RECUEIL DE TERMINOLOGIE

UTILISÉE LORS DU CHANTIER CADRE DE SÉCURITÉ DE L'INFOROUTE GOUVERNEMENTALE

SECRÉTARIAT DU CONSEIL DU TRÉSOR

Sous-secrétariat aux marchés publics et aux technologies de l'information

Direction des la coordination gouvernementale en technologies de l'information

Service des orientations et politiques de renouvellement

24 NOVEMBRE 1997

RECUEIL DE TERMINOLOGIE

Document produit par :
la Direction de la coordination gouvernementale en technologies de l'information

Ce document a été compilé par :
M. Yvan Lauzon
Secrétariat du Conseil du trésor (SCT)
Sous-secrétariat aux marchés publics et aux technologies de l'information
Direction de la coordination gouvernementale en technologies de l'information

Avec l'aide des membres du Comité aviseur interministériel :
M. Michel Després
Secrétariat du Conseil du trésor
M. Claude Francoeur
Société de l'assurance automobile du Québec
Me François Lajeunesse
Secrétariat de l'autoroute de l'information
M. Ross Lamarre
Ministère du Revenu du Québec
Me Michel Léonard
Ministère de la Justice du Québec
Me André Lord
Ministère du Revenu du Québec
M. Michel Marchand
Régie de l'assurance maladie du Québec
M. Raynald Perron
Secrétariat du Conseil du trésor
M. Bernard Plante
Secrétariat du Conseil du trésor
M. Michel Rosciszewski
Secrétariat de l'autoroute de l'information
M. Pierre P. Tremblay
Secrétariat du Conseil du trésor

Pour toute question ou commentaire :
M. Yvan Lauzon
Téléphone : (514) 873-7237
Télécopieur : (514) 873-7749
Courrier électronique : Yvan.Lauzon@SCT1.gouv.qc.ca

*** REMERCIEMENTS ***
Remerciement à toutes les personnes qui ont contribué à la révision du présent document et plus particulièrement aux personnes suivantes qui l'ont commenté : M. Robert Cusson, consultant en sécurité informatique et Me Thierry Piette Coudol, avocat à la cour de Paris et expert technique

Remerciements également à Mme Pauline Prince, terminologue, qui a contribué à la production des deux lexiques figurant à la fin de cet ouvrage.

LISTE DES SOURCES CONSULTÉES

1) Vocabulaire général de la Sécurité informatique
* Gestion de la sécurité * Sécurité physique * Sécurité logique *
* Délits informatiques * Continuité de service *
/ Carole Verreault (OLF). Publications du Québec. 1996. 142 p.

2) Manuel de la sécurité de la technologie de l'information
/ Services gouvernementaux Canada. 1993. 50 P. + 50 P. (bilingue)

3) Lignes directrices (de l'OCDE) régissant la Politique de cryptographie
/ Organisation de Coopération et de Développement Économique (OCDE). 1997-03-27.
(http://www.oecd.org/dsti/iccp/legal/crypto_pr.html)

4) Schéma directeur interministériel des téléprocédures
/ Cosiform-Cerfa. Paris. 1997-04.
(http://www.cerfa.gouv.fr/teleproc/glossaire.htm

5) La sécurité de l'information électronique : Directive concernant la sécurité de l'information électronique et des actifs informationnels
/ SCT-SSMPTI-DCGTI (Auparavant sous le MCQ). 1993. 12 p.

6) Entrust - MG 5 (Version 2)
/ Centre de sécurité des télécommunications (CST-CSE) du gouvernement du Canada. 1996-08. 41 p.

7) Infrastructure des Clés Publiques : Cadre général des politiques et des pratiques de certification
/ Centre de sécurité des télécommunications (Warwick Ford et Marcus Leech). 1996-08-15.

8) La certification dans l'environnement électronique
/ OECD - Organisation de Coopération et de Développement Economique. 1997-10-13.

9) Governement of Canada (GoC)- Public Key Infrastructure (PKI)
/ Centre de sécurité des télécommunications (CST-CSE) du gouvernement du Canada.. 1997-11-05.

10) Réseau de communication de données et communication entre systèmes ouverts: Annuaire: Recommandation
/ UIT-T X.509. 1993-11.

11) Mandat de l'Autorité de gestion de la politique (AGP) de l'Infrastructure à clé publique du gouvernement du Canada.
/ Gouvernement du Canada (CTE). 1996-05-16.

*** REMARQUES ***

(Comité)
Cette mention indique que la définition a été élaborée par le Comité aviseur interministériel du Chantier « Cadre de sécurité de l'Inforoute gouvernementale ».
(Comité, S-3)

Cette mention indique que la définition a été construite par le Comité aviseur interministériel en s'inspirant de la définition apparaissant dans la source (3).

DÉFINITIONS

Acheminement erroné
Acheminement erroné d'un itinéraire de communication prévu pour un utilisateur vers un autre utilisateur. (Comité, Source 10)

Algorithme de chiffrement
Système qui transforme des données afin d'en dissimuler ou d'en révéler le contenu sémantique et qui utilise au moins un paramètre secret. Cette définition inclut à la fois les algorithmes symétriques et les algorithmes asymétriques. Dans le cas d'un algorithme symétrique, les données sont dissimulées ou révélées en utilisant un paramètre secret. Dans le cas d'un algorithme asymétrique, les données sont dissimulées en utilisant un paramètre public et révélées en utilisant un paramètre secret, ou l'inverse. (Comité, S-4)

Analyse de risques
(ou Étude de risque)
(ou Évaluation des menaces et des risques) (EMR)
Activité qui consiste à identifier toutes les menaces et tous les risques informatiques de l'organisation, à les quantifier et à en établir la hiérarchie. (Comité, S-1)

Analyse de trafic
L'observation de l'information relative à une communication entre utilisateurs (c'est-à-dire absence/présence, fréquence, sens, séquence, type, volume, etc.). (S-10)

