Ébauche pour consultation

Principes d'authentification électronique

Préparé par : Direction générale du commerce électronique
Industrie Canada

Pour : Groupe de travail sur les principes d'authentification

Date : Le 23 juin 2003

TABLE DES MATIÈRES

Partie A : Introduction

Contexte

Les parties prenantes canadiennes- les personnes physiques, les entreprises et les administrations publiques - partagent un intérêt commun : faire en sorte que les communications électroniques soient sûres. Étant donné que notre utilisation des réseaux électroniques publics continue d'évoluer, passant d'une simple recherche d'information sur Internet à l'échange d'information et d'argent, nous avons besoin d'une plus grande assurance que ces messages et ces transactions sont sûrs et que nos renseignements personnels sont protégés. L'authentification peut faire beaucoup pour répondre à ce besoin et pour instaurer la confiance chez les utilisateurs.

> *L'authentification est un processus qui atteste des attributs des parties prenantes à une communication électronique ou de l'intégrité de la communication.*

Les présents principes sont conçus pour servir de points de repère à l'élaboration, à la prestation et à l'utilisation des services d'authentification au Canada. Ils sont censés former la base des codes de conduite, des initiatives bénévoles et des lignes directrices qui sont adoptés aux exigences de secteurs industriels ou gouvernementaux précis. Pour les personnes physiques et les entreprises qui utilisent les services d'authentification, les principes sont censés constituer une source d'information utile et un point de repère au regard duquel elles peuvent évaluer les services offerts sur le marché.

Les principes ont été élaborés par un groupe de travail qui a été convoqué par Industrie Canada et qui est formé de personnes provenant généralement de l'industrie, d'associations professionnelles, de groupes de consommateurs et de divers niveaux de gouvernement. Les personnes suivantes ont participé au Groupe de travail :

Bell Canada	David Masse, Conseiller juridique principal
Comité consultatif canadien, Sécurité des TI	Alice Sturgeon, Présidente
Association des banquiers canadiens	Gary Ferris, Conseiller, Opérations bancaires
Association du Barreau canadien	Mairi MacDonald
Institut Canadien des Comptables Agréés	Bryan Walker, Directeur principal, Groupe des innovations
Association canadienne des paiements	Michaela McBean, Agente principale, Services des paiements
CataAlliance	Dave Paterson, Directeur exécutif
Association des comptables généraux accrédités du Canada	Bruce Hutton, Vice-président, CGA Ontario
Deloitte & Touche LLP Canada	Jane Dargie, Consultante principale, Sécurité des affaires électroniques
	Richard Kitney, Directeur, Sécurité des affaires électroniques
Digital Discretion Inc.	Stéphanie Perrin, Présidente
Fidelity Investments	Heleen Krzycki, Directrice, Solutions d'affaires
Finances Canada	Andrew Rector, Division du secteur financier
Gowling Lafleur Henderson LLP	Michael Power
Industrie Canada (Direction générale du commerce électronique)	Peter Ferguson, Directeur, Élaboration des politiques
	Jane Hamilton, Conseillère principale en politiques
Industrie Canada (Bureau de la consommation)	Susan Gardiner, Analyste principale des politiques
Association canadienne de la technologie de l'information	Bill Munson, Directeur exécutif, Politiques et Planification
Bureau d'assurance du Canada	Randy Bundus, Conseil général et secrétaire général
	Ron Bilyk, Agent de conformité, Zurich Amérique du Nord
Juricert	Ron Usher, Vice-président
Province de la Colombie-Britannique	Brent Grover, Conseiller principal, Services de gestion
Province de l'Ontario	John Gregory, Conseiller général, Direction des politiques, Procureur général
Centre pour la défense de l'intérêt public	Philippa Lawson, Conseillère principale
RBC Groupe financier	David Braidwood, Gestionnaire principal , Normes et Sécurité
	Rosemarie Gage, Gestionnaire principale, Politique sur les transactions électroniques
Conseil canadien du commerce de détail	Ken Morrison
Scotiabank	Phil Griffiths, Vice-président
Conseil canadien des normes	Begonia Lojk, Gestionnaire des programmes de normalisation
Spyrus Inc.	Alice Sturgeon, Architecte des politiques sur les systèmes
Teranet Inc.	Nancy Peng, Gestionnaire de produits, Services de sécurité
Secrétariat du Conseil du Trésor	Susan Bryant, Directrice, Secrétariat de l'ICP

Université d'Ottawa (École de droit) — Greg Hagen
Visa Canada Association — Susan MacKeown, Directrice, e-VISA Canada

Les membres du Groupe de travail sont d'accord pour dire que la présente version des principes doit être distribuée pour qu'un plus grand nombre d'intervenants puisse les examiner et faire en sorte que les principes reflètent la plus vaste gamme possible de points de vues et d'intérêts.

1. Terminologie et concepts

Les principes ont rapport à l'authentification dans son sens large et tiennent compte des aspects politiques, juridiques et techniques. Par conséquent, les expressions utilisées s'appliquent aux parties prenantes, aux actions et aux techniques qui touchent tous les aspects de l'authentification, qu'elle soit considérée d'un point de vue technique, juridique ou commercial.

Les concepts définis reflètent le contexte canadien. Ces concepts sont tous des composantes de l'authentification dans son sens large; chaque concept est lié aux autres et aucun ne devrait être considéré de manière isolée.

Authentification : *Processus qui atteste des attributs des parties prenantes à une communication électronique ou de l'intégrité de la communication.*

Commentaire : L'*authentification* électronique est utilisée pour promouvoir la confiance dans l'activité électronique. Les parties prenantes ont l'assurance que les autres parties prenantes à une communication électronique ont été authentifiées par des méthodes technologiques et qu'elles peuvent se fier à ces autres parties prenantes, ainsi qu'à l'intégrité de la communication, dans la mesure précisée par l'authentificateur. Les méthodes et les spécifications technologiques utilisées sont souvent basées sur des techniques cryptographiques.

