



Industrie
Canada

Industry
Canada

PRINCIPES D'AUTHENTIFICATION ÉLECTRONIQUE

Cadre canadien

Mai 2004

Canada 

On peut obtenir cette publication sur supports multiples, sur demande. Communiquer avec le Centre de diffusion de l'information dont les coordonnées suivent.

Pour obtenir des exemplaires supplémentaires de la présente publication, s'adresser au :

Centre de diffusion de l'information
Direction générale des communications et du marketing
Industrie Canada
Bureau 268D, tour Ouest
235, rue Queen
Ottawa (Ontario) K1A 0H5

Téléphone : (613) 947-7466

Télécopieur : (613) 954-6436

Courriel : **publications@ic.gc.ca**

Cette publication ainsi que des renseignements supplémentaires concernant les principes sont offerts par voie électronique sur le Web (<http://strategis.ic.gc.ca/authen-fr>).

Autorisation de reproduction

À moins d'indication contraire, l'information contenue dans cette publication peut être reproduite, en tout ou en partie et par quelque moyen que ce soit, sans frais et sans autre permission d'Industrie Canada, pourvu qu'une diligence raisonnable soit exercée afin d'assurer l'exactitude de l'information reproduite, qu'Industrie Canada soit mentionné comme organisme source et que la reproduction ne soit présentée ni comme une version officielle ni comme une copie ayant été faite en collaboration avec Industrie Canada ou avec son consentement.

Pour obtenir l'autorisation de reproduire l'information contenue dans cette publication à des fins commerciales, faire parvenir un courriel à **copyright.droitdauteur@communication.gc.ca**.

N.B. Dans cette publication, la forme masculine désigne tant les femmes que les hommes.

N° de catalogue lu64-16/2004

ISBN 0-662-67949-0

54046B



Contient
10 p. 100 de
matières recyclées

TABLE DES MATIÈRES

Introduction	2
Pourquoi et comment utiliser les principes	4
Au sujet des principes	6
Concepts et terminologie	6
Portée et nature des principes	9
Principes	12
Principe 1 : Responsabilités des parties prenantes	12
Principe 2 : Gestion du risque	14
Principe 3 : Sécurité	16
Principe 4 : Protection des renseignements personnels	18
Principe 5 : Obligations d'information	20
Principe 6 : Traitement des plaintes	22
Informations supplémentaires et références	24

INTRODUCTION

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 en ligne, 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 des communications électroniques peut faire beaucoup pour répondre à ce besoin et

pour instaurer la confiance chez les utilisateurs.

Les présents principes d'authentification électronique sont conçus pour servir de points de repère à l'élaboration, à la prestation et à l'utilisation des services d'authentification au Canada. Les principes sont censés former la base des codes de conduite, des initiatives bénévoles et des lignes directrices adaptés aux exigences d'industries spécifiques et du gouvernement. Pour les personnes physiques et les entreprises qui utilisent les services d'authentification, les principes sont censés constituer une source d'information utile ainsi que des points de repère au regard desquels elles peuvent évaluer les services offerts sur le marché.

Les principes ont été élaborés par le Groupe de travail sur les principes d'authentification 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 organisations suivantes ont participé au groupe de travail et aidé à l'élaboration des principes :

Alliance canadienne de technologie de pointe	Industrie Canada (Direction générale sur le commerce électronique et Bureau de la consommation)
Association canadienne de la technologie de l'information	Institut Canadien des Comptables Agréés
Association canadienne des paiements	Juricert Services Inc.
Association des banquiers canadiens	Province de l'Ontario
Association des comptables généraux accrédités du Canada	Province de la Colombie-Britannique
Association du Barreau canadien	Scotiabank
Bell Canada	Secrétariat du Conseil du Trésor du Canada
Bureau d'assurance du Canada	Spyrus Inc.
Centre pour la défense de l'intérêt public	Teranet Inc.
Conseil canadien des normes	Visa Canada Association
Conseil canadien du commerce de détail	
Deloitte & Touche LLP Canada	
Digital Discretion Inc.	
École de droit de l'Université d'Ottawa	
Gowling Lafleur Henderson LLP	
Groupe financier RBC	

POURQUOI ET COMMENT UTILISER LES PRINCIPES

Les principes visent à orienter l'élaboration, la mise en œuvre et l'utilisation des produits et des services d'authentification au Canada. Ils sont complémentaires de la structure de gouvernance¹ 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.

