Secrétariat du Conseil du Trésor du Canada
Treasury Board of Canada Secretariat
Canada

Ligne directrice sur l’assurance de l’identité

Publié : le 04 mars 2016

Publié par le Secrétariat du Conseil du Trésor du Canada
90 rue Elgin, Ottawa, Ontario, K1A 0R5, Canada

N° de catalogue BT22-165/2016F-PDF
ISBN : 978-0-660-09760-2

Ce document est disponible sur Canada.ca, le site Web du gouvernement du Canada.

Ce document est disponible en médias substituts sur demande.

Nota : Pour ne pas alourdir le texte français, le masculin est utilisé
pour désigner tant les hommes que les femmes.

Also available in English under the title: Guideline on Identity Assurance

Ligne directrice sur l’assurance de l’identité

1. Objet

La présente Ligne directrice appuie la mise en uvre des exigences minimales requises pour établir l'identité[Note en bas de page1] d'une personne selon un niveau d'assurance donné. Les niveaux d'assurance de l'identité sont définis à l'annexe B de la *Norme sur l'assurance de l'identité et des justificatifs*, et les exigences minimales requises pour établir un niveau d'assurance de l'identité sont décrites à la section 6.4.1 et à l'annexe C. Cette Norme a été publiée à l'appui de la *Politique sur la sécurité du gouvernement* et de la *Directive sur la gestion de l'identité*.

L'établissement de l'identité consiste en la création d'un document d'identité faisant autorité que d'autres utilisent en toute confiance pour l'accès ultérieur à des activités, programmes et services du gouvernement. La présente Ligne directrice vise à normaliser l'établissement des renseignements sur l'identité des personnes relativement aux programmes et services du gouvernement. La Ligne directrice vise également à promouvoir des pratiques uniformes en matière d'assurance de l'identité, tout en permettant aux organisations gouvernementales de disposer de la souplesse nécessaire pour innover et gérer les risques de façon appropriée. Enfin, la Ligne directrice vise également à contribuer à la mise en uvre d'une approche progressive pour la fédération de l'identité qui comprend notamment le recours à des services normalisés d'authentification des justificatifs.

1.1 Public

La présente Ligne directrice est destinée aux utilisateurs suivants :

- Les **gestionnaires de la prestation de programmes et de services** qui sont chargés d'assurer l'uniformité dans l'identification des clients (particuliers et entreprises), des employés et des fournisseurs du gouvernement du Canada en tant que composante essentielle des exigences relatives à la prestation de leur programme ou service;
- Les **praticiens de la sécurité** qui sont chargés de recommander, de concevoir, d'élaborer ou de fournir des solutions pour satisfaire aux exigences relatives à la prestation des programmes et services.

1.2 Application et utilisation

La présente Ligne directrice :

- s'applique dans les situations où il est nécessaire de pouvoir identifier de façon unique des personnes afin de fournir un service ou d'exécuter une transaction, ou aux fins d'administration d'un programme;
- s'applique à la fois aux services externes et aux services internes du gouvernement du Canada;
- n'impose aucune exigence additionnelle en plus de ce qui est prescrit dans la *Norme sur l'assurance de l'identité et des justificatifs*;
- peut s'appliquer aux décisions en matière d'accès, d'autorisation ou d'admissibilité;
- peut s'appliquer dans la détermination des relations entre des personnes, des organisations et des appareils. Il est entendu que ces relations servent à accorder l'autorité ou la permission d'agir pour le compte d'autres. Bien que des exemples de telles relations soient présentés, ils ne doivent pas être interprétés comme une orientation à respecter;
- doit être utilisée en conjonction avec la *Ligne directrice sur la définition des exigences en matière d'authentification*, qui fournit aux organisations gouvernementales un cadre d'évaluation pour la détermination de leurs besoins spécifiques en matière de niveaux d'assurance de l'identité;
- ne recommande pas des technologies, architectures ou solutions spécifiques, ni ne recommande l'utilisation de documents spécifiques ou de techniques spécifiques d'authentification de documents;
- peut être utilisée à l'appui des vérifications de sécurité liées à l'identité, telles que décrites dans la *Norme sur le filtrage de sécurité*;
- peut être utilisée à l'appui de la mise en uvre de la *Politique sur les services*.

On trouvera une liste annotée des politiques, normes, lignes directrices et cadres utilisés à l'appui ou en relation avec l'assurance de l'identité à l'annexe B.

Pour satisfaire aux exigences de la Norme, les organisations gouvernementales élaborent des pratiques de gestion de l'identité et d'autres outils de manière à mettre en uvre une approche cohérente, uniforme, normalisée et interopérable à l'échelle du gouvernement du Canada. Ces pratiques et outils seront partagés dans GCpédia et pourront être incorporés à de futures versions de la présente Ligne directrice.

2. Introduction

2.1 L'approche du gouvernement du Canada en matière d'assurance de la qualité

L'identité constitue l'élément central de la majorité des processus opérationnels du gouvernement, et forme le point de départ pour l'établissement de la confiance dans les interactions entre le public et le gouvernement. Après l'établissement des renseignements sur l'identité relatifs à une personne, toutes les activités subséquentes du gouvernement, allant de la prestation de services à l'octroi d'avantages et d'admissibilité, seront fondées sur l'exactitude et l'utilisation légitime de ces renseignements. Dans le cas de nombreuses rencontres de service ou transactions avec des clients, les organisations gouvernementales doivent veiller à ce qu'elles interagissent réellement avec la personne appropriée de manière à réaliser

leurs objectifs en matière de prestation de leurs programmes et services. Par exemple, lorsqu'une personne fait une demande de passeport canadien, elle doit produire certains documents pour faire la démonstration de son identité.

La gestion des renseignements sur l'identité est une responsabilité partagée entre les différents ordres de gouvernements au Canada. Il existe de nombreuses sources autorisées par différentes lois et réglementations fédérales, provinciales et territoriales qui recueillent des renseignements relatifs aux personnes, tels que les données de l'état civil, la situation juridique ou professionnelle et l'admissibilité à différents avantages. Dans la plupart des cas, un document ou certificat est délivré à la personne, qui l'utilisera ensuite pour faire la preuve de son identité et des renseignements personnels connexes.

Au Canada, il n'existe aucun document dont la seule raison d'être est de confirmer l'identité d'une personne. On utilise plutôt une série de documents délivrés par différents ordres de gouvernements. Cette approche décentralisée a permis jusqu'à présent d'offrir des services appropriés aux Canadiens. Cependant, elle peut poser des difficultés lorsqu'il s'agit d'offrir une expérience de service uniformisée entre les différents ordres de gouvernements et de lutter contre les activités frauduleuses.

Les documents matériels constituent encore maintenant le mode prédominant de présentation d'une preuve d'identité pour accéder aux programmes et services du gouvernement du Canada. Alors que les méthodes numériques sont de plus en plus souvent utilisées, des représentations numériques de l'identité peuvent être acceptées en remplacement de documents matériels. Les gouvernements sont conscients des économies de coûts possibles pouvant résulter de l'utilisation de solutions numériques et d'une infrastructure commune. Alors que les programmes et services gouvernementaux sont de plus en plus interconnectés et interdépendants, il devient beaucoup plus important de gérer le risque lié à l'identité de façon collaborative, au-delà des frontières des organisations et des administrations.

En 2011, pour tenir compte de cet environnement en évolution, le gouvernement du Canada a publié le document *Fédérer la gestion de l'identité au gouvernement du Canada : Une mise en contexte*, qui décrit une vision et une approche globale qui permet à la confiance-établie par les processus internes de gestion de l'identité-de franchir encore davantage les frontières organisationnelles au sein du gouvernement du Canada et avec les autres administrations. Dans le cadre de ce document, plusieurs concepts clés ont été définis officiellement, notamment « l'assurance de l'identité » et « l'assurance des justificatifs », et ils ont par la suite été officialisés dans des instruments de politique subséquents du Conseil du Trésor.

2.2 Instruments de politique du Conseil du Trésor en matière d'identité

Les instruments de politique du Conseil du Trésor en matière d'identité comprennent une directive, une norme et deux lignes directrices publiées en vertu de la *Politique sur la sécurité du gouvernement*.

- La *Directive sur la gestion de l'identité*, en vigueur depuis juillet 2009, appuie les pratiques efficaces de gestion de l'identité en décrivant les exigences qui aident les ministères à établir, utiliser et valider les identités.
- La *Norme sur l'assurance de l'identité et des justificatifs*, en vigueur depuis février 2013, vise à veiller à ce que le risque lié à l'identité soit géré de façon uniformisée et collaborative au sein du gouvernement du Canada et avec les autres administrations et les différents secteurs industriels. La Norme est appuyée par deux lignes directrices.
- La *Ligne directrice sur la définition des exigences en matière d'authentification*, publiée en novembre 2012, appuie la mise en uvre des exigences 6.1.1, 6.1.2 et 6.1.3 de la *Norme sur l'assurance de l'identité et des justificatifs*. Par souci de commodité, ces exigences sont répétées ici :
    - **6.1.1** Cibler et évaluer les risques en lien avec l'identité et les justificatifs à l'aide d'une évaluation des préjudices pour le programme, l'activité, le service ou la transaction;
    - **6.1.2** Choisir les contrôles de l'identité et des justificatifs nécessaires pour respecter les exigences en lien avec le niveau d'assurance précisé à l'annexe B [de la Norme];
    - **6.1.3** S'assurer de respecter les exigences minimums pour l'établissement du niveau d'assurance de l'identité précisées dans l'annexe B [de la Norme].
- La *Ligne directrice sur l'assurance de l'identité* (le présent document) appuie la mise en uvre de l'exigence 6.1.4 de la Norme :
    - **6.1.4** S'assurer de respecter les exigences minimums pour l'établissement du niveau d'assurance de l'identité précisées dans l'annexe C [de la Norme].

La section 3 de la présente Ligne directrice explique en détail comment satisfaire à ces exigences.

2.3 Assurance de l'identité et niveaux d'assurance de l'identité

La grande majorité des programmes et services gouvernementaux doivent s'assurer de bien identifier les personnes avec qui ils interagissent. En ce qui a trait aux services externes, la personne est normalement un client d'un programme ou service gouvernemental. Pour ce qui est des services internes, la personne est un employé, ou un fonctionnaire agissant au nom d'une organisation gouvernementale.

Ces différents contextes peuvent donner lieu à des risques distincts qui doivent être gérés différemment. Par exemple, le fait de ne pas confirmer correctement la bonne personne comme étant un client peut mener au versement de prestations à la mauvaise personne (un risque pour l'intégrité des programmes). De même, le fait de ne pas confirmer correctement la bonne personne comme étant un employé peut mener à la divulgation non autorisée de renseignements (un risque pour la sécurité de l'information ou une atteinte à la vie privée, si des renseignements personnels venaient à être divulgués). Peu importe le contexte, on peut utiliser les principes de l'assurance de l'identité pour s'assurer systématiquement qu'une organisation gouvernementale transige bien avec la bonne personne.

Par définition, « l'assurance de l'identité » est une mesure de la certitude (ou un degré de confiance) qu'une personne, une organisation ou un appareil est bien celui qu'il affirme être. On utilise l'assurance de l'identité pour répondre à la question « À

quel degré êtes-vous sûr d'être confronté à la bonne personne/à la bonne organisation/au bon appareil? ».[Note en bas de page2]

En plus de faciliter la gestion du risque, une approche normalisée à l'assurance de l'identité permet aux personnes d'interagir avec les programmes et services gouvernementaux qui utilisent, ou qui comptent sur, des processus d'établissement de l'identité exécutés par une autre entité. Par exemple, une personne peut faire la preuve de son identité une seule fois, en fonction d'exigences normalisées, et par la suite de nombreux autres programmes et services pourront se fier à l'identité établie antérieurement pour cette personne. Ceci constitue le principe fondateur de la fédération, qui est décrite plus en détail à la section 3.9 du présent document.

Des niveaux multiples d'assurance de l'identité permettent aux programmes et services gouvernementaux d'effectuer des opérations en fonction du niveau de risque. Dans le cas de certains services, le niveau de risque est faible tandis que pour d'autres services, il peut être plus élevé. Par exemple, le niveau de risque associé à la prestation d'information météorologique personnalisée à une personne est faible, tandis que le niveau de risque associé à l'acceptation d'une demande de passeport est plus élevé.

Les différents niveaux d'assurance de l'identité permettent aussi aux organisations gouvernementales de gérer leurs coûts et de concevoir des solutions optimales fondées sur des services ou capacités normalisés pour des niveaux d'assurance différents (ou plus faibles) tout en gérant de façon appropriée le risque résiduel.

Le **Tableau 1** décrit les niveaux d'assurance de l'identité définis dans la *Norme sur l'assurance de l'identité et des justificatifs*.

Tableau 1 : Niveaux d'assurance de l'identité

Niveau	Description
4	**Besoin d'un niveau très élevé d'assurance que la personne est celle qu'elle affirme être.** Une compromission pourrait raisonnablement entraîner des préjudices graves, sinon catastrophiques.
3	**Besoin d'un niveau élevé d'assurance que la personne est celle qu'elle affirme être.** Une compromission pourrait raisonnablement entraîner des préjudices modérés, sinon graves.
2	**Besoin d'un certain niveau d'assurance que la personne est celle qu'elle affirme être.** Une compromission pourrait raisonnablement entraîner des préjudices minimes, sinon modérés.
1	**Besoin d'un faible niveau d'assurance que la personne est celle qu'elle affirme être.** Une compromission pourrait raisonnablement entraîner des préjudices inexistants, sinon minimes.

Les niveaux normalisés sont numérotés de un à quatre; chaque niveau décrit un degré de confiance requis qui correspond à une plage de préjudices potentiels pouvant survenir si le niveau d'assurance correspondant n'est pas atteint et maintenu. La section 3.2 du présent document explique comment une organisation gouvernementale doit déterminer le niveau d'assurance de l'identité requis.