Authentification
i) Processus qui permet d'établir si une personne, un poste de travail, un système ou une procédure est autorisé à accéder à des données particulières ou à exécuter certaines opérations. La validation du mot de passe, par exemple, est une forme d'authentification. Il peut également s'agir d'une mesure permettant de valider une transmission ou un message, de même qu'à vérifier si le demandeur possède les autorisations requises. (S-2)
ii) Fonction permettant d'établir la validité de l'identité déclarée d'un utilisateur, d'un dispositif ou d'une autre entité au sein d'un système d'information ou de communication. (S-8)

Authentification électronique
Processus par lequel la signature numérique est vérifiée, afin de s'assurer, avant tout autre traitement, que le signataire autorisé peut être identifié avec certitude, que l'intégrité des données autorisées a été préservée et que les données sont originales. (S-6)

Authenticité
Caractère d'une information dont l'origine et l'intégrité sont établies. (Comité, S-1)

Autorisation
(Voir permission)

Autorisation électronique
Processus par lequel une signature électronique est associée à des transactions commerciales, afin d'indiquer qu'une personne ayant un pouvoir délégué approprié a réellement autorisé le traitement ultérieur des données. (S-6)

Autorité de certification
Autorité reconnue et de confiance délivrant des certificats électroniques d'identité, après vérification de l'identité de la personne ou du dispositif (ex : Site WEB). (Comité, S-1)

Autorité de certification centrale
(ou AC centrale)
Autorité de certification supérieure (ou de niveau 0) dans la hiérarchie de l'ICP. Elle offre des services centralisés de gestion des clés et des certificats à toutes les autres autorités de certification. (Comité, S-11)

Autorité de gestion de la politique (AGP)
(ou Autorité de gestion de politique)
Entité chargée d'élaborer les politiques et principes directeurs généraux devant être utilisés par tous les participants. (S-7)

Autorité locale d'enregistrement (ALE)
Une autorité dont l'objet est d'assurer un soutien local à un ensemble d'utilisateurs qui sont physiquement éloignés de leur autorité de certification supérieure immédiate. Une autorité d'enregistrement locale effectue un sous-ensemble de fonctions qui relèvent d'une autorité de certification. (S-11)

Bastion
(Voir: Garde-barrière)

Biclé
Ensemble constitué d'une clé publique et d'une clé privée mathématiquement liées entre elles, formant une paire unique et indissociable pour le chiffrement et le déchiffrement des données, et appartenant à une seule entité. (S-1)

Carte à microcircuit
(ou Carte à mémoire)
(ou Carte à circuit intégré)
Carte informatique contenant un microcircuit avec sa ou ses mémoires, ses circuits logiques ou un microprocesseur associé, et capable de mémoriser ou de traiter des informations. (S-1)

Carte à microprocesseur
(ou Carte à microcalculateur)
(ou Carte à puce)
(ou Carte intelligente)
(ou Carte à mémoire)
Carte à microcircuit dotée d'un microprocesseur permettant l'enregistrement et la restitution d'informations, ainsi que le traitement des données reçues de l'extérieur ou contenues dans les mémoires. (S-1)

Carte à pistes magnétiques
(ou Carte magnétique)
Carte informatique pourvue d'une surface magnétisable sur laquelle sont stockées les données par enregistrement magnétique. (S-1)

Certificat
(ou Certificat électronique d'identité)
Message émis par une autorité de certification, lequel garantit l'authenticité des clés publiques contenues dans un répertoire. (Comité, S-1)

Certification
Vérification indépendante de certaines informations relatives aux transactions dans l'environnement électronique. (S-8)

Chiffrement
Opération par laquelle est substitué, à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale. (S-1)

Classification
Assignation de valeurs à certains attributs d'un objet, lesquelles valeurs caractérisent la sensibilité de cet objet et, conséquemment, la protection à lui accorder. (S-1)

Clé cryptographique
(ou Clef cryptographique)
(ou clé cryptographique)
Appellation générique pour un algorithme cryptographique servant à transformer, valider, authentifier, chiffrer ou déchiffrer des informations. (Comité, S-3)

Clé de chiffrement
Algorithme servant au chiffrement des données. (Comité, S-1)

Clé privée
Composante de la biclé, laquelle est connue de son unique propriétaire et utilisée par lui seul pour déchiffrer un message dont il est le destinataire, ou pour signer un message dont il est l'émetteur. (S-1)

Clé publique
Composante de la biclé, laquelle est stockée dans un répertoire accessible à tous les membres d'un réseau ou d'une organisation, et permettant de transmettre en toute confidentialité des messages à son unique propriétaire, ou d'authentifier à l'arrivée des messages émis par ce dernier. (S-1)

Clé secrète
Clé de chiffrement que se partage l'expéditeur et le destinataire d'un message, le premier pour chiffrer le message, le second pour le déchiffrer (S-1)

Code d'authentification de message (CAM)
(ou Code d'intégrité de message)
(ou Code de détection de modification)
Sceau électronique produit par un algorithme à clé secrète et permettant de garantir l'intégrité du message à l'arrivée. (S-1)

Code utilisateur
(ou Code d'identification)
Chaîne de caractères qui permet d'identifier d'une façon spécifique un utilisateur de systèmes informatiques. Les codes utilisateurs sont généralement publics, mais doivent être associés à un mot de passe secret. (S-2)

Confiance
En général, on peut dire d'une personne « fait confiance » à une autre quand elle suppose que l'autre se comportera exactement de la façon dont elle l'entend. (Comité, S-11).

Confidentialité
Propriété qu'ont les données ou l'information ne sont ni rendues disponibles, ni divulguées aux personnes, entités ou processus non autorisés. (Comité, S-3).

