



CAN/DGSI 103-1:2023
NORME NATIONALE DU CANADA

Deuxième édition
2023-04

Confiance et identité numérique – Partie 1 : Notions fondamentales

35.030



- Page laissée intentionnellement vierge -

Table des matières

Introduction.....	ix
1 Portée.....	1
2 Références normatives.....	1
3 Termes et définitions	1
4 Cadre de confiance.....	17
4.1 Notions fondamentales	17
4.2 Gestion de l'identité.....	18
5 Direction	19
5.1 Rôle de la direction de l'organisation	19
6 Planification	19
6.1 Gestion des risques et des mesures d'atténuation.....	19
6.2 Objectifs et planification	20
6.3 Planification de changements	20
7 Soutien	20
7.1 Ressources	20
7.2 Compétences	21
7.3 Connaissances.....	21
7.4 Communication.....	21
7.5 Documentation	22
8 Processus opérationnels.....	23
8.1 Processus de détermination des renseignements sur l'identité.....	23
8.2 Processus de détermination de la preuve d'identité	23
8.3 Processus d'acceptation de la preuve d'identité.....	24
8.4 Processus de validation des renseignements sur l'identité.....	24
8.5 Processus de résolution de l'identité.....	24
8.6 Processus d'établissement de l'identité	25
8.7 Processus de vérification de l'identité.....	25
8.8 Processus de continuité de l'identité.....	25
8.9 Processus de maintien de l'identité.....	25
8.10 Processus d'établissement de liens pour déterminer l'identité	26

8.11	Processus de détermination des renseignements sur la relation	26
8.12	Processus de détermination de la preuve de relation	27
8.13	Processus d'acceptation de la preuve de relation	27
8.14	Processus de validation des renseignements sur la relation	27
8.15	Processus de résolution de la relation	27
8.16	Processus d'établissement de la relation	28
8.17	Processus de vérification de la relation	28
8.18	Processus de continuité de la relation	28
8.19	Processus de maintien de la relation	29
8.20	Processus de suspension de la relation	29
8.21	Processus de rétablissement de la relation	29
8.22	Processus de révocation de la relation	29
8.23	Processus de délivrance d'un justificatif	30
8.24	Processus de liaison justificatif-authentifant	30
8.25	Processus de validation des justificatifs	30
8.26	Processus de vérification des justificatifs	31
8.27	Processus de maintien du justificatif	31
8.28	Processus de suspension d'un justificatif	31
8.29	Processus de recouvrement d'un justificatif suspendu	32
8.30	Processus de révocation d'un justificatif	32
8.31	Processus de formulation de l'avis de consentement	32
8.32	Processus de présentation de l'avis de consentement	33
8.33	Processus de demande de consentement	33
8.34	Processus d'enregistrement du consentement	34
8.35	Processus d'examen du consentement	34
8.36	Processus de renouvellement du consentement	35
8.37	Processus d'expiration du consentement	35
8.38	Processus de révocation du consentement	36
8.39	Processus de création d'une signature	36
8.40	Processus de vérification de la signature	36
Bibliographie		37

- Page laissée intentionnellement vierge -

Avant-propos

L'Institut des normes de gouvernance numérique (INGN) élabore des normes de gouvernance de la technologie numérique adaptées à une utilisation planétaire. L'INGN collabore avec des experts, avec des partenaires au pays et à l'étranger et avec le public pour établir des normes nationales visant à réduire les risques pour la population et les organisations canadiennes qui adoptent et utilisent des technologies novatrices dans l'économie numérique d'aujourd'hui.

Ses normes sont élaborées conformément aux *Exigences et lignes directrices – Accréditation des organismes d'élaboration de normes* (13 juin 2019) du Conseil canadien des normes (CCN).

Soulignons que certains éléments de la présente norme peuvent faire l'objet de droits de brevet. L'INGN ne saurait être tenu responsable de ne pas avoir indiqué ces droits. Les droits de propriété intellectuelle répertoriés lors de l'élaboration de la présente norme figurent dans l'introduction.

Pour en savoir plus sur l'INGN :

Institut des normes de gouvernance numérique

1000, promenade Innovation, bureau 500

Ottawa (Ontario) K2K 3E7

dgc-cgn.org/fr

Les Normes nationales du Canada sont élaborées par les organismes titulaires de l'accréditation du CCN, conformément aux exigences et lignes directrices de ce dernier. On trouvera des renseignements supplémentaires sur les Normes nationales du Canada au www.ccn.ca.