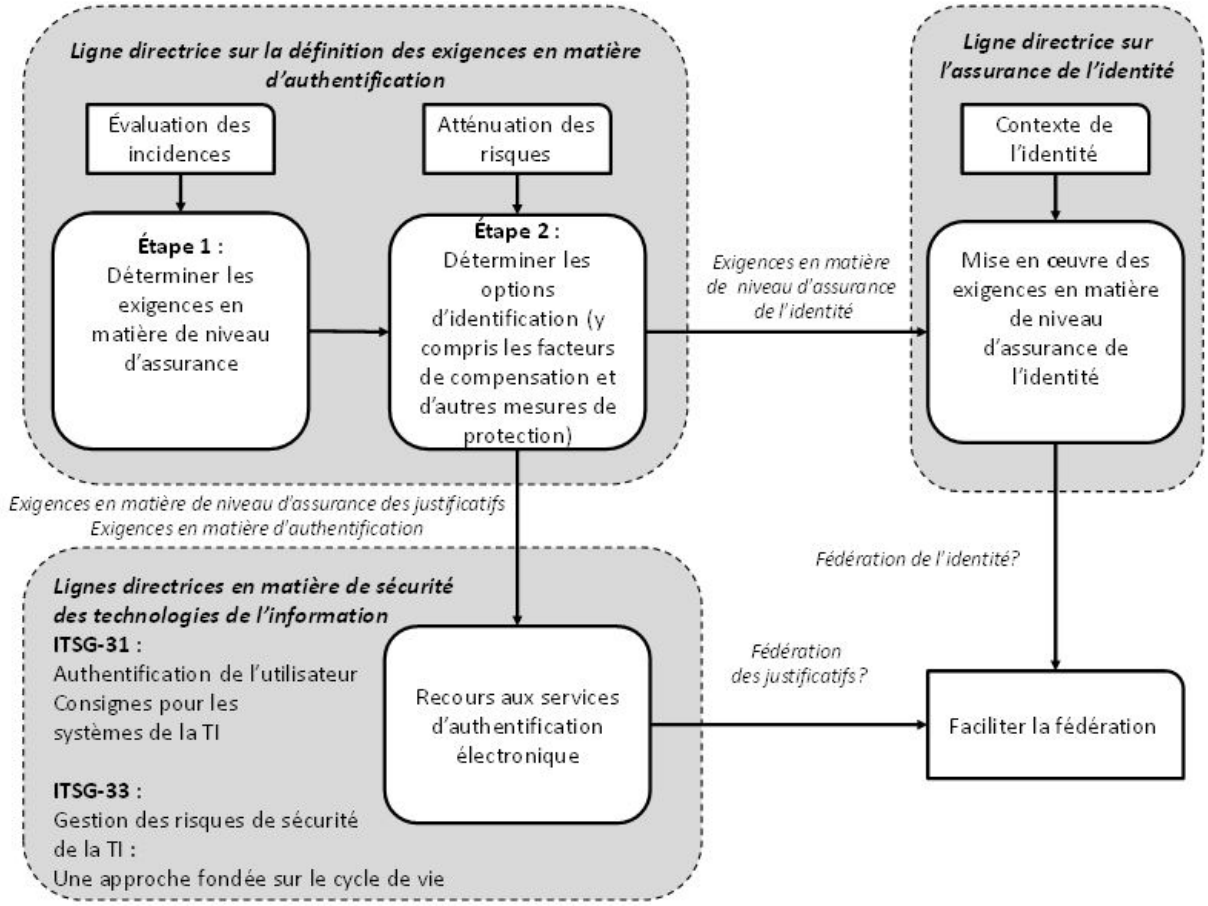
3. Lignes directrices sur la mise en uvre d'un niveau donné d'assurance de l'identité

3.1 Exécution d'une évaluation du niveau d'assurance

Il faut exécuter dans un premier temps une évaluation du niveau d'assurance afin de déterminer le niveau d'assurance requis. Le document d'accompagnement, la *Ligne directrice sur la définition des exigences en matière d'authentification*, décrit un processus en deux étapes utilisé pour déterminer le niveau requis.

La figure 1 présente une vue globale du processus d'évaluation du niveau d'assurance requis et des processus de conception TI dans le contexte des lignes directrices connexes du gouvernement du Canada.

Figure 1. Contexte des lignes directrices connexes du gouvernement du Canada



[Version textuelle : Figure 1. Contexte des lignes directrices connexes du gouvernement du Canada]

La *Ligne directrice sur la définition des exigences en matière d'authentification* décrit le processus d'évaluation en deux étapes :

Étape 1

- **Détermination du niveau d'assurance requis**, c'est-à-dire le niveau de confiance global requis pour mener à bien une activité de programme, un service ou une transaction. L'évaluation du niveau d'assurance se fait au moyen de la feuille de travail présentée à l'annexe A de la *Ligne directrice sur la définition des exigences en matière d'authentification*.

Étape 2

- **Détermination des options d'authentification** qui seront utilisées pour mettre en uvre le niveau d'assurance requis déterminé à l'étape 1. Ces options d'authentification sont :
    1. L'**exigence relative au niveau d'assurance** spécifie les exigences minimales pour l'établissement de l'identité d'une personne pour un niveau d'assurance donné. L'exigence relative au niveau d'assurance constitue le principal intrant pour la présente Ligne directrice.
    2. L'**exigence relative au niveau d'assurance des justificatifs** spécifie les exigences minimales pour veiller à ce qu'une personne ait conservé le contrôle d'un justificatif qui lui avait été délivré et que le justificatif n'a pas été compromis. Les lignes directrices sur la mise en uvre de ces exigences sont décrites dans le document ITSG-31, *Guide sur l'authentification des utilisateurs pour les systèmes TI* du CST.
    3. Les **exigences en matière d'authentification** sont les exigences minimales en matière de conception technique ou de processus opérationnels qui sont nécessaires pour exécuter un processus d'authentification électronique ou manuel. Les lignes directrices sur la mise en uvre de ces exigences sont décrites dans les documents ITSG-31 et ITSG-33, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* du CST.

La *Ligne directrice sur la définition des exigences en matière d'authentification* présente aussi des recommandations au sujet d'autres mécanismes d'atténuation des risques.

- Les **facteurs de compensation** sont des mesures supplémentaires utilisées au cours du processus d'authentification pour réduire un risque. Un facteur de compensation est censé atténuer les risques résiduels ou contrer les nouvelles possibilités de menace. Exemple : demander à une personne de répondre à des questions additionnelles lorsque son justificatif a été authentifié à partir d'un appareil ou d'un emplacement antérieurement inconnu.
- Les **autres mesures de protection** sont des mesures supplémentaires utilisées en plus du processus

d'authentification pour réduire les risques ou assurer l'intégrité d'un programme. Il peut s'agir de mécanismes de contrôle de la sécurité utilisés dans des processus subséquents ou d'indicateur utilisés pour initier des exceptions ou des interventions.

3.2 Exigences en matière de niveau d'assurance de l'identité

La présente section décrit en détail la mise en uvre des exigences spécifiées à l'annexe C de la *Norme sur l'assurance de l'identité et des justificatifs*.

On utilise quatre catégories d'exigences pour établir un niveau d'assurance de l'identité. Les quatre catégories sont indiquées ci-dessous, accompagnées d'un énoncé de haut niveau de l'objectif de contrôle et d'une brève description.

Unicité. *Une identité doit être unique*

L'unicité permet de distinguer les personnes les unes des autres et, s'il y a lieu, de les identifier de façon unique. L'unicité est aussi utilisée pour déterminer les exigences en matière de renseignements sur l'identité.

Preuve de l'identité. *Une preuve de l'identité doit corroborer les affirmations formulées par une personne.*

Une preuve de l'identité appuie l'intégrité et l'exactitude des affirmations formulées par une personne. Le nombre de preuves nécessaires pour confirmer l'exactitude des renseignements sur l'identité et leur lien avec la personne dépend du niveau d'assurance requis déterminé par le programme ou service. La *Norme sur l'assurance de l'identité et des justificatifs* définit deux catégories de preuves de l'identité : les preuves de l'identité essentielles et les preuves à l'appui de l'identité (voir la section 3.4 du présent document).

Exactitude de l'information confirmant l'identité. *L'information confirmant l'identité d'une personne doit être exacte, complète et à jour.*

L'exactitude permet d'assurer la qualité des renseignements sur l'identité en veillant à ce que l'information représente la personne avec véracité, qu'elle soit complète et qu'elle soit à jour. On peut confirmer l'exactitude en utilisant une source faisant autorité ou en corroborant différentes sources d'information dans les situations où aucune source faisant autorité n'est disponible.

Lien entre l'information confirmant l'identité et la personne. *L'information confirmant l'identité d'une personne qui formule une affirmation doit être reliée à cette personne.*

Le lien permet de veiller à ce que les renseignements sur l'identité concernent bel et bien la personne qui fait l'affirmation, qu'ils ne sont pas associés à une autre personne et qu'ils reflètent bien comment la personne est connue au sein d'une collectivité ou est juridiquement reconnue au sein d'une administration.

Par souci de commodité, le tableau 2 de *l'annexe C de la Norme sur l'assurance de l'identité et des justificatifs* est reproduit ici. Le tableau 2 présente les exigences minimales par catégorie liées à chaque niveau d'assurance.

Tableau 2. Exigences minimales pour établir un niveau d'assurance de l'identité

Exigence	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Unicité	Définir les renseignements sur l'identité Définir le contexte	Définir les renseignements sur l'identité Définir le contexte	Définir les renseignements sur l'identité Définir le contexte	Définir les renseignements sur l'identité Définir le contexte
Preuve de l'identité	Aucune restriction quant à ce qui peut être fourni à titre de preuve de l'identité	**Une** preuve de l'identité	**Deux** preuves de l'identité (Dont au moins une est une preuve essentielle)	**Trois** preuves de l'identité (Dont au moins une est une preuve essentielle)
Exactitude de l'information confirmant l'identité	Acceptation de l'affirmation de soi à titre de confirmation des renseignements sur l'identité	Information sur l'identité correspond de façon acceptable à l'affirmation par une personne et à la preuve de l'identité **et** Confirmation que la preuve de l'identité provient d'une autorité compétente	Information sur l'identité correspond de façon acceptable à l'affirmation par une personne et à toutes les preuves de l'identité **et** Confirmation de la preuve de l'identité à l'aide d'une source faisant autorité **et** Confirmation que la preuve de l'identité provient d'une autorité compétente, à l'aide d'une source faisant autorité **ou** Inspection par un examinateur d'expérience	Information sur l'identité correspond de façon acceptable à l'affirmation par une personne et à toutes les preuves de l'identité **et** Confirmation de la preuve de l'identité à l'aide d'une source faisant autorité **et** Confirmation que la preuve de l'identité provient d'une autorité compétente, à l'aide d'une source faisant autorité **ou** Inspection par un examinateur d'expérience

Lien entre l'information confirmant l'identité et la personne	Aucune exigence	Aucune exigence	Au moins **un** des éléments suivants : i. Confirmation basée sur les connaissances ii. Confirmation des caractéristiques biologiques ou comportementales iii. Confirmation par un arbitre de confiance iv. Confirmation de possession matérielle	Au moins **trois** des éléments suivants : i. Confirmation basée sur les connaissances ii. Confirmation des caractéristiques biologiques ou comportementales iii. Confirmation par un arbitre de confiance iv. Confirmation de possession matérielle

3.3 Exigences en matière d'unicité

3.3.1 Unicité

L'unicité permet de veiller à ce que les personnes puissent être distinguées les unes des autres et que le bon service soit dispensé à la bonne personne au bon moment. L'unicité réduit le risque que la mauvaise personne reçoive un service ou touche une prestation destinés à quelqu'un d'autre.

L'unicité est nécessaire dans les situations où un service doit fournir un produit ou une prestation à une personne spécifique - par exemple, la **même** personne qui s'était précédemment enregistrée ou inscrite. Dans certaines situations, l'identité d'une personne n'est pas requise ni même souhaitée, comme par exemple l'identité d'un répondant à une enquête.

L'unicité, par elle-même, ne détermine pas l'admissibilité ou la qualification à un service ou une prestation. Néanmoins, les renseignements recueillis pour déterminer l'unicité peuvent également être utilisés à des fins de détermination de l'admissibilité ou de la qualification et peuvent donc être assujettis à d'autres exigences législatives et exigences relatives au respect de la vie privée. Dans les situations où une transaction comporte au moins deux motifs (par exemple, pour déterminer à la fois l'identité et une qualification), les utilisations prévues des renseignements recueillis doivent être clairement indiquées.

3.3.2 Définition du contexte de l'identité

Les organisations gouvernementales mettent leurs programmes ou leurs services en uvre dans un environnement donné ou en fonction d'un éventail de circonstances qu'on appelle le contexte de l'identité. Le contexte de l'identité est déterminé plus spécifiquement par des facteurs comme le mandat, la population cible (c'est-à-dire les clients) et d'autres responsabilités stipulées dans des lois ou des accords.

La compréhension et la définition du contexte de l'identité aident les organisations gouvernementales à déterminer les exigences en matière d'unicité. Le contexte de l'identité aide à déterminer quels renseignements sur l'identité sont requis et lesquels ne le sont pas. Il aide également à déterminer des points communs avec d'autres organisations gouvernementales ou d'autres administrations, et à établir si les renseignements sur l'identité et les processus d'assurance peuvent être exploités d'un contexte à l'autre.

Le contexte de l'identité peut être envisagé selon le point de vue de la personne, de l'organisation gouvernementale ou du gouvernement du Canada. Par exemple, un contexte de l'identité peut être l'ensemble des services externes offerts aux citoyens, ou encore l'ensemble des services internes offerts aux employés.