Contrôle d'accès
Processus par lequel les données d'identification que fournit une personne ou toute autre entité sur elle-même pour avoir accès à un centre ou à un système informatiques sont comparées à des valeurs de référence définies touchant cette entité, permettant ainsi l'autorisation ou le refus de l'accès demandé, qu'il soit physique ou logique (S-1)

Cryptogramme
(Voir: Texte chiffré)

Cryptographie
Discipline qui comprend les principes, les moyens et les méthodes de transformation des données afin de dissimuler leur contenu, de prévenir des modifications non détectées et (ou) de prévenir son utilisation non autorisée. (S-11)

Déclaration relative aux pratiques de certification
(Voir: Énoncé de pratique de certification)

Déchiffrement
Signifie la fonction inverse du chiffrement. (S-3)

Dématérialisation d'un document
Transformation d'un document sous support papier par son équivalent (image ou seulement identité de contenu) sous forme électronique. (Comité, S-4)

Détecteur de virus
Logiciel qui détecte soit des virus particuliers soit une activité virale. (Comité, S-2)

Détenteur d'un actif informationnel
Personne à qui est assignée par délégation du sous-ministre ou du dirigeant d'organisme, aux fins de la sécurité, la responsabilité d'un actif informationnel dont le gouvernemental est propriétaire. (Comité, S-5)

Détenteur de clés
Signifie une personne ou entité qui possède ou contrôle des clés cryptographiques. (S-3)

Disponibilité
Propriété qu'ont les données, l'information et les systèmes d'information et de communication d'être accessibles et utilisables en temps voulu et de la manière requise. (S-3)

Donnée
Signifie la représentation d'informations d'une manière adaptée à la communication, à l'interprétation, au stockage ou au traitement. (S-3 & S-8)

Donnée confidentielle
Donnée qui ne peut être communiquée ou rendue accessible qu'aux personnes ou autres entités autorisées. (S-1)

Données à caractère nominative
(ou Données à caractère personnel)
Signifie toute information relative à une personne physique identifiée ou identifiable. (S-3)

Donnée non classée
Donnée dont la perte n'a que des conséquences mineures et qui n'est pas protégée contre la divulgation. (S-1)

Donnée sensible
(ou Donnée critique)
(ou Donnée vitale)
Donnée dont la divulgation, l'altération, la perte ou la destruction risquent de paralyser ou de mettre en péril soit un service, soit l'organisation elle-même, et qui, de ce fait, devient vulnérable. (Comité, S-1)

Droit d'accès
Droit accordé à une personne ou à toute autre entité d'avoir accès à des donnés ou programmes déterminés et de les exploiter d'une façon particulière. (S-1)

Énoncé de pratiques de certification
(ou Déclaration relative aux pratiques de certification)
Une déclaration des pratiques dont se sert une autorité de certification quand elle émet des certificats. Une déclaration des pratiques de certification peut prendre la forme d'une déclaration faite par l'autorité de certification concernant la nature de son système fiable et les pratiques qu'elle emploie, ou il peut s'agir d'une loi ou d'un règlement auquel satisfait l'autorité de certification. Elle peut également faire partie du contrat conclu entre l'autorité de certification et l'abonné ou y être intégrée par renvoi. (S-11)

Étude de risque
(Voir: Analyse de risque)

Évaluation de la menace et des risques (EMR)
(Voir: Analyse de risque)

Évaluation des menaces et des risques (EMR)
(Voir: Analyse de risque)

Fausse identité
Prétention d'un utilisateur à se faire passer pour un autre utilisateur afin d'avoir accès à l'information ou d'acquérir des privilèges supplémentaires. (S-10)

Fiabilité
(ou Sûreté de fonctionnement)
Propriété d'un système informatique capable d'assurer ses fonctions sans défaillances, dans des conditions préalablement définies et sur une période déterminée. (S-1)

Fournisseur
Une corporation, une société, une coopérative ou une personne physique faisant affaires et en mesure de contracter avec le gouvernement, une unité administrative d'un ministère ou d'un organisme ou tout fonds spécial qui fournit des services ou des biens à un détenteur, à un utilisateur ou à un autre fournisseur. (S-5)

Garde-barrière
(ou Bastion)
Dispositif informatique qui permet le passage sélectif des flux d'information entre un réseau interne et un réseau public, ainsi que la neutralisation des tentatives de pénétration en provenance du réseau public. (S-1)

Gestion de la sécurité informatique
Ensemble des activités ayant trait à la planification, à l'organisation et au contrôle de la sécurité informatique. (S-1)

Gestion des clés
Ensemble des activités ayant trait à la production, au stockage, à la distribution, à la suppression, à l'archivage et au remplacement des clés de chiffrement. (S-1)

Habilitation
(Voir: Permission)

Infrastructure à clé publique (ICP)
(ou Infrastructure à clés publiques)
(ou Infrastructure des clés publiques)
Ensemble de technologies, de normes et de politiques qui permettent d'assurer un environnement sécuritaire aux échanges électroniques sur les réseaux ouverts, comme Internet. L'ICP engendre, distribue, gère et archive les clés, les certificats et les listes de révocation des certificats qui doivent être affichés dans les répertoires électroniques X.500. (Comité)

Intégrité
Signifie la propriété que les données ou l'information n'ont pas été modifiées ou altérées de manière non autorisée. (S-3 & S-8)

Intégrité du système
Propriété d'un système informatique protégé contre les dysfonctionnements, les agressions et les attaques. (S-1)

Interception d'identité
L'identité d'un ou de plusieurs des utilisateurs intervenant dans une communication est notée pour mauvaise utilisation. (S-10)

Interception de données
Observation de données d'utilisateur au cours d'une communication par un utilisateur non autorisé. (S-10)

Interopérabilité des méthodes cryptographiques
Capacité pour de multiples méthodes cryptographiques de techniquement fonctionner ensemble. (S-3)
Voir aussi : interpérabilité des méthodes cryptographiques
portabilité des méthodes cryptographiques

Jeton personnel
Élément que l'on utilise afin d'associer à une personne donnée une clé particulière (ou un ensemble de clés), de l'information sur ces privilèges d'autorisation, ainsi que des fonctions de traitement cryptographique. Un jeton physique (ex., une carte à puce, carte PCMCIA, disquette) peut habituellement fonctionner avec plusieurs applications, et elle n'est donc pas utilisée uniquement aux fins de l'ICP. On peut utiliser un tel jeton pour des applications multiples si les politiques locales de sécurité le permettent. (Comité, S-6)

Journal
Relevé chronologique des opérations informatiques, constituant un historique de l'utilisation des programmes et des systèmes sur une période donnée. (S-1)