La structure de gouvernance qui s'applique aujourd'hui aux services d'authentification au Canada est constituée entre autres, de la Politique du Canada en matière de cryptographie de 1998, de lois fédérales et provinciales, y compris la *Loi sur la protection des renseignements personnels et les documents électroniques* de 2000, 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* (janvier 2004).

Les principes d'authentification électronique 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. Les principes 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 œuvre et de l'évaluation d'un processus d'authentification.

Les intervenants qui participent à la conception, à la mise en œuvre 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

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 œuvre des services d'authentification au Canada.

sont adaptés aux exigences du gouvernement et des secteurs industriels. On encourage fortement de telles initiatives, 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 points de repère aux personnes physiques et aux entreprises qui utilisent l'authentification. Bien que les principes définissent les responsabilités des parties prenantes (principe 1) et traitent d'aspects de la gestion du risque (principe 2), ils n'abordent pas la question des obligations qui pourraient incomber aux diverses parties qui participent au processus d'authentification, notamment celles de la protection ou de la responsabilité des consommateurs. L'interprétation des principes ne devrait pas attribuer la responsabilité aux utilisateurs finals. Des 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. Bien que les

principes aient été définis de sorte à inclure des développements prévisibles, ces derniers sont sujets à révision puisqu'il faudra 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 les principes sont toujours les bienvenus et devraient être adressés à :

Richard Simpson
Directeur général
Direction générale sur le
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 ou 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 de ce Groupe sera évaluée et modifiée s'il y a lieu à mesure que le contexte d'authentification évoluera.

AU SUJET DES PRINCIPES

CONCEPTS ET TERMINOLOGIE

Les principes qui suivent ont pour objet l'authentification des communications électroniques dans son sens large. Les concepts et les termes employés dans le présent document se rapportent donc à toutes les parties prenantes, les mesures

et les techniques incluant tous les aspects de l'authentification, que ce soit du point de vue technique, juridique ou commercial. Chaque concept ou terme se rapporte aux autres; aucun d'eux ne devrait être considéré isolément.

Fonctions

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

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.

Définitions

Les définitions existantes, particulièrement celles établies par des groupes de normalisation internationale comme l'Organisation internationale de normalisation (ISO), ont été considérées par le Groupe de travail sur les principes d'authentification lors de l'établissement des principes. Toutefois, en raison de la portée générale des principes, ces définitions ne correspondaient nécessairement pas à l'emploi qu'on en fait dans des milieux particuliers.²

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

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

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.

COMMUNICATION ÉLECTRONIQUE. Transmission, message ou transaction électronique.

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

L'authentification est censé promouvoir la confiance dans la communication électronique. Les parties prenantes à une communication électronique ont l'assurance que les autres parties prenantes 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 (l'autorité dési-

² Par exemple, la définition d'*authentification* englobe le concept d'« authentification de message », qui correspond aux procédés utilisés pour assurer l'intégrité des messages. De plus, le terme *non-répudiation* n'a pas été défini en relation avec les principes. Ce terme est couramment employé pour décrire une norme technique à laquelle le processus d'authentification doit répondre. Ce terme est toutefois trompeur dans un contexte général, car il laisse faussement entendre une conclusion de droit.

gnée 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). Les parties prenantes se fient à l'authentification d'une communication électronique dans la mesure où elles peuvent évaluer la fiabilité de l'authentification. Les méthodes et les spécifications technologiques utilisées pour l'authentification sont souvent basées sur des techniques cryptographiques.

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 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'à 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.

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.

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.

PORTÉE ET NATURE DES PRINCIPES

Ces principes se rapportent à l'authentification des communications électroniques 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, entre des organisations et des personnes physiques (les consommateurs et les citoyens), et entre des personnes physiques.