Le CCN est une société d'État qui fait partie du portefeuille d'Innovation, Sciences et Développement économique Canada (ISDE). Pour améliorer la compétitivité économique du Canada et le bien-être collectif de sa population, le CCN dirige et facilite l'élaboration et l'utilisation de normes nationales et internationales. Il coordonne aussi la participation du pays à l'élaboration des normes et définit des stratégies pour promouvoir les efforts de normalisation canadiens.

Le CCN fournit des services d'accréditation à divers clients, dont des organismes de certification de produits, des laboratoires d'essai et des organismes d'élaboration de normes. La liste des programmes du CCN et des organismes accrédités peut être consultée sur le site www.ccn.ca.

- Page laissée intentionnellement vierge -

Introduction

Voici la deuxième version de la norme CAN/DGSI 103-1:2023, Confiance et identité numérique – Partie 1 : Notions fondamentales.

Cette nouvelle mouture est le fruit du savoir et de l'expertise du comité technique 4 (CT 4) de l'INGN sur la confiance et identité numérique, un regroupement de plus de 185 grands penseurs – décideurs, universitaires, chefs de file du secteur, représentants des autorités de réglementation et de la société civile de tout le Canada, etc. Elle a été approuvée par un groupe avec droit de vote formé par le comité technique et réunissant cinq producteurs, trois représentants du secteur public et d'autorités de réglementation, cinq utilisateurs et cinq représentants de la collectivité.

Toutes les unités de mesure utilisées sont exprimées conformément au Système international d'unités (SI).

La norme est soumise à l'examen du comité technique au plus tard un an après sa date de publication, après quoi elle peut être rééditée, révisée, maintenue ou abandonnée.

Bien que son but premier soit énoncé sous la rubrique « Portée », il est important de retenir qu'il incombe à l'utilisateur de juger si elle convient à une application donnée. La norme se veut également applicable indépendamment de la technologie utilisée.

Elle est destinée à des fins d'évaluation de la conformité.

ICS 35.030

THIS NATIONAL STANDARD OF CANADA IS AVAILABLE IN BOTH FRENCH AND ENGLISH.

- Page laissée intentionnellement vierge -

Confiance et identité numérique – Partie 1 : Notions fondamentales

1 Portée

La présente norme fixe les exigences minimales à respecter ainsi qu'un ensemble de mesures de contrôle afin d'établir et d'entretenir la confiance dans les services et systèmes numériques qui, dans le cadre du mandat d'une *organisation*, établissent ou emploient des *identités* ou *justificatifs* en ce qui concerne les données sur les *personnes* ou *organisations*. La norme peut s'appliquer aux services et systèmes numériques qui s'utilisent dans un seul *contexte de l'identité* aussi bien qu'à ceux qui s'utilisent et s'étendent dans plusieurs de ces contextes, par exemple dans une fédération de *justificatifs* ou d'*identités*.

La norme ne *doit* pas avoir pour effet de :

- a. créer un bris de conformité à tout accord ou à toute exigence, obligation, norme ou directive juridiques, réglementaires ou contractuels auxquels l'utilisateur de ladite norme serait autrement assujetti;
- b. privilégier ou imposer une méthode, un processus ou une application technologiques en particulier.

2 Références normatives

Le présent document ne comprend aucune référence normative.

3 Termes et définitions

Pour les besoins du présent document, les termes, expressions et définitions ci-dessous s'appliquent. Les termes définis dans cette section sont en italique dans le corps du texte.

acceptation de la preuve d'identité

Processus qui consiste à confirmer que la *preuve d'identité* (physique ou électronique) présentée est acceptable.

acceptation de la preuve de relation

Processus qui consiste à confirmer que la preuve (physique ou électronique) présentée pour attester une *relation* est acceptable.

affirmation

Déclaration exprimée au moyen d'un ou plusieurs *attributs*. Les *affirmations* sont faites par les *émetteurs*. Voir aussi « Affirmation du sujet » et « Affirmation de la relation ».

affirmation concernant un sujet

Déclaration sur un *sujet*. L'*affirmation concernant un sujet* est exprimée au moyen d'un ou

de plusieurs *attributs d'entité*.

affirmation de relation

Déclaration au sujet d'une association qui existe entre deux *sujets* ou plus. Une *affirmation de relation* est exprimée au moyen d'un ou de plusieurs *attributs de relation*.

attribut d'entité

Propriété ou caractéristique d'*entité*.