Journalisation
Enregistrement dans un journal des opérations informatiques effectuées dans un système. (S-1)

Manipulation
Remplacement, insertion, suppression ou mise en désordre de données d'utilisateur au cours d'une communication par un utilisateur non autorisé. (S-10)

Mappage des politiques
Reconnaître que, quand une autorité de certification dans un domaine certifie une autorité de certification dans un autre domaine, il est possible qu'une politique de certification particulière dans le second domaine puisse être considérée comme équivalente (mais pas nécessairement identique sous tous ses aspects) à une politique de certification dans le premier domaine. (S-11)

Méthodes cryptographiques
Désigne les techniques, services, systèmes et produits cryptographiques et les systèmes de gestion de clés. (S-3)

Mobilité des méthodes cryptographiques
Possibilité technique de fonctionner dans divers pays ou diverses infrastructures d'information et de communication. (S-3)
Voir aussi : interopérabilité des méthodes cryptographiques
portabilité des méthodes cryptographiques

Mode « en direct »
(ou Mode connecté)
On dit que deux ordinateurs travaillent en mode connecté quand ils fonctionnent en même temps et échangent immédiatement (en temps réel) à travers un réseau de transmission de données, les informations qui leur sont nécessaires. (S-4)

Mode « en lot »
(ou mode boîte aux lettres, si « messagerie »)
Mode d'échange désynchronisé où chaque ordinateur dispose dans le serveur intermédiaire d'une boîte aux lettres ou sont stockées les informations qui lui sont destinées. Ces informations sont organisées en messages comprenant une enveloppe (informations nécessaires à l'acheminement comprenant les références du destinataire et certaines informations de service comme les demandes d'accusé de réception) et les informations elles-mêmes formant le corps du message. (S-4)

Mot de passe
Liste secrète de caractères qui, combiné à un code utilisateur public, forme un identificateur unique désignant un utilisateur particulier. Les mots de passe ne doivent, en aucun cas, être divulgués à une autre personne, ou insérés dans une procédure d'entrée en communication automatisée (séquence d'entrée en communication). (S-2)

Nœud de gestion ICP
Un nœud de gestion est responsable de l'administration d'un ensemble spécifique d'entités de chiffrement, d'entités de signature numérique, d'autorités locales d'enregistrement (ALE) et (ou) de nœuds de gestion ICP subalternes. La responsabilité d'exploiter un nœud de gestion est assignée à une organisation, un ministère, un organisme, un groupe ou une section. Cette responsabilité peut être déléguée à des nœuds subalternes. Chaque nœud de gestion représente un niveau précis, correspondant à sa distance logique du nœud de niveau 0. Un nœud de gestion comprend des fonctions d'autorité de certification, c.-à-d. qu'il peut émettre des certificats de clé publique et des listes de révocation de certificat. (Comité, S-6)

Non-répudiation
Désigne une propriété obtenue par des méthodes cryptographiques, d'empêcher une personne ou une entité de nier avoir exécuté une action particulière en relation avec les données (par exemple mécanismes de non-répudiation d'origine; d'attestation d'obligation, d'intention ou d'engagement; ou d'établissement de la propriété). (S-3 & S8)

Notarisation
Enregistrement des éléments essentiels d'une transaction entre deux parties par un notaire. (Comité)

Numéro d'identification personnel - NIP)
(ou Code confidentiel)
(ou Code personnel)
(ou Code secret)
(ou Numéro secret)
Authentifiant prenant la forme d'un code numérique et attribué à un utilisateur, permettant à ce dernier d'obtenir l'accès à un ordinateur en ligne et d'y effectuer l'opération désirée. (S-1)

Permission
(ou Autorisation)

(ou Habilitation)
Attribution de droits d'accès à une entité par une autorité. (S-1)

Piste de vérification
(ou Piste de contrôle)
Ensemble de données consignées dans un journal relatives aux opérations d'un système, lequel ensemble permet la reconstitution et l'examen exhaustif des séquences d'événements informatiques ayant mené à un résultat déterminé, en vue de la vérification informatique. (S-1)

Plan de continuité
Composante essentielle du plan de sécurité informatique, qui prévoit toutes les circonstances d'arrêt d'exploitation des ressources informatiques, de même que toutes les mesures palliatives et curatives applicables à chacun des cas d'indisponibilités, afin que soit assurée, sur site ou hors site, la continuité du service. (S-1)

Plan de reprise des opérations (PRO)
Plan permettant de prendre les mesures nécessaires en vue d'assurer la reprise des opérations essentielles (et non seulement des services informatiques) en cas de désastre ou d'interruption prolongée du service normal. (S-2)

Plan de sécurité informatique
Projet élaboré sous forme de document, comportant un ensemble d'objectifs précis à atteindre et de mesures à mettre en œuvre en vue de l'application de la politique de sécurité informatique. (S-1)

Plan d'urgence
Plan décrivant en détail les mesures nécessaires à la remise en état d'un service ou d'un système informatique. Il peut s'agir d'un plan autonome ou encore d'une partie du Plan de reprise des opérations. (S-2)

Politique d'identification et d'authentification
Ensemble de règles servant à l'identification et l'authentification des détenteurs de certificats. (S-7)

Politique de certification
Ensemble de règles nommé qui détermine l'applicabilité d'un certificat à une clientèle ou à une classe particulière d'applications ayant des exigences de sécurité communes. Par exemple, un politique de certification particulière pourrait définir l'applicabilité d'un type de certificat pour l'authentification des transactions d'échange de données informatisées pour le commerce de marchandises comprises dans une fourchette de prix donnée. (S-7)

Politique de fonctionnement de l'AC
Pratiques suivies par une autorité de certification pour l'exploitation de ses services, par exemple, la fréquence d'émission des listes de certificats révoqués et les procédures à suivre pour récupérer les preuves stockées. (S-7)

Politique de gestion des clés
Mesures prises par une autorité de certification pour protéger ses propres clés cryptographiques et celles de ses abonnés. Les abonnés pourraient également être tenus de protéger, dans une certaine mesure, leurs propres clés cryptographiques. (S-7)

