibles de la clé et en vérifiant si le texte clair qui en résulte a un sens. Toutes choses étant égales, la solidité du cryptogramme est proportionnelle à la longueur de la clé de chiffrement (ou la longueur en bits), qui détermine le nombre de permutations possibles. La solidité du cryptogramme double chaque fois que l'on ajoute un bit à la longueur de la clé. En juillet 1997, il a fallu 96 jours et 78 000 ordinateurs branchés sur Internet pour déchiffrer un message chiffré à l'aide du système de chiffrement symétrique DES (Data Encryption Standard), algorithme à clé secrète qui utilise une seule clé de 56 bits. On estime qu'il faudrait aux mêmes ressources informatiques 67 ans pour déchiffrer un algorithme à clé secrète utilisant une clé de 64 bits et bien plus de 13 milliards de fois l'âge de l'univers pour déchiffrer une clé de 128 bits. Naturellement, grâce aux connaissances d'experts, au matériel spécialisé et à d'énormes fonds, on peut accélérer quelque peu le processus. En 1993, un mathématicien canadien a proposé de concevoir une machine qui, selon lui, coûterait un million de dollars et serait capable de mener à bien une attaque en force contre une clé DES de 56 bits en trois heures et demie en moyenne[4]. Cependant, même avec ces ressources, il faudra au moins 10 ans pour déchiffrer une clé de 80 bits.

Cryptographie à clé secrète

La cryptographie à clé secrète peut être utilisée pour chiffrer des données, pour les stocker ensuite sur un support électronique (disquette ou disque dur) ou les transmettre à un proche associé. Toutefois, cette méthode est fort limitée en soi, car elle ne convient pas à la diffusion générale sur des réseaux publics entre utilisateurs qui ne se connaissent pas. Dans le cas de la cryptographie à clé secrète, les deux parties doivent au préalable se communiquer la clé unique qui sera utilisée aux fins du chiffrement et du déchiffrement. Si l'on a recours au chiffrement en raison de l'insécurité de la voie de communication (p. ex., un réseau informatique), il est évident qu'il ne faut pas transmettre la clé secrète par la même voie, car n'importe qui pourrait la copier et déchiffrer toutes les données. On reconnaît généralement que les principaux problèmes que rencontre la cryptographie à clé secrète sur les réseaux

3. Parfois, quand on fait référence à l'information originale, on parle de « texte clair » et, après chiffrement, on parle de « texte chiffré ». Le déchiffrement consiste à renverser le processus et à transformer le « texte chiffré » en « texte clair ». L'« algorithme cryptographique » (que l'on appelle parfois « chiffre ») est la fonction mathématique utilisée pour le chiffrement et le déchiffrement. En cryptographie, la sécurité est liée au fait que, même si l'algorithme est connu de tous, il existe des millions, voire des trillions de « clés » possibles qui auraient pu servir au chiffrement. Par exemple, si la longueur est de 56 bits, il existe environ 72 quadrillions de clés possibles.
4. Pour obtenir des précisions, voir M. J. Wiener « Efficient DES Key Search », TR-244, School of Computer Science, Carleton University, mai 1994; également dans *Proceedings*, Crypto '93, Springer-Verlag, 1993.

ouverts ont trait à la distribution des clés et à la variabilité dimensionnelle (la variabilité dimensionnelle recouvre non seulement la notion d'accroissement du nombre d'utilisateurs, mais aussi la notion selon laquelle les réseaux ouverts comprennent des entités de taille différente, allant des particuliers aux multinationales, ainsi que des transactions dont le volume et la valeur varient).

Cryptographie à clé publique

La cryptographie à clé publique offre cependant une solution à ces deux problèmes puisqu'elle prévoit l'utilisation d'une paire de clés différentes, quoique connexes. Chaque utilisateur détient une clé privée et une clé publique. La clé privée demeure confidentielle et n'est connue que de l'utilisateur; l'autre clé peut être rendue publique et être transmise à chaque correspondant par l'entremise du réseau ou mieux encore, publiée dans un annuaire sûr, qui est presque l'équivalent électronique d'un annuaire de téléphone. Pour utiliser ce système, l'émetteur chiffrerait un message à l'aide de la clé publique du destinataire, qui pourrait le déchiffrer uniquement à l'aide de sa clé privée. La cryptographie à clé publique permet donc la transmission de données en toute sécurité sur des réseaux ouverts, comme Internet, sans qu'il soit nécessaire d'échanger une clé secrète au préalable. Les parties qui ne se connaissent pas peuvent ainsi échanger et authentifier des informations et mener des affaires en toute sécurité.

Outre la capacité de chiffrer les données pour protéger leur caractère confidentiel, certaines formes de cryptographie à clé publique permettent également aux détenteurs de la clé d'authentifier par la suite leurs documents à l'aide d'une clé privée qui crée une signature numérique[5]. Cette technique garantit également l'intégrité des documents et permet aux destinataires de déterminer rapidement si un message a été modifié de quelque façon que ce soit pendant la transmission.

Bien que la cryptographie à clé publique comporte des avantages certains par rapport à la cryptographie à clé secrète en ce qui a trait à l'utilisation sur des réseaux publics ouverts, la cryptographie à clé secrète possède ses propres qualités qui sont indispensables pour une variété d'applications[6]. Les cryptographies à clé publique et à clé secrète seront utilisées conjointement pour protéger des informations sensibles stockées

5. L'émetteur « signe » un message à l'aide de la clé privée. La signature se fait par l'application d'un algorithme de chiffrement au message lui-même ou à un petit bloc de données lié d'une certaine façon au message (p. ex., un « résumé du message » qui est une valeur unique générée par la compression à sens unique des données).
6. En général, la cryptographie à clé secrète est plus rapide que la cryptographie à clé publique. La méthode courante consiste donc à tirer parti de cet avantage en employant la cryptographie à clé secrète pour chiffrer un document et en utilisant par la suite la cryptographie à clé publique pour chiffrer uniquement la clé secrète.

dans les ordinateurs et transmises par l'intermédiaire de réseaux de communication.

Autorités de certification

Si la cryptographie à clé publique doit fonctionner à grande échelle aux fins du commerce électronique, l'un des principaux problèmes à résoudre concerne la distribution des clés publiques. Certains logiciels, comme le PGP (« Pretty Good Privacy »), qui est facilement accessible sur Internet, obligent les utilisateurs à distribuer leur clé publique à d'autres utilisateurs, approche qui fonctionne bien dans de petits groupes fermés[7]. Toutefois, un annuaire sûr et accessible est indispensable à la distribution de clés publiques à grande échelle — notamment quand elles sont associées à des procédures visant à assurer que telle clé publique appartient vraiment à tel utilisateur.

Pour y parvenir, on peut entre autres avoir recours à une **autorité de certification**, un agent de confiance qui gère la distribution des clés publiques ou des **certificats** contenant ces clés[8]. Parfois, l'expression « **tiers de confiance** » est employée comme synonyme d'autorité de certification, mais les deux expressions ne sont pas toujours utilisées tout à fait dans le même sens[9].

Un « certificat » est un formulaire électronique (semblable à la version électronique d'un permis de conduire, d'un passeport ou d'une carte de location de vidéocassettes) renfermant la clé publique du détenteur de la clé et certains renseignements signalétiques qui confirment que le détenteur de la clé et l'émetteur du certificat (autorité de certification) sont bien qui ils prétendent être.

L'un des principaux avantages du recours à un agent de confiance auxiliaire est que ce dernier décharge les particuliers de la distribution des clés et de la gestion d'un grand nombre de relations[10] dans un environnement complexe à niveaux de sécurité multiples (la relation de sécurité qu'une personne établit avec une banque ou un hôpital sera différente de celle qu'elle établira avec une connaissance ou une librairie en direct). Il ne s'agit toutefois pas simplement d'une question de commodité ou d'efficacité. En signant le certificat à l'aide de sa clé, l'autorité de certification, « relie » l'identité du détenteur de clé à un certificat renfermant la clé publique, assurant

7. Cette approche est satisfaisante si une personne peut échanger sa clé publique directement avec un ami ou un proche associé. La confiance commence à s'estomper lorsque les clés publiques sont échangées avec des amis d'amis. Par exemple, certaines personnes joignent en annexe à leur message électronique une copie de leur clé publique qu'ils affichent dans une tribune publique, comme les groupes de discussion USENET. Tout se gâte cependant si, disons, Virginie, se faisant passer pour Alice, affiche un message dans une tribune publique et joint sa propre clé publique; tous les messages destinés à Alice sont alors par la suite chiffrés avec la clé de Virginie.
8. Les expressions « autorité de certification » ou « infrastructure auxiliaire » seront utilisées tout au long du document. Lorsqu'on établit des autorités de certification dans une hiérarchie ou qu'on relie ces autorités avec d'autres avec lesquelles il y a eu certification réciproque, on parle d'Infrastructure à clé publique (ICP).
9. Certains auteurs affirment que l'expression « autorité de certification » est plus générale et qu'un « tiers de confiance » est une autorité de certification à laquelle s'appliquent des dispositions particulières à des fins d'accès légitime. Le document de consultation publique du Royaume-Uni définit un « tiers de confiance » comme une entité à laquelle d'autres entités font confiance en ce qui a trait aux services et aux activités liés à la sécurité. (*Licensing of Trusted Third Parties for the Provision of Encryption Services*, Department of Trade and Industry, Royaume-Uni, ***http://www.dti.gov.uk/pubs/pubs/index.html***). La définition du Royaume-Uni souligne l'aspect « tiers » du concept, ce qui a amené certains auteurs à laisser entendre qu'une autorité de certification établie par une société à ses fins d'utilisation personnelle n'était pas un « tiers de confiance ».
10. Tout utilisateur entretiendra probablement des centaines, voire des milliers de relations dont le niveau de sécurité requis variera; en conséquence, ce qu'il faut, c'est une liste de toutes les personnes avec lesquelles un utilisateur désirera peut-être communiquer ou faire affaire, en quelque sorte, un genre d'annuaire téléphonique.

ainsi l'authentification[11] et la non-répudiation, dans le but de préserver la confiance dans le système.