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

Les 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 œuvre 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 œuvre les processus d'authentification sont encouragées à dépasser les points de repère que les principes établissent 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 œuvre des processus d'authentification varie 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 définissent 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 processus d'authentification devraient être efficaces, efficaces, fiables et faciles à appliquer; ils devraient également respecter les intérêts des personnes physiques et morales. 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 la protection des renseignements personnels pour les Canadiens oblige les responsables de la conception et de la mise en œuvre 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 afin d'assurer la compatibilité avec les innovations internationales dans le domaine de l'authentification.

Le Canada 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.

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 2).

Les responsabilités particulières des parties prenantes se rattachent à la fonction ou aux fonctions qu'elles exercent, dont les suivantes :

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. Lorsque l'administrateur délègue 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 5). La responsabilité qu'ont les utilisateurs finals de protéger l'information concernant le processus

d'authentification peut être limitée par des obligations juridiques ou contractuelles. Tel est le cas lorsque celles-ci obligent les utilisateurs à divulguer de l'information se rapportant au processus 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 œuvre 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 qu'elles 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 afin de 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 œuvre et appuyer l'infrastructure qui permet l'authentification.

PRINCIPE 2 : GESTION DU RISQUE

Les risques liés aux processus d'authentification des communications électroniques 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 (par exemple 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.

Détermination

Les risques devraient être déterminés dans la mesure du possible. Les risques peuvent être financiers, incluant les dommages immédiats, directs et indirects issus d'une exécution défectueuse ou d'un retard d'exécution de la communication; ils peuvent aussi se

rapporter, entre autres, à la perte de confidentialité ou de renseignements personnels, à des dommages à la réputation et au vol d'identité.

Évaluation

La gravité et l'incidence possible des risques devraient être évaluées. Lorsqu'on évalue les risques, il faut prêter une attention spéciale aux circonstances où l'on fait confiance au processus d'authentification; en outre, il peut être utile de tenir compte des responsabilités liées à chacune des six fonctions (voir le principe 1).

Gestion

Les risques devraient être gérés jusqu'à hauteur de la plus grande efficacité économique, c'est-à-dire qu'ils doivent être assumés, évités, réaffectés ou atténués. Le risque est efficace sur le plan économique lorsque le risque résiduel qu'une partie prenante assume après avoir géré les risques avec prudence n'est pas plus grand que les avantages qu'elle tire de sa participation.

Rôle des contrats

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 égales³, il peut être nécessaire de prendre des mesures pour protéger les intérêts des parties les plus faibles.⁴

Processus de décision

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 œuvre des processus d'authentification à voir à ce que leurs produits et leurs services soient sûrs et fiables.

3 Un exemple d'un tel cas sont les contrats qui imposent la durée des services aux utilisateurs.

4 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 gouvernemental 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.⁵

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 dans la conception et la mise en œuvre 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 généralement reconnues.

Protection, détection et réaction

S'il y a lieu, toutes les parties prenantes devraient être mises au courant et, en tout temps, être conscientes des risques pour la sécurité, des menaces connues et des vulnérabilités ainsi que des mesures de protection 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 en tout temps agir de

5 Le principe de la sécurité reconnaît et adopte les *Lignes directrices de l'OCDE [Organisation de coopération et de développement économiques] régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité* (voir page 24). Le texte intégral des *Lignes directrices* se trouve en ligne à l'adresse suivante: www.oecd.org/dataoecd/16/22/15582260.pdf.

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 devraient respecter les droits des parties prenantes, conformément aux principes démocratiques d'une société ouverte.

Les technologies de l'information évoluent rapidement. Par conséquent, une saine 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 que les parties prenantes devraient jouer pour prévenir, détecter et régler les incidents.

Examen et évaluation

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'ils 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. Un tel examen devrait faire partie intégrante de l'accréditation et de la certification au regard des normes généralement reconnues.