Il est recommandé que les organisations gouvernementales tiennent compte des éléments suivants lorsqu'elles définissent ou spécifient le contexte de l'identité pour un programme ou service spécifique :

- Les bénéficiaires prévus d'un service. Les bénéficiaires peuvent être de l'extérieur du gouvernement fédéral (par exemple, citoyen, entreprise, non-Canadien, organisme sans but lucratif), ou à l'intérieur du gouvernement fédéral (par exemple, ministère).
- La taille, les caractéristiques et la composition de la clientèle.
- Les points communs avec d'autres services à l'échelle du gouvernement.
- Les organisations gouvernementales dont le mandat est semblable.
- L'utilisation de services partagés.

3.3.3 Définition des renseignements sur l'identité

Le terme « identité » est défini dans la *Norme sur l'assurance de l'identité et des justificatifs* comme une référence ou une désignation utilisée pour faire la distinction entre une personne, une organisation ou un appareil unique et précis.[Note en bas de page3]

Les renseignements sur l'identité sont jugés être valides dans un contexte de l'identité spécifique (voir la section 3.3.2). Dans

un contexte de l'identité, il est essentiel de pouvoir distinguer les personnes les unes des autres, de manière à ce que les services soient dispensés aux bonnes personnes.

Conformément à la *Directive sur la gestion de l'identité*, il incombe aux organisations gouvernementales de vérifier la légitimité d'une identité lorsque :

- l'identification unique d'une personne, d'une organisation ou d'un appareil est requise pour les besoins de l'administration d'un programme ou d'un service fédéral prévu par la loi;
- la divulgation de l'identité d'une personne, d'une organisation ou d'un appareil est requise pour bénéficier d'un service gouvernemental, participer à un programme du gouvernement ou devenir membre d'une organisation gouvernementale.[Note en bas de page4]

Une propriété ou caractéristique associée à une personne identifiable est appelée attribut d'identité ou élément de donnée sur l'identité. Les « renseignements sur l'identité »constituent l'ensemble des attributs d'identité qui sont à la fois :

- suffisants pour faire la distinction entre différentes personnes au sein d'un contexte de l'identité;
- suffisants pour décrire une personne en fonction des exigences du programme ou du service.

L'attribut d'identité ou l'ensemble d'attributs d'identité utilisé pour distinguer une personne, une organisation ou un appareil unique et particulier peut aussi constituer un identificateur. Il est recommandé d'utiliser les mêmes attributs d'identité en tant qu'identificateurs ou de les utiliser de manière continue au fil du temps. Dans de nombreuses situations, la continuité n'est pas possible, et les organisations gouvernementales peuvent alors choisir de créer ou d'utiliser un identificateur attribué. Cet identificateur est normalement constitué d'une chaîne numérique ou alphanumérique qui est générée automatiquement et qui permet de faire une distinction entre deux ou plusieurs personnes sans recourir à d'autres attributs d'identité.

On peut utiliser des attributs additionnels pour mieux distinguer des personnes similaires ou pour faciliter la reconnaissance d'une personne spécifique. Ces attributs ne sont pas nécessairement propres à une seule personne (par exemple, la couleur des cheveux et la taille) ou peuvent changer au fil du temps.

Au moment de définir ou de déterminer la suffisance de renseignements sur l'identité pour un contexte spécifique de prestation d'un service ou d'administration d'un programme, les organisations gouvernementales, pour des raisons de protection de la vie privée, doivent faire une distinction entre les renseignements sur l'identité et les renseignements personnels propres au programme, car il peut y avoir chevauchement entre les deux. Cette distinction permet de veiller à ce que l'utilisation des renseignements sur l'identité soit conforme aux fins pour lesquelles les renseignements sur l'identité ont été recueillis à l'origine et que lesdits renseignements puissent être gérés séparément ou bénéficier d'une protection supplémentaire grâce à des contrôles appropriés de sécurité et de protection de la vie privée.[Note en bas de page5]

Afin de réduire au minimum les risques liés à la vie privée, les organisations gouvernementales doivent éliminer dans la mesure du possible les chevauchements entre les renseignements sur l'identité et les renseignements personnels propres au programme. Cependant, dans les situations où un chevauchement est nécessaire, une bonne pratique consiste à décrire les deux utilisations. Par exemple, la date de naissance peut être utilisée à la fois pour confirmer l'unicité de l'identité (en tant que renseignement sur l'identité) et comme critère d'admissibilité en fonction de l'âge (en tant que renseignement personnel propre au programme).

Les éléments suivants doivent être pris en considération pour déterminer la suffisance de renseignements sur l'identité :

- Les renseignements sur l'identité qui doivent servir à décrire une personne réelle ou à distinguer une personne des autres dépendent de l'exactitude des renseignements sur l'identité requis (voir la section 3.5).
- Pour des raisons de protection de la vie privée et de sécurité, par exemple la protection des identités de certaines personnes, certains attributs d'identité peuvent être des identificateurs attribués de façon aléatoire, des pseudonymes, des identifiants d'utilisateurs ou des noms d'utilisateurs.
- Exemples de renseignements sur l'identité : pour des personnes-nom, date de naissance, sexe; pour des organisations-numéro d'enregistrement d'entreprise; pour des appareils informatiques et de télécommunications-numéros de série et identifiants de réseaux.
- Un identificateur peut être un attribut d'identité unique attribué et géré par le programme ou le service.
- Les identificateurs attribués peuvent propres à un programme ou service spécifique. Exemples d'identificateurs internes : clé de bases de données, identificateur globalement unique.
- Les identificateurs attribués peuvent être fournis à d'autres programmes; toutefois, des considérations concernant la protection de la vie privée ou des lois peuvent imposer des restrictions à cette pratique.
- Les identificateurs existants ou attribués antérieurement qui satisfont aux exigences en matière d'unicité peuvent être utilisés comme renseignements sur l'identité. Les organisations gouvernementales doivent cependant savoir que l'utilisation de ces identificateurs peut être assujettie à des restrictions ou peut avoir des incidences sur la vie privée.
- Certains identificateurs peuvent faire l'objet de restrictions imposées par des lois ou des politiques. Par exemple, la *Directive sur le numéro d'assurance sociale* stipule des restrictions spécifiques encadrant la collecte, l'utilisation, la conservation, la divulgation et l'élimination du numéro d'assurance sociale du gouvernement du Canada.

3.4 Exigences en matière de preuve de l'identité

Une preuve de l'identité est un enregistrement de données conservé par une source faisant autorité qui appuie l'intégrité et l'exactitude des affirmations d'identité formulées par une personne. La nature d'une preuve suffisante de l'identité dépend du niveau d'assurance requis, comme l'illustre le tableau 2.

3.4.1 Preuves de l'identité essentielles et preuves à l'appui de l'identité

La *Norme sur l'assurance de l'identité et des justificatifs* définit deux catégories de preuves de l'identité :

- Les **preuves de l'identité essentielles** établissent les renseignements de base sur l'identité comme le ou les prénoms, le nom de famille, la date de naissance, le sexe et le lieu de naissance. Exemples : dossiers de naissance, de décès, d'immigration ou de citoyenneté provenant d'un bureau de l'état civil ou des autorités de l'immigration.
- Les **preuves à l'appui de l'identité** corroborent les preuves de l'identité essentielles et permettent d'établir un lien entre des renseignements sur l'identité et une personne. Elles peuvent comprendre également de l'information supplémentaire, comme une photo, une signature ou une adresse. Exemples : le dossier d'assurance sociale; le dossier de droit de se déplacer, de conduire ou d'obtenir de l'assurance maladie; le dossier de mariage, de décès ou de changement de nom provenant d'une autorité compétente.[Note en bas de page6]

Pour la définition des exigences ou procédures opérationnelles, une bonne pratique consiste à désigner les documents par leur nom spécifique (par exemple, passeport, permis de conduire), référant à leur raison d'être originale, plutôt que par la désignation générale « documents d'identité ».

3.4.2 Utilisation des preuves de l'identité

Il est recommandé que les organisations gouvernementales utilisent les preuves de l'identité uniquement aux fins suivantes :

- pour recueillir des renseignements sur l'identité d'une personne suffisants pour assurer la prestation d'un programme ou d'un service à cette personne;
- pour vérifier que les renseignements sur l'identité sont exacts, complets et à jour;
- pour veiller à ce que les renseignements sur l'identité soient liés à la personne qui formule une affirmation d'identité. On notera que les exigences en matière de lien ne s'appliquent pas aux niveaux d'assurance 1 et 2.

Il est recommandé que les organisations gouvernementales mettent en place des processus qui leur permettent de veiller à ce que les renseignements sur l'identité d'une personne :

- soient conservés seulement pendant la période nécessaire;
- soient éliminés lorsqu'ils ne sont plus nécessaires, c.-à-d. au décès de la personne ou au moment de son retrait volontaire d'un programme ou service.

Dans certaines situations, les renseignements sur l'identité recueillis en tant que preuves de l'identité (par exemple, âge, lieu de résidence, statut de citoyen) peuvent aussi être utilisés pour déterminer l'admissibilité ou la qualification à un programme. Les organisations gouvernementales doivent veiller à ce que toute utilisation additionnelle de tels renseignements sur l'identité soit bien permise par les lois applicables.

Une preuve de l'identité peut être présentée ou acceptée sous les formes suivantes :

Preuve documentaire
: Toute information sur support matériel pouvant servir de preuve (on considère généralement qu'il s'agit d'information couchée sur papier, mais de façon plus générale ce terme englobe également les preuves autres que sur support matériel).

Preuve électronique ou numérique
: Toute donnée enregistrée ou préservée sur quelque support que ce soit dans un ordinateur ou un dispositif semblable. Exemples : enregistrements dans une base de données, journaux d'audit ou documents produits au moyen d'un logiciel de traitement de texte.

Les exigences en matière de preuve de l'identité spécifiées au tableau 3 sont indépendantes de la forme dans laquelle la preuve est présentée. De plus, les différentes preuves de l'identité, lorsque des preuves multiples sont exigées, doivent provenir de, ou être émises par, des sources faisant autorité différentes.

3.4.3 Critères d'acceptabilité pour les preuves de l'identité

Le tableau 3 présente les critères d'acceptabilité pour les preuves de l'identité essentielles et les preuves à l'appui de l'identité. Les organisations gouvernementales doivent adapter les critères d'acceptabilité au contexte de prestation de leur programme ou service spécifique.

Tableau 3. Critères d'acceptabilité pour les preuves de l'identité

Catégorie de preuve de l'identité	Critères d'acceptabilité et exemples

	Critères d'acceptabilité :
	• La preuve provient d'une source faisant autorité qui
	  ◦ relève de l'autorité d'une administration fédérale, provinciale ou territoriale, ou d'une administration locale équivalente à l'étranger;[Note du tableau 3i]
	  ◦ est utilisée pour préserver des données de l'état civil spécifiques ou pour déterminer un

	statut juridique.
Preuves de l'identité essentielles	• Les renseignements sur l'identité qui sont incomplets ou incompatibles avec des renseignements fournis par la personne (p. ex., dans le cas d'un changement de nom) peuvent nécessiter une confirmation additionnelle par la source faisant autorité, ou des preuves additionnelles à l'appui de l'identité.

Sources faisant autorité, enregistrements et documents acceptables :

- enregistrements de la statistique de l'état civil utilisés pour la délivrance des certificats de naissance;
- enregistrements du statut juridique utilisés pour la délivrance des certificats de citoyenneté et de naturalisation et des cartes de résident permanent;
- autres enregistrements faisant autorité prévus par des lois propres à des ministères.

Critères d'acceptabilité :

- la preuve provient d'une source faisant autorité qui relève de l'autorité d'une organisation approuvée.[Note du tableau 3ii];

Si elle est acceptée en conjonction avec des preuves de l'identité essentielles (Niveau 3 et Niveau 4) :

Preuves à l'appui de l'identité	• les preuves à l'appui de l'identité doivent être compatibles avec les renseignements fournis par les preuves de l'identité essentielles; • des preuves additionnelles à l'appui de l'identité peuvent être requises si les renseignements sur l'identité sont incomplets ou incohérents (p. ex., dans le cas d'un changement de nom); • il pourrait être nécessaire d'obtenir une approbation ou une certification pour veiller à ce que la preuve à l'appui de l'identité est soit copie conforme d'un document original.

Sources faisant autorité, enregistrements et documents acceptables :

- enregistrement ou documents de permis et d'immatriculation utilisés pour la délivrance d'un permis de conduire;
- passeport ou certificat de statut d'Indien;
- qualifications professionnelles utilisées pour la délivrance de titres professionnels.

Table 3 Notes

Tableau 3 Note **i**

Lorsque les sources faisant autorité ne font pas partie des administrations canadiennes, les critères d'acceptabilité seront établis grâce à une approche fondée sur la gestion des risques par l'organisation gouvernementale.

Retour à la référence de la note i

Tableau 3 Note **ii**

La nature d'une organisation approuvée dépend du contexte du programme ou service gouvernemental. Par conséquent, les organismes fédéraux doivent officialiser leurs propres définitions et critères pour les organisations approuvées. Il peut s'agir de sociétés d'État, d'établissements d'enseignement supérieur, d'organismes publics ou d'organisations commerciales qui sont assujettis à une réglementation et à une surveillance.

Retour à la référence de la note ii

3.4.4 Facteurs à prendre en considération pour les enfants, les mineurs et autres personnes vulnérables

Les enfants, les mineurs et autres personnes vulnérables sont plus susceptibles d'être exploités à des fins criminelles, et la falsification de leurs documents peut mener à des conséquences plus graves. La prestation de services à ces personnes comporte souvent des circonstances spéciales et des facteurs de risque additionnels. Par exemple :

- Les enfants, les mineurs et autres personnes vulnérables peuvent ne pas posséder des preuves de l'identité suffisantes pour satisfaire aux exigences spécifiées dans la *Norme sur l'assurance de l'identité et des justificatifs*.
- Le demandeur peut ne pas être le destinataire ou le bénéficiaire du service. Il est possible qu'un parent, un parent ayant la garde ou un tuteur légal fasse une demande d'inscription à un service ou un programme pour le compte d'un enfant, d'un mineur ou autre personne vulnérable.