Étant donné les différences entre les fonctions de signature numérique (authentification, non-répudiation et intégrité) et la fonction de chiffrement (confidentialité), de nombreux systèmes cryptographiques requièrent deux paires de clés : une paire pour les signatures numériques et l'autre pour assurer le chiffrement pour des raisons de confidentialité. Faute d'infrastructure auxiliaire des autorités de certification, l'utilisateur doit générer les paires de clés publique et privée pour les signatures numériques et la confidentialité. Avec une infrastructure auxiliaire, il existe différentes options.

Les paires de clé requises pour les signatures numériques devraient être générées par l'application de l'utilisateur et la clé publique devrait être signée par l'autorité de certification et distribuée aux fins d'utilisation. Pour limiter le risque de fraude, la clé de signature privée ne devrait jamais quitter l'application de l'utilisateur.

Souvent, la paire de clés requises aux fins de confidentialité est générée par l'autorité de certification, qui doit posséder une copie de sauvegarde, de façon à ce qu'on puisse récupérer les données chiffrées en cas de perte de la clé privée ou d'atteinte à son intégrité.

La réalisation d'une copie de sauvegarde de la clé secrète (que l'on appelle également archivage des clés)[12] est l'une des nombreuses méthodes dont on dispose pour assurer un accès légitime au texte clair. Mentionnons également comme méthodes d'accès ou de « **récupération des clés** », **l'encapsulage de la clé** (par exemple, une **clé de session** ou une **clé de chiffrement de longue durée** est elle-même chiffrée à l'aide de la clé publique d'un agent de récupération des clés) ou des techniques de dérivation des clés (par exemple, l'approche proposée au Royal Holloway College[13] de Londres, qui permet la régénération de la clé secrète à l'une des extrémités de la communication avec les tiers de confiance ayant fourni au départ les éléments mathématiques utilisés pour générer la clé).

11. Étant donné que le certificat dans son ensemble constitue un document électronique qui a été signé de façon numérique par l'autorité de certification (par exemple un résumé du message du certificat est chiffré à l'aide de la clé privée de l'autorité de certification), aucun changement non autorisé ne peut être apporté au certificat sans que la modification ne soit décelée (c'est-à-dire que toute modification engendrerait une valeur de hachage différente).
12. L'« archivage des clés » est une expression générale désignant l'entreposage d'une copie de sauvegarde des clés de chiffrement (ou de parties de clé lorsque chaque clé de chiffrement est divisée et détenue par plus d'une entité). Entre autres méthodes d'archivage des clés, mentionnons l'entiercement des clés, qui consiste à entreposer les clés ou des parties de clé directement chez un ou plusieurs dépositaires légaux (c'est-à-dire une entité autre que le propriétaire de la clé). Selon le modèle, le dépositaire pourrait être un fournisseur de services du secteur privé ou un organisme public.
13. Nigel Jeffries, Chris Mitchell et Michael Walker. *Combining TTP-Based Key Management with Key Escrow*, Information Security Group, Royal Holloway College, University of London, 19 avril 1996.

Partie 2 : La politique actuelle en matière de cryptographie au Canada

Par le passé, la cryptographie était presque exclusivement la chasse gardée des gouvernements. Elle était employée afin de protéger les secrets militaires ou diplomatiques et était généralement intégrée au matériel. La politique cadre actuelle du Canada a été instaurée dans ce contexte et c'est pourquoi elle se limite à des contrôles d'exportation de cryptographie.

Le Canada est l'un des 33 pays signataires d'une entente (l'Arrangement de Wassenaar)[14], qui exige le contrôle des exportations d'une longue liste de « marchandises à double usage »[15], y compris la cryptographie. Le Canada a tenu compte de cet arrangement dans son régime national[16], qui limite l'exportation de matériel ou de logiciels de chiffrement personnalisés. Le règlement canadien sur le contrôle des exportations est destiné à empêcher la circulation de certains produits susceptibles de nuire aux intérêts stratégiques du Canada ou de ses alliés.

Jusqu'à tout récemment, les produits matériels ou logiciels de chiffrement personnalisés à clé de 40 bits ou moins pouvaient être exportés. Les institutions bancaires et financières étaient autorisées à exporter des produits DES de 56 bits. Le 24 décembre 1996, le Canada a modifié sa politique pour une période d'essai de 12 mois, et autorisé l'exportation, vers la plupart des pays, de logiciels de chiffrement personnalisés de 56 bits et de matériel comportant un logiciel de chiffrement. Cette période a été prolongée jusqu'au 30 juin 1998.

Le Canada ne limite pas l'exportation de produits de signature numérique et, à l'instar de la plupart des signataires de l'Arrangement de Wassenaar, il permet l'exportation de logiciels à grande diffusion ou de logiciels du domaine public utilisés à des fins

14. Les lignes directrices du Canada portant sur le contrôle des exportations ont été adoptées sous la forme d'un régime national conforme aux obligations internationales du Canada précisées par le Comité de coordination du contrôle des échanges stratégiques (COCOM), dont le Canada est membre depuis 1950. Le COCOM avait au départ pour mandat de préserver la supériorité technologique de l'Occident en réduisant l'exportation des technologies militaires, nucléaires et à double usage des nations industrielles occidentales vers l'Union soviétique et d'autres pays communistes. Le COCOM a été aboli le 31 mars 1994 et remplacé par une entente modifiée. L'Arrangement de Wassenaar relatif au contrôle multilatéral des exportations pour les armes conventionnelles et les marchandises et technologies à double usage (d'après la ville du même nom située à proximité de La Haye), où cinq séries de négociations ont eu lieu entre 1993 et 1995, vise à fournir un cadre permettant de faire échec aux nouvelles menaces à la sécurité dans le monde de l'après-guerre froide.

15. Les produits à double usage ont des applications militaires et civiles.

16. Les pouvoirs légaux ont été conférés en vertu de la *Loi sur les licences d'exportation et d'importation* de 1947. L'alinéa 3d) de la Loi, « mettre en œuvre un accord ou un engagement intergouvernemental », est invoqué afin d'ajouter des articles à la Liste des marchandises d'exportation contrôlée, qui est un règlement. L'Arrangement de Wassenaar, y compris les articles sur la cryptographie, constitue l'« accord intergouvernemental » en question mis en œuvre en vertu de la Loi susmentionnée.

de chiffrement[17], de n'importe quelle puissance. Le Canada autorise l'exportation vers les États-Unis de toute quantité de logiciels de chiffrement personnalisés ou de matériel comportant un logiciel de chiffrement intégré (comme le font les États-Unis à l'égard du Canada), et aucune licence d'exportation n'est requise.

Il n'existe, au Canada, aucun obstacle à l'importation ou à l'utilisation de produits cryptographiques. Les particuliers et les entreprises y sont libres d'utiliser et de vendre des logiciels de chiffrement de n'importe quelle puissance. L'exportation de produits cryptographiques aux fins d'utilisation par des citoyens canadiens ou des firmes canadiennes à l'étranger, quoique contrôlée, est habituellement autorisée.

Pour une nouvelle politique en matière de chiffrement

Compte tenu des changements dans l'offre et la demande mondiales de produits cryptographiques, il est impératif de revoir la politique. Aujourd'hui, les entreprises et les particuliers utilisent de plus en plus de produits cryptographiques puissants qu'on peut se procurer sous forme de logiciels scellés à grande diffusion ou de logiciels du domaine public offerts sur Internet. La demande mondiale de produits cryptographiques augmente, et de nombreux pays commencent à en concevoir et à en fabriquer. Simultanément, les autorités policières et les services de sécurité nationale s'inquiètent des profondes répercussions qu'aura, sur leurs enquêtes, l'utilisation généralisée de produits de chiffrement puissants leur interdisant toute forme d'accès. Nombreux sont les pays qui revoient leur politique en matière de cryptographie à la lumière de ces pressions et du rôle de ces technologies dans le commerce électronique.

Devant ces pressions, le gouvernement fédéral a demandé au Comité consultatif canadien sur l'autoroute de l'information (CCAI) de lui fournir un avis sur les mesures requises afin de satisfaire aux exigences en matière de sécurité propres au commerce électronique.

Dans son rapport de septembre 1995[18], le Comité a vu le besoin d'adopter une technologie et une structure juridique garantissant la protection et la confidentialité des renseignements personnels, financiers et sensibles, qu'ils soient conservés dans des bases

17. La note générale sur les logiciels, formulée en vertu du COCOM dans les années 1980, est intégrée à la liste de contrôle de l'Arrangement de Wassenaar, bien qu'elle ait pour but d'exclure certains articles de l'Arrangement (c'est-à-dire les soustraire aux contrôles). L'effet de cette note, en ce qui a trait à la cryptographie, est d'exclure des contrôles tous les logiciels de grande diffusion et du domaine public, seule l'exportation d'applications logicielles personnalisées et de matériel étant sujette au contrôle. Certains analystes affirment que la Note a été formulée à une époque où peu de gens avaient conscience du rôle prépondérant que joueraient les logiciels de cryptographie de masse ou du domaine public. Cinq pays, dont les États-Unis et le Royaume-Uni, dérogent à la Note et contrôlent l'exportation de ces logiciels.

18. *Contact, Communauté, Contenu : Le défi de l'autoroute de l'information*. Rapport du Comité consultatif sur l'autoroute de l'information, septembre 1995. Disponible à l'adresse suivante : (**http://strategis.ic.gc.ca/CCAI**).

de données ou transmis par des réseaux publics. Le Comité a demandé :

- la tenue de consultations publiques, afin de déterminer la meilleure façon de concilier l'utilisation et la circulation légitimes de données, la protection des renseignements personnels, les droits civils, les droits de la personne, l'application de la loi et les intérêts en matière de sécurité nationale dans une politique sur la sécurité nationale;
- un niveau de sécurité de base sur l'autoroute de l'information qui garantisse l'intégrité et l'authentification des messages, ainsi que des mesures raisonnables quant à la protection des communications à caractère privé et à la protection des renseignements personnels;
- un examen public des algorithmes et des normes de chiffrement, et la liberté de les choisir;
- un partenariat entre le gouvernement fédéral, les provinces et territoires, le secteur privé et d'autres intervenants afin d'établir des normes de sécurité acceptables pour tous et d'essayer de les faire reconnaître au Canada et à l'étranger par les partenaires commerciaux du Canada;
- un rôle de premier plan pour le gouvernement fédéral, qui mettra au point des services assurant la protection des renseignements personnels, leur intégrité et leur authentification sur l'autoroute de l'information, en créant une infrastructure à clé publique uniforme répondant à ses besoins.