Communication électronique *: Transmission, message ou transaction électronique.*

Commentaire : Les parties prenantes se fient à l'authentification d'une communication électronique dans la mesure où elles peuvent évaluer la fiabilité de l'authentification.

Attributs : *Information concernant l'identité, les privilèges ou les droits d'une partie prenante ou d'une autre entité authentifiée.*

Commentaire : L'authentification comme telle dépend de certaines activités préalables qui autorisent les parties prenantes, sur présentation de certains *attributs* donnés, à prendre part à une communication électronique authentifiée. Les attributs peuvent être inhérents, comme l'identité, ou assignés, comme un privilège de prendre part à une transaction donnée. L'autorisation relève d'une autorité désignée. Il existe de nombreux modèles pour octroyer une telle autorisation. Par exemple, pour être autorisé, un simple échange d'information peut ne nécessiter que la présentation d'un nom d'utilisateur et d'un mot de passe. Un système électronique établi pour communiquer des renseignements hautement confidentiels et privés peut, par ailleurs, nécessiter la présentation en personne d'une ou deux pièces d'identité fiables ainsi que la présentation de caractéristiques personnelles distinctes, comme les empreintes digitales. Un autre modèle peut désigner un employeur comme autorité : c'est alors ce dernier qui autorise un groupe d'employés à échanger, en son nom, des communications électroniques d'après les fonctions du poste de chacun.

Les attributs d'une partie prenante peuvent avoir rapport avec l'identité d'une personne. Il se peut aussi que les attributs requis concernent les droits ou les privilèges qu'a cette personne de prendre part à une communication électronique. Dans le dernier cas, il se peut que l'identité personnelle d'un partie prenante n'ait pas à être communiquée aux autres parties prenantes.

Partie prenante : *Personne ou organisation qui participe à un processus d'authentification, que ce soit directement ou par l'intermédiaire d'une autre entité authentifiée, comme un service de transmission de données ou un objet de données, un périphérique ou un programme logiciel.*

Commentaire : Les processus d'authentification attestent souvent des attributs d'entités non humaines. Par exemple, une organisation participant à un processus d'authentification peut choisir d'authentifier un serveur. Le cas échéant, les attributs du serveur peuvent avoir trait aux privilèges qui lui ont été assignés de communiquer avec d'autres serveurs ou clients du système.

Authentificateur : *Autorité désignée qui confirme les attributs d'une partie prenante ou d'une entité et qui en atteste ensuite auprès des autres parties prenantes à la communication électronique.*

Intégrité : *Assurance que l'information contenue dans une communication électronique n'a pas été modifiée ou corrompue durant le processus de communication.*

***Note*:** La « non-répudiation » est une expression qui n'est pas définie ni utilisée en rapport avec les présents principes. L'expression est communément utilisée pour décrire une norme

technique que doit respecter un processus d'authentification. Toutefois, l'expression est trompeuse dans un contexte plus général parce qu'elle sous-entend, à tort, une conclusion de droit.

2. Fonctions

Aux fins des présents principes, on considère que le processus d'authentification comporte six fonctions de base. Leur importance relative dépend du but et de la structure du processus d'authentification. Ces fonctions de base peuvent être ainsi décrites.

Administration de l'authentification
Administrer la mesure ou les mesures conçues pour confirmer les attributs d'une partie prenante et la mesure ou les mesures conçues pour appuyer la crédibilité d'une partie prenante qui soutient posséder ces attributs et, par conséquent, être authentifiée.

Spécification
Établir ou choisir un processus d'authentification et un mécanisme d'exécution.

Utilisation finale
Envoyer ou recevoir une communication électronique authentifiée et se fier à l'authentification des attributs.

Élaboration de normes
Établir des normes qui appuient l'élaboration continue de processus conçus pour faciliter l'authentification des communications électroniques.

Évaluation de la conformité
Observer les pratiques liées à l'authentification et en faire des évaluations éclairées afin de s'assurer que les politiques, les procédures et les normes appropriées sont respectées.

Prestation d'infrastructure
Fournir la capacité technique qui permet l'authentification, y compris les fonctions permettant d'authentifier l'identité ou l'intégrité des communications électroniques ou fournir la technologie sous-jacente utilisée pour communiquer par voie électronique.

3. Pourquoi et comment utiliser ces principes

Les principes visent à orienter l'élaboration, la mise en oeuvre et l'utilisation des produits et des services d'authentification au Canada. Ils sont complémentaires à la structure de gouvernance[1] existante pour l'authentification, car ils établissent des points de repère qui font en sorte que les produits et les services d'authentification incorporent de saines pratiques commerciales, répondent aux besoins des Canadiens et sont acceptés à l'échelle internationale.

Le structure de gouvernance qui s'applique aujourd'hui aux services d'authentification au Canada est constituée notamment des lois fédérales et provinciales pertinentes, y compris la *Loi sur la protection des renseignements personnels et les documents électroniques* de 2000, la *Politique du Canada en matière de cryptographie* de 1998, les *Principes régissant la protection des consommateurs dans le commerce électronique*, qui ont été élaborés en 2001, et le *Code canadien de pratiques pour la protection des consommateurs dans le commerce électronique*, qui a été approuvé en principe en janvier 2003.