Il est recommandé que les organisations gouvernementales appliquent les lignes directrices suivantes pour la prestation de services à des enfants, des mineurs et autres personnes vulnérables :

- Mettre en place des mesures de protection supplémentaires ou des facteurs de compensation afin de réduire le risque et pour initier des exceptions ou des interventions, le cas échéant.
- Confirmer que le demandeur (par exemple, un parent ou tuteur) est légalement autorisé à faire une demande ou à

obtenir un service pour le compte de l'enfant, du mineur ou autre personne vulnérable.

Un programme gouvernemental peut décider d'inclure des exigences en matière de preuve de l'identité pour un parent ou un tuteur dans ses exigences en matière de preuve de l'identité pour l'enfant, le mineur ou autre personne vulnérable. Par exemple, le passeport d'un parent pourrait être utilisé comme preuve à l'appui de l'identité de l'enfant.

On notera que les recommandations présentées dans la présente section ne désignent pas le représentant autorisé qui peut agir au nom d'autres personnes - par exemple, des parents agissant pour le compte d'enfants, ou des avocats agissant pour le compte de demandeurs.

3.4.5 Lignes directrices sur la détermination des preuves à fournir selon le niveau d'assurance de l'identité

Le **Tableau 4** présente les lignes directrices à respecter pour la détermination des preuves de l'identité à fournir selon les différents niveaux d'assurance présentés au tableau 3. Les critères sont indépendants du format (papier ou électronique) dans lequel les preuves sont présentées.

Tableau 4. Lignes directrices sur la détermination des preuves à fournir selon le niveau d'assurance de l'identité

Niveau d'assurance	Exigences formulées à l'annexe C de la Norme	Lignes directrices[Table 4 note *]
Niveau 1	Aucune restriction quant à ce qui peut être fourni à titre de preuve de l'identité	• Présenter aux personnes un avis écrit stipulant que toute déclaration fausse ou trompeuse peut constituer une violation des modalités ou conditions. • Enregistrer dans un journal d'audit le fait qu'une personne a fait une déclaration.
Niveau 2	**Une** preuve de l'identité	• Une seule preuve de l'identité essentielle **ou** une seule preuve à l'appui de l'identité est requise. • Spécifier que les preuves de l'identité essentielles sont préférables à des preuves à l'appui de l'identité, si une rigueur accrue doit être appliquée. • Présenter aux personnes un avis écrit stipulant que l'utilisation non autorisée de preuves de l'identité peut mener à un refus de service ou constituer un motif de poursuite criminelle.
Niveau 3	**Deux** preuves de l'identité (dont au moins une doit être une preuve de l'identité essentielle)	• Il peut s'agir de deux preuves de l'identité essentielles; **ou** d'une preuve de l'identité essentielle et d'une preuve à l'appui de l'identité. • Les deux preuves de l'identité doivent provenir de sources faisant autorité différentes ou indépendantes (certaines sources peuvent émettre plus d'un type de document). • Il est recommandé que les deux preuves de l'identité émis par des sources différentes ne soient pas d'un même type. (Une telle situation peut se produire, bien que rare. Par exemple, une source peut cesser d'exister et une autre source peut émettre de nouveau le même document.)
Niveau 4	**Trois** preuves de l'identité (dont au moins une doit être une preuve de l'identité essentielle)	• La rigueur de cette exigence peut être renforcée, le cas échéant, en exigeant deux preuves de l'identité essentielles. • Tout renforcement de la rigueur doit préférablement être énoncé sous la forme d'une exigence additionnelle en matière de gestion des risques liés au programme.

Table 4 Notes

Table 4 Note *****

Il est entendu que les lignes directrices énoncées pour un niveau donné (p. ex., Niveau 3) s'ajoutent aux lignes directrices énoncées pour les niveaux inférieurs (p. ex., Niveau 1 et Niveau 2).

Retour à la référence de la note *

3.5 Exigences en matière d'exactitude des renseignements sur l'identité

3.5.1 Confirmation de l'exactitude des renseignements sur l'identité

Les exigences en matière d'exactitude permettent d'assurer la qualité des renseignements sur l'identité. Les renseignements sur l'identité doivent représenter la personne avec véracité et doivent être complets et à jour. Afin d'assurer l'exactitude des renseignements sur l'identité, il faut prendre en considération les facteurs suivants :

- **Les renseignements sur l'identité sont corrects.** Les renseignements sur l'identité peuvent changer au fil du temps à la suite de certains événements de la vie (p. ex., le mariage). Afin de maintenir leur exactitude, les renseignements sur l'identité doivent être actualisés de temps à autre.
- **Les renseignements sur l'identité sont liés à une personne réelle.** Les renseignements sur l'identité sont liés à une personne qui existe réellement. Dans la majorité des cas, la personne est toujours vivante, mais il arrive aussi que la personne soit décédée, puisque les renseignements sur l'identité d'une personne ne disparaissent pas après son décès.
- **Les renseignements sur l'identité se rapportent à la bonne personne.** Dans les grandes populations, certaines personnes peuvent présenter les mêmes renseignements sur l'identité que d'autres, ou des renseignements similaires - par exemple le nom, le sexe et la date de naissance. L'exigence d'unicité permet de régler la situation, mais il reste toujours possible que les renseignements sur l'identité soient reliés à la mauvaise personne.

La validation de l'identité est le processus permettant de confirmer l'exactitude des renseignements sur l'identité tels qu'établis par une partie ayant autorité[Note en bas de page7]. Tout dépendant des exigences propres au programme ou service et des considérations relatives à la protection des renseignements personnels, les organisations gouvernementales peuvent valider les renseignements sur l'identité au moyen de différentes sources faisant autorité. Par exemple, une date de naissance peut être validée électroniquement en consultant un registre provincial de la statistique de l'état civil.

S'il n'est pas possible de valider des renseignements sur l'identité en consultant une source faisant autorité, on peut utiliser d'autres méthodes, comme la corroboration des renseignements en utilisant une ou plusieurs preuves de l'identité. Il est recommandé aux organisations gouvernementales de tenir compte des considérations relatives aux fraudes décrites à la section 3.7.2.

Lorsque les sources faisant autorité ne font pas partie des administrations canadiennes, l'exactitude des renseignements sur l'identité sera établie grâce à une approche fondée sur la gestion des risques.

La détermination de l'exactitude des renseignements sur l'identité nécessite de confirmer que la personne existe actuellement ou a déjà existé (était en vie mais est maintenant décédée). Les renseignements sur l'identité doivent être liés à une personne réelle (vivante ou décédée) et non pas à une personne inexistante ou erronée.

L'exactitude des renseignements sur l'identité ne dépend aucunement du fait que la personne soit vivante ou décédée. Les renseignements sur l'identité d'une personne ne disparaissent pas après son décès. Après son décès, il sera particulièrement important que les renseignements sur l'identité d'une personne soient utilisés correctement par les personnes autorisées par exemple, par le conjoint survivant ou l'exécuteur testamentaire.

Des éléments comme la graphie et les variations phonétiques, les changements de nom et des alphabets différents peuvent compliquer la validation de l'exactitude de certains renseignements sur l'identité. Dans ces circonstances, il peut être difficile de stipuler des critères de correspondance exacte. Il pourrait être nécessaires pour les organisations gouvernementales de recourir à des méthodes de correspondance approximative ou de correspondance statistique pour déterminer s'il y a correspondance acceptable entre des renseignements sur l'identité et un enregistrement qui fait autorité.

Un identificateur attribué (voir la section 3.3.3) repose toujours sur une correspondance exacte. Dans les situations où l'intégrité d'un identificateur peut être déterminée au moyen d'un algorithme mathématique (p. ex., une somme de contrôle), il convient d'utiliser cette méthode dans le cadre du processus de validation.

Le tableau 5 présente des lignes directrices sur la détermination des exigences en matière d'exactitudes des renseignements sur l'identité présentées au tableau 1. Ces lignes directrices s'appliquent uniquement à l'établissement de l'exactitude des renseignements sur l'identité.

Tableau 5. Lignes directrices sur la détermination de l'exactitude des renseignements sur l'identité en fonction du niveau d'assurance

Niveau d'assurance	Exigences stipulées à l'annexe C de la Norme	Lignes directrices[Table 5 note *]
Niveau 1	Acceptation de l'affirmation de soi à titre de confirmation des renseignements sur l'identité	• Aviser les personnes qu'elles sont tenues de fournir des renseignements exacts sur elles-mêmes. • Aviser les personnes que toute déclaration fausse ou trompeuse peut donner lieu à une réduction de la qualité du service ou constituer une violation des modalités ou conditions. • Enregistrer dans un journal d'audit la date de la déclaration ainsi que les dates où les avis ont été présentés.
	Information sur l'identité correspond de façon acceptable à l'affirmation	• Demander aux personnes de confirmer que leurs renseignements sur l'identité correspondent bien à elles-mêmes et qu'ils sont compatibles avec la preuve de l'identité fournie. • Aviser les personnes que toute déclaration fausse ou trompeuse peut constituer un motif de poursuite criminelle. • Confirmer que la preuve de l'identité (en format papier ou électronique) a été délivrée légitimement par une administration qui est approuvée ou reconnue par l'organisation gouvernementale.

Niveau 2	par une personne et à la preuve de l'identité **et** Confirmation que la preuve de l'identité provient d'une autorité compétente	• Confirmer la validité ou l'intégrité du document, y compris les renseignements qu'il contient (p. ex., inspection des caractéristiques de sécurité, sommes de contrôle), et valider les certificats électroniques en validant l'autorité de délivrance et en vérifiant les listes de certificats révoqués. • Afficher un avertissement ou une mise en garde lorsqu'un utilisateur cherche à obtenir une validation auprès d'une source faisant autorité si l'enregistrement ou la preuve fait l'objet d'un signalement pour une raison quelconque (p. ex., fraude, date d'expiration atteinte). • Si aucun processus de validation à distance par voie électronique n'est disponible (p. ex., s'il n'existe aucun système d'accès à distance ou connectivité à un réseau), on peut utiliser un processus local ou manuel de validation. • Enregistrer dans un journal d'audit la nature des preuves utilisées.
Niveau 3	Information sur l'identité correspond de façon acceptable à l'affirmation par une personne et à toutes les preuves de l'identité **et** Confirmation de la preuve de l'identité essentielle à l'aide d'une source faisant autorité **et** Confirmation que la preuve à l'appui de l'identité provient d'une autorité compétente, à l'aide d'une source faisant autorité **ou** Inspection par un examinateur d'expérience	• Utiliser des méthodes d'appariement formel pour déterminer l'exactitude dans les limites de tolérance spécifiées (p. ex., variations de l'orthographie des noms). • Confirmer que les renseignements sur l'identité correspondent, dans les limites de tolérance spécifiées, avec toutes les preuves de l'identité présentées. • Valider les renseignements sur l'identité qui sont présentés en tant que preuves de l'identité essentielles en utilisant les enregistrements faisant autorité les plus à jour disponibles auprès d'une source faisant autorité. Au besoin, on peut utiliser des sources multiples. • Déterminer l'exactitude des renseignements sur l'identité en utilisant une approche fondée sur la gestion des risques lorsque la source faisant autorité ne fait pas partie des administrations canadiennes. • Faire évaluer l'exactitude des renseignements sur l'identité par un examinateur d'expérience dans les situations où les lignes directrices susmentionnées ne s'appliquent pas. • Enregistrer dans un journal d'audit les résultats du processus de confirmation.
Niveau 4	Information sur l'identité correspond de façon acceptable à l'affirmation par une personne et à toutes les preuves de l'identité **et** Confirmation de la preuve de l'identité essentielle à l'aide d'une source faisant autorité **et** Confirmation que la preuve à l'appui de l'identité provient d'une autorité compétente, à l'aide d'une source faisant autorité **ou** Inspection par un examinateur d'expérience	• Utiliser l'équivalent des exigences du Niveau 3 pour évaluer la preuve de l'identité, mais mettre en place des critères d'appariement plus rigoureux afin de déterminer leur exactitude dans les limites de tolérance spécifiées. Si un appariement excède une limite de tolérance spécifiée, il doit être traité comme une exception et géré selon une approche fondée sur la gestion des risques. • Comme pour le Niveau 3, faire évaluer l'exactitude des renseignements sur l'identité par un examinateur d'expérience dans les situations où les lignes directrices susmentionnées ne s'appliquent pas. Documenter les cas exceptionnels; il pourrait être nécessaire d'approuver des exceptions spécifiques et de mettre en place des procédures d'atténuation des risques. • Enregistrer dans un journal d'audit les résultats du processus de confirmation, y compris les situations où un appariement excède une limite de tolérance spécifiée.

Table 5 Notes

Table 5 Note *

Il est entendu que les lignes directrices énoncées pour un niveau donné (p. ex., Niveau 3) s'ajoutent aux lignes directrices énoncées pour les niveaux inférieurs (p. ex., Niveau 1 et Niveau 2).

Retour à la référence de la note *

3.6 Exigences en matière de liens avec une personne

Les exigences en matière de liens avec une personne permettent de veiller à ce que les renseignements sur l'identité concernent bel et bien la personne qui fait l'affirmation. Les liens permettent de veiller à ce que les renseignements sur l'identité se rapportent bien à une personne réelle qui utilise ses propres renseignements sur l'identité - c'est-à-dire que les renseignements sur l'identité ne sont pas utilisés frauduleusement par un imposteur.

Le processus de détermination des liens avec une personne est habituellement exécuté lorsqu'une personne sans relation ou association antérieure avec un programme ou service entreprend une transaction pour la première fois. Par exemple, une première rencontre avec un processus d'inscription à un programme ou un service nécessite normalement que la personne produise une preuve de son identité.