Le gouvernement fédéral a donné sa réponse initiale en mai 1996 dans un rapport intitulé *La société canadienne à l'ère de l'information : Pour entrer de plain-pied dans le XXIe siècle*[19]. Il y souligne l'importance du commerce électronique, moyen qu'il préfère entre tous pour faire des affaires, à l'interne et à l'extérieur. Il s'y engage également à travailler en étroite collaboration avec le secteur privé, les autres pouvoirs publics et d'autres intervenants afin d'élaborer et de mettre en œuvre des politiques, des normes et des protocoles en vue de la création d'un système de commerce électronique étendu et fonctionnant sans accroc.

19. La version intégrale du rapport peut être consultée à l'adresse suivante : (*http://strategis.ic.gc.ca/CCAI*).

Infrastructure à clé publique du gouvernement du Canada

L'Infrastructure à clé publique (ICP) du gouvernement du Canada[20] est au centre de cette initiative. En effet, c'est elle qui servirait de base à l'utilisation des signatures numériques et au déroulement sécuritaire des transactions électroniques internes et externes. Plusieurs ministères et organismes gouvernementaux participent activement à la mise au point de l'ICP et à l'implantation de ses technologies de base. Chaque ministère utilise les technologies de l'ICP et établit des autorités de certification afin d'assurer la protection de ses fichiers et de ses communications par réseau aux fins d'applications commerciales électroniques telles que le courrier électronique, l'échange de données, l'accès aux bases de données et les interactions sur le Web. L'ICP du gouvernement du Canada sera entièrement opérationnelle à la fin de 1998.

Cette ICP reliera le secteur privé et les ICP institutionnelles adhérant aux mêmes normes de protection des renseignements personnels, d'intégrité et de sécurité, afin d'assurer aux Canadiens des transactions électroniques sûres, faciles et ininterrompues. La meilleure façon d'y parvenir consistera à travailler en partenariat avec l'industrie et d'autres paliers de gouvernement, et à respecter les normes et pratiques reconnues à l'échelle internationale.

Si l'on veut que l'ICP remplisse ses fonctions tant pour le gouvernement fédéral que pour les particuliers qui veulent accéder aux services fédéraux, il faut instaurer un cadre juridique qui régira les signatures numériques. Le gouvernement examine les modifications qu'il faudra apporter à la législation fédérale pour reconnaître l'utilisation des signatures numériques et des dossiers électroniques et lever les obstacles juridiques à la prestation de services électroniques.

Examen de la politique canadienne en matière de chiffrement

Le gouvernement est en train d'examiner la politique en matière de cryptographie en vigueur au Canada et surtout la question du chiffrement aux fins de confidentialité. Les observations du public au sujet du présent document de discussion seront donc du plus haut intérêt pour l'orientation de cet examen.

---

20. *Livre blanc sur l'Infrastructure à clé publique du gouvernement du Canada*, Centre de la sécurité des télécommunications, mai 1997 (**http://www.cse-cst.gc.ca/cse/francais/gov.html**).

Le gouvernement s'engage à élaborer un cadre stratégique harmonieux, conforme aux lignes directrices de l'OCDE régissant la politique de cryptographie[21], qui protège l'information vitale de nature économique et financière détenue par le secteur privé canadien, assure la protection des renseignements personnels et la liberté d'expression, et préserve la sécurité publique et la sécurité nationale.

La version révisée de la politique en matière de cryptographie devrait en particulier :

- permettre de bénéficier des avantages économiques et sociaux qui découleront d'un commerce électronique mondial devenu plus sûr grâce à la cryptographie;
- donner aux entreprises et au public confiance dans les autorités de certification, les autres fournisseurs de services cryptographiques et les fournisseurs de produits cryptographiques au Canada;
- résoudre les problèmes posés par la demande d'accès légitime aux communications chiffrées en temps réel et aux données chiffrées stockées;
- résoudre le problème auquel se heurtent les organismes nationaux de sécurité chargés de la collecte de données, en raison de la diffusion internationale de produits de cryptographie puissants.

Les sections qui suivent présentent les principaux facteurs dont il faudra tenir compte dans l'élaboration de la nouvelle politique. Sont ensuite exposées trois séries de solutions aux fins d'évaluation et de commentaires.

21. Le Canada a participé en 1997 à l'élaboration des lignes directrices de l'OCDE régissant la politique de cryptographie (***http://www.oecd.org/dsti/sti/it/secur/index.htm***). Il s'agit d'une série de huit principes dont les pays devraient tenir compte en élaborant leur cadre stratégique.

Partie 3 : Facteurs dont le Canada devra tenir compte dans sa politique en matière de cryptographie

Dans l'élaboration d'une politique harmonieuse en matière de chiffrement, le Canada, à l'instar de nombreux pays, est confronté à la difficulté suivante : trouver un juste équilibre entre les questions fondamentales liées à la protection des renseignements personnels, aux droits individuels et aux intérêts commerciaux et l'obligation de l'État de se donner les moyens de se protéger et de protéger ses citoyens contre les diverses menaces pesant sur la sécurité publique.

Il est possible de satisfaire aux exigences relatives à la protection des renseignements personnels et au commerce électronique de plusieurs façons tout en permettant, à différents degrés, un accès légitime à l'information ou aux communications aux fins de sécurité, d'application de la loi et de réglementation. Chaque solution exige de la part de tous les intervenants des compromis, qui supposent tous des sacrifices, même si le prix à payer diffère selon la solution envisagée[22]. Si la nécessité de concilier les intérêts commerciaux, la protection des renseignements personnels et l'accès légitime de la société et de ses membres n'est pas nouvelle, elle a pris une nouvelle dimension aujourd'hui, en raison de la récente évolution technologique et de ses répercussions actuelles ou futures sur les activités légitimes et illégitimes. Au nombre des changements importants, mentionnons les suivants :

- le recours à la cryptographie robuste augmente, étant donné qu'il devient facile de trouver des logiciels de chiffrement et des ordinateurs capables de chiffrer et déchiffrer les données facilement;
- le recours aux moyens de télécommunications se prêtant au chiffrement (courrier électronique et autres données transmises par Internet ou d'autres supports informatiques) augmente rapidement en tant que moyen de communication personnelle et moyen de communication

22. Chaque solution fait appel à une série différente d'éléments techniques et opérationnels, a des répercussions juridiques et des conséquences sur les coûts et comporte des dimensions difficiles à évaluer, comme la sécurité publique, la souveraineté et les libertés civiles. Aucune solution ne peut garantir pleinement l'accès légitime, bien que certaines puissent le faire mieux que d'autres.

commerciale sous de nombreuses formes;

- l'utilisation accrue de téléphones cellulaires a incité à mettre au point du matériel numérique et a mené au chiffrement de leurs signaux dans certains cas;
- le recours accru aux ordinateurs et aux réseaux informatiques dans le cadre d'activités commerciales, et le besoin de protéger les renseignements personnels et d'assurer la sécurité ont amené les entreprises à stocker les documents commerciaux dans des installations informatiques sûres ou sous une forme chiffrée.

Pour élaborer une politique harmonieuse, le Canada devra tenir compte des facteurs analysés ci-dessous. D'autres pays industrialisés doivent composer avec les mêmes facteurs. Leur évaluation de ces facteurs et les politiques qu'ils adopteront en fin de compte revêtiront également une importance capitale pour le Canada, puisque nombre des applications pratiques de la cryptographie concernent des communications transnationales.

Commerce électronique

Étant donné qu'un nombre croissant de transactions se font non plus sur des réseaux fermés mais sur des réseaux ouverts[23], la cryptographie devient indispensable au commerce électronique. Par le passé, le commerce électronique, comme l'échange de données informatisées ou le transfert électronique de fonds, s'effectuait en grande partie sur des réseaux fermés. Dans le contexte commercial mondial, on ne pourra tirer pleinement parti du commerce électronique que si l'on passe à des réseaux ouverts.

Toutefois, les réseaux ouverts posent divers problèmes de sécurité, y compris en ce qui concerne l'authentification des parties qui communiquent, l'intégrité des données communiquées, la confidentialité des renseignements exclusifs ou personnels et l'assurance que les transactions ont été autorisées par les utilisateurs légitimes. Sans la cryptographie pour assurer la fiabilité des signatures numériques et des services de protection de la confidentialité offerts de façon conviviale et rentable, on risque de ne pouvoir régler ces problèmes.

23. Un réseau fermé relie des utilisateurs qui entretiennent déjà une relation contractuelle et se font mutuellement confiance, comme les clients et les employés d'une banque. Souvent, le système fermé utilisait divers moyens techniques; par exemple, les parties employaient le chiffrement de bout en bout sur des lignes privées. Par comparaison, Internet constitue l'exemple le plus connu de réseau ouvert. Il s'agit d'un vaste réseau interconnecté composé de milliers de réseaux (chacun d'entre eux ayant ses propres formes d'administration qui créent un environnement complexe allant de la quasi-anarchie jusqu'aux multiples politiques de sécurité commerciale, en passant par les services communautaires coopératifs).