Politique de sécurité de l'AC
L'ensemble des règles fixées par l'autorité en matière de sécurité qui régit l'utilisation et la prestation de services et des installations de sécurité.. (S-11)

Politique de sécurité informatique
Énoncé général émanant de la direction d'une organisation, et indiquant la ligne de conduite adoptée relativement à la sécurité informatique, à sa mise en œuvre et à sa gestion. (S-1)

Politique de sécurité locale
Mesures prises par une autorité de certification pour s'assurer que son environnement est sûr. Cela peut comprendre des mesures de protection pour assurer la sécurité physique, la sécurité du personnel, l'assurance du produit et la vérification. Les abonnés pourraient également être tenus d'assurer la sécurité de leur propre environnement. (S-7)

Portabilité des méthodes cryptographiques
Possibilité technique d'être adapté pour fonctionner sur de multiples systèmes. (S-3)

Profil des certificats et des listes de certificats révoqués
Les règlements et les principes directeurs relatifs à l'utilisation de champs et d'extensions particuliers des certificats et des listes. (S-7)

Programme de sécurité informatique
Ensemble ordonné et formalisé des opérations permettant l'atteinte des objectifs établis et la mise en œuvre des mesures décrites dans le plan de sécurité informatique. (S-1)

Protection de la confidentialité
(ou Protection de la vie privée)
Mise en vigueur d'un ensemble de mesures administratives, techniques et physiques visant à prévenir les intrusions dans la vie privée des personnes ou dans les affaires privées des personnes et des organisations, lesquelles intrusions découlent spécifiquement de la collecte, du traitement, de la dissémination et de la divulgation d'informations ayant trait à ces personnes ou à ces organisations. (S-1)

Qualificatif de politique
Information dépendante d'une politique qui accompagne un identificateur de politique de certification dans un certificat X.509. (S-7)

Reconnaissance mutuelle
(ou reconnaissance réciproque)
Reconnaissance entre Autorités de certification. (Comité)

Redéfilement
Enregistrement et écoute ultérieure d'une communication. (Source 10)

Refus de service
Empêchement ou interruption d'une communication ou encore retard d'opérations temporelles critiques. (S-10)

Registre des autorités de la sécurité
Répertoire, recueil ou fichier dans lequel sont inscrites les désignations effectuées et les délégations consenties aux fins de la gestion de la sécurité ainsi que les responsabilités qui y sont rattachées. (S-5)

Rejet
Démenti d'un utilisateur d'avoir participé en partie ou pendant toute sa durée, à une communication. (S-10)

Renseignements classifiés
Renseignements de nature délicate qui visent la défense et le maintien de la stabilité sociale, politique et économique du pays. Les renseignements classifiés sont regroupés par ordre croissant de sensibilité dans les catégories suivantes : confidentiel, secret et très secret. (S-2)

Renseignements de nature délicate
Renseignements qui sont soit classifiés soit désignés. (S-2)

Renseignements désignés
(ou Renseignements protégés)
Il s'agit de renseignements de nature délicate qui ne sont pas d'intérêt national (voir également Renseignements classifiés) mais doivent tout de même faire l'objet d'une protection spéciale contre toute divulgation sans permission. Parmi ceux-ci, mentionnons : les dossiers personnels, les dossiers médicaux, les enquêtes de la police et les renseignements de nature industrielle particulière. Les renseignements désignés sont catégorisés, par ordre croissant, comme étants sensible, particulièrement sensible et très sensible. Les renseignements désignés peuvent faire l'objet d'une exemption de divulgation au public. Les termes désignés et protégés sont souvent utilisés l'un pour l'autre. Les renseignements protégés sont répartis dans les catégories protégé A, protégé B et protégé C correspondant respectivement à sensible, particulièrement sensible et très sensible. (S-2)

Répertoire
Inventaire des renseignements concernant des objets et qui offre à ses utilisateurs des services qui leur permettent d'avoir accès à l'information.(Comité, S-11)

Répertoire des clés publiques
Inventaire des clés publiques et de leurs propriétaires respectifs, lequel est produit et authentifié par une Autorité de certification, et que consultent les membres d'un réseau détenteurs de biclés pour s'échanger des messages. (Comité, S-1)

Répudiation
Fait, pour une personne ou pour toute autre entité engagée dans une communication par voie informatique, de nier avoir participé à tout ou partie des échanges. (S-1)

Sceau électronique
(ou Verrou)
Bloc de données dont le contenu est le résultat d'un calcul complexe réalisé à partir d'un message à transmettre, qui est ajouté à ce message par l'expéditeur, et dont le recalcul à l'arrivée permet de vérifier l'origine et l'intégrité du message auquel il a été attaché. (S-1)

Scellement
(ou Verrouillage)
Action qui consiste à adjoindre à un message à transmettre un sceau électronique permettant de garantir l'origine et l'intégrité de ce message. (S-1)

Signataire
Entité imputable (soit une personne en particulier, soit une personne ayant un rôle organisationnel) qui génère des signatures numériques. (S-6)

Signature électronique
(ou Signature numérique)
(ou Signature informatique)
Données annexées à un document électronique qui permet à une personne qui reçoit ce document de démontrer qui est la source des données, d'en attester l'intégrité, ainsi que d'assurer de l'adhésion de l'émetteur au contenu de ce document. (Comité)
Note : Pour certains, la signature numérique est un type de signature électronique utilisant la cryptographie asymétrique.