Le processus de détermination des liens avec une personne est aussi appelé « vérification de l'identité ». La vérification de l'identité est un processus différent de la validation de l'identité. La vérification de l'identité est le processus permettant de confirmer que les renseignements sur l'identité présentés concernent bel et bien la personne qui fait l'affirmation.

3.6.1 Méthodes de détermination des liens avec une personne

La *Norme sur l'assurance de l'identité et des justificatifs* décrit quatre méthodes pouvant être utilisées pour déterminer les liens avec une personne.[Note en bas de page8]

- La **confirmation basée sur les connaissances** permet de comparer de l'information personnelle ou privée afin de confirmer l'identité d'une personne. Exemples d'information pouvant être utilisée pour la confirmation basée sur les connaissances : mots de passe, numéros d'identification personnelle, questions personnelles, information propre à un programme, information financière ou sur le crédit.
- La **confirmation des caractéristiques biologiques ou comportementales** permet de comparer les caractéristiques biologiques (anatomiques et physiologiques) afin d'établir un lien vers une personne. Exemple : la comparaison d'une photo et d'une personne.
- La **confirmation par un arbitre de confiance** permet de se fier à un arbitre de confiance pour établir un lien avec la personne. L'arbitre de confiance est déterminé selon les critères propres au programme. Exemples d'arbitres de confiance : répondants, notaires et agents agréés.
- La **confirmation de possession matérielle** nécessite la possession physique ou la présentation de preuves pour établir l'identité d'une personne.

Les organisations gouvernementales doivent déterminer quelle méthode ou combinaison de méthodes elles utiliseront pour déterminer les liens en fonction des exigences de leur programme. Dans la sélection des méthodes appropriées, ils doivent tenir compte des considérations pertinentes en matière d'opérations, de protection de la vie privée et de questions juridiques.

Tableau 6. Exemples de méthodes de détermination des liens avec une personne

Type de méthode	Exemples de méthode
Confirmation basée sur les connaissances	• **Confirmation statique basée sur les connaissances :** Utilisation de renseignements personnels recueillis antérieurement ou établis à un moment précis dans le temps (p. ex., à l'occasion d'un processus d'enregistrement). • **Confirmation dynamique basée sur les connaissances :** Utilisation de renseignements personnels recueillis ou générés au fil du temps (plutôt qu'établis à un moment précis dans le temps).
Confirmation des caractéristiques biologiques ou comportementales	• **Comparaison des traits faciaux :** Comparaison manuelle des traits faciaux figurant sur la preuve de l'identité à ceux de la personne, ou utilisation d'un système automatisé de reconnaissance faciale. • **Comparaison de l'iris :** Comparaison des empreintes rétiniennes d'une personne à des empreintes recueillies antérieurement. • **Comparaison des empreintes digitales :** Comparaison de la structure physique des empreintes digitales d'une personne à des fins de reconnaissance. • **Comparaison de la voix :** Détection et reconnaissance de la parole pour comparaison à une empreinte vocale recueillie antérieurement. • **Comparaison de la signature :** Comparaison de la signature d'une personne à une signature associée à la preuve de l'identité. • **Analyse des données :** Utilisation de renseignements recueillis antérieurement pour identifier les caractéristiques, tendances ou comportements qui sont attribuables à la

	personne.
Confirmation par un arbitre de confiance[Note du tableau 6 *]	• **Répondant :** Une personne qui a accepté d'assumer la responsabilité de la confirmation des renseignements fournis par une autre personne. • **Notaire :** Une personne ou organisation titulaire d'une licence qui lui permet de faire prêter serment et d'attester des signatures relativement à des documents juridiques. • **Agent agréé :** Une personne autorisée à se porter garante d'une autre personne ou à agir pour son compte.

Physical possession confirmation	• **Démonstration physique de contrôle :** Démonstration physique par une personne de la possession ou du contrôle exclusif d'un document sécurisé ou d'un objet physique (p. ex., jeton) qui avait été antérieurement délivré à la personne :
	  ◦ dans le cas d'un document sécurisé, la confirmation peut comporter sa présentation pour examen de ses caractéristiques de sécurité ou pour sa validation;
	  ◦ dans le cas d'un objet physique sécurisé, la confirmation peut comporter une interaction sécurisée avec un processus de validation physique ou électronique.
	• Dans les deux cas, ces processus peuvent nécessiter la présence physique de la personne. Toutefois cette exigence n'empêcherait pas la possibilité de recourir à des processus de démonstration physique activés à distance.

Notes du tableau 6

Note du tableau 6 *****

Il est recommandé que les organisations gouvernementales élaborent des critères documentés pour les arbitres de confiance.

Retour à la référence de la note *

3.6.2 Lignes directrices en matière de méthodes de détermination des liens

Le tableau 7 présente les lignes directrices sur la sélection d'une méthode permettant de confirmer les liens entre des renseignements sur l'identité et une personne spécifique.

Tableau 7. Lignes directrices en matière de méthodes de détermination des liens en fonction du niveau d'assurance

Niveau d'assurance	Exigences	Lignes directrices[Note du tableau 7 *]
Niveau 1	Aucune exigence	• Utiliser des méthodes appropriées pour veiller à ce que l'interaction se fasse avec une personne **réelle** (et non pas un processus automatisé).
Niveau 2	Aucune exigence	• Utiliser des méthodes appropriées pour veiller à ce que l'interaction initiale et les interactions subséquentes puissent être reliées à la **même** personne qui formule les affirmations. Pour ce faire, on peut compter sur une assurance des justificatifs fournie par un service d'authentification.
Niveau 3	Au moins **une** des méthodes suivantes : • Confirmation basée sur les connaissances • Confirmation des caractéristiques biologiques ou comportementales • Confirmation par un arbitre de confiance • Confirmation de	• Ces méthodes d'établissement de liens doivent être utilisées en plus, ou séparément, d'une assurance des justificatifs fournie par un service d'authentification. • L'efficacité des méthodes d'établissement de liens dépend de facteurs tels que le contexte de prestation du service, le contexte des menaces et la preuve que la personne est disposée à ou en mesure de fournir. Il faut s'assurer de sélectionner et d'élaborer des méthodes d'établissement de liens qui n'imposent pas un fardeau excessif aux personnes ou qui n'induisent pas involontairement des vulnérabilités ou des risques (p. ex., en utilisant des renseignements personnels de nature délicate qui pourraient avoir une incidence négative s'ils venaient à être divulgués). • On peut renforcer les méthodes d'établissement de liens en sélectionnant une combinaison de techniques décrites au Tableau 6 (plutôt qu'une seule technique par méthode). Par exemple, une méthode de confirmation basée sur les connaissances peut combiner des méthodes statiques et dynamiques de confirmation basée sur les connaissances.

	• Confirmation de possession matérielle	• De même, pour la confirmation des caractéristiques biologiques ou comportementales, la méthode peut inclure une combinaison de techniques. Par exemple, la confirmation des caractéristiques biologiques ou comportementales peut combiner la combinaison des traits faciaux et la comparaison des empreintes digitales.
Niveau 4	Au moins **trois** des méthodes suivantes : • Confirmation basée sur les connaissances • Confirmation des caractéristiques biologiques ou comportementales • Confirmation par un arbitre de confiance • Confirmation de possession matérielle	• Veiller à ce que les méthodes d'établissement de liens utilisées soient indépendantes les unes des autres (l'utilisation d'une méthode ne peut pas compromettre l'utilisation d'une autre méthode).

Notes du tableau 7

Note du tableau 7 *****

Il est entendu que les lignes directrices énoncées pour un niveau donné (p. ex., Niveau 3) s'ajoutent aux lignes directrices énoncées pour les niveaux inférieurs (p. ex., Niveau 1 et Niveau 2).

Retour à la référence de la note * referrer

3.7 Facteurs à prendre en considération en matière de risque et de fraude

3.7.1 Facteurs à prendre en considération en matière de risque

Les principes de gestion du risque lié à l'identité sont similaires à ceux employés pour d'autres risques ministériels; cependant, il faut tenir compte de certains facteurs spécifiques propres à l'identité :

- Le risque lié à l'identité est difficile à gérer pour une seule organisation ou par un seul programme ou service au sein d'une organisation. Les facteurs à prendre en considération peuvent ne pas être sous le contrôle direct de l'organisation ou ne pas être assujettis à l'autorité de l'administration. Par exemple, un ministère peut compter sur certains documents pour identifier les personnes, mais pourrait ne pas être en mesure de déterminer si ces documents ont été volés ou sont faux.
- L'incidence du risque lié à l'identité ne se limite pas à une seule organisation. Une erreur ou une activité frauduleuse qui a seulement une faible incidence pour une organisation donnée peut avoir une incidence beaucoup plus élevée pour une autre organisation. Par exemple, un document obtenu de façon frauduleuse auprès d'un ministère pourra être utilisé pour obtenir un avantage considérable auprès d'un autre ministère.

Les facteurs de risque ci-dessous sont liés à l'identité des personnes :

- Une personne peut être associée à des renseignements sur l'identité erronés; par exemple, deux personnes distinctes peuvent avoir des noms et des dates de naissance identiques. Cette situation peut donner lieu à une confusion potentielle entre des services et droits.
- Les renseignements sur l'identité peuvent être inexacts ou périmés. Certains événements de la vie, comme un mariage, peuvent entraîner un changement de nom. Des erreurs de saisie des données peuvent se traduire par la transposition de dates et de noms.
- Les renseignements sur l'identité peuvent être affirmés par des parties dont il n'est pas possible de déterminer la fiabilité ou l'autorité. Ainsi, une personne, telle qu'un nouvel arrivant ou un visiteur au Canada, peut présenter des renseignements sur l'identité qui sont possiblement exacts mais impossibles à valider auprès d'une source faisant autorité.
- Les renseignements sur l'identité peuvent être utilisés par une personne autre que leur propriétaire légitime ou son représentant autorisé, par exemple si une personne utilise les renseignements sur l'identité appartenant à une autre personne. Si cette utilisation est intentionnelle, elle pourrait être considérée comme une fraude en matière d'identité en vertu du paragraphe 403(1) du *Code criminel*.
- Il est possible d'utiliser des faux documents pour étayer une identité. Une personne peut utiliser ou modifier une copie d'un certificat de naissance qui avait initialement été délivré à une autre personne pour assumer son identité. Une telle utilisation est considérée comme une fraude en matière d'identité.
- La documentation peut être insuffisante. Une personne peut posséder des documents dont l'authenticité ne peut pas

être confirmée ou qui ne peuvent pas être validés auprès d'une source faisant autorité.

3.7.2 Facteurs à prendre en considération en matière de fraude

Les organisations gouvernementales doivent se familiariser avec les différentes méthodes employées par les fraudeurs, puisque ces méthodes peuvent poser des risques pour le respect des exigences stipulées dans la *Norme sur l'assurance de l'identité et des justificatifs*.

La fraude fondée sur des documents repose sur l'acquisition, la production ou l'altération frauduleuse de documents délivrés par une autorité. Ce type de fraude comporte plusieurs techniques :

- **Fabrication ou contrefaçon de documents :** Fabrication non autorisée de documents au moyen d'appareils et de processus disponibles sur le marché ouvert ou acquis par des moyens non autorisés. Elle nécessite la simulation ou la réplication des caractéristiques de sécurité ou de personnalisation d'un document authentique.
- **Altération documents délivrés légitimement :** Altération non autorisée d'un document légitime existant. Exemple : modification de la date de naissance pour obtenir un nouveau droit, modification de la photographie et des données biographiques de manière à les faire correspondre à un faux titulaire.

La fraude fondée sur des enregistrements repose sur la création, l'insertion, l'altération ou la suppression non autorisées d'enregistrements faisant autorité qui sont sous le contrôle d'une institution. La création de faux enregistrements ou l'altération d'enregistrements existants peut donner lieu à la délivrance de documents ou de droits qui ne sont pas légitimes. Ce type de fraude comporte plusieurs techniques :

- **Agent de menace externe :** Création, insertion, altération ou suppression non autorisées d'enregistrements faisant autorité par des agents de menace externes qui se sont introduits dans le système hébergeant les enregistrements.
- **Délit d'initié ou collusion :** Création, insertion, altération ou suppression non autorisées d'enregistrements faisant autorité par des personnes en situation de confiance ou qui ont accès à des renseignements personnels ou de nature délicate.

La fraude fondée sur un imposteur repose sur l'utilisation frauduleuse des renseignements sur l'identité relatifs à une autre personne, que cette personne soit réelle ou fictive. Ce type de fraude comporte plusieurs techniques :

- **Utilisation de la preuve de l'identité d'une autre personne qui est inconnue.** S'il souhaite utiliser l'identité d'une autre personne, l'imposteur peut modifier son apparence ou modifier la preuve de l'identité. Dans ces situations, l'imposteur n'a pas habituellement une connaissance approfondie de la victime, et l'utilisation frauduleuse peut être détectée grâce à l'une des méthodes de confirmation décrites à la section 3.6.1.
- **Utilisation de la preuve de l'identité d'une autre personne qui est connue.** Le fraudeur peut agir en tant qu'imposteur (voir ci-dessus). Il peut aussi tenter d'agir pour le compte d'une autre personne en invoquant un rôle ou une relation non autorisé. Il faut utiliser des méthodes additionnelles pour veiller à ce qu'une personne agisse bien de façon légitime pour le compte d'une autre personne.
- **Utilisation de la preuve de l'identité d'une autre personne dont l'identité a été fabriquée.** Il s'agit du type de fraude le plus sophistiqué, qui peut être utilisé en conjonction avec une fraude fondée sur des documents et/ou une fraude fondée sur des enregistrements. En raison de son degré élevé de sophistication, ce type de fraude est habituellement associé à des agents de menace extrêmement motivés, tels que le crime organisé.