Les principes devraient être surtout utiles aux intervenants qui participent à la conception, à l'élaboration et au déploiement des services et des produits d'authentification. Les principes établissent les fonctions et les responsabilités des parties prenantes aux processus d'authentification et ils fournissent un cadre d'évaluation et de gestion des risques liés à ces responsabilités. Ils font aussi état des questions de sécurité, de protection des renseignements personnels, de divulgation et de traitement des plaintes dont il faut tenir compte à chaque étape de la conception, de l'élaboration, de la mise en oeuvre et de l'évaluation d'un processus d'authentification.

Les intervenants qui participent à la conception, à la mise en oeuvre et à l'exécution courante des processus d'authentification sont encouragés non seulement à respecter les principes, mais aussi à les faire connaître. Les principes devraient constituer la base des codes de conduite, des initiatives volontaires et des lignes directrices qui sont adaptés aux exigences de secteurs industriels et gouvernementaux précis. On encourage fortement de telles initiatives sectorielles, car elles peuvent offrir des avantages stratégiques sur les marchés nationaux et internationaux.

Les principes sont censés être une source d'information utile et servir de point de repère aux personnes physiques et aux entreprises qui utilisent l'authentification. D'autres lois ou d'autres mesures pourraient être adoptées afin de répondre aux besoins des utilisateurs finals, particulièrement en ce qui concerne les risques et les responsabilités assumés par les personnes physiques participant aux processus d'authentification.

Le milieu de l'authentification est dynamique et les technologies en cause continueront d'évoluer. Même si on a tout fait pour définir des principes susceptibles de tenir compte des développements prévisibles, ces derniers pourront être révisés au besoin pour tenir compte des percées technologiques importantes, des changements dans les caractéristiques du marché et des nouveautés internationales. Les commentaires et les points de vue sur ces principes sont toujours les bienvenus et devraient être adressés à :

Richard Simpson
Directeur général
Direction générale du commerce électronique
Industrie Canada
300, rue Slater, pièce D2090
Ottawa (Ontario)
K1A 0C8

Les commentaires peuvent aussi être envoyés par télécopieur au (613) 941-0178 ou par courriel à authen@ic.gc.ca.

Les principes seront examinés au moins tous les cinq ans et ils peuvent être révisés plus souvent au besoin. Le Groupe de travail sur les principes d'authentification est chargé de l'examen et de la révision périodiques des principes. La composition du Groupe sera évaluée et modifiée s'il y a lieu à mesure que le contexte d'authentification évoluera.

[1] L'expression « structure de gouvernance » désigne la gamme d'outils stratégiques, d'instruments réglementaires et de directives d'autoréglementation qui ont trait à l'élaboration et à la mise en oeuvre des services d'authentification au Canada.

4. Portée et nature

Ces principes se rapportent à l'authentification électronique dans son sens large.

Les principes sont censés s'appliquer aux processus d'authentification utilisés en rapport avec les communications électroniques entre des entreprises ou des administrations publiques et d'autres organisations du même genre, entre de telles organisations et des personnes physiques, comme les consommateurs et les citoyens, et entre des consommateurs et des citoyens.

Il peut exister toutes sortes de relations entre les authentificateurs et les utilisateurs finals, et entre les utilisateurs finals. Nombreuses sont ces relations qui seront régies par une entente. Les principes sont censés orienter l'élaboration de ces ententes et s'appliquer à la gamme complète de ces relations.

Ls parties à des contrats négociés sont habituellement les mieux placées pour déterminer les modalités qui conviennent à leurs besoins particuliers. Toutefois, les principes revêtent une importance particulière dans les situations où une partie peut ne pas avoir la possibilité de négocier les modalités de son interaction avec l'autre partie (ou les autres parties) à la transaction.

Les principes devraient être considérés et appliqués comme s'ils formaient un tout.

Les dispositions des divers principes sont interreliées et interdépendantes; les principes ne peuvent pas atteindre leurs buts s'ils sont mis en oeuvre sélectivement, quoiqu'ils peuvent ne pas tous s'appliquer dans tous les cas. Les personnes chargées d'appliquer les principes pour définir ou mettre en oeuvre les processus d'authentification sont encouragées à dépasser les points de repère établis par les principes et à les élargir en vue de répondre aux exigences de leur application ou de leur contexte de sécurité particulier.

Les principes sont de nature très générale et ils sont neutres sur le plan technologique.

Les Canadiens peuvent choisir parmi une variété de technologies pour authentifier leurs communications électroniques, selon la nature de la communication particulière et les exigences des parties prenantes.

La mise en oeuvre des processus d'authentification variera aussi en fonction des objectifs commerciaux ou légaux à atteindre ainsi que des caractéristiques de l'environnement dans lequel la communication électronique se fera, comme les besoins en matière de sécurité et de protection des renseignements personnels et les autres obligations législatives ou réglementaires. Ces facteurs définiront la fonctionnalité requise d'un processus d'authentification et, dans certains cas, ils définiront même le type d'authentification utilisé.

Les principes sont conçus de manière à favoriser un marché juste et concurrentiel qui fonctionne bien pour les produits et les services d'authentification.

Les principes reflètent les intérêts des entreprises et des administrations publiques et ils tiennent compte des points de vue des consommateurs. Chaque fois que la chose est possible, les principes laissent place au choix : choix de la technologie, choix des services, des solutions et du degré de confiance par les utilisateurs finals et choix des outils utilisés pour assurer la conformité.

Les principes mettent l'accent sur la proportionnalité.

Le niveau de responsabilité et de risque assumé par chaque partie prenante au processus d'authentification devrait être raisonnablement proportionnel au niveau de connaissance que celle-ci devrait posséder et au niveau de contrôle qu'elle devrait exercer ainsi qu'à la nature et à la valeur de la communication électronique même. Étant donné que les parties prenantes peuvent accomplir des fonctions multiples, qui peuvent être combinées différemment, le niveau de risque et de responsabilité assumé par une partie prenante peut varier selon ces fonctions.