Dans l'univers des réseaux ouverts et dans un environnement de plus en plus caractérisé par l'incertitude et la concurrence économique mondiale, le chiffrement robuste permet aux sociétés de se protéger contre la collecte de renseignements touchant la concurrence et contre les menaces criminelles; elle leur permet aussi de protéger l'information et les communications sensibles, entre autres, dans les cas suivants :

- Les entreprises commencent à utiliser Internet pour communiquer et accéder aux banques d'information commerciales. Les gens d'affaires en déplacement ainsi que les télétravailleurs doivent souvent échanger avec leur établissement d'appartenance des informations sensibles — renseignements commerciaux, information sur les soumissions et stratégies de marketing. Le chiffrement permet de s'assurer que seuls les utilisateurs autorisés ont accès aux données; il permet aussi de protéger l'information sensible contre toute consultation non autorisée ou utilisation malveillante.
- Le chiffrement permet la protection des communications nécessaires aux organisations virtuelles et aux partenariats stratégiques. La plupart des entreprises d'aujourd'hui comptent des bureaux responsables de la recherche-développement, de la production et des ventes dans diverses localités du pays ou à l'étranger. Dans certains cas, des partenaires occasionels ont accès à des bases de données internes dans le cadre de coentreprises tout en étant des concurrents dans d'autres occasions. Il convient désormais de protéger un large éventail de propriété intellectuelle, comme les secrets commerciaux, les avant-projets, les dessins et les documents d'exploitation qui, jamais auparavant, n'ont été transmis via des réseaux ouverts.
- Il devient de plus en plus fréquent de mettre directement à la disposition des consommateurs, par l'intermédiaire de réseaux ouverts, des informations et des produits culturels ainsi que des logiciels. La télévision par satellite et la télévision payante sont deux exemples de recours au chiffrement pour protéger la propriété intellectuelle contre toute utilisation frauduleuse.
- Pour que les transactions puissent se faire en direct, il faut gagner la confiance du consommateur. Celui-ci ne sera disposé à effectuer des achats via Internet que s'il a la certitude que ses transactions sont protégées. Le chiffrement constitue l'un des moyens d'assurer la confidentialité des numéros de carte de crédit et d'autres renseignements personnels. Les lois sur la protection des données qui obligent les utilisateurs de données à protéger la confidentialité encourageront davantage le recours au chiffrement.

- Étant donné que les gouvernements optent de plus en plus pour la prestation de services par des tiers ou en direct, les citoyens voudront de plus en plus avoir l'assurance que toute information sensible, comme les renseignements sur l'emploi et le revenu, les renseignements médicaux et autres, sont protégés au maximum.

Différents types de transactions requièrent différentes catégories de solutions afin de satisfaire à ces exigences. Certaines entreprises protégeront leurs communications internes entre succursales en établissant des réseaux privés virtuels ou en utilisant des machines à chiffrer afin de garantir la sécurité de la transmission de données par Internet. D'autres organisations, depuis les multinationales jusqu'aux entreprises de taille moyenne, peuvent établir leurs propres autorités de certification afin de satisfaire les exigences cryptographiques en vue d'un commerce électronique sûr par courrier électronique et d'un large éventail d'applications nécessitant des services d'autorisation, d'authentification et d'intégrité. Les banques qui établissent leurs propres autorités de certification pour permettre le télépaiement par Internet ou encore les institutions financières qui ont mis en œuvre le protocole de la transaction électronique sécuritaire (protocole SET) pour les transactions par carte de crédit ont été les premières à adopter les méthodes cryptographiques. D'autres entreprises peuvent choisir de s'adresser à des fournisseurs de services cryptographiques qui offrent une série de services reposant sur des certificats à l'appui d'un large éventail de fonctions d'authentification, de non-répudiation, d'intégrité et de confidentialité. En fait, les autorités de certification qui offrent des services aux entreprises sont déjà à l'œuvre au Canada et ailleurs.

Chacun de ces modes de prestation de services de sécurité reposant sur la cryptographie soulève une série de questions, non seulement sur le plan commercial mais aussi en ce qui a trait à l'accès légitime. On s'interroge, entre autres, sur les points suivants :

- la nature des clés employées (clés de session jetables pour les données en transit qui sont effacées après leur utilisation ou clés d'encapsulage de longue durée);
- le contrôle des clés cryptographiques à chaque étape de leur cycle de vie, en commençant par la génération de clés jusqu'à leur archivage ou leur destruction (est-il exercé par le propriétaire de données ou par un agent de confiance autre que le propriétaire?);
- les différences entre le chiffrement de données stockées et le chiffrement de communications en temps réel.

Les entreprises doivent évaluer l'importance de leurs fonds d'information, la valeur qu'elles y attachent, ainsi que leurs capacités et leurs ressources en ce qui a trait à la

technologie de l'information. Étant donné la diversité des scénarios possibles, il existe une demande expresse en faveur de la liberté de choix des algorithmes, de la sélection de normes et de la mise en œuvre. La confiance dans la technologie et l'infrastructure est essentielle à l'essor commercial.

Pour faciliter le commerce électronique à l'échelle mondiale, l'infrastructure auxiliaire, y compris les procédures et les composantes physiques, devrait être conçue de façon à assurer l'interopérabilité entre les utilisateurs desservis par les autorités de certification de pays différents ayant des politiques nationales différentes. Les politiques nationales en matière de cryptographie visent à instaurer un certain degré de confiance parmi les utilisateurs et fournisseurs de services d'un pays. L'interopérabilité requiert toutefois une certaine forme d'uniformisation entre les politiques de chaque pays. Les organisations commerciales internationales demandent sans cesse que la mise en œuvre de la politique nationale d'un pays n'entrave pas l'interopérabilité et n'entame pas la confiance dans l'infrastructure d'un autre pays.

À l'intérieur des frontières nationales, il existe de toute évidence des domaines où il semble possible de parvenir à un consensus et d'autres où il subsiste des problèmes. Par exemple, on reconnaît la nécessité pour les entreprises de disposer d'une copie de sauvegarde de la clé de chiffrement privée. Les clés de sauvegarde devraient être utilisées quand un employé oublie le mot de passe qui lui donne accès à sa clé privée, en cas de défaillance technologique ou encore si le détenteur de la clé ne travaille plus pour l'entreprise. La décision d'utiliser une copie de sauvegarde de la clé est prise par le propriétaire de données, c'est-à-dire l'entreprise plutôt que l'employé. Il importe de concevoir les mécanismes de sauvegarde des clés de façon à ne pas diminuer la protection cryptographique offerte.

Bien qu'une analyse de rentabilisation ait été effectuée pour la récupération des données stockées, la récupération des clés en vue de communications chiffrées en temps réel (p. ex., appels téléphoniques, sessions en temps réel entre deux ordinateurs sur un réseau et application à distance ou accès à une base de données) n'est pas nécessaire dans une même mesure sur le plan commercial. Dans les sessions

en temps réel, les parties à la communication ont déjà déchiffré la voix ou les données à chaque extrémité. Si une session chiffrée tourne mal, la personne rappelle tout simplement, et établit une nouvelle session chiffrée. Il n'est pas nécessaire de récupérer les clés dans ce cas[24]. Bien que certaines entreprises aient peut-être besoin de générer une vérification à rebours des transactions en temps réel, ces fonctions devraient logiquement être introduites avant le cryptage plutôt qu'après. Diverses institutions financières qui emploient couramment le chiffrement ont également besoin d'importantes fonctions de vérification. Il apparaît cependant que peu d'entre elles ont mis en œuvre des procédures de récupération des clés pour les données en transit.

Il est clair que les organismes d'application de la loi et les entreprises visent des objectifs identiques, soit que la cryptographie protège les renseignements exclusifs et les secrets commerciaux et contribue en général à protéger l'industrie et les consommateurs contre la fraude et d'autres activités illicites. Par ailleurs, la cryptographie satisfait aux objectifs en matière de sécurité nationale, dans la mesure où elle permet de protéger la souveraineté, les infrastructures nationales et les précieuses données qu'elles contiennent.

En tant qu'outil favorisant le commerce électronique, la cryptographie accroît la compétitivité des entreprises et stimule la création d'emplois et la croissance industrielle. Des politiques gouvernementales qui encouragent l'innovation et la normalisation faciliteront la mise au point d'infrastructures et de produits rentables et conviviaux en plus d'aider à répandre le commerce électronique. Des mesures réglementaires risquent de freiner l'évolution du marché des services et des produits issus de la technologie de l'information, et de créer des obstacles au commerce international. Si les mesures de contrôle réglementaire peuvent rendre le recours à la cryptographie plus difficile pour les criminels, la mise en œuvre des systèmes peut également se révéler fort coûteuse pour le gouvernement et le secteur privé. En bout de ligne, il est d'ailleurs possible qu'on ne parvienne pas à empêcher les criminels de les contourner, par exemple, en utilisant le double chiffrement.

---

24. On peut imaginer des circonstances exceptionnelles (p. ex., des soupçons à l'égard d'un employé) dans lesquelles une entreprise pourrait se voir contrainte d'intercepter les communications chiffrées de ses employés. Si tel était le cas, il serait toutefois plus facile d'amorcer la surveillance avant que la communication ait été chiffrée plutôt que de s'attaquer au problème plus compliqué qui se pose une fois que la communication a été chiffrée.

Le défi stratégique consiste à trouver des solutions qui limitent les pratiques criminelles sans nuire aux intérêts légitimes, qu'ils soient commerciaux, institutionnels ou individuels. Le Canada est, de toute évidence, tenu de protéger ses citoyens contre les activités criminelles et illégales. En outre, on ne saurait nier les avantages économiques concurrentiels et sociaux qui découlent d'une société civile sécuritaire, comme celle que l'on connaît au Canada.

En ce qui a trait au commerce électronique, il convient également d'analyser la demande attentivement. Le Canada jouit d'une réputation bien méritée en tant que chef de file dans les secteurs des télécommunications et des logiciels, et il possède d'excellents atouts dans le créneau des produits cryptographiques. Son industrie est bien placée pour accroître sa part du marché mondial qui devrait passer de 600 millions de dollars américains en 1996 à 5 milliards de dollars américains d'ici l'an 2000[25]. Pour ne pas laisser échapper ces débouchés, l'industrie cryptographique canadienne demande l'adoption de politiques qui encouragent l'innovation et qui lui permettent d'être sur un pied d'égalité avec ses concurrents étrangers.

Accès légitime de l'État

Les réseaux informatiques ont créé de nouvelles possibilités en ce qui concerne les communications personnelles et commerciales, mais ça n'a pas été sans répercussions néfastes sur la capacité des organismes d'application de la loi de protéger le public. La nouvelle technologie a également produit de nouvelles formes d'activité criminelle, de nouvelles façons de commettre d'anciens crimes et de nouvelles façons de dissimuler des preuves. L'utilisation généralisée de la cryptographie robuste soulève des inquiétudes dans ce contexte, car elle peut créer des obstacles importants à la détection des activités criminelles et nuire aux enquêtes. À cela s'ajoutent les menaces pour la sécurité ainsi que la nécessité d'inspecter les documents mécanographiques pour vérifier la conformité aux exigences commerciales, fiscales, environnementales et à d'autres exigences légales et réglementaires.