PRINCIPE 4 : PROTECTION DES RENSEIGNEMENTS PERSONNELS

Les organisations engagées dans la conception ou l'exécution des processus d'authentification devraient se conformer aux normes de protection des données énoncées dans les codes de pratique (codes en matière de protection des renseignements personnels) en plus de se conformer aux lois et à la jurisprudence (lois en matière de protection des renseignements personnels)⁶ applicables. En particulier, la collecte, l'utilisation et la divulgation de renseignements personnels⁷ 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. Par exemple, une authentification plus poussée 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 person-

nels 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.

6 Les lois générales de protection des renseignements personnels dans le secteur privé qui sont actuellement en vigueur incluent la *Loi sur la protection des renseignements personnels et les documents électroniques* (loi fédérale) et les lois adoptées par l'Alberta, la Colombie-Britannique et le Québec. Les autres provinces ainsi que les territoires peuvent choisir d'adopter des lois générales de protection des renseignements personnels. Des lois fédérales, provinciales et territoriales en matière de protection des renseignements personnels qui s'appliquent au secteur public 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 l'Association canadienne de normalisation, (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, à titre d'annexe 1. Le 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.

7 Conformément à la définition de la *Loi sur la protection des renseignements personnels et les documents électroniques*: « tout renseignement concernant un individu identifiable ».

Si la collecte de renseignements personnels est nécessaire, elle doit être réduite au minimum. L'utilisation ou la divulgation de renseignements personnels devrait également être réduite au minimum. Les renseignements personnels ne devraient être recueillis, utilisés ou divulgués qu'avec le consentement éclairé de la personne physique.

Les renseignements personnels ne devraient être conservés qu'aux fins d'authentification.

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 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'organisation 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 qui est divulguée concernant les services d'authentification 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.

Étendue et nature de la divulgation

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.

Notification

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.

Lien aux autres principes

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 4 de la protection des renseignements traite plus en profondeur des renseignements personnels et de leur divulgation.

Les obligations d'information doivent du même coup être considérées de concert avec le principe 1 (responsabilités des parties prenantes) et le principe 2 (gestion du risque).

PRINCIPE 6 : TRAITEMENT DES PLAINTES

Les organisations qui mettent en œuvre un processus d'authentification devraient élaborer une méthode de traitement des plaintes permettant aux parties prenantes de répondre à ces plaintes de façon efficace et efficiente, et de régler les problèmes d'inobservation de façon appropriée.

Les processus de traitement des plaintes devraient refléter les éléments suivants.

Visibilité

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

Accessibilité

Le processus de traitement des plaintes devrait être facilement accessible à toutes les parties prenantes et l'organisation doit faire en sorte qu'il soit facile d'obtenir des renseignements sur les détails du règlement des différends. Le processus et l'information à l'appui devraient être faciles à comprendre et à utiliser par les personnes physiques faisant des plaintes. Ils devraient 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 œuvre 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.

Confidentialité et protection des renseignements personnels

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

Reddition de comptes

Les organisations devraient s'assurer qu'une personne physique désignée ou qu'une unité identifiable de l'organisation soit responsable de la consignation systématique des plaintes et de leur règlement, et qu'elle rende compte des actions et des décisions de l'organisation relativement au 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.

INFORMATIONS SUPPLÉMENTAIRES ET RÉFÉRENCES

INFORMATIONS SUPPLÉMENTAIRES

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

1. 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.

2. Responsabilité

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

3. Réaction

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

4. Éthique

Les parties prenantes doivent respecter les intérêts légitimes des autres parties prenantes.

5. Démocratie

La sécurité des systèmes et réseaux d'information doit être compatible

avec les valeurs fondamentales d'une société démocratique.

6. Évaluation des risques

Les parties prenantes doivent procéder à des évaluations des risques.

7. Conception et mise en œuvre de la sécurité

Les parties prenantes doivent intégrer la sécurité en tant qu'un élément essentiel des systèmes et réseaux d'information.

8. Gestion de la sécurité

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

9. Réévaluation

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

RÉFÉRENCES

Voir <http://strategis.ic.gc.ca/authen-fr> pour obtenir une bibliographie générale renfermant des ouvrages de référence nationaux ou internationaux, ainsi que les documents sources spécifiques de chaque principe.