Les principes mettent l'accent sur la protection des renseignements personnels.

Les principes reconnaissent que le cadre juridique qui existe au Canada pour la protection des renseignements personnels évolue et ils tiennent compte de la façon dont les normes de protection des renseignements personnels s'appliquent à l'authentification. Les principes visent la jonction entre les pratiques liées au respect de la vie privée et les pratiques liées à l'amélioration de la sécurité. L'importance de cette question pour les Canadiens oblige les responsables de la conception et de la mise en oeuvre des mesures d'authentification électronique à voir comment

leurs systèmes peuvent le mieux respecter la protection des renseignements personnels à chaque étape du processus.

Les principes ont été élaborés de manière à être compatibles avec les innovations internationales dans le domaine de l'authentification.

Le Canada s'est engagé à continuer de participer aux différents forums internationaux qui traitent de la nécessité de créer des cadres mondiaux pour l'authentification. Cette participation fait en sorte que l'approche du Canada reste alignée sur celle des autres pays, ce qui permet à l'industrie canadienne d'être concurrentielle sur le marché international.

Partie B : Principes

Principe 1 : Responsabilités des parties prenantes

Les parties prenantes à un processus d'authentification devraient être conscientes des fonctions qu'elles accomplissent et des responsabilités liées à ces fonctions. Les responsabilités des parties prenantes sont proportionnelles au niveau de connaissance que celles-ci devraient posséder et au niveau de contrôle qu'elles devraient exercer.

Toutes les parties prenantes devraient agir prudemment et prendre des mesures raisonnables pour s'informer de la nature du processus d'authentification, notamment des exigences et des limites du processus, pour protéger l'information liée au processus et pour gérer les risques auxquels elles s'exposent (voir le principe n° 2).

En outre, les parties prenantes acceptent les responsabilités précises qui se rattachent à la fonction ou aux fonctions qu'elles accomplissent.

Administration de l'authentification
Il incombe à l'administrateur d'appliquer des mesures appropriées et éprouvées de sorte que les autres parties prenantes puissent avoir confiance dans la crédibilité des attributs revendiqués. Si l'administrateur a délégué une partie de la fonction d'administration à un tiers, il lui appartient de s'assurer que le tiers applique aussi des processus appropriés et éprouvés.

Spécification
La partie prenante responsable de la spécification est chargée de choisir un système, comme une infrastructure ou un processus d'authentification, qui répond aux exigences de protection des renseignements personnels et de sécurité et aux autres exigences politiques et juridiques liées à une communication électronique. Cela peut comprendre le mécanisme par lequel on vérifie l'autorisation d'une partie prenante de prendre part à une communication électronique et l'intégrité de la communication comme telle.

Utilisation finale
La responsabilité qu'ont les utilisateurs finals de s'informer du processus d'authentification est limitée par la mesure dans laquelle une information claire et évidente leur est divulguée (voir le principe n° 5). La responsabilité qu'ont les utilisateurs finals de protéger l'information concernant le processus d'authentification peut être limitée par les obligations juridiques et contractuelles qui les obligent à divulguer de l'information concernant les mécanismes qu'ils utilisent pour déterminer la fiabilité des communications électroniques.

Élaboration de normes
Les parties responsables de l'élaboration de normes sont chargées de veiller à ce que les normes soient solides, extensibles et adaptables afin d'encourager l'uniformité dans la mise en oeuvre de l'authentification. Cette responsabilité englobe l'incorporation d'une vaste gamme de points de vue et de pratiques exemplaires dans les normes proposées, ce qui permet de voir à ce quelles soient pertinentes, actuelles et continuellement applicables. Une élaboration de normes prudente tient compte des technologies et des pratiques internationales existantes et émergentes.

Évaluation de la conformité
Il incombe aux responsables de l'évaluation de la conformité de maintenir et d'appliquer des connaissances et des pratiques professionnelles et actuelles de manière à pouvoir fournir une évaluation raisonnée et éclairée des processus d'authentification.

Prestation d'infrastructure
Les prestataires d'infrastructure sont chargés de respecter les pratiques exemplaires et les normes pour mettre en oeuvre et appuyer l'infrastructure qui permet l'authentification.

Principe 2 : Gestion du risque

Les risques liés aux processus d'authentification électronique devraient être déterminés, évalués et gérés d'une manière raisonnable, juste et efficace.

Les responsabilités des parties prenantes en matière de gestion des risques sont proportionnelles au niveau de connaissance que celles-ci devraient posséder et au niveau de contrôle qu'elles devraient exercer. On reconnaît que la capacité des parties prenantes de déterminer, d'évaluer et de gérer les risques varie considérablement et qu'on ne peut pas raisonnablement attendre de certaines parties prenantes (p. ex. les consommateurs et les petites entreprises) qu'elles déterminent, évaluent et gèrent les risques dans la même mesure que les parties prenantes qui ont accès à des ressources plus importantes ou qui définissent les relations de travail. Compte tenu de ce qui précède :

- Les risques devraient être déterminés dans la mesure du possible. Les risques peuvent être matériels (comme les risques concrets ou les risques financiers qui comprennent les dommages immédiats, directs et indirects issus d'une exécution défectueuse ou d'un retard d'exécution) ou moraux (comme la perte de confidentialité ou de protection des renseignements personnels, les dommages à la réputation, le vol d'identité, etc.).

- Les risques devraient être évalués au regard de leur gravité et de leur incidence possible. Lorsqu'on évalue les risques, il faut prêter une attention spéciale au point et au moment où l'on fait confiance au processus d'authentification. Lors de l'évaluation des risques, il peut être utile de tenir compte des responsabilités liées à chacune des six fonctions (voir le principe n° 1).