Sinistre informatique
Événement grave d'origine naturelle ou humaine, accidentelle ou intentionnelle, occasionnant des pertes et des dommages importants à un système ou à un centre informatiques. (S-1)

Système cryptographique à clé publique
(ou Système à clé publique)
(ou Système à deux clés)
(ou Système à clé révélée)
(ou Système asymétrique)
Système cryptographique faisant appel à une biclé pour le chiffrement et le déchiffrement d'un message, ce qui n'oblige pas à l'échange préalable d'une clé secrète entre les interlocuteurs en communication. (S-1)

Système de gestion électronique de clés
Signifie un système de production, de stockage, de distribution, de reprise, de suppression, d'archivage, de certification ou d'application des clés cryptographiques. (S-3 & S-8)

Texte chiffré
(ou Message chiffré)
(ou Cryptogramme)
Données rendues inintelligibles du fait de leur chiffrement, qui ne peuvent donc être comprises et exploitées que par les seules entités en possession de la clé permettant de les déchiffrer. (S-1)

Texte en clair
Signifie des données intelligibles. (S-3)

Tiers certificateur de clés publiques de signature
Autorité chargée de certifier, de distribuer, de gérer (date d'expiration, révocation, etc) les clés publiques destinées à la signature électronique et éventuellement leurs supports. (S-4)

Tiers de confiance
(ou Tierce partie de confiance)
Autorité de sécurité à laquelle des entités communicantes accordent leur confiance pour l'authentification de leurs transactions, et qui peut ainsi certifier l'authenticité des messages émis. (S-1)

Vérification informatique
Examen périodique d'un échantillon d'événements informatiques survenus pendant une période donnée à partir d'un certain nombre de postes utilisateurs dans une organisation, afin de détecter les erreurs ainsi que les comportements anormaux ou fraduleux. (S-1)

Verrou
(Voir Sceau électronique)

Verrouillage
(Voir: Scellement)

Virus
Programme inséré dans un système informatique dans le but de causer des dommages nuisibles et néfastes. Les virus peuvent se multiplier et s'agripper à d'autres programmes (les infecter) ou au secteur d'initialisation des disquettes, des disques durs ou d'autres supports de données. Les virus sont transmis lorsqu'un programme infecté est exécuté sur un système non infecté ou qu'une disquette infectée est utilisée par un système non infecté. (S-2)

LEXIQUE FRANÇAIS-ANGLAIS

algorithme de chiffrement	encryption algorithm; encipherment algorithm
analyse de risque; étude de risque; évaluation des menaces et des risques	risk analysis
analyse de trafic	traffic analysis
auditeur	auditor
authentification	authentication
authentification de l'origine ; authentification de l'origine des données	data origin authentication
authentification de l'utilisateur	user authentication
authentification de message	message authentication
authentification électronique	electronic authentication
authentification réciproque ; authentification mutuelle ; reconnaissance mutuelle	two-way authentication
autorisation (voir permission)	authorization (see permission)
autorisation électronique	electronic authorization
autorité de certification (AC)	certification authority (CA)
autorité de gestion de la politique (AGP)	policy managing authority
autorité locale d'enregistrement (ALE)	recording local authority
bastion (voir garde-barrière) ---	
biclé	encryption and decryption key pair; key pair carte badge; card
carte à logique câblée	wired logic card
carte à mémoire simple ; carte à simple mémoire simple	smart card
carte à microcircuit ; carte à mémoire ; carte à circuit intégré	internal circuit card; microcircuit card; smart card
carte microprocesseur ; carte à puce ; carte intelligente	microprocessor card; chip card
carte à pistes magnétiques ; carte magnétique	magnetic-stripe card; magnetic card
carte informatique	memory card
certificat	certificate
certification	certification
chiffrement	encryption; encipherment
classification	cryptographic key
clé cryptographique classification clé de chiffrement	encryption key; encipherment key; encryption key
clé privée private	key
clé publique ; clé révélée	public key
clé secrète	secret key
code confidentiel ; code personnel ; code secret ; numéro d'identification personnel (NIP) ; numéro secret	personal identification number (PIN)
code d'authentification de message (CAM) ; code d'intégrité de message ; code de détection de modification	message authentication code (MAC)
code utilisateur ; code d'identification	user identification code; user ID

confidentialité	confidentiality
contrôle d'accès logique	logical access control
cryptogramme (voir texte chiffré)	cryptogram (see ciphertext)
cryptographie	cryptography
Data Encryption Standard (DES)	Data Encryption Standard (DES)
déchiffrement	decryption; decipherment
dématérialisation d'un document	dematerialization
détecteur de virus	virus detection software; detection virus-screening program
détenteur	holder
détenteur de clés	key holder
disponibilité	availability
donnée	data
donnée confidentielle	confidential data
données à caractère personnel	personal data; personal information
donnée non classée	unclassified data
donnée sensible ; donnée critique ; donnée vitale	sensitive data; critical data
droit d'accès	access right
élément de politique	policy element
énoncé de pratiques de certification (EPC)	certification practice statement (CPS)
entité de chiffrement	à encryption entity; encipherment entity
entité de signature numérique	digital signature entity
entité finale	final entity
étude de risque (voir analyse de risque)	risk analysis
évaluation de la menace et des risques (EMR) (voir analyse de risque)	risk analysis
falsification de donnée	data manipulation
fausse identité	false identity
fiabilité (ou sûreté de fonctionnement)	reliability
fournisseur	supplier
garde-barrière ; bastion ; pont-levis électronique ; cloison étanche ; garde-fou	electronic firewall; network firewall; firewall
gestion de la sécurité informatique	computer security management
gestion des clés	key management
habilitation (voir permission)	clearance (see permission)
information électronique	electronic information
infrastructure à clé publique (ICP)	public key infrastructure (PKI)
installation	installation; plant; facilities
intégrité	integrity
intégrité des données	data integrity
intégrité du système	system integrity
interception d'identité	identity interception
interception de données	data interception
interopérabilité	interoperability
jeton personnel	personal token
journal	log
journalisation	logging
méthodes cryptographiques	cryptographic methods