La sécurité publique, la lutte contre la criminalité, la sécurité nationale et la conformité aux règlements, tous ces domaines exigent des organismes compétents une participation rapide et efficace à la collecte de données exactes et de preuves sur les activités des criminels. Au nombre des

25. Dataquest.

organismes qui jouent un rôle de premier plan, mentionnons la GRC, les services de police locaux et provinciaux, le Service canadien du renseignement de sécurité, Revenu Canada (Impôt, Douanes et Accise), le Bureau fédéral de la concurrence et les organismes fédéraux et provinciaux responsables de l'application des lois environnementales. Ces organismes sont chargés de déceler les menaces et de détecter les activités criminelles, depuis le terrorisme, les crimes violents et les infractions contre les biens jusqu'aux fraudes touchant les systèmes financiers et commerciaux nationaux et internationaux, de mener leur enquête et d'engager des poursuites.

L'efficacité de ces organismes à détecter l'activité criminelle, à mener leur enquête et à poursuivre les délinquants dépend souvent de leur capacité d'assurer une surveillance électronique des communications et de perquisitionner dans des endroits où de l'information pertinente est peut-être conservée. Les ordinateurs font partie du matériel visé par les fouilles. Ces tâches ne sont assumées, conformément à la *Charte canadienne des droits et libertés*, au *Code criminel* et à d'autres lois, qu'avec l'autorisation d'un tribunal, qui évalue le bien-fondé de la violation de la vie privée des suspects et des personnes qui communiquent avec eux. La Charte [art. 1, 8, et 24 (2)], qui autorise les fouilles, les perquisitions et les saisies « dans des limites qui soient raisonnables et dont la justification puisse se démontrer dans le cadre d'une société libre et démocratique » et qui permet l'utilisation des preuves, sauf si leur utilisation « est susceptible de déconsidérer l'administration de la justice », reconnaît la nécessité d'assurer cette surveillance.

Comme le recours aux télécommunications électroniques et aux radiocommunications ainsi que la capacité technique de les surveiller ont évolué, on a reconnu dans l'ensemble des pays industrialisés la nécessité légitime pour les organismes de l'État d'être autorisés à surveiller les communications, pour autant que des mécanismes de protection judiciaire et légale soient en place. Des principes similaires s'appliquent aux fouilles et aux inspections des lieux, qui s'étendent maintenant à la fouille ou à l'inspection d'ordinateurs et de réseaux. En réglementant ces activités, les constitutions nationales, la loi et les décisions des tribunaux ont toujours concilié le besoin de protéger les intérêts fondamentaux du respect de la vie privée et les intérêts tout aussi fondamentaux de la sécurité publique.

L'utilisation croissante de la cryptographie robuste engendrera certains avantages sur le front de la lutte contre la criminalité en assurant une protection technique des renseignements confidentiels, comme ceux utilisés pour effectuer des transactions financières par voie électronique, mais elle constitue également une menace qu'il ne faut pas sous-estimer pour la capacité

d'assurer une surveillance électronique légitime et autorisée. Bien que l'on puisse encore obtenir des autorisations judiciaires, ceux qui interceptent des renseignements chiffrés se révèlent incapables de les lire, ce qui crée deux difficultés de taille :

- il pourrait devenir difficile, voire impossible, de déterminer si l'information interceptée est vraiment visée par l'autorisation qui a été donnée de l'intercepter;
- il pourrait devenir difficile pour les autorités de déchiffrer l'information ou encore de le faire à temps pour l'utiliser efficacement ou pour prendre des mesures afin de prévenir le préjudice.

Dans de nombreux cas, la rapidité d'accès à l'information est indispensable pour mener à bien des enquêtes, car les mesures adoptées par la suite dépendent de l'information et ne peuvent être efficaces si elles sont prises trop tard. Cette observation est particulièrement valable pour les systèmes informatiques, qui peuvent être utilisés pour déplacer, dissimuler ou effacer d'importantes quantités d'informations par une simple pression sur un touche. Dans certains cas, c'est la rapidité d'action qui peut permettre d'empêcher qu'un crime ou un acte terroriste soit commis.

L'essor des télécommunications mondiales a créé de nouvelles possibilités d'infractions au Canada et à l'étranger ainsi que de nouveaux obstacles à l'efficacité des contrôles.

La possibilité d'avoir recours à des télécommunications protégées facilitera toute forme d'activité illégale qui requiert des efforts coordonnés ou concertés de la part de nombreuses personnes situées à des endroits différents, et les gouvernements ont l'obligation de s'attaquer au problème. Voici des exemples de missions qui sont confiées couramment aux organismes canadiens :

- protéger les Canadiens et la souveraineté nationale contre le terrorisme, la déstabilisation politique et économique ou des menaces similaires émanant d'États étrangers ou de groupes organisés;
- déceler l'utilisation d'ordinateurs et de télécommunications à des fins de transfert illégal ou de trafic de stupéfiants, d'armes et d'autres produits dangereux ou illégaux et engager des poursuites;
- déceler l'utilisation d'ordinateurs et de télécommunications aux fins du blanchiment de fonds provenant d'activités criminelles et engager des poursuites;
- déceler l'utilisation d'ordinateurs et de télécommunications aux fins du transfert illégal d'information (comme la pornographie infantile, la propagande haineuse, la propriété intellectuelle ou des secrets commerciaux ou d'État) et engager des poursuites.

Les délinquants peuvent utiliser des ordinateurs et la technologie des réseaux pour commettre sous une

nouvelle forme des crimes qui existaient déjà, comme c'est le cas de la diffusion de la pornographie infantile sur Internet. La facilité d'accès à des télécommunications protégées, qui simplifie le travail des entreprises légitimes, risque tout autant de simplifier la tâche des criminels. Mentionnons, entre autres, l'utilisation des ordinateurs et des télécommunications pour transférer les recettes de la criminalité tout en dissimulant leur origine et le recours à ces télécommunications par les criminels et les groupes de terroristes pour organiser et coordonner leurs activités.

Dans certains cas, l'accès légitime à des données chiffrées stockées ne revêt pas un caractère aussi urgent que l'interception de communications en cours, mais il représente un problème beaucoup plus vaste. Un grand nombre de lois fédérales et provinciales prévoient l'inspection de documents commerciaux ordinaires en vue de vérifier la conformité aux lois fiscales, aux contrôles d'import-export, aux normes environnementales ou sanitaires, aux règlements sur la concurrence ou le commerce et à de nombreux autres textes. Ces activités légitimes d'application et d'inspection peuvent être entravées par l'utilisation généralisée de la cryptographie robuste, même pour des raisons de sécurité commerciale légitimes.

Les organismes d'application de la loi, de réglementation et de sécurité reconnaissent clairement les avantages commerciaux importants et légitimes liés à la protection de la vie privée qui découleront de l'utilisation de télécommunications chiffrées à des fins d'applications personnelles et commerciales. Ils reconnaissent également que ces avantages ouvrent aussi de nouvelles portes aux activités criminelles et accroissent les menaces pour la sécurité. Pour assumer comme il se doit leurs responsabilités à l'égard de la protection du Canada et des Canadiens contre ces menaces, les organismes concernés doivent disposer de certains moyens grâce auxquels les données chiffrées pourront être décodées et lues dans un délai et à un coût raisonnables. Il faudra parvenir à concilier sur le plan politique, juridique et technologique les intérêts liés à la protection de la vie privée et le développement de communications commerciales efficaces, d'une part, et la protection de la société, d'autre part.

Droits de la personne et libertés civiles

Pour les raisons susmentionnées, il existe des motifs légitimes d'assurer dans certains cas à l'État un accès légitime à des données chiffrées. Dans les faits, pour assurer cet accès, on peut généralement limiter l'utilisation de produits cryptographiques à ceux qui peuvent être déchiffrés et lus au besoin ou exiger de ceux qui possèdent les clés qu'ils déchiffrent les messages sur demande. Les solutions politiques fondamentales et les moyens pratiques de les mettre en œuvre soulèvent des préoccupations concernant les droits fondamentaux, principalement en ce

qui a trait à la protection de la vie privée et à la liberté d'expression.

En fin de compte, il convient d'évaluer les coûts et les avantages de chaque politique possible en matière de cryptographie en ce qui a trait aux droits fondamentaux, aux intérêts commerciaux, à la sécurité publique et à la lutte contre la criminalité. Il faudra ainsi évaluer quels seront les avantages de la limitation du chiffrement sur le plan de la sécurité et de la lutte contre la criminalité, et déterminer s'ils l'emportent sur les dommages susceptibles d'être causés par la non-réglementation du chiffrement. Pour compliquer davantage la situation, l'incidence globale de la cryptographie et la possibilité de la réglementer sont des inconnues à ce stade. Ainsi, même si l'on accordait à l'État un certain accès légitime aux textes clairs, on ne sait pas si les organismes chargés de l'application de la loi et responsables de la sécurité demeureraient capables d'assumer leurs responsabilités en conséquence.

Il est difficile de savoir si ces mesures permettent une application de la loi et un maintien de la sécurité acceptables pour les Canadiens, car tout cadre de référence cohérent évolue également. Au cours des dernières décennies, les nouvelles technologies ont sensiblement amélioré la capacité technique d'assurer diverses formes d'accès légitime. Les systèmes de stockage, de transmission et de récupération des données permettent de stocker d'importantes quantités de renseignements personnels, de les récupérer rapidement et d'effectuer des recherches automatiques. Ces systèmes facilitent l'application de la loi, tout en créant de nouvelles activités criminelles et de nouveaux moyens d'éviter la détection pour ceux qui le désirent afin de dissimuler leurs activités. La possibilité que l'information soit interceptée par ceux qui ne devraient pas y avoir accès accroît fortement les préoccupations concernant les droits fondamentaux de protection des renseignements personnels, et il apparaît indispensable d'instaurer des mécanismes de protection efficaces puisque la quantité d'informations auxquelles on peut avoir accès a augmenté.