- Les risques devraient être gérés jusqu'à hauteur de la plus grande efficience économique, c'est-à-dire qu'ils doivent être assumés, évités, réaffectés ou atténués. La gestion des risques est efficiente sur le plan économique si le risque résiduel qu'une partie prenante assume après avoir appliqué des principes de gestion prudente des risques n'est pas plus grand que les avantages qu'elle tire de sa participation.

- Les contrats peuvent être utilisés pour encadrer la participation de chaque partie prenante. Les contrats devraient indiquer clairement les risques assumés par chaque partie et répartir les risques de manière raisonnable, juste et efficiente. Dans le cas des contrats qui ne sont pas négociés librement entre parties égales[1], il peut être nécessaire de prendre des mesures pour protéger les intérêts des parties les plus faibles[2].

- Peu importe les moyens utilisés pour attribuer les risques, l'attribution devrait être raisonnable et juste et tenir compte de la capacité des parties prenantes de gérer les risques ou d'absorber les pertes. Elle devrait aussi inciter les parties chargées de l'élaboration et de la mise en oeuvre des processus d'authentification à voir à ce que leurs produits et leurs services soient sûrs et fiables.

[1] Par exemple, les contrats qui imposent la durée des services aux utilisateurs.

[2] Les mesures en ce sens peuvent être prises au niveau du secteur d'activité et se traduire par l'inclusion de dispositions dans les codes ou au niveau gouvemental et se traduire par l'adoption de politiques ou de lois.

Principe 3 : Sécurité

Toutes les parties prenantes à un processus d'authentification devraient être responsables et comptables de la sécurité en proportion des rôles qu'elles ont joués dans ce processus. Toutes les parties prenantes sont chargées de contribuer à atténuer les risques grâce à de saines pratiques en matière de sécurité. Toutefois, il appartient principalement aux prestataires d'infrastructure et aux intervenants dans l'administration de l'authentification de concevoir et d'offrir des systèmes basés sur des politiques et des procédures qui tiennent compte des lois, des règlements, des politiques, des normes industrielles et du contexte socio-culturel pertinents [1].

La sécurité de l'information a pour objet d'atténuer les risques inhérents au partage d'information par voie électronique. Les prestataires d'infrastructure et les intervenants dans la spécification et l'administration des processus d'authentification prennent souvent l'initiative de concevoir et de mettre en oeuvre des mécanismes de sécurité et ils ont donc intérêt à sensibiliser davantage les autres parties prenantes en les renseignant sur ces mécanismes et sur le rôle qu'elles ont à jouer dans leur maintien (par exemple, choix et protection des mots de passe des utilisateurs). Les mécanismes de sécurité devraient se conformer aux normes applicables généralement reconnues.

S'il y a lieu, toutes les parties prenantes devraient être mises au courant et rester conscientes des risques pour la sécurité, des menaces connues et des vulnérabilités ainsi que des parades existantes. Dans un processus d'authentification, un incident de sécurité qui touche une seule partie prenante peut avoir des répercussions pour toutes les parties prenantes. Les parties prenantes devraient donc toujours agir de manière à prévenir de tels incidents et elles devraient être prêtes à répondre de façon appropriée et capables de le faire. Les parties prenantes devraient échanger des informations au sujet des menaces, des vulnérabilités et des risques connus, car c'est une mesure de prévention efficace qui permet d'accroître la vigilance au niveau de la détection et d'assurer une réponse opportune. Les mesures de sécurité de l'information efficaces devraient être proportionnelles au risque pour l'information et respecter les droits des parties prenantes, conformément aux principes démocratiques d'une société ouverte.

Les technologies de l'information évoluent très rapidement. Par conséquent, une saine pratique de gestion de la sécurité consisterait à faire en sorte que toutes les parties prenantes soient informées de manière fiable des menaces nouvelles et existantes et du rôle qu'elles devraient jouer pour prévenir, détecter et régler les incidents.

Il est essentiel d'examiner et d'évaluer continuellement les programmes de sécurité afin d'en assurer l'efficacité permanente. Les responsables de l'établissement des processus d'authentification et les prestataires d'infrastructure en particulier, de concert avec les autres parties prenantes au processus d'authentification, devraient vérifier et prouver qu'elles adhèrent à de saines pratiques de gestion de la sécurité, chacun en proportion du rôle qu'il joue. Une personne indépendante du processus d'authentification devrait examiner périodiquement les pratiques de sécurité associées au processus, et un tel examen devrait faire partie intégrante de tout processus d'accréditation et de certification au regard des normes généralement reconnues.

[1] Le principe de la sécurité reconnaît et adopte les *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité*. Les neuf principes des *Lignes directrices de l'OCDE* sont résumés à la partie C du présent document. Le texte intégral des *Lignes directrices*, se trouve en ligne à l'adresse suivante http://www.oecd.org/pdf/M00034000/M00034292.pdf tout comme les renvois aux normes internationales pertinentes concernant la sécurité des TI, la vérification d'authentification, l'accréditation, les lignes directrices sur la certification et les autres documents d'intérêt qui traitent de la sécurité des processus d'authentification.

Principe 4 : Protection des renseignements personnels

Toutes les organisations engagées dans la conception ou l'exécution des processus d'authentification devraient au moins se conformer aux normes de protection des données énoncées dans les lois, la jurisprudence et les codes de pratique (lois et codes en matière de protection des renseignements personnels)[1] applicables. En particulier, la collecte, l'utilisation et la divulgation de renseignements personnels[2] devraient être réduites au minimum dans le contexte de l'authentification.