mobilité	mobility
mode connecté	on-line
mode « en direct »	direct connection
mode « messagerie »	messaging mode
mot de passe	password
nœud de gestion ICP PKI	management node
non-répudiation	non-repudiation
notarisation	notarization
numéro d'identification personnel (NIP)	personal identification number (PIN)
permission ; autorisation ; habilitation	permission; authorizasion; clareance
piste de vérification ; piste de contrôle	security audit trail; audit trail
plan de reprise des opérations (PRO)	operations recovery plan
plan de sécurité informatique	computer security plan
plan d'urgence	emergency plan
politique d'identification et d'authentification	identification and authentication policy
politique de certification	certification policy
politique de fonctionnement de l'AC	CA operational policy
politique de gestion des clés	key management policy
politique de sécurité informatique	computer security policy; security policy
politique de sécurité locale local	security policy
portabilité	portability
procédure de sécurité informatique	transposition de protocole
profil des certificats et des listes de certificats révoqués	cancelled certificates and lists of certificate profile
programme de sécurité informatique	security procedure; computer security program; security program
protection de la confidentialité ; protection de la vie privée	privacy protection; protection of data privacy
qualificatif de politique	policy qualification
réacheminement	rerouting
reconnaissance mutuelle (voir authentification réciproque)	two-way authentication
refus de service	denial of service
registre des autorités de la sécurité	security authorities register
rejet	reject
renseignements classifiés	classified information
renseignements de nature délicate	sensitive information
renseignements désignés	designated information
répertoire de clés publiques	public key directory
répudiation	repudiation
(Rivest, Shamir et Adleman)	(Rivest, Shamir et Adleman)
sceau électronique ; verrou	authenticator; integrity lock
scellement ; verrouillage	spray paint; integrity locking
serveur Web	Web server
signataire	officer signing
signature électronique ; signature numérique ; signature informatique	digital signature
sinistre informatique	computer disaster; disaster
supercarte intelligente	supersmart card

système cryptographique à clé publique ; système à clé publique ; système à deux clés ; système à clé révélée ; système asymétrique	public-key cryptosystem (PKC); system; two-key system
système de gestion de clés	key management system
système d'information	information system
technologie de l'information	information technology
télécopieur protégé	protected fax
télépaiement	telepayment
télétraitement	teleprocessing
télétransmission	teletransmission
texte chiffré ; message chiffré ; cryptogramme	Ciphertext; cryptotext cryptogram
texte en clair	plain text
tiers de confiance	trusted third party; trusted authentication authority
tiers certificateur de clés publiques de signature	signature public key third party certifier
transmission de données	data transmission
transposition de protocole	protocol translation
utilisateur ; usager	user
validation d'un module cryptographique	cryptographic module validation
vérificateur	auditor
vérification informatique	computer audit
verrou (voir sceau électronique)	integrity lock (see authenticator)
verrouillage (voir scellement)	integrity locking (see spray paint)

LEXIQUE ANGLAIS-FRANÇAIS

access right	droit d'accès
auditor	auditeur, vérificateur
authentication	authentification
authenticator; integrity lock	sceau électronique; verrou
authorization (see permission)	autorisation (voir permission)
availability	disponibilité
badge; card	carte
cancelled certificates and lists of certificates profile	profil des certificats et des listes de certificats révoqués
CA operational policy	politique de fonctionnement de l'AC
certificate	certificat
certification	certification
certification authority (CA)	autorité de certification (AC)
certification policy	politique de certification
certification practice statement (CPS)	énoncé de pratiques de certification (EPC)
ciphertext; cryptotext; cryptogram	texte chiffré; message chiffré; cryptogramme
classification	classification
classified information	renseignements classifiés
clearance (see permission)	habilitation (voir permission)
computer audit	vérification informatique
computer disaster; disaster	sinistre informatique
computer security management	gestion de la sécurité informatique
computer security plan	plan de sécurité informatique
computer security policy; security policy	politique de sécurité informatique
computer security program; security program	programme de sécurité informatique
confidential data	donnée confidentielle
confidentiality	confidentialité
cryptogram (see ciphertext)	cryptogramme (voir texte chiffré)
cryptographic key	clé cryptographique
cryptographic methods	méthodes cryptographiques
cryptographic module validation	validation d'un module cryptographique
cryptography	cryptographie
data	données
Data Encryption Standard (DES)	Data Encryption Standard (DES)
data integrity	intégrité des données
data interception	interception de données
data manipulation	falsification de données
data origin authentication	authentification de l'origine ; authentification de l'origine des données
data transmission	transmission de données
decryption; decipherment	déchiffrement
designated information	renseignements désignés
dematerialization	dématérialisation
denial of service	refus de service
digital signature	signature électronique ; signature numérique ; signature informatique
digital signature entity	entité de signature numérique

direct connection	mode «en direct»
public key directory	répertoire de clés publiques
electronic authentication	authentification électronique
electronic authorization	autorisation électronique
electronic firewall; network firewall; firewall	garde-barrière ; bastion ; pont-levis électronique ; cloison étanche ; garde-fou
electronic information	information électronique
emergency plan	plan d'urgence
encryption algorithm; encipherment algorithm	algorithme de chiffrement
encryption and decryption key pair; key pair	biclé
encryption; encipherment	chiffrement
encryption entity; encipherment entity	entité de chiffrement
encryption key; encipherment key; data encryption key	clé de chiffrement
false identity	fausse identité
final entity	entité finale
firewall	bastion (voir garde-barrière)
holder	détenteur
identification and authentication policy	politique d'identification et d'authentification
identity interception	interception d'identité
information system	système d'information
information technology	technologie de l'information
installation; plant; facilities	installation
integrity	intégrité
integrity lock (see authenticator)	verrou (voir sceau électronique)
integrity locking (see spray paint)	verrouillage (voir scellement)
internal circuit card; microcircuit card; smart card	carte à microcircuit ; carte à mémoire ; carte à circuit intégré
interoperability	interopérabilité
key-distribution center (KDC); key distributing center; network security center (NSC)	centre de distribution de clés
key holder	détenteur de clés
key management	gestion des clés
key management policy	politique de gestion des clés
local security policy	politique de sécurité locale
log	journal
logging	journalisation
logical access control	contrôle d'accès logique
magnetic-stripe card; magnetic card	carte à pistes magnétiques ; carte magnétique
memory card	carte informatique
message authentication	authentification de message
message authentication code (MAC)	code d'authentification de message (CAM) ; code d'intégrité de message ; code de détection de modification
messaging mode	mode « messagerie »