3.8 Facteurs à prendre en considération en matière d'intégration

Les exigences en matière de niveaux d'assurance de l'identité s'inscrivent habituellement dans un ensemble plus exhaustif d'exigences liées à un programme ou service qui sont elles-mêmes intégrées à des processus ou systèmes opérationnels plus généraux. La présente section décrits différents facteurs à prendre en considération pour intégrer les exigences en matière de niveaux d'assurance de l'identité aux processus ou systèmes opérationnels. Par exemple, un ministère peut décider d'intégrer ces exigences à un processus d'inscription des clients à l'appui d'un programme spécifique. Un autre ministère peut décider de mettre en uvre les exigences en créant un processus d'assurance de l'identité qui pourra être incorporé à de nombreux programmes et services.

Quelle que soit l'approche d'intégration retenue, les organisations gouvernementales doivent être en mesure de démontrer comment elles satisfont aux exigences en matière de niveaux d'assurance de l'identité déterminées pour leurs programmes et services.

Pour la mise en uvre des exigences en matière d'assurance de l'identité, il est recommandé que les organisations gouvernementales tiennent compte des facteurs suivants :

- Les exigences sont indépendantes du mode de prestation et de la technologie utilisés. Cette indépendance appuie l'engagement du gouvernement du Canada à l'égard de l'accès et de la prestation de services multimodes.
- Une saine pratique consiste à envisager des options additionnelles d'accès et de prestation qui répondent le mieux aux besoins des clients, qui permettent l'accessibilité pour un vaste éventail de personnes handicapées et qui favorisent l'adoption grâce à une approche fondée sur la confiance.
- Les exigences peuvent être mises en uvre en collaboration avec d'autres organisations gouvernementales membre d'une même fédération (voir la section 3.9).
- Lorsqu'ils intègrent les exigences de la *Norme sur l'assurance de l'identité et des justificatifs* à leurs processus ou systèmes opérationnels, les organisations gouvernementales doivent veiller à ce que les procédures d'assurance de l'identité soient autant que possible efficientes et invisibles pour les clients.

3.9 Facteurs à prendre en considération en matière de fédération

Une fédération est un accord de coopération entre des entités autonomes qui ont convenu de travailler ensemble. Elle peut se composer d'organisations des secteurs public et privé, de différents ordres de gouvernements ou de pays multiples. De nombreuses fédérations sont de nature plus informelle : elles sont fondées sur des pratiques partagées et des objectifs communs qui ont été élaborés au fil du temps. Alors que ces fédérations informelles prennent de la maturité, leurs ententes informelles sont remplacées par des cadres de fiabilité et des processus d'évaluation convenus par toutes les parties qui englobent des ententes contractuelles, des ententes de service, des obligations juridiques ainsi que des mécanismes de règlement des différends.

Les fédérations deviennent une option particulièrement intéressante lorsqu'il existe une nécessité opérationnelle de fournir des services en ligne de façon transparente à travers les frontières ministérielles et juridictionnelles, en englobant des fournisseurs des secteurs public et privé. Combler de tels besoins nécessite un niveau de confiance entre divers types d'organisations qui peuvent avoir des mandats divergents et relever d'autorités différentes. Un cadre de fiabilité stipule la conformité aux normes convenues par les parties, officialise les processus d'évaluation et définit les rôles et les responsabilités des parties.

3.9.1 Établissement d'une approche pancanadienne

Le gouvernement du Canada s'est engagé à aider les partenaires fédéraux, provinciaux, territoriaux et municipaux à respecter les exigences associées à leurs programmes et services respectifs, en utilisant des processus communs fiables.

Le gouvernement du Canada collabore avec les autres ordres de gouvernements à l'élaboration d'une approche pancanadienne à la fédération de l'identité qui respecte l'autonomie et les lois des différents ordres de gouvernements. En novembre 2014, la Table des SM FPT sur la collaboration en matière de prestation de services a approuvé la *Norme pancanadienne sur la validation de l'identité,*[Note en bas de page9] qui uniformise les demandes et réponses de validation des renseignements sur l'identité et des renseignements personnels échangées par les organisations fédérales, provinciales, territoriales et municipales.

Il est recommandé que les organisations gouvernementales incorporent la *Norme pancanadienne sur la validation de l'identité* à la planification de la mise en uvre de leurs programmes et services.

3.9.2 Établissement d'un modèle fédératif

La présente Ligne directrice peut servir de cadre pour aider une organisation gouvernementale à adopter un modèle fédératif et à compter sur des services fiables assurés par d'autres organisations. Plutôt que de mettre en uvre elle-même les exigences nécessaires en matière d'assurance de l'identité, une organisation gouvernementale pourra choisir d'adopter un modèle fédératif. Cependant, avant de devenir membre d'une fédération, une organisation gouvernementale doit veiller à ce que certains éléments clés du modèle fédératif soient mis en uvre au sein de son propre contexte organisationnel, plus spécifiquement les rôles de la partie ayant autorité et de la partie en confiance.

Une partie ayant autorité est définie dans la *Norme sur l'assurance de l'identité et des justificatifs* comme un membre de la fédération qui offre des assurances (de justificatifs ou d'identité) à d'autres membres (parties en confiance). Une partie en confiance est un membre de la fédération qui reçoit des assurances (de justificatifs ou d'identité) d'autres membres (parties ayant autorité). Une unité d'une organisation peut assumer le rôle d'une partie ayant autorité, tandis que les autres unités assument le rôle de la partie en confiance. Par exemple, un système ministériel de ressources humaines (RH) pourra jouer le rôle de la partie ayant autorité en ce qui concerne les renseignements sur les employés, tandis que le système ministériel de sécurité responsable de la délivrance des cartes d'identification des employés jouera le rôle de la partie en confiance.

Le Tableau 8 décrit les principaux facteurs à prendre en considération dans la sélection des unités qui assumeront les rôles de la partie ayant autorité et de la partie en confiance.

Tableau 8. Facteurs à prendre en considération pour la mise en uvre d'un modèle fédératif

Rôle organisationnel	N'est pas membre d'une fédération	Est membre d'une fédération
Assume le rôle	**Facteurs à prendre en considération pour l'organisation :** • peut être une partie ayant autorité pour sa propre organisation; • peut produire des preuves de l'identité essentielles ou des preuves à l'appui de l'identité qui pourront être utilisées par d'autres organisations; • peut fournir des assurances de l'identité **seulement** pour sa propre organisation (ne peut pas fournir des assurances de l'identité hors de l'organisation); • peut fournir des renseignements sur	**Facteurs à prendre en considération pour l'organisation :** • peut être une partie ayant autorité pour les membres de la fédération (en plus de sa propre organisation); • peut produire des preuves de l'identité essentielles ou des preuves à l'appui de l'identité qui pourront être utilisées par d'autres organisations; • peut fournir des assurances de l'identité aux parties en confiance de la fédération;

Assume le rôle d'une partie ayant autorité	l'identité à l'appui d'un processus de validation de l'identité dans une autre organisation; • est responsable de la gestion du risque lié à l'identité associé à sa propre organisation. **Les organisations doivent :** • mettre en uvre les exigences de la *Norme sur l'assurance de l'identité et des justificatifs* (la Norme) au niveau d'assurance requis. Exemple : Un système ministériel de RH qui tient à jour des dossiers d'employés faisant autorité. **Facteurs à prendre en considération pour l'organisation :** • peut utiliser des preuves de l'identité essentielles et des preuves à l'appui de l'identité fournies par une autre organisation; • peut utiliser des renseignements sur l'identité validés par une autre organisation; • le risque lié à l'identité demeure la responsabilité de l'organisation; • le risque propre au programme demeure la responsabilité de l'organisation.	parties en confiance de la fédération; • peut répartir les conséquences du risque lié à l'identité lorsqu'elle fournit des assurances de l'identité aux parties en confiance de la fédération (à un niveau d'assurance donné). **Les organisations doivent :** • mettre en uvre les exigences de la Norme au niveau d'assurance requis; • participer en tant que partie ayant autorité au sein de la fédération et respecter les critères de la fédération établis par le dirigeant principal de l'information du gouvernement du Canada.
Assume le rôle d'une partie en confiance	**Les organisations doivent :** • mettre en uvre les exigences de la Norme au niveau d'assurance requis; **ou** • conclure une entente avec une autre partie pour mettre en uvre les exigences de la Norme pour son compte (p. ex., protocole d'entente, accord bilatéral). Exemple : Un système ministériel de sécurité qui compte sur des dossiers d'employés faisant autorité tenus à jour par un système ministériel de RH.	**Facteurs à prendre en considération pour l'organisation :** • peut compter sur des assurances de l'identité fournies par une partie ayant autorité dans la fédération (à un niveau d'assurance donné); • peut partager un risque lié à l'identité lorsqu'elle compte sur des assurances de l'identité (à un niveau d'assurance donné); • le risque propre au programme demeure la responsabilité de l'organisation. **Les organisations doivent :** • participer en tant que partie en confiance au sein de la fédération; **et** • respecter les critères de la fédération établis par le dirigeant principal de l'information du gouvernement du Canada.

3.9.3 Adoption de cadres de fiabilité

Le gouvernement du Canada participe à l'élaboration d'un cadre de fiabilité pancanadien qui facilitera la collaboration avec les autres administrations et l'évaluation des cadres de fiabilité de l'industrie en vue de leur utilisation par le gouvernement du Canada. La *Norme sur l'assurance de l'identité et des justificatifs*, ainsi que la présente Ligne directrice, feront partie intégrante de ce cadre de fiabilité. Les organisations gouvernementales peuvent avoir la certitude que la Norme et son cadre d'application ont été conçus pour appuyer l'adoption des cadres de fiabilité existants et émergeants.

3.10 Autres facteurs à prendre en considération en matière de politiques et de lois

En mettant en uvre les exigences relatives à l'assurance de l'identité, les organisations gouvernementales doivent s'assurer de respecter les autres instruments de politique et lois applicables. Par exemple, une autre politique peut stipuler qu'une organisation gouvernementale doit utiliser un identificateur attribué spécifique ou peut permettre uniquement la collecte d'un ensemble spécifique d'attributs pouvant être utilisés comme renseignements sur l'identité.

3.10.1 *Loi sur la protection des renseignements personnels* et *Politique sur la protection de la vie privée*

En mettant en uvre les exigences en matière d'assurance de l'identité, les organisations gouvernementales doivent respecter la *Loi sur la protection des renseignements personnels* et la *Politique sur la protection de la vie privée*. Elles doivent tenir

compte du droit des personnes à la vie privée, tout en assurant l'accès à leurs renseignements personnels et en s'assurant de leur exactitude.

Les renseignements relatifs à un particulier identifiable sont considérés comme étant des renseignements personnels et sont donc assujettis à la *Loi sur la protection des renseignements personnels.* La collecte, l'utilisation, la divulgation ou l'élimination de renseignements sur l'identité doivent être conformes à la *Loi sur la protection des renseignements personnels* et à la loi habilitante du ministère. Tous les renseignements sur l'identité doivent être considérés comme un sous-ensemble des « renseignements personnels », tels que définis par la *Loi sur la protection des renseignements personnels*. Les organisations gouvernementales sont invitées à consulter leurs conseillers juridiques afin de veiller à ce que leur gestion des renseignements sur l'identité respecte leur loi habilitante.

La *Politique sur la protection de la vie privée* et ses directives, normes et lignes directrices connexes relatives à la vie privée s'appliquent également aux renseignements sur l'identité. Les organisations gouvernementales doivent cerner, évaluer, surveiller et atténuer les risques liés à la vie privée pouvant découler de la création, la collecte, l'utilisation, la conservation, la divulgation et l'élimination de renseignements sur l'identité.

Il importe que les organisations gouvernementales fassent la distinction entre les renseignements recueillis à l'appui des exigences en matière d'assurance de l'identité et les autres renseignements personnels qui sont recueillis, utilisés, conservés et éliminés dans le contexte d'un programme ou service spécifique. Une distinction insuffisante entre les renseignements sur l'identité et les renseignements propres à un programme ou service pourrait avoir des incidences sur la vie. Ceci est particulièrement important, par exemple, lorsque des renseignements sur l'identité sont recueillis et utilisés à l'appui de plusieurs services connexes.

Des renseignements sur l'identité peuvent être recueillis, utilisés, conservés, divulgués et éliminés dans le cadre d'un processus opérationnel plus général, par exemple le traitement des inscriptions ou la détermination de l'admissibilité. Si les renseignements sur l'identité doivent être extraits de renseignements existants propres à un programme, les organisations gouvernementales doivent s'assurer de respecter la *Politique sur la protection de la vie privée*, notamment en veillant à ce que l'utilisation des renseignements sur l'identité est conforme à la ou aux raisons d'être originales pour lesquelles les renseignements avaient été obtenus ou compilés.

Il existe de nombreuses façons de protéger les renseignements sur l'identité, par exemple le stockage des enregistrements dans des dépôts de données différents, le chiffrement des données et la substitution ou le mappage des identificateurs. Peu importe le mécanisme utilisé, les renseignements obtenus doivent être traités comme des renseignements personnels.

3.10.2 *Politique sur les services*

Les organisations gouvernementales fédérales doivent respecter la *Politique sur les services.* En mettant en uvre les exigences en matière d'assurance de l'identité, les organisations gouvernementales doivent évaluer la conception de services fortement axés vers le client qui sont à la fois intégrés, simples, pratiques et fournis en temps opportun.

Les organisations gouvernementales, lorsqu'elles élaborent de nouveaux services et transforment leurs services existants, sont invitées à pousser leur réflexion au-delà des processus fondés sur les documents et des mises en uvre fondées sur des technologies spécifiques. Afin d'assurer leur participation au sein d'une fédération élargie de gestion de l'identité, les organisations gouvernementales sont également invitées à normaliser les pratiques, processus et technologies qui peuvent être déployés au-delà de leur propre organisation selon une approche qui permet néanmoins de préserver la confiance et l'intégrité.

Pour obtenir de plus amples renseignements sur le respect des exigences en matière de prestation de services, veuillez consulter la *Politique sur les services*.