L'authentification fondée sur l'identité peut entrer en conflit avec les questions de protection des renseignements personnels. Une authentification plus poussée, par exemple, peut nécessiter la collecte et la comparaison d'une plus grande quantité de renseignements personnels. Toutefois, il est essentiel à la sécurité et à la protection des renseignements personnels de réduire au minimum la collecte, l'utilisation et la divulgation de renseignements personnels dans le contexte de l'authentification. Des mesures de protection des renseignements personnels peuvent en fait contribuer à la sécurité des processus d'authentification.

Administration de l'authentification

L'administration de l'authentification devrait faire intervenir la collecte de renseignements personnels seulement lorsqu'elle est nécessaire. Les renseignements personnels recueillis ne devraient être utilisés qu'aux fins d'authentification. L'authentification d'une entreprise devrait focaliser sur les attributs de l'entreprise plutôt que sur les attributs personnels des employés individuels.

Si la collecte de renseignements personnels est nécessaire, elle doit être réduite au minimum. La conservation, l'utilisation ou la divulgation des renseignements personnels devraient aussi être réduites au minimum.

Des renseignements personnels devraient être recueillis, conservés, utilisés ou divulgués seulement avec le consentement éclairé de la personne physique.

Spécification et prestation d'infrastructure

Les processus d'authentification doivent être conçus de manière à exiger que le moins possible de renseignements personnels soient recueillis, utilisés et divulgués. La conception des

[1] Les lois générales de protection des renseignements personnels dans le secteur privé actuellement en vigueur englobent la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) (loi fédérale) et la *Loi sur la protection des renseignements personnels dans le secteur privé* (loi du Québec) (projet de loi 68). Les provinces autres que le Québec peuvent aussi adopter des lois générales de protection des renseignements personnels. Des lois en matière de protection des renseignements personnel du secteur public fédéral/provincial et des lois de protection des renseignements personnels propres à un secteur peuvent aussi s'appliquer.

Le *Code type sur la protection des renseignements personnels* de la CSA, CAN/CSA-Q830-96, a été incorporé dans la loi fédérale intitulée *Loi sur la protection des renseignements personnels et les documents électroniques*, L. C. 2000, chap. 5 (LPRPDE), à titre d'annexe 1. Ce code a été élaboré par un groupe de travail multipartite et adopté par le Conseil canadien des normes à titre de norme nationale en 1996. Beaucoup de codes de pratiques industriels traitent aussi de la protection des renseignements personnels.

[2] Conformément à la définition de la LPRPDE : « tout renseignement concernant un individu identifiable ».

processus devrait tenir compte des droits d'accès des parties prenantes et de l'obligation qu'ont les organisations de communiquer de l'information au sujet de leurs politiques en matière de protection des renseignements personnels. Les organisations qui utilisent des processus d'authentification conçus par d'autres sont chargées de faire en sorte que ces processus protègent les renseignements personnels.

Utilisation finale

Les utilisateurs finals des processus et des services d'authentification devraient prendre des mesures raisonnables pour s'assurer que les renseignements personnels placés sous leur contrôle sont protégés contre la collecte, l'utilisation ou la divulgation non autorisée.

Élaboration de normes

Les normes d'authentification devraient être élaborées en pleine conformité avec les principes concernant la protection des renseignements personnels qui sont énoncés dans les lois et les codes sur la protection des renseignements personnels. La protection des renseignements personnels devrait être explicitement enchâssée dans les normes d'authentification. Les responsables de l'élaboration des normes devraient tenir compte de la concordance entre les mesures qui contribuent à la protection des renseignements personnels et celles qui sont conçues pour assurer la sécurité des processus d'authentification.

Évaluation de la conformité

L'évaluation de la conformité devrait notamment déterminer si l'entité en question se conforme aux principes de protection des renseignements personnels énoncés dans les lois et les codes. Les évaluateurs de la conformité devraient protéger la confidentialité des renseignements personnels dont ils prennent connaissance dans le contexte de leurs évaluations, conformément aux lois et aux codes sur la protection des renseignements personnels.

Principe 5 : Obligations d'information

Les parties prenantes qui offrent des services d'authentification devraient divulguer des informations aux autres parties prenantes afin de faire en sorte que toutes les parties prenantes soient conscientes des risques et des responsabilités inhérents à leur participation.

L'information divulguée devrait inclure les politiques, les pratiques et les procédures et indiquer si les services sont examinés ou vérifiés régulièrement.

Une divulgation appropriée exige que l'information soit suffisamment détaillée pour l'objectif visé, qu'elle soit formulée en langage simple et qu'elle soit évidente. Les trois facteurs auront une incidence sur la connaissance de l'information divulguée que les autres parties prenantes devraient raisonnablement posséder.

L'information divulguée *ne* devrait *pas* inclure les informations liées à la sécurité qui, si elles étaient divulguées, introduiraient des vulnérabilités et augmenteraient le risque. Toutefois, la quantité et la nature des informations divulguées devraient permettre aux parties prenantes de comprendre leurs responsabilités et de prendre des décisions éclairées en matière de gestion du risque, pour ce qui est de la confiance à accorder à l'authentification. La portée et la nature de l'information peuvent varier selon que l'utilisateur final est une personne physique ou une organisation.

Les parties prenantes devraient être informées de l'accessibilité d'une telle information et des changements qui y sont apportés. Il se peut qu'une preuve de la notification soit exigée, selon la nature du processus d'authentification et des applications connexes.

Les parties prenantes qui offrent des services d'authentification devraient divulguer leur politique et leurs pratiques en matière de collecte de renseignements personnels. Le principe de la protection des renseignements traite plus en profondeur des renseignements personnels et de leur divulgation (voir le principe n° 4).

Les obligations d'information doivent être considérées de concert avec les principes n° 1 (responsabilités) et n° 2 (gestion du risque).