Comme c'est le cas dans de nombreux pays démocratiques, les droits des Canadiens à un certain degré de protection de leur vie privée et à la libre expression sont protégés par la Constitution. L'article 8 de la Charte autorise les fouilles, les perquisitions et les saisies dans des limites qui sont raisonnables, et le paragraphe 2b) garantit le droit à la libre expression. Les droits à la protection de la vie privée risquent d'empêcher l'État de déchiffrer les données sans avoir en main des preuves relativement convaincantes, et le droit à la liberté d'expression peut s'étendre à la production de produits cryptographiques et à leur utilisation pour protéger les messages transmis ou les données stockées.

Ces garanties sont importantes, mais pas absolues. L'atteinte à la vie privée, y compris la saisie de données ou l'interception de communications, doit être justifiée et autorisée par les tribunaux. La liberté d'expression peut protéger le droit d'une personne à créer ou à utiliser la cryptographie, mais elle pourrait être limitée par la loi, dans des limites qui sont raisonnables et dont la justification peut se démontrer dans le cadre d'une société libre et démocratique (art. 1). La façon dont ces dispositions s'appliqueraient à la réglementation de la cryptographie au Canada dépendra beaucoup des exigences établies et de leur mode d'application. En plus de limiter les politiques et les lois susceptibles d'être adoptées, elles serviront à protéger les droits individuels, une fois qu'elles seront en vigueur.

De tout temps, les atteintes à la vie privée par l'État sous la forme de fouilles, de saisie ou de surveillance électronique ont été justifiées par le fait que l'organisme compétent possédait une preuve concrète de méfait ou qu'il avait de bonnes raisons de croire que la personne visée était impliquée dans un délit. Ce sont ces critères qu'appliquent les tribunaux lorsqu'ils ont à décider entre protection de la vie privée et intérêt de l'État.

Les mêmes principes s'appliqueraient à l'information chiffrée, mais le déchiffrement de l'information n'est pas identique aux précédents que l'on connaît, à savoir saisir des preuves en appliquant un mandat de perquisition ou intercepter des communications moyennant une autorisation judiciaire. Si le déchiffrement requiert l'accès à des clés, leur saisie en application d'un mandat ordinaire préviendrait le destinataire qu'il fait l'objet d'une enquête. Dans un système où les clés seraient détenues par une tierce partie et où l'on pourrait se les procurer auprès d'elle, l'expéditeur et le destinataire qui sont les cibles de la surveillance ne seraient pas alertés. Toutefois, cela suppose que tous deux fournissent les clés, même s'il n'y a pas de surveillance, de soupçon ou d'enquête judiciaire suite à un délit. Dans ces cas, l'enquête judiciaire devrait être menée au moment même de l'utilisation des clés de chiffrement, ce qui ne serait fait que pour l'infime minorité de messages et de clés auxquels l'État aurait cherché à avoir un accès légitime. Il faudrait donc trouver d'autres protections pour la majorité des clés.

À l'échelle internationale, on utilise le chiffrement, les réseaux informatiques et d'autres moyens de communication pour faire état des violations des droits de la personne et pour protéger la sécurité des défenseurs des droits de la personne dans des pays répressifs. Les gouvernements soucieux de protéger les droits de la personne et la démocratie devraient faire le maximum

pour préserver et protéger ces efforts[26]. Ils devraient réfléchir aux conséquences éventuelles de leur politique de contrôle des exportations pour les défenseurs des droits de la personne. Par exemple, des pays qui contrôleraient l'utilisation intérieure ou l'exportation de produits de chiffrement qui n'ont pas de fonction de récupération permettant aux États d'accéder aux données, décourageraient probablement les entreprises de produire ces technologies. Il serait donc difficile aux défenseurs des droits de la personne et de la démocratie de se procurer des technologies auxquelles des gouvernements répressifs n'auraient pas accès.

Sécurité technique

L'application de la Charte canadienne et des prescriptions de la loi imposées par les tribunaux (p. ex., la portée d'un mandat) règle certains des problèmes fondamentaux liés à la protection de la vie privée et à la liberté d'expression que soulève l'accès légitime de l'État, mais elle ne garantit pas que la mise en place de mécanismes d'autorisation de cet accès ne créera pas, par inadvertance, des lacunes sur le plan de la sécurité dont des intérêts illicites[27] pourraient tirer parti. D'un point de vue technique, les produits cryptographiques robustes sont difficiles à « percer » par des attaques en force menées à partir de puissants ordinateurs. Si les produits commerciaux s'avèrent un tant soit peu déficients, le marché le remarquera probablement rapidement et le problème sera réglé. Il ne sera pas facile d'empêcher que des mécanismes d'accès intégrés aux systèmes pour les fins légitimes de l'État puissent être utilisés illégalement. La vulnérabilité même, le cas échéant, dépendra de la nature des mécanismes d'accès. Si les clés sont conservées par les autorités de certification ou les tiers de confiance, par exemple, il faut prendre des précautions contre le vol. Si une autre forme d'accès était créée dans le logiciel de chiffrement, il serait possible qu'une personne autre que les personnes autorisées par les tribunaux puissent découvrir comment l'utiliser.

Les partisans de contrôles moins stricts de l'utilisation du chiffrement font valoir qu'en Australie (rapport Walsh)[28], aux États-Unis (rapport du National Research Council)[29] et en Europe (la Commission européenne)[30], des études indépendantes réalisées par des experts en cryptographie ont cerné

26. Certains des arguments retenus au nom des droits de la personne ont été présentés par l'American Association for the Advancement of Science (**http://www.aaas.org/spp/dspp/este/briefings/crypto/**).
27. Voir le rapport d'éminents experts américains en cryptographie du secteur privé (1997) intitulé *The Risks of Key Recovery, Key Escrow and Trusted Third-Party Encryption*, (**http://www.crypto.com/key_study/report.shtml**).
28. Walsh, Gerald. *Review of Policy Relating to Encryption Technologies*, rapport terminé le 10 octobre 1996 pour la Division de la sécurité, ministère du Procureur général, gouvernement de l'Australie et publié en vertu de la *Freedom of Information Act*, juin 1997. (**http://www.efa.org.au/Issues/Crypto/Walsh/**).
29. Dam, Kenneth & Herbert Lin (sous la dir.). *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**)

plusieurs avantages liés au chiffrement, mais également une série de problèmes inhérents aux propositions visant à limiter l'éventail de produits de chiffrement — principalement les difficultés techniques, l'efficacité et le coût associés aux plans les plus complets de récupération des clés. Ils n'ont pas recommandé que les gouvernements exigent à ce stade l'entiercement de clés ou des fonctions de récupération des clés. Parallèlement, notre politique doit respecter nos engagements internationaux.

Relations internationales

Le Canada, qui commerce avec toutes les régions du monde, est membre de nombreuses instances internationales. Il sait donc pertinemment que d'autres pays étudient différentes politiques de chiffrement possibles. Le Canada devra examiner attentivement la voie qu'emprunteront les principaux pays exportateurs ainsi que les blocs commerciaux, comme l'ALENA et l'Union européenne, notamment, afin de ne pas ériger d'obstacles inutiles au commerce mondial, et veiller à ce que son industrie et ses intérêts économiques ne soient pas désavantagés.

Actuellement, on ne sait pas avec certitude comment la plupart des pays régleront le problème du contrôle des exportations et des contrôles intérieurs. Certains ont instauré des contrôles intérieurs des importations et de l'utilisation, tandis que d'autres étudient la question. Si certains se prononcent en faveur du contrôle des exportations de façon à influer directement sur les types de produits mis en marché sur leur territoire, d'autres semblent peu disposés à imposer des contraintes au marché du chiffrement. Il est indéniable que le contexte international aura une influence sur la politique canadienne. Le Canada est signataire de plusieurs conventions et traités internationaux qui protègent la liberté d'expression, la liberté de la presse et des communications, la vie privée et les droits de la personne en général. Mais il est également signataire de l'Arrangement de Wassenaar et de plusieurs autres conventions internationales favorisant l'adoption de mesures policières efficaces pour contrer le trafic de stupéfiants, le blanchiment d'argent et le terrorisme. Les engagements que nous avons pris envers nos alliés et la communauté internationale et nos obligations internationales limitent nos options.

Toute position de principe nationale qui serait totalement en désaccord avec celle de nos alliés risquerait de nuire aux relations de longue date en matière de sécurité. Une politique en désaccord avec les énoncés d'autres pays producteurs risque d'être inefficace. Si le Canada est le seul pays à exercer des contrôles, il lui sera difficile d'empêcher la contrebande de logiciels non conformes qui entreront sur son territoire sur disquette ou par voie électronique. La politique en matière de cryptographie est un

enjeu de taille, car les logiciels de chiffrement robuste et les ordinateurs portatifs suffisamment puissants pour faire fonctionner ces logiciels sont devenus courants. Comme toute autre donnée, le logiciel de chiffrement robuste se transfère facilement d'un endroit ou d'un pays à l'autre à l'aide d'Internet, ce qui rend les contrôles à l'importation et à l'exportation difficiles.

Partie 4 : Options en matière de politique

Le gouvernement doit arrêter une ligne de conduite en matière de cryptographie propre à favoriser la croissance du commerce électronique tout en satisfaisant aux exigences des droits de la personne, des libertés civiles de l'application de la loi et de la sécurité nationale. À cette fin, il souhaite obtenir les commentaires du public dans les trois domaines suivants : chiffrement des données stockées, chiffrement des communications en temps réel et contrôle à l'exportation des produits de chiffrement. Plusieurs solutions sont décrites ci-dessous pour chacun de ces domaines. Pour que la ligne de conduite choisie soit des plus harmonieuses, il se peut qu'une combinaison ou des variantes des éléments de ces trois domaines soient indiquées.