3.10.3 *Code criminel* du Canada

Les organisations gouvernementales doivent se familiariser avec l'applicabilité potentielle des sections suivantes du *Code criminel*, notamment les définitions de « pièce d'identité » et de « renseignements sur l'identité » telles qu'elles s'appliquent dans le contexte du Code :

- **Paragraphes 56.1(1) et (2)** relativement à l'utilisation de pièces d'identité associées à une autre personne.
- **Paragraphe 56.1(3)** relativement à la définition de « pièce d'identité », dans le contexte des paragraphes 56.1(1) et 56.1(2).
- **Paragraphes 57(1) à 57(6)** relativement à l'utilisation du passeport canadien.
- **Article 402.1** relativement à la définition de « renseignements sur l'identité ». On notera qu'il s'agit d'une définition plus restreinte des renseignements sur l'identité qui s'applique aux articles 402.2 et 403 relativement au vol d'identité et à la fraude à l'identité.
- **Article 402.2** relativement à la possession illégale de renseignements sur l'identité (vol d'identité).
- **Article 403** relativement à l'usurpation frauduleuse du nom d'une autre personne.

3.10.4 Autres politiques et lois

En plus des politiques et lois susmentionnées, les organisations gouvernementales doivent déterminer si d'autres instruments de politique ou lois peuvent s'appliquer dans leur contexte spécifique.

4. Références

Lois

- *Code criminel*
- *Loi sur la protection des renseignements personnels et les documents électroniques*
- *Loi sur la protection des renseignements personnels*
- *Règlement sur la protection des renseignements personnels*

Instruments de politique du gouvernement du Canada

- *Directive sur la gestion de la sécurité ministérielle*
- *Directive sur la gestion de l'identité*
- *Directive sur les rôles et responsabilités en matière de gestion de l'information*
- *Directive sur l'évaluation des facteurs relatifs à la vie privée*
- *Directive sur les pratiques relatives à la protection de la vie privée*
- *Directive sur les demandes de renseignements personnels et de correction*
- *Directive sur la tenue de documents*
- *Directive sur le numéro d'assurance sociale*
- *Ligne directrice sur la définition des exigences en matière d'authentification*
- *ITSG-31 : Guide sur l'authentification des utilisateurs pour les systèmes TI*
- *ITSG-33 : La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*
- *Politique sur la sécurité du gouvernement*
- *Politique sur la gestion de l'information*
- *Politique sur la protection de la vie privée*
- *Politique sur les services*
- *Norme sur l'assurance de l'identité et des justificatifs*
- *Norme sur le filtrage de sécurité*

Pour obtenir de plus amples détails sur ces instruments et d'autres ressources, y compris des documents de l'industrie et des documents internationaux, veuillez consulter l'annexe B.

5. Renseignements additionnels

5.1 Date de la prochaine révision

La présente Ligne directrice sera réexaminée et mise à jour au besoin.

5.2 Demandes d'information et commentaires

Si vous souhaitez obtenir une interprétation de tout aspect de la présente Ligne directrice, veuillez communiquer avec le Bureau des demandes de renseignements du public du Secrétariat du Conseil du Trésor.

Annexe A : Principaux termes et définitions

Les principaux termes utilisés dans la présente Ligne directrice sont fondés sur des définitions qui font autorité tirées de la *Norme sur l'assurance de l'identité et des justificatifs*, des définitions provenant de lignes directrices connexes et de documents de référence de l'industrie ainsi que des définitions créées par le groupe de travail pour les besoins de la présente Ligne directrice.

assurance :
Une mesure de certitude que l'énoncé ou le fait est juste. (Source : *Norme sur l'assurance de l'identité et des justificatifs*)

assurance de l'identité :
Une mesure d'assurance que la personne, l'organisation ou l'appareil est bien celui qu'il affirme être. (Source : *Norme sur l'assurance de l'identité et des justificatifs*)

assurance des justificatifs :
L'assurance qu'une personne, une organisation ou un appareil a conservé le contrôle de ce qui lui a été confié (p. ex., clé, jeton, document, identificateur) et que le justificatif n'a pas été compromis (p. ex., falsifié, corrompu, modifié). (Source : *Norme sur l'assurance de l'identité et des justificatifs*)

attribut :
Voir « Attribut d'identité ».

attribut d'identité :
Propriété ou caractéristique associée à une personne identifiable; aussi appelé élément de donnée sur l'identité.

authentification :
Le processus d'établissement de la vérité ou de l'authenticité en vue de la génération d'une assurance. (Source : *Ligne directrice sur la définition des exigences en matière d'authentification*).

biométrie :

Un terme générique utilisé à la fois pour décrire une caractéristique ou pour décrire un processus. Il peut faire référence à une caractéristique biologique (anatomique et physiologique) ou comportementale mesurable permettant la reconnaissance automatisée d'une personne. Ce terme peut également faire référence à des méthodes automatisées de reconnaissance d'un individu en fonction de caractéristiques biologiques (anatomiques et physiologiques) ou comportementales mesurables. (Source : Glossaire de la International Biometrics & Identification Association).

cadre de fiabilité :

Système formalisé permettant de préserver la confiance que les membres d'une fédération ont les uns envers les autres. Un cadre de fiabilité vient étayer formellement les relations de confiance en stipulant le respect de certaines normes, en formalisant les processus d'évaluation et en définissant les rôles et les responsabilités des parties à des ententes multipartites.

confirmation basée sur les connaissances :

Un processus qui permet de comparer de l'information personnelle ou privée afin de confirmer l'identité d'une personne. Exemples d'information pouvant être utilisée pour la confirmation basée sur les connaissances : les mots de passe, les numéros d'identification personnelle, les questions personnelles, l'information propre à un programme et l'information financière ou sur le crédit. (Source : *Norme sur l'assurance de l'identité et des justificatifs*)

confirmation de possession matérielle :

Un processus qui nécessite la possession physique ou la présentation de preuves pour établir l'identité d'une personne. (Source : *Norme sur l'assurance de l'identité et des justificatifs*)

confirmation des caractéristiques biologiques ou comportementales :

Un processus qui permet de comparer les caractéristiques biologiques (anatomiques et physiologiques) afin d'établir un lien vers une personne, par exemple, la comparaison d'une photo et d'une personne. (Source : *Norme sur l'assurance de l'identité et des justificatifs*)

confirmation par un arbitre de confiance :

Un processus qui permet de se fier à un arbitre de confiance pour établir un lien avec la personne. L'arbitre de confiance est déterminé selon les critères propres au programme. Exemples d'arbitres de confiance : les répondants, les notaires et les agents agréés. (Source : *Norme sur l'assurance de l'identité et des justificatifs*)

contexte de l'identité :

Ensemble de circonstances, situation ou scénario dans lesquels un particulier interagit avec d'autres particuliers ou avec une organisation.

établissement de l'identité :

Création d'un enregistrement de l'identité qui fait autorité auquel d'autres se fieront pour des activités, programmes et services gouvernementaux subséquents.

fédération :

Une entente de coopération entre des entités autonomes qui ont accepté de travailler ensemble. Une fédération repose sur des relations de confiance et des normes pour faciliter l'interopérabilité. (Source : *Norme sur l'assurance de l'identité et des justificatifs*)

gestion de l'identité :

L'ensemble de principes, de pratiques, de processus et de procédures utilisés pour respecter le mandat d'une organisation et ses objectifs en lien avec l'identité. (Source : *Norme sur l'assurance de l'identité et des justificatifs*)

Identité :

Une référence ou une désignation utilisée pour faire la distinction entre une personne, une organisation ou un appareil unique et spécifique. (Source : *Norme sur l'assurance de l'identité et des justificatifs*)

identificateur :

Ensemble des attributs d'identité servant à distinguer une personne, une organisation ou un appareil unique donné.

identificateur attribué :

Chaîne numérique ou alphanumérique qui est générée automatiquement et qui permet de faire une distinction entre deux ou plusieurs personnes sans recourir à d'autres attributs d'identité.

justificatif :

Un objet physique ou électronique unique (ou identificateur) émis à une personne, une organisation ou un appareil ou en lien avec celui-ci. (Source : *Norme sur l'assurance de l'identité et des justificatifs*)

lien :

Processus permettant de déterminer que les renseignements sur l'identité concernent bel et bien la personne qui fait l'affirmation.

niveau d'assurance :

Un niveau d'assurance sur lequel d'autres peuvent se fier. (Source : *Norme sur l'assurance de l'identité et des justificatifs*)

niveau d'assurance de l'identité :

Le niveau d'assurance que la personne, l'organisation ou l'appareil est bien celui qu'il affirme être. (Source : *Norme sur l'assurance de l'identité et des justificatifs*)

niveau d'assurance du justificatif :

Le niveau d'assurance qu'une personne, une organisation ou un appareil a conservé le contrôle de ce qui lui a été confié (p. ex., clé, jeton, document, identificateur) et que le justificatif n'a pas été compromis (p. ex., falsifié, corrompu, modifié). (Source : *Norme sur l'assurance de l'identité et des justificatifs*)

notification des renseignements sur l'identité :

Notification de la possibilité que des renseignements sur l'identité aient été modifiés ou aient été exposés à des facteurs de risque - par exemple, détection d'une utilisation frauduleuse ou utilisation de documents périmés.

partie ayant autorité :

Un membre de la fédération qui offre des assurances de justificatifs ou d'identité à d'autres membres (parties utilisatrices). (Source : *Norme sur l'assurance de l'identité et des justificatifs*)

partie en confiance :

Un membre de la fédération qui reçoit des assurances de justificatifs ou d'identité d'autres membres (parties ayant autorité).

(Source : *Norme sur l'assurance de l'identité et des justificatifs*)

preuve documentaire :
Toute information sur support matériel pouvant servir de preuve (on considère généralement qu'il s'agit d'information couchée sur papier, mais de façon plus générale ce terme englobe également les preuves autres que sur support matériel).

preuve de l'identité :
Un document provenant d'une source faisant autorité et qui confirme l'intégrité et l'exactitude des affirmations d'identité formulées par une personne. Il existe deux catégories de preuves de l'identité :

preuve de l'identité essentielle :
La preuve de l'identité qui comprend de l'information de base, comme le nom de famille, le ou les prénoms, la date de naissance, le sexe et le lieu de naissance. Exemples : dossiers de naissance, d'immigration ou de citoyenneté provenant d'une autorité au sein de la compétence pertinente;

preuve à l'appui de l'identité :
La preuve de l'identité qui corrobore la preuve essentielle et permet d'établir un lien entre l'information d'identification et la personne concernée. Elle peut comprendre également de l'information supplémentaire, comme une photo, une signature ou une adresse. Exemples : dossier d'assurance sociale; dossier de droit de se déplacer, de conduire ou d'obtenir de l'assurance maladie; dossier de mariage, de décès ou de changement de nom provenant d'une autorité compétente.

(Source : *Norme sur l'assurance de l'identité et des justificatifs*)

preuve électronique ou numérique :
Toute donnée enregistrée ou préservée sur quelque support que ce soit dans un ordinateur ou un dispositif semblable. Exemples : enregistrements dans une base de données, journaux d'audit ou documents produits au moyen d'un logiciel de traitement de texte.

relation de confiance :
Entente établie qui permet d'assurer la confiance entre les parties de la relation.

renseignements sur l'identité :
Ensemble des attributs d'identité suffisant pour distinguer un particulier de tous les autres particuliers, et suffisant pour décrire ce particulier selon les exigences du programme ou du service.

risque en lien avec l'identité :
Le risque qu'une personne, une organisation ou un appareil ne soit pas celui qu'il affirme être. (Source : *Norme sur l'assurance de l'identité et des justificatifs*)

risque lié aux justificatifs :
Le risque qu'une personne, une organisation ou un appareil ait perdu le contrôle du justificatif qui lui a été délivré. (Source : *Norme sur l'assurance de l'identité et des justificatifs*)

source faisant autorité :
Une collection ou un registre de dossiers entretenu par une autorité qui respecte les critères établis. (Source : *Norme sur l'assurance de l'identité et des justificatifs*)

validation de l'identité :
Processus permettant de confirmer l'exactitude de renseignements sur l'identité établie par une partie ayant autorité.

vérification de l'identité :
Processus permettant de confirmer que les renseignements sur l'identité présentés concernent bel et bien la personne qui fait l'affirmation.

Annexe B : Références annotées

Instruments de référence du Conseil du Trésor

Cette section présente un résumé des politiques, directives, normes et lignes directrices encadrant la gestion de l'information, la sécurité de la TI et la protection des renseignements personnels.

Politique sur la sécurité du gouvernement

La *Politique sur la sécurité du gouvernement* a pour objectif de veiller à ce que les administrateurs généraux gèrent efficacement les activités de sécurité au sein des organisations gouvernementales et contribuent à la gestion efficace de la sécurité à l'échelle du gouvernement. La Politique est appuyée par deux directives :

- *Directive sur la gestion de la sécurité ministérielle*. Cette Directive a pour objectif d'assurer une gestion efficiente, efficace et responsable de la sécurité dans les organisations gouvernementales.
- *Directive sur la gestion de l'identité*. L'objectif de cette Directive consiste à s'assurer d'instaurer des pratiques efficaces de gestion de l'identité en donnant un aperçu des exigences qui aideront les organisations gouvernementales à établir, à utiliser et à valider l'identité.

La Directive sur la gestion de l'identité est appuyée par une norme et deux lignes directrices :

- *Norme sur l'assurance de l'identité et des justificatifs. L'objectif de cette Norme consiste à veiller à ce que les risques en lien avec l'identité soient gérés de façon uniforme et collaborative à l'échelle du gouvernement du Canada et au sein d'autres compétences et secteurs de l'industrie.*
- *Ligne directrice sur la définition des exigences en matière d'authentification*. Cette Ligne directrice présente des consignes pour l'exécution d'évaluations du niveau d'assurance et pour la détermination des options d'authentification. Elle fait référence

spécifiquement à la section 3.0, « Processus d'évaluation du niveau d'assurance ».
- *Ligne directrice sur l'assurance de l'identité*. Cette Ligne directrice présente des consignes pour la mise en uvre des exigences spécifiées à l'annexe C de la *Norme sur l'assurance de l'identité et des justificatifs*.