Principe 6 : Traitement des plaintes

Chaque fois que des processus ou services d'authentification sont mis en oeuvre, un processus de traitement des plaintes devrait être offert afin de permettre aux parties prenantes de régler les plaintes avec efficacité et efficience et de répondre de manière appropriée aux problèmes de non-conformité.

Les processus de traitement des plaintes devraient incorporer les principes suivants :

Visibilité
L'information sur les modalités de dépôt des plaintes devrait être communiquée à toutes les parties prenantes et au leur personnel et aux autres parties intéressées et devrait inclure des renseignements complets sur le processus de traitement des plaintes.

Accessibilité
Un processus de traitement des plaintes devrait être facilement accessible à toutes les parties prenantes et faire en sorte qu'il soit facile d'obtenir des renseignements sur les détails du règlement des différends. Pour les personnes physiques qui ont des plaintes à faire, le processus et l'information à l'appui devraient être faciles à comprendre et à utiliser, être expliqués en langage simple et être accessibles dans les langues des produits et des services offerts à l'origine.

Rapidité de réaction
Les plaintes devraient faire l'objet d'une étude rapide et minutieuse. Elles devraient être examinées du point de vue de la sécurité et réglées en priorité, selon les répercussions négatives qu'elles pourraient avoir sur les parties prenantes en cause ou sur la mise en oeuvre de l'authentification dans l'ensemble.

Équité et objectivité
Chaque plainte devrait être réglée de manière objective grâce au processus de traitement des plaintes et le règlement devrait être équitable pour le plaignant et pour la partie prenante visée par la plainte.

Frais
L'accès au processus de traitement des plaintes ne devrait rien coûter au plaignant à moins que les frais aient été déterminés et que le plaignant les aient acceptés à l'avance.

Confidentialité et protection des renseignements personnels
Les renseignements personnels sur les plaignants devraient être accessibles seulement aux points de l'organisation qui en ont besoin et ils doivent être activement protégés contre toute divulgation à moins que le plaignant consente expressément à la divulgation.

Reddition de comptes
Les organisations offrant des services d'authentification devraient veiller à ce qu'une personne physique nommée ou une unité identifiable de l'organisation soit chargée de consigner systématiquement les plaintes et les règlements des plaintes et de faire rapport sur les actions et les décisions de l'organisation en ce qui concerne le traitement des plaintes.

Amélioration continue
L'amélioration continue de la qualité des produits et services est facilitée par le processus de traitement des plaintes qui est basé sur les commentaires des clients et d'autres parties. Le processus même de traitement des plaintes devrait être surveillé en permanence et examiné et évalué à la lumière des commentaires.

Plaintes non réglées
Dans les cas où les plaintes ne peuvent pas être réglées à l'interne, les organisations devraient être prêtes à utiliser les processus de règlement des plaintes de tiers, à la demande du plaignant, y compris les processus administrés par des tiers du secteur privé. Toutefois, les plaignants devraient continuer à avoir accès au système de justice.

Partie C : Informations supplémentaires/Bibliographie

1. Informations supplémentaires

Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information

i. ***Sensibilisation***
Les parties prenantes doivent être sensibilisées au besoin d'assurer la sécurité des systèmes et réseaux d'information et aux actions qu'elles peuvent entreprendre pour renforcer la sécurité.

ii. ***Responsabilité***
Les parties prenantes sont responsables de la sécurité des systèmes et réseaux d'information.

iii. ***Réaction***
Les parties prenantes doivent agir avec promptitude et dans un esprit de coopération pour prévenir, détecter et répondre aux incidents de sécurité.

iv. ***Éthique***
Les parties prenantes doivent respecter les intérêts légitimes des autres parties prenantes.

v. ***Démocratie***
La sécurité des systèmes et réseaux d'information doit être compatible avec les valeurs fondamentales d'une société démocratique.

vi. ***Évaluation des risques***
Les parties prenantes doivent procéder à des évaluations des risques.

vii. ***Conception et mise en oeuvre de la sécurité***
Les parties prenantes doivent intégrer la sécurité en tant qu'un élément essentiel des systèmes et réseaux d'information.

viii. **Gestion de la sécurité**
Les parties prenantes doivent adopter une approche globale de la gestion de la sécurité.

ix. ***Réévaluation***
Les parties prenantes doivent examiner et réévaluer la sécurité des systèmes et réseaux d'information et introduire les modifications appropriées dans leur politiques, pratiques, mesures et procédures de sécurité.

2. Bibliographie

GÉNÉRALITÉS

National - Contexte

Industrie Canada - Politiques en commerce électronique - Authentification
http://e-com.ic.gc.ca/francais/authen/index.html

Politique du Canada en matière de cryptographie
Gouvernement du Canada, 1998
http://e-com.ic.gc.ca/francais/crypto/631d11.html

National - Initiatives connexes et documents de référence

a) Généralités

Loi sur la protection des renseignements personnels et les documents électroniques, L. C. 2000, chap. 5, Partie 2
http://lois.justice.gc.ca/fr/2000/5/index.html

Loi uniforme sur le commerce électronique
Conférence pour l'harmonisation des lois au Canada
http://www.ulcc.ca/fr/us/index.cfm?sec=1&sub=1u1

*Loi concernant le cadre juridique des technologies de l'information (*2001)
Province de Québec
http://www.autoroute.gouv.qc.ca/loi_en_ligne/loi/texteloi.html

Initiatives statutaires actuelles au Canada: commerce électronique, Ministère de la Justice Canada
http://canada.justice.gc.ca/fr/ps/ec/sriec.html

Gouvernement du Canada, Conseil du Trésor, Politique sur l'autorisation et l'authentification électroniques
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/TBM_142/2-2_f.asp