attribut d'identité

Propriété ou caractéristique (également appelée « donnée d'identité ») associée à une *entité* identifiable. Les *attributs d'identité* d'une *entité* sont un sous-ensemble des *attributs d'entité* de l'*entité*.

attribut de relation

Propriété ou caractéristique d'une association entre deux *entités* ou plus.

attribut du justificatif

Propriété ou caractéristique d'un *justificatif*.

attribut

Propriété ou caractéristique d'un élément. Voir également « attribut d'entité », « attribut de relation », « attribut d'identification » et « attribut d'identité ».

authentifiant / authentificateur

Quelque chose qu'un *titulaire* contrôle et qui est utilisé pour prouver que ce *titulaire* a conservé le contrôle sur un *justificatif* délivré.

authentification

Voir « vérification des justificatifs » et « vérification de l'identité ».

avis des renseignements sur l'identité

Divulgaration de *renseignements sur l'identité* d'une *entité* par une partie faisant autorité à une partie utilisatrice qui est déclenchée par un *événement fondamental*, un changement des *renseignements d'identité* ou une indication que les *renseignements d'identité* ont été exposés à un facteur de risque (p. ex. décès de la *personne*, abandon de la charte, utilisation de documents expirés, atteinte à la vie privée, utilisation frauduleuse des *renseignements sur l'identité*).

biométrie

Terme général utilisé pour décrire une caractéristique ou un processus. Il peut s'agir d'une caractéristique biologique (anatomique et physiologique) ou comportementale mesurable, qui peut être utile à la reconnaissance automatisée. Elle peut également faire référence à des méthodes automatisées de reconnaissance d'une personne en fonction de

caractéristiques biologiques (anatomiques et physiologiques) et comportementales mesurables.

cadre de confiance

Ensemble de principes, de définitions, de normes, de spécifications, de *critères de conformité* et d'approche d'évaluation convenus.

CANAFE

Centre d'analyse des opérations et déclarations financières du Canada (*CANAFE*). C'est l'unité responsable du renseignement financier au Canada. Son mandat est de faciliter les initiatives de détection, de prévention et de dissuasion du blanchiment d'argent et du financement d'activités terroristes.

charge utile d'un justificatif

Ensemble d'une ou plusieurs *affirmations* faites sur un ou plusieurs *sujets*.

client

Destinataire prévu d'un extrait de service. Les *clients* externes sont généralement des *personnes* (citoyens, résidents permanents, etc.) ou des *organisations* (des secteurs public et privé). Les *clients* internes sont généralement des employés et des entrepreneurs.

CNUDCI

Commission des Nations Unies pour le droit commercial international (*CNUDCI*). Le mandat de la *CNUDCI* est de promouvoir l'harmonisation et l'unification progressives du droit commercial international par le biais de conventions, de lois types et d'autres instruments qui traitent de domaines clés du commerce, du règlement des différends à la passation et à la vente de biens.

confiance dans l'identité (d'une organisation)

Confiance que les *renseignements sur l'identité* de l'*organisation* sont exacts.

confiance dans l'identité (d'une personne)

Confiance que la *personne* est bien celle qu'elle affirme être.

confiance dans la relation

Confiance dans le fait que la ou les *personnes* sont bien celles qu'elles affirment être, dans l'exactitude des *renseignements sur l'identité* de la ou des *organisations*, et dans la *preuve de la relation*.

confiance dans le justificatif

Confiance qu'un *titulaire* exerce un contrôle sur un *justificatif* délivré et que ce *justificatif* est valide.

confiance

Assurance que l'on peut avoir qu'une déclaration est vraie.

confirmation de possession matérielle

Méthode de *vérification de l'identité* qui exige la possession physique ou la présentation d'éléments de preuve (p. ex. *justificatif*) pour prouver que le *sujet* qui présente les *renseignements sur l'identité* contrôle l'*identité*.

confirmation de présentation

Détermination par le *vérificateur* de l'exactitude de la *présentation*.

confirmation des caractéristiques biologiques ou comportementales

Méthode de *vérification de l'identité* qui utilise des caractéristiques biologiques (anatomiques et physiologiques) (p. ex. visage, empreintes digitales, rétines) ou comportementales (p. ex. rythme de frappe au clavier, démarche) pour prouver que le *sujet* qui présente les *renseignements sur l'identité* contrôle l'*identité*.