Chiffrement des données stockées

Le libre jeu du marché

Cette solution consiste à s'en tenir aux méthodes actuelles. Dans ce cas, on n'adoptera pas de nouvelle loi et on n'imposera pas de nouvelles conditions de délivrance de permis aux particuliers, aux autorités de certification, aux fournisseurs de services cryptographiques ou aux producteurs. Les résultats seront déterminés par le marché, et les entreprises et les particuliers seront libres de déterminer le degré de sécurité qu'ils requièrent d'un fournisseur de services ou encore le type de cryptographie qu'ils choisissent de se procurer et d'appliquer.

Cette démarche suppose que les entreprises et les particuliers prendront leurs précautions afin de ne pas perdre à jamais d'importantes données en créant leurs propres clés de sauvegarde. Ils seront libres de choisir le lieu ou la personne à qui seront confiées les clés — coffre-fort, avocat, groupe de sécurité de l'entreprise ou tiers offrant ces services spécialisés. L'accès légitime au texte clair (c'est-à-dire des données stockées qui ont été déchiffrées) ne sera accordé que dans la mesure où les particuliers et les entreprises adoptent des techniques de récupération des données (comme des copies de sauvegarde des clés de déchiffrement).

L'absence de copies de sauvegarde posera un problème aux organismes d'application de la loi qui doivent enquêter sur des crimes en procédant à des fouilles et à des saisies en vertu d'un mandat légitime. Bien que les grandes entreprises considèrent que la sauvegarde de données stockées constitue une bonne pratique d'affaires qui réduit les risques de perte, de vol ou d'utilisation frauduleuse des clés par les employés, il est à prévoir que toutes les entreprises ne le feront pas. Par conséquent, le libre jeu du

marché ne suffira pas pour garantir toutes les formes d'accès légitime.

En cas de non-réglementation, le consommateur risque d'être amené à évaluer lui-même la sécurité requise. Compte tenu de la complexité des produits cryptographiques, il se peut que les consommateurs aient du mal à faire le bon choix, ce qui sera source d'incertitudes sur le marché.

Normes minimales

Cette solution consiste à adopter une autre approche au terme de laquelle le gouvernement encouragerait activement la création d'une copie de sauvegarde des clés de chiffrement ou prendrait des dispositions visant la récupération des données commerciales. En gros, le gouvernement définirait une norme minimale ou une série de pratiques pour que les autorités de certification ou d'autres entreprises offrant des services de gestion des clés puissent récupérer les données ou les clés. On encouragerait l'adoption de cette norme ou de ces mesures de base en sensibilisant les entreprises et en collaborant avec les fournisseurs de services au sujet des codes industriels et de l'autoaccréditation. L'industrie, les fournisseurs et les utilisateurs pourraient être invités à proposer une série de pratiques raisonnables ou de codes, prévoyant la sauvegarde des clés, qui pourraient être mis en œuvre grâce à une autoréglementation de l'industrie.

L'Infrastructure à clé publique du gouvernement du Canada pourrait également être utilisée pour favoriser l'adoption d'une norme de ce genre, en prévoyant la certification réciproque uniquement avec des fournisseurs de services du secteur privé qui respectent les normes de sauvegarde et de récupération. Cette mesure entraînerait l'établissement d'une « liste blanche » de sociétés et d'autorités de certification qui, selon le gouvernement fédéral, adoptent de bonnes pratiques d'affaires. Ce genre de mesure encouragerait les particuliers et les entreprises à adopter volontairement des mesures de récupération des données et à mieux satisfaire aux besoins relatifs à l'application de la loi et à la sécurité nationale.

L'existence d'une liste d'autorités de certification approuvées par le gouvernement fédéral pourrait aider les consommateurs à faire des choix difficiles. Une série de normes minimales réduirait l'incertitude et, compte tenu du rôle stimulant de la cryptographie, accélérerait l'adoption du commerce électronique.

Accès obligatoire

Par ailleurs, le gouvernement pourrait également adopter des lois instaurant l'accès obligatoire des organismes chargés de veiller à l'application de la loi en interdisant l'utilisation de produits de chiffrement dépourvus de fonctions de récupération des clés. Il pourrait ainsi interdire l'existence d'autorités de certification au Canada, à moins que ces dernières

s'engagent, sur réception d'une ordonnance du tribunal, à donner accès au texte clair aux organismes d'application de la loi. Cette mesure permettrait avant tout de réduire l'éventail de produits offerts au Canada à ceux dotés d'une fonction d'archivage ou d'encapsulage des clés.

Pour s'assurer que les particuliers ne contournent pas la loi en utilisant un chiffrement supplémentaire de non-récupération des clés ou en ayant recours à une autorité de certification étrangère ne gardant pas ou n'archivant pas les clés, le gouvernement pourrait interdire la fabrication, l'importation et l'utilisation de produits sans fonction de récupération des clés au Canada.

Chiffrement des communications en temps réel

Ordonnances d'aide et conditions des licences

Le maintien du statu quo est une solution possible. Sur réception d'une ordonnance du tribunal, les entreprises de télécommunications sont actuellement tenues d'aider, dans la mesure du possible, à déchiffrer les communications chiffrées qui passent par leurs installations. Ces entreprises seraient vraisemblablement capables de déchiffrer ce qu'elles ont chiffré au départ, mais il pourrait y avoir des difficultés, car leurs systèmes ne sont pas forcément configurés pour garder des copies de sauvegarde des clés de chiffrement pour les sessions de communication individuelles.

À l'heure actuelle, les technologies de chiffrement sont principalement utilisées par certaines entreprises en vue d'assurer la confidentialité des communications numériques sans fil. Les seuls fournisseurs de services de communications tenus de donner accès aux communications en clair aux organismes chargés de veiller à l'application de la loi et responsables de la sécurité nationale sont les nouveaux fournisseurs de services de communications personnelles sans fil et de services locaux de télécommunications multipoint. Il s'agit d'une condition imposée à l'obtention de permis d'exploitation qui s'applique uniquement au chiffrement utilisé par ces fournisseurs de communication sans fil[31].

Étant donné que les télécommunications passent actuellement d'une situation de monopole à un environnement concurrentiel, le domaine ne manquera pas d'attirer un nombre

31. Pour obtenir plus de détails, consulter le site suivant : (*http://spectrum.ic.gc.ca/pcs/frndoc/index.html*).

croissant d'intervenants et les technologies se multiplieront. Une combinaison d'approches pourrait introduire de nouvelles règles du jeu entre les fournisseurs de services de communications. Si l'utilisation du chiffrement s'intensifie comme prévu, la combinaison choisie pourrait également exacerber le problème de l'accès légitime aux textes en clair.

Obligations des entreprises de télécommunications

Le gouvernement fédéral pourrait également exiger, en vertu de la loi, de toutes les entreprises de télécommunications qui fournissent des services de chiffrement et sont soumises à sa réglementation qu'elles soient en mesure, sur réception d'une ordonnance d'un tribunal, de déchiffrer des messages pour les organismes chargés de veiller à l'application de la loi et à la sécurité nationale. Il faudrait alors que le gouvernement fédéral collabore avec les provinces et territoires, pour qu'ils imposent les mêmes obligations aux entreprises de télécommunications soumises à leur réglementation. L'adoption d'une telle démarche permettrait à la police de continuer à avoir recours à l'interception approuvée par un tribunal pour prévenir la criminalité et enquêter. Cette approche présente l'avantage de préserver l'équilibre actuel dans les règles du jeu entre les fournisseurs de services sans fil et câblés, mais elle pourrait engendrer des coûts d'infrastructure supplémentaires que devraient assumer les utilisateurs. Une démarche axée sur les entreprises de télécommunications ne toucherait pas les fournisseurs de services Internet qui décideront peut-être d'offrir des services de chiffrement pour les communications en temps réel, comme le téléphone Internet, et n'empêcherait pas non plus l'emploi du chiffrement par les utilisateurs finaux.

Contrôles obligatoires

En plus des prescriptions faites par la loi aux entreprises de télécommunications décrites ci-dessus, la troisième solution nécessiterait l'adoption d'une loi faisant obligation à toute autorité de certification qui fournit des clés aux fins du chiffrement de communications en temps réel (par ex., téléphone Internet chiffré, Telnet chiffré) d'aider à déchiffrer des communications si une ordonnance d'un tribunal le demande. Aux fins de l'application de la loi, l'exhaustivité exigerait que l'on interdise aux utilisateurs qui chiffrent leurs propres messages d'utiliser des produits sans fonction de récupération des clés ou qu'on les oblige à fournir au transporteur de télécommunications ou à une autorité de certification la clé nécessaire avant la transmission. Le logiciel ou le matériel de chiffrement serait requis pour générer une troisième clé de message en vue d'un déchiffrement légal ou pour incorporer une clé générale accessible uniquement en vertu d'une ordonnance du tribunal. Les entreprises de télécommunications ne pourraient transmettre que des messages en clair ou chiffrés par le logiciel ou le matériel de récupération des clés.

Contrôle des exportations

Assouplissement des contrôles

Le gouvernement pourrait assouplir le contrôle actuel des exportations de matériel et de logiciels personnalisés de cryptographie. Le gouvernement a le choix entre deux types de libéralisation : soit adopter la politique d'exportation la plus libérale des pays exportateurs de produits cryptographiques, soit assouplir les contrôles puisque des produits semblables de cryptographie robuste sont offerts sur les marchés étrangers. Les deux solutions favoriseraient la croissance de l'industrie cryptographique canadienne.

Le Canada, à l'instar des 32 autres pays signataires, est tenu de respecter les modalités d'une entente internationale (l'Arrangement de Wassenaar relatif au contrôle multilatéral des exportations pour les armes conventionnelles et les marchandises et technologies à double usage, conclu en 1996), qui stipule les produits nécessitant des licences d'exportation, sans toutefois prévoir l'approbation ou le refus de licences. Si le Canada adoptait des changements pour aligner sa politique sur les politiques les plus libérales d'autres pays, il se démarquerait de la majorité des autres pays (en particulier des États-Unis et de ses autres alliés en matière de sécurité nationale). Cette mesure serait considérée comme une initiative agressive dans le cadre de l'Arrangement de Wassenaar et risquerait de susciter des pressions internationales en faveur de l'adoption d'une politique plus restrictive. En revanche, reconnaître l'offre étrangère est une pratique courante employée pour d'autres produits contrôlés et par d'autres pays signataires de l'Arrangement de Wassenaar.