Secrétariat du Conseil du Trésor du Canada, Politique de gestion de l'Infrastructure clé publique au gouvernement du Canada
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/PKI/pki_f.asp

Gouvernement du Canada, Politiques de certification de signatures numeriques
http://www.cio-dpi.gc.ca/pki-icp/guidedocs/ds-cert-policy/introduction_f.asp

*Les codes volontaires : Guide d'élaboration et d'utilisation (*1998)
Gouvernement du Canada (Industrie Canada et Conseil du Trésor)
http://strategis.ic.gc.ca/SSGF/ca00863f.html

b) Protection des consommateurs

Principes régissant la protection des consommateurs dans le commerce électronique (1999)
Industrie Canada
http://strategis.ic.gc.ca/SSGF/ca01185f.html

Code canadien de pratiques pour la protection des consommateurs dans le commerce électronique
Industrie Canada
http://strategis.ic.gc.ca/pics/ca/eng_consumerprotection03.txt

Code de pratique canadien des services de cartes de débit (1996, révisé en 2002)
Industrie Canada
http://strategis.ic.gc.ca/SSGF/ca01581f.html

International - Initiatives connexes et documents de référence

Directive 1999/93/CE sur un Cadre communautaire pour les signatures électroniques (1999)
Le Parlement européen et le Conseil de l'Union européenne
http://europa.eu.int/ISPO/docs/policy/docs/399L0093/fr.pdf

Lignes directrices de l'OCDE régissant la protection des consommateurs dans le contexte du commerce électronique (2000)
http://www.oecd.org/EN/document/0,,EN-document-44-1-no-20-320-0,00.html
http://www.olis.oecd.org/olis/2002doc.nsf/LinkTo/dsti-cp(2002)4-final

International Consensus Principles for Electronic Authentication (1999)
Internet Law and Policy Forum
http://www.ilpf.org/events/intlprin.htm

Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (1999)
The Internet Engineering Task Force
ftp://ftp.isi.edu/in-notes/rfc2527.txt

Electronic Authentication: Issues Relating to its Selection and Use (2002)
Coopération économique Asie-Pacifique
http://www.apectelwg.org/apecdata/telwg/eaTG/EA_text.pdf

Loi type de la CNUDCI sur les signatures électroniques (2001)
http://www.uncitral.org/french/texts/electcom/ml-elecsign.pdf

Dialogue mondial des entreprises
http://www.gbde.org/authentication.html

Digital Signature Guidelines (1996)
American Bar Association
http://www.abanet.org/scitech/ec/isc/dsgfree.html

PRINCIPES

Principe 1 : Responsabilités des parties prenantes

Normes pour un marché numérique mondial : Cadre canadien de normalisation du commerce électronique (1998)
http://e-com.ic.gc.ca/francais/strat/doc/normes.pdf

Principe 2 : Gestion du risque

BITS Framework for Managing Technology Risk for Information Technology (IT) Service Provider Relationships (2001)
BITS Financial Services Roundtable
http://www.bitsinfo.org/FrameworkVer32.doc

Electronic Commerce: Who Carries the Risk of Fraud (2000)
Foundation for Information Policy Research, Royaume-Uni

http://elj.warwick.ac.uk/jilt/oo-3/bohm.html

Principe 3 : Sécurité

Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information (2002)
Organisation de coopération et de développement économiques
http://www.oecd.org/pdf/M00034000/M00034292.pdf

Norme de sécurité relative aux technologies de l'information du gouvernement du Canada
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23RECON-1_f.asp

ICP du gouvernement du Canada - Politiques et méthodes
http://www.cio-dpi.gc.ca/pki-icp/index_f.asp

AIPCA/ICCA Trust Services
www.aicpa.org/assurance/webtrust/princip.htm

PKI Assessment Guidelines (2001)
American Bar Association
http://www.abanet.org/scitech/ec/isc/pagv30.pdf

ISO 17799 Code de pratique pour la gestion de sécurité d'information (2000)
http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35&ICS2=40&ICS3=

ISO TR 13335 Lignes directrices pour la gestion de la sécurité des technologies de l'information
http://www.iso.org/iso/fr/CatalogueDetailPage.CatalogueDetail?CSNUMBER=21733&ICS1=35&ICS2=40&ICS3=

EESSI European Electronic Signatures Standards Initiative
http://www.ictsb.org/eessi/EESSI-homepage.htm

Principe 4 : Protection des renseignements personnels

Loi sur la protection des renseignements personnels et les documents électroniques, L. C. 2000, chap. 5, Partie 1 (2000)
Gouvernement du Canada
http://lois.justice.gc.ca/fr/2000/5/index.html

*Authentication Through the Lens of Privacy (*2003)
National Research Council, National Academies, États-Unis
http://www.nap.edu/books/0309088968/html/

Webtrust Program for Online Privacy (2000)
American Institute of Certified Public Accountants (AICPA)/Institut Canadien des Comptables Agréés (ICCA)
http://www.webtrust.org/privacy_fin.htm

Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals (2001)
Office of the Federal Privacy Commissioner, Australie

Principe 5 : Obligations d'information

Code canadien de pratiques pour la protection des consommateurs dans le commerce électronique
Industrie Canada

http://strategis.ic.gc.ca/pics/ca/eng_consumerprotection03.txt

Principe 6 : Traitement des plaintes

Projet de comité de l'ISO, ISO/CD 10018 : Gestion des réclamations
Organisation internationale de normalisation
http://www.iso.org/iso/fr/commcentre/news/2002/iso10018.html

AS/NZS 4269 *Complaints Handling*
http://www.standards.com.au/catalogue/script/Details.asp?DocN=stds000012657