NOTE : La *confirmation des caractéristiques biologiques ou comportementales* est obtenue au moyen du modèle défi-réponse : les caractéristiques biologiques ou comportementales enregistrées sur un document ou dans un magasin de données sont comparées au *sujet* qui présente les *renseignements sur l'identité*.

confirmation fondée sur les connaissances

Méthode de *vérification de l'identité* qui utilise des *renseignements personnels* ou des secrets partagés pour prouver que le *sujet* qui présente les *renseignements sur l'identité* contrôle bel et bien l'*identité*.

NOTE : La *confirmation fondée sur les connaissances* est obtenue au moyen du modèle défi-réponse : le *sujet* qui présente les *renseignements sur l'identité* se voit poser des questions, réponses que seuls lui et le *vérificateur* doivent connaître (p. ex. renseignements financiers, historique de crédit, secret partagé, clé cryptographique, code d'accès envoyé par la poste, mot de passe, numéro d'identification personnel, *identificateur attribué*).

confirmation par un arbitre de confiance

Méthode de *vérification de l'identité* qui fait intervenir un arbitre de confiance pour prouver que le *sujet* présentant les *renseignements sur l'identité* contrôle l'*identité*. Le type d'arbitre de confiance et son acceptabilité sont déterminés par des critères propres au programme; il peut s'agir d'une caution, d'un notaire, d'un comptable, d'un agent certifié, etc.

contexte de l'identité

Environnement ou ensemble des circonstances dans lesquelles une *organisation* exerce ses activités et dans lesquelles elle offre ses programmes et ses services. Le *contexte de l'identité* est déterminé par des facteurs comme le mandat, la population cible (c'est-à-dire les *clients*, la clientèle), et les autres responsabilités établies en vertu d'une loi ou d'une

entente.

continuité de l'identité

Processus qui consiste à confirmer dynamiquement que le *sujet* a une existence continue dans le temps (c'est-à-dire une « présence authentique »). Ce processus peut être utilisé afin de veiller à ce qu'aucune activité frauduleuse ou malveillante n'est ou n'a été effectuée et de lutter contre la mystification.

continuité de la relation

Processus qui consiste à confirmer dynamiquement qu'une *relation* entre deux *sujets* ou plus a une existence continue dans le temps.

création d'une signature

Processus qui consiste à créer une *signature*.

critères de conformité

Ensemble d'énoncés d'exigences définissant ce qu'il faut pour assurer l'intégrité d'un *processus atomique*.

délivrance d'un justificatif

Processus consistant à créer un *justificatif* à partir d'un ensemble d'*affirmations* sur un ou plusieurs *sujets* et à attribuer le *justificatif* à un *titulaire*.

demande de consentement

Processus qui consiste à demander à une *personne* si elle consent ou ne consent pas – selon la forme de l'énoncé d'avis présenté – à quelque chose, ce qui entraîne une décision d'affirmation (« oui ») ou de refus (« non ») de consentement.

dénomination sociale

Voir « nom fondamental » et « nom principal ».

détermination de la preuve d'identité

Processus de détermination de la *preuve d'identité* acceptable (matérielle ou électronique).

détermination de la preuve de relation

Processus visant à déterminer ce qu'est la preuve (physique ou électronique) acceptable d'une *relation*.

détermination des renseignements sur l'identité

Processus qui consiste à déterminer le *contexte de l'identité*, les exigences en matière de *renseignements sur l'identité* et l'*identificateur*.

détermination des renseignements sur la relation

Processus de détermination du contexte de la *relation*, des exigences en matière de *renseignements sur la relation* et de *l'identificateur de relation*.

devrait/devraient

Indique une recommandation.

doit/doivent

Indique une exigence.

écosystème numérique

Ensemble d'outils et de systèmes variés, et les acteurs qui les créent, qui interagissent avec eux, qui les utilisent et qui les refont.

eIDAS

Règlement sur l'identification électronique et les services de confiance pour les opérations électroniques (eIDAS). C'est un règlement de l'Union européenne qui supervise les services d'identification électronique et de confiance pour les transactions électroniques dans le marché intérieur de l'Union européenne. Il régit les signatures électroniques, les transactions électroniques, les organismes concernés et leurs processus d'intégration afin de fournir aux utilisateurs un moyen sécuritaire de faire des affaires en ligne, comme le transfert de fonds électroniques ou les transactions avec les services publics.

élément de donnée d'identité

Voir « attribut d'identité ».