Maintien de la politique actuelle

Le gouvernement peut également s'en tenir à sa politique actuelle, qui repose sur les listes de marchandises contrôlées de l'Arrangement, et en vertu des politiques actuelles d'approbation et de refus, permettre l'exportation d'une quantité illimitée de produits de signature numérique ou de logiciels de grande diffusion ou du domaine public utilisés pour le chiffrement. Il peut également autoriser l'exportation vers les États-Unis d'une quantité illimitée de logiciels personnalisés de chiffrement ou de matériel doté d'un logiciel de chiffrement (vu que ces exportations ne requièrent pas de licences) et l'exportation de logiciels personnalisés de chiffrement et de matériel doté d'un logiciel de chiffrement dont les clés atteignent jusqu'à 56 bits. Le Canada pourrait continuer à ne pas privilégier les produits à fonction de récupération des clés ou, au contraire, invoquer l'offre de ces produits à l'étranger pour accorder aux produits à fonction de récupération des clés un certain traitement préférentiel à l'exportation.

Élargissement des contrôles

Le gouvernement pourrait élargir les contrôles à l'exportation des logiciels de grande diffusion et du domaine public, soit en coopération

avec d'autres partenaires de l'Arrangement de Wassenaar ou unilatéralement. Parallèlement à cette mesure, il pourrait supprimer le contrôle des formes plus faibles de chiffrement ou adopter d'autres mesures visant à minimiser l'incidence sur les entreprises. Le gouvernement pourrait également élargir les contrôles tout en assouplissant ceux qui visent les produits à fonction de récupération des clés. L'exportation de la cryptographie robuste ne serait autorisée que si les produits possèdent des mécanismes de récupération des clés approuvés. Mais, à moins que ces mesures ne soient prises par tous les autres pays producteurs de cryptographie, les fabricants canadiens ne seront pas sur un pied d'égalité avec les fabricants de pays dont la politique est plus libérale. Les différentes interprétations par divers pays de ce qui est une notion acceptable de récupération des clés pourraient également fausser les règles du jeu.

Questions adressées au public

Le gouvernement du Canada met à jour sa politique en matière de cryptographie afin de protéger l'information vitale de nature économique et financière détenue par le secteur privé canadien, les renseignements personnels et la liberté d'expression tout en continuant d'assumer ses responsabilités en matière d'application de la loi et de sécurité nationale. Le gouvernement demande votre avis sur les questions suivantes :

- Comment évaluez-vous la faisabilité, le coût et la compatibilité internationale des lignes de conduite possibles décrites ci-dessus et quelle solution préférez-vous pour :
  - les données stockées,
  - les communications en temps réel,
  - le contrôle des exportations?

Nous aimerions également avoir votre opinion sur les questions plus générales qui suivent :

- Que peuvent faire les gouvernements pour accélérer la mise en place de l'infrastructure qui permettrait au public d'avoir accès à des services de cryptographie et de participer en toute sécurité à un commerce électronique sûr?
- De quelle façon le gouvernement peut-il concilier les besoins du commerce électronique, de la protection des renseignements personnels et de l'application de la loi? Devrait-on imposer des conditions aux fournisseurs de services de cryptographie du secteur privé et aux particuliers? L'approche volontaire serait-elle efficace?
- Quels contrôles, le cas échéant, devrait-on imposer aux activités des entreprises de télécommunications, aux exploitants de réseaux à valeur ajoutée, aux revendeurs, aux fournisseurs de services Internet et à d'autres sociétés qui offrent le chiffrement des communications en temps réel? Qui devrait assumer le coût de ces contrôles?
- Quels changements au régime d'exportation aideraient le gouvernement à concilier ses intérêts en matière de sécurité nationale et les besoins des gens d'affaires canadiens, y compris l'industrie de la cryptographie?

Glossaire

Autorité de certification : tiers qui vérifie les justificatifs d'identité d'une entité, qui génère des certificats pouvant être utilisés par ces entités afin de prouver leurs attributs à d'autres, et qui tient à jour des dossiers adéquats afin de montrer l'association entre l'entité et les justificatifs d'identité qui ont été certifiés. Par ailleurs, les autorités de certification gèrent, distribuent et archivent les certificats et les listes de révocation de certificats.

Certificat : document électronique qui renferme les justificatifs d'identité d'une entité et qui est signé par l'autorité de certification qui a vérifié ces justifications.

Chiffrement : transformation d'un texte clair en un texte chiffré. Souvent, on utilise le terme « cryptage » pour désigner plus précisément la transformation de données par l'utilisation de la cryptographie afin de produire des données inintelligibles (données chiffrées) en vue d'assurer leur confidentialité.

Clé de chiffrement de longue durée : dans la cryptographie à clé publique, une clé de chiffrement de longue durée serait associée à une entité (p. ex., un particulier, un mandataire ou un processus automatisé) pour une longue période, parfois un ou deux ans. Cette clé donne accès à toutes les données chiffrées à l'aide de cette clé pendant toute la durée de son utilisation. Une clé de chiffrement de longue durée peut être comparée à une clé de session.

Clé de session : clé de chiffrement qui peut être utilisée uniquement pour une seule session, puis être détruite; parfois appelée clé de transaction. Pour les protocoles avec connexion (comme ceux utilisés dans les communications en temps réel), on utilise généralement une clé de session uniquement pour la durée de la connexion (à moins que le temps de connexion soit suffisamment long pour justifier plus d'une clé de session). Une nouvelle clé de session est générée pour chaque nouvelle session (par exemple, chaque fois que quelqu'un fait un appel téléphonique confidentiel, une clé de session différente sera générée). Dans de nombreuses applications du courrier électronique qui emploient la cryptographie à clé publique et la cryptographie à clé secrète, l'expression « clé de session » est parfois employée pour décrire la clé symétrique générée pour chiffrer le document en question. Dans ce cas, la clé symétrique sera probablement chiffrée à l'aide de la clé publique du destinataire afin de faciliter l'échange de clés.

Cryptographie à clé publique : forme de cryptographie utilisant un algorithme cryptographique qui emploie deux clés connexes, une clé publique et une clé privée. Les deux clés ont pour caractéristique que, avec la clé publique, il est impossible sur le plan calcul de dériver la clé privée. La cryptographie à clé publique est aussi

appelée cryptographie asymétrique. Les systèmes de cryptographie à clé publique accomplissent trois grandes fonctions : 1) chiffrement et déchiffrement; 2) signatures numériques; 3) échange de clés. Si certains algorithmes peuvent accomplir ces trois fonctions, d'autres ne peuvent en accomplir qu'une seule.

Cryptographie à clé secrète : forme de cryptographie qui utilise la même clé pour chiffrer et déchiffrer. Aussi appelée « cryptographie symétrique ».

Déchiffrement : fonction inverse du déchiffrement. Transformation d'un texte chiffré en un texte clair.

Encapsulage des clés : technique par laquelle une clé de session est « enveloppée », c'est-à-dire chiffrée à l'aide d'une autre clé appartenant à un tiers (comme l'agent de récupération des clés). Dans les applications du courrier électronique, la clé enveloppée est généralement stockée dans l'en-tête du message. Dans les communications en temps réel, la clé enveloppée peut être transmise pendant le colloque de reconnaissance initiale qui établit une connexion confidentielle.

Fonction de hachage : fonction qui établit une correspondance entre une chaîne binaire de longueur arbitraire et une chaîne binaire de longueur fixe et qui a les propriétés suivantes : 1) il est impossible sur le plan calcul de trouver une donnée d'entrée qui correspond à une donnée de sortie préétablie; 2) il est impossible sur le plan calcul de trouver deux données d'entrée distinctes qui correspondent à la même donnée de sortie.

Hachage : fonction mathématique qui permet de passer d'un grand (voire très grand) domaine à un domaine moindre. Elle peut être utilisée pour réduire un message qui serait trop long en une valeur de hachage ou une contraction du message qui est suffisamment compacte pour être utilisée comme donnée d'entrée dans un algorithme de signature numérique.

Infrastructure à clé publique : environnement de matériel, de logiciels, de personnes, de procédés et de politiques qui emploie la technologie de la signature numérique pour faciliter une association vérifiable entre la composante publique d'une clé publique asymétrique et un utilisateur final particulier. La clé publique peut être fournie aux fins de signature numérique et d'échange ou de négociation de la clé de chiffrement du message.

Récupération des clés : large éventail de techniques permettant de récupérer un texte clair à partir d'un texte chiffré quand le tiers responsable du déchiffrement ne possède pas la clé de déchiffrement (c'est-à-dire que la clé est perdue; le mot de passe chiffrant la clé a été oublié; les mandataires autorisés des tribunaux qui, autre-ment, n'auraient pas accès à la clé cryptographique). La récupération peut prendre les formes suivantes : 1) récupération d'une clé de chiffrement de longue durée d'une entité qui a été

conservée dans un endroit secondaire (parfois appelé sauvegarde commerciale de la clé ou entiercement selon la personne qui contrôle les clés de sauvegarde); 2) encapsulage des clés; ou 3) techniques de dérivation des clés grâce auxquelles la clé confidentielle sera régénérée à l'une des extrémités de la communication par le tiers de confiance qui a fourni les éléments mathématiques originaux utilisés pour générer la clé.

Signature numérique : transformation cryptographique des données qui, une fois associées à une unité de données (comme un fichier électronique), fournit les services d'authentification de l'origine, d'intégrité des données et de non-répudiation du signataire.

Texte chiffré : données chiffrées.

Texte clair : données intelligibles.

Tiers de confiance : responsable de la sécurité ou son agent à qui l'on fait confiance relativement à certaines activités liées à la sécurité. Souvent, l'expression est employée pour désigner une autorité de certification à laquelle quelqu'un d'autre que le propriétaire de données fait appel.

Références et ressources

Infrastructure à clé publique du gouvernement du Canada — **http://www.cse-cst.gc.ca/cse/francais/ gov.html**

Lignes directrices régissant la politique de cryptographie, OCDE, 1997 — **http://www.oecd.org/dsti/sti/it/secur/ index.htm**