microprocessor card; chip card	carte à microprocesseur ; carte à puce ; carte intelligente
mobility	mobilité
non-repudiation	non-répudiation
notarization	notarisation
officer signing	signataire
on-line	mode connecté
operations recovery plan	plan de reprise des opérations (PRO)
password	mot de passe
permission; authorization; clearance	permission ; autorisation ; habilitation
personal data; personal information	données à caractère personnel
personal identification number (PIN)	numéro d'identification personnel (NIP) code confidentiel ; code personnel ; code secret ; numéro secret
personal token	jeton personnel
PKI management node	nœud de gestion ICP
plain text	texte en clair
policy element	élément de politique
policy managing authority	autorité de gestion de la politique (AGP)
policy qualification	qualificatif de politique
portability	portabilité
privacy protection; protection of privacy; protection of data privacy	protection de la confidentialité ; protection de la vie privée
private key	clé privée
protected fax	télécopieur protégé
protocol translation	transposition de protocole
public key	clé publique ; clé révélée
public-key cryptosystem (PKC); public-key system; two-key system	système cryptographique à clé publique ; système à clé publique ; système à deux clés ; système à clé révélée ; système asymétrique
public key infrastructure (PKI)	infrastructure à clé publique (ICP)
key management system	système de gestion de clés
recording local authority	autorité locale d'enregistrement (ALE)
reject	rejet
reliability	fiabilité (ou sûreté de fonctionnement)
repudiation	répudiation
rerouting	réacheminement
risk analysis	analyse de risque ; étude de risque ; évaluation des menaces et des risques
risk analysis	étude de risque (voir analyse de risque)
risk analysis	évaluation de la menace et des risques (EMR) (voir analyse de risque)
(Rivest, Shamir et Adleman)	(Rivest, Shamir et Adleman)
secret key	clé secrète
security audit trail; audit trail	piste de vérification; piste de contrôle
security authorities register	registre des autorités de la sécurité
security procedure	procédure de sécurité informatique
sensitive data; critical data	donnée sensible ; donnée critique ; donnée vitale
sensitive information	renseignements de nature délicate

signature public key third party certifier	tiers certificateur de clés publiques de signature
simple smart card	carte à mémoire simple ; carte à simple mémoire
spray paint; integrity locking	scellement; verrouillage
supplier	fournisseur
system integrity	intégrité du système
telepayment	télépaiement
teleprocessing	télétraitement
teletransmission	télétransmission
traffic analysis	analyse de trafic
trusted third party ; trusted authentication authority	tiers de confiance
two-way authentication	authentification réciproque ; authentification mutuelle ; reconnaissance mutuelle
two-way authentication	reconnaissance mutuelle (voir authentification réciproque)
unclassified data	donnée non classée
user	utilisateur; usager
user authentication	authentification de l'utilisateur
user identification code; user ID	code utilisateur ; code d'identification
virus detection software; detection program; virus-screening program	détecteur de virus
Web server	serveur Web
wired logic card	carte à logique câblée

LISTE DES ABRÉVIATIONS ET ACRONYMES

AAE	Autorisation et authentification électroniques
ABA	American Bar Association
AC	Autorité de certification
ACC	Autorité de certification centrale
AE	Autorité d'enregistrement
AGP	Autorité de gestion des politiques
ALE	Autorité locale d'enregistrement
ANSI	American National Standards Institute (norme américaine)
APC	Autorité de politique de certification
API	Interface de programme d'application
CCITT	Comité consultatif international télégraphique et téléphonique
CDC	Centre de distribution des clés
CEAP	Programme d'homologation et d'évaluation des matériels de cryptographie
CEI	Commission électrotechnique internationale
CICS	Système de contrôle de l'information
CST	Centre de la sécurité des télécommunications
DES	Data Encryption Standard (norme américaine)
DSA	Digital Signature Algorithm
DSS	Norme américaine de signature numérique
EMA	Évaluation de la menace et des risques
EMR	Évaluation de la menace et des risques
EPC	Énoncé de pratiques de certification
ESN	Entité de signature numérique
FIPS	Federal Information Processing Standard (É.-U.)
GQ	Gouvernement du Québec
GC	Gouvernement du Canada
GUSA	Gouvernement des États-Unis
GRC	Gendarmerie royale du Canada
GSS	Generic Security Services (norme Internet)
ICP	Infrastructure de clés publiques
IETF	Internet Engineering Task Force
IP	Protocole Internet
IPRA	Internet Policy Registration Authority
ISO	Organisation internationale de normalisation
LAR	Liste des autorités révoquées
LCR	Liste de certificats révoqués
LRC	Liste de révocations des certificats
MAC	Message Authentication Code
MD2	Message Digest version 2 (algorithme de hachage)
MD5	Message Digest version 5 (algotithme de hachage)
MDS	Système d'exploitation à mémoire virtuelle multiple

MSP	Message Security Protocol
NIP	Numéro d'identification personnel
NIST	National Institute of Standards and Technology (É.-U.)
NSA	National Security Agency (É.-U.)
NSN	Nortel Secure Networks
PC	Politique de certification
PCMCIA	Personal Computer Memory Card International Association
PDSO	Packet Data Security Overlay
PKCS	Normes de cryptographie à clé publique
PKITWG	Public-Key Infrastructure Technical Working Group (É.-U.)
PKIX	Public-Key Infrastructure (X.509)
RSA	Algorithme de Rivest-Shamir-Adleman
SEP	Secure Exchange Protocol
SGC	Services de gestion des certificats
SGEC	Système de gestion électronique des clés
SHA	Secure Hash Algorithm
S/MIME	Secure/Multipurpose Internet Mail Extension
SMTP	Simple Mail Transfer Protocol
SPKM	Simple Public Key Mechanism
STI	Sécurité des technologies de l'information
TCP	Protocole de contrôle de transmission
TSR	Programme résidant en mémoire
UIT	Union internationale des télécommunications (autrefois CCITT)
URL	Uniform Resource Locator (adresse sur le World Wide Web)
X.400	Recommandations de l'UIT-T sur les Systèmes de messagerie
X.500	Recommandations de l'UIT-T sur le Système d'annuaire (répertoire)