Politique sur la protection de la vie privée

La *Politique sur la protection de la vie privée* a pour objectifs de :

- faciliter la conformité législative et règlementaire, ainsi que renforcer l'application efficace de la *Loi sur la protection des renseignements personnels* et du Règlement par les institutions fédérales;
- assurer l'application uniforme de pratiques et procédures dans l'administration de la *Loi* et du Règlement afin que les requérants obtiennent de l'aide pour présenter une demande de renseignements personnels;
- assurer la protection et la gestion efficace des renseignements personnels en cernant, en évaluant, en surveillant et en atténuant les risques d'entrave à la vie privée dans les programmes et activités du gouvernement dans le cadre desquels des renseignements personnels sont créés, recueillis, utilisés, conservés, divulgués ou détruits.

La Politique sur la protection de la vie privée est appuyée par les directives suivantes :

- *Directive sur l'évaluation des facteurs relatifs à la vie privée*. Cette Directive exige que les organisations gouvernementales mènent une évaluation des facteurs relatifs à la vie privée pour chaque programme ou activité nouveau ou ayant fait l'objet de modifications importantes qui comporte la création, la collecte, l'utilisation, la conservation, la divulgation et l'élimination de renseignements personnels.
- *Directive sur les pratiques relatives à la protection de la vie privée*. Cette Directive facilite la mise en uvre et la publication des pratiques de gestion de la vie privée saines et uniformes régissant la création, la collecte, l'utilisation, la conservation, la divulgation et l'élimination des renseignements personnels dont les institutions fédérales sont responsables.
- *Directive sur les demandes de renseignements personnels et de correction*. Cette Directive établit des pratiques et des procédures uniformes pour le traitement des demandes d'accès aux renseignements personnels sous le contrôle d'institutions fédérales et le traitement des demandes de correction de renseignements personnels qui ont été, sont ou peuvent être utilisés à des fins administratives.

Politique sur la gestion de l'information

L'objectif de la *Politique sur la gestion de l'information* consiste à assurer une gestion de l'information efficace à l'appui de la mise en uvre des programmes et des services; à assurer des processus décisionnels efficaces; à faciliter la reddition de comptes, la transparence et la collaboration; et à préserver l'information et veiller à l'accès à l'information et aux documents pour le bienfait de la génération actuelle et des générations à venir.

La Politique sur la gestion de l'information est appuyée par les directives suivantes :

- *Directive sur les rôles et responsabilités en matière de gestion de l'information. Cette Directive établit les rôles et les responsabilités de tous les employés des ministères et organismes à l'appui de l'administrateur général dans la gestion efficace de l'information au sein de leur organisation.*
- *Directive sur la tenue de documents. Cette Directive assure l'adoption de pratiques efficaces de tenue de documents qui permettent aux ministères de créer, d'acquérir, de saisir, de gérer et de protéger l'intégrité des ressources documentaires ayant une valeur opérationnelle relativement à l'exécution des programmes et à la prestation des services du gouvernement du Canada.*

Politique sur les services

La *Politique sur les services* a pour objectif de mettre en place une approche stratégique et cohérente en matière de conception et de prestation de services internes intégrés et externes du gouvernement du Canada qui est axée sur les clients, obtient des gains d'efficience opérationnelle et favorise une culture de l'excellence en ce qui a trait à la gestion des services.

La Politique sur les services est appuyée par les lignes directrices suivantes :

- *Ligne directrice sur les ententes de services - Synthèse*. Cette Ligne directrice donne aux gestionnaires et aux cadres supérieurs de programmes et des services un aperçu des concepts et étapes clés de l'établissement d'ententes de services.
- *Ligne directrice sur les ententes de services - Éléments essentiels.* Cette Ligne directrice fournit des conseils, des indications, des exemples pratiques et des modèles aux personnes chargées d'établir des ententes de services ou de réviser des ententes préparées par l'autre partie dans une relation de service en constante évolution.
- Ligne directrice sur les normes de service. Cette Ligne directrice *fournit une orientation générale sur l'utilisation de normes de service à l'échelle du gouvernement du Canada. D'autres documents provenant d'autres centres décisionnels du Secrétariat du Conseil du Trésor et portant sur des normes de service liées à des types précis de services, comme les subventions et les contributions, les affaires réglementaires et les ressources humaines, viennent compléter la Ligne directrice.*

On trouvera des lignes directrices et outils connexes en suivant les liens susmentionnés.

Autres lignes directrices et normes connexes

La présente section décrit des lignes directrices et des normes de l'industrie connexes pour la gestion de l'information, pour la protection de la TI et des renseignements personnels et pour utilisation en conjonction avec la présente Ligne directrice.

Évaluation des menaces et des risques

Les organisations gouvernementales peuvent vouloir mener des évaluations plus généralisées des risques en matière de sécurité, à titre de mesure additionnelle, lorsqu'elles procèdent à la mise en uvre les exigences minimales stipulées à l'annexe C de la *Norme sur l'assurance de l'identité et des justificatifs*. Par exemple, une évaluation des risques en matière de sécurité peut être utile pour cibler les agents de menace très spécialisés liés à un environnement en ligne en rapide évolution, ainsi que les vulnérabilités possibles qui découlent des technologies plus récentes, comme les tablettes et les téléphones mobiles.

Lignes directrices sur la sécurité de la TI

Afin d'obtenir des directives sur l'authentification liée aux systèmes de la TI et la prestation de services électroniques, les organisations gouvernementales devraient consulter les lignes directrices suivantes publiées par le Centre de la sécurité des télécommunications du Canada :

- *ITSG-31 - Guide sur l'authentification des utilisateurs pour les systèmes TI*. Cette Ligne directrice décrit les méthodes de conception et de sélection des solutions d'authentification des utilisateurs.
- *ITSG-33 - La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*. Cette Ligne directrice décrit le cadre dans lequel sont exécutées les activités de gestion du risque lié à la sécurité de la TI au niveau des organisations gouvernementales et au niveau des systèmes d'information.

Normes et protocoles à l'appui de la fédération

Plusieurs documents ont été créés pour appuyer la gouvernance de l'authentification électronique et l'octroi de contrats nécessaires. Les organisations gouvernementales sont invitées à consulter ces documents, qu'on peut obtenir en communiquant avec la Direction du dirigeant principal de l'information (voir la section 5.2 de la présente Ligne directrice).

- *Solutions technologiques d'authentification électronique - Architecture et spécifications de l'interface - Version 2.0 : Profil de mise en place*. Ce document décrit le profil de mise en place et l'interface de messagerie requis pour les services d'authentification des justificatifs du gouvernement du Canada. Le profil de mise en place est fondé sur le Profil du gouvernement électronique publié par l'Initiative Kantara et décrit les exigences et contraintes supplémentaires propres au gouvernement du Canada.
- *Fédération de l'identité*. La Direction du dirigeant principal de l'information élabore actuellement des critères pour encadrer la participation officielle à la fédération du gouvernement du Canada. On peut obtenir de plus amples renseignements à ce sujet en communiquant avec la Direction du dirigeant principal de l'information.

Élaboration de normes pancanadiennes

Les organisations gouvernementales sont invitées à se familiariser avec les normes qui favorisent une approche pancanadienne. Des normes pancanadiennes sont actuellement en cours d'élaboration par le Sous-comité sur la gestion de l'identité (SCGI), une entité intergouvernementale qui relève du Conseil des dirigeants principaux de l'information du secteur public (CDPISP) et du Conseil de la prestation des services du secteur public (CPSSP) (les Conseils mixtes). Ces deux conseils sont appuyés par l'Institut des services axés sur les citoyens.

- *Norme pancanadienne sur la validation de l'identité*. Ce document uniformise les demandes et réponses de validation des renseignements sur l'identité et des renseignements personnels échangées par les organisations fédérales, provinciales, territoriales et municipales.

Utilisation et adoption d'autres cadres, normes et lignes directrices

Les organisations gouvernementales sont invitées à utiliser et à adopter d'autres cadres, normes et lignes directrices, s'il y a lieu. L'industrie et le gouvernement ont adopté le modèle d'assurance à quatre niveaux décrit à l'annexe C de la *Norme sur l'assurance de l'identité et des justificatifs*, aussi illustré au tableau 1. Cependant, il existe quelques différences entre ce modèle et les autres cadres, normes et lignes directrices. En utilisant ces ressources connexes, les organisations gouvernementales doivent tenir compte des facteurs suivants :

- **Respect du modèle d'assurance à quatre niveaux.** Malgré certaines variations entre les descriptions et les définitions, le modèle d'assurance à quatre niveaux a été accepté par la collectivité mondiale et il est considéré comme étant normalisé pour toutes les normes et lignes directrices. Les exigences opérationnelles, les normes techniques et les accords doivent tous respecter ce modèle à quatre niveaux.
- **Séparation de l'identité et de l'assurance des justificatifs.** L'approche pancanadienne établit une distinction explicite entre l'identité et l'assurance des justificatifs. D'autres normes ne font pas cette distinction; par conséquent, il peut exister des dépendances entre différentes catégories d'exigences. En appliquant d'autres normes connexes, les organisations gouvernementales doivent vérifier si les exigences s'appliquent à leur contexte particulier.
- **Officialisation d'un processus d'adoption des normes.** Les normes en matière d'identité et les pratiques connexes continuent à évoluer. Les organisations gouvernementales doivent officialiser un processus d'adoption des normes, en tenant compte de leur application spécifique (ou non-application) dans leur contexte.

On notera que le gouvernement du Canada procède actuellement à la formalisation d'un processus d'adoption des cadres de fiabilité qui permettra d'approuver l'utilisation des cadres de fiabilité de l'industrie et du secteur public. On trouvera ci-dessous une liste non exhaustive de cadres, normes et lignes directrices qui peuvent être utilisés :

- *Federal Identity and Credential Access Management* (FICAM) *Trust Framework Provider Adoption Process* (TFPAP) du gouvernement américain. Le processus TFPAP est le mécanisme utilisé par le gouvernement américain pour tirer parti des justificatifs d'identité normalisés par l'industrie que les citoyens possèdent déjà, pour utiliser dans les sites Web du gouvernement.
- *E-Authentication Guidance for Federal Agencies* (OMB M-04-04). Ce document stipule que les organismes doivent réexaminer les transactions électroniques nouvelles et existantes afin de veiller à ce que les processus d'authentification fournissent le niveau d'assurance approprié. Le document établit et décrit quatre niveaux d'assurance de l'identité pour les transactions électroniques nécessitant une authentification.
- *Electronic Authentication Guideline* (NIST SP 800 63-2).Ce document présente des lignes directrices techniques pour les organismes fédéraux américains qui mettent en uvre des systèmes d'authentification électronique. La présente Ligne directrice appuie la mise en uvre de la ligne directrice OMB M-04-04.
- *Technologies de l'information - Techniques de sécurité - Cadre d'assurance de l'authentification d'entité* (ISO/IEC 29115:2013).Ce document présente des directives sur les technologies de contrôle et les processus et activités de gestion connexes. Il établit de plus des critères d'assurance à utiliser pour atténuer les menaces relatives à l'authentification, communiquer les résultats d'une transaction d'authentification et protéger les renseignements personnels identifiables associés au processus d'authentification.
- *Cadre d'assurance des justificatifs d'identité de Kantara.* Ce cadre se compose d'une série de documents décrivant des niveaux d'assurance, un système d'évaluation et des exigences de certification pour les services de confirmation de l'identité, ainsi que des services d'établissement de la robustesse des justificatifs et de gestion des justificatifs.
- *Requirements and Implementation Guidelines for Assertion, Evidence and Verification of Personal Identity* (ANSI/NASPO-IDPV-2014). Ce document est une ébauche de norme American National Standard qui décrit un processus, établit des exigences et fournit des lignes directrices sur l'affirmation, la résolution et la vérification de l'identité des personnes.

Notes en bas de page

Note en bas de page fn1

Pour une définition de l'identité et des autres termes utilisés dans la présente Ligne directrice, voir l'Annexe A.

Renvoi à la référence de la note en bas de page 1

Note en bas de page fn2

La présente Ligne directrice s'applique seulement aux personnes.

Renvoi à la référence de la note en bas de page 2

Note en bas de page fn3

Norme sur l'assurance de l'identité et des justificatifs, annexe A

Renvoi à la référence de la note en bas de page 3

Note en bas de page fn4

Directive sur la gestion de l'identité, paragraphe 3.5.

Renvoi à la référence de la note en bas de page 4

Note en bas de page fn5

D'autres lois applicables comme la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels* exigent des contrôles additionnels.

Renvoi à la référence de la note en bas de page 5

Note en bas de page fn6

Norme sur l'assurance de l'identité et des justificatifs, annexe A

Renvoi à la référence de la note en bas de page 6

Note en bas de page fn7

La validation de l'identité est aussi désignée sous le nom de validation des renseignements sur l'identité. La meilleure référence sur la validation de l'identité est la *Norme pancanadienne sur la validation de l'identité* (non publiée), que l'on peut obtenir en communiquant avec la Division de la gestion de la sécurité et de l'identité de la Direction du dirigeant principal de l'information.

Renvoi à la référence de la note en bas de page 7

Note en bas de page fn8

Norme sur l'assurance de l'identité et des justificatifs, Annexe A.

Renvoi à la référence de la note en bas de page 8

Note en bas de page fn9

La *Norme pancanadienne sur la validation de l'identité* sera publiée dans le site Web de l'Institut des services axés sur les citoyens et dans GCpédia

Renvoi à la référence de la note en bas de page 9