émetteur

Entité qui présente une ou plusieurs *affirmations* sur un ou plusieurs *sujets*, crée un *justificatif* à partir de ces *affirmations* et attribue le *justificatif* à un *titulaire*.

enregistrement des justificatifs

Déclaration de *l'émetteur* selon laquelle *l'émetteur* délivre un type de *justificatif*. La déclaration peut comprendre une définition du format des *justificatifs*.

enregistrement du consentement

Processus qui consiste à stocker de manière persistante et sécurisée un énoncé d'avis et la décision de consentement connexe de la *personne*. Peuvent aussi être consignés les *renseignements sur l'identité* de la personne, la version de l'avis de consentement qui lui a été présentée, la date et l'heure auxquelles l'avis de consentement a été présenté et, le cas échéant, la date d'expiration ou de révocation de la décision de consentement. Une fois les renseignements relatifs au consentement stockés, une notification sur la décision de consentement est envoyée aux parties concernées.

entité

Existence distincte et indépendante, comme une *personne* ou une *organisation*, qui peut être assujettie à des lois, des politiques ou des règlements dans un contexte, et qui peut avoir certains droits, devoirs et obligations. Une entité peut remplir un ou plusieurs des quatre rôles (c'est-à-dire *sujet*, *émetteur*, *titulaire* ou *vérificateur*) dans l'*écosystème numérique*.

entité atomique

Entité qui ne peut pas être décomposée en unités plus petites. Les personnes sont des *entités atomiques*. Voir également « entité composée ».

entité composée

Entité qui comprend une ou plusieurs *entités atomiques* et/ou une ou plusieurs *entités composées* subordonnées. Les *organisations* sont des *entités composées*. Voir également « entité atomique ».

établissement de l'identité

Processus consistant à créer le dossier d'*identité* d'un *sujet* au sein d'une population.

établissement de la relation

Processus de consignation de l'existence d'une *relation* entre deux *sujets* ou plus.

établissement de liens pour déterminer l'identité

Processus de mise en correspondance entre un ou des *identificateurs attribués* et un *sujet* donné.

événement fondamental

Épisodes distincts importants qui se produisent dans la vie d'une *personne* ou d'une *organisation*. En vertu de la loi, un *événement fondamental* doit être enregistré auprès d'une entité gouvernementale et est assujéti à la législation et à la réglementation. Exemples d'*événements fondamentaux* du côté des *personnes* : naissance ou mortinaissance, adoption, légitimation, reconnaissance de la parentalité, immigration, obtention du droit de résidence légale, citoyenneté naturalisée, changement de nom, mariage ou annulation du mariage, séparation légale, divorce, mort. Exemples d'*événements fondamentaux* du côté des *organisations* : enregistrement de la charte, fusion, regroupement, abandon de charte, dissolution.

examen du consentement

Processus qui consiste à rendre visibles pour la *personne* qui a donné le consentement les détails d'une décision de consentement enregistrée.

expiration du consentement

Processus qui consiste à suspendre la validité d'une décision (d'affirmation) de consentement en raison du dépassement de la date ou heure d'expiration.

formulation de l'avis de consentement

Processus consistant à produire un énoncé d'avis de consentement décrivant les *renseignements personnels* qui sont recueillis ou qui peuvent l'être; les parties auxquelles les *renseignements personnels* sont transmis (connues au moment de la présentation); les fins auxquelles les *renseignements personnels* sont recueillis, utilisés ou divulgués; le risque de préjudice et d'autres conséquences de la collecte, de l'utilisation ou de la divulgation; la façon dont les *renseignements personnels* seront traités et protégés; la période d'application de l'avis de consentement; la *personne* ou l'*entité* ayant compétence ou autorité pour l'énoncé d'avis de consentement émis, et quelles sont les modalités de révocation de tout consentement donné, en tout ou en partie, en vertu de l'avis. Ce processus devrait être effectué conformément à toute exigence de la législation et de la réglementation applicables.

GAFI

Groupe d'action financière sur le blanchiment de capitaux (GAFI). C'est l'organisme mondial de surveillance du blanchiment d'argent et du financement du terrorisme. Cet organe intergouvernemental établit des normes internationales visant à prévenir ces activités illégales et les dommages qu'elles causent à la société. En tant qu'organe d'élaboration des politiques, le GAFI s'efforce de susciter la volonté politique nécessaire pour apporter des réformes législatives et réglementaires nationales dans ces domaines.

genre

Identité sociale, comme le fait d'être un homme, une femme, une personne non binaire ou une personne bispirituelle.

gestion de l'identité

Ensemble de principes, de pratiques, de processus et de procédures utilisés pour réaliser le mandat d'une *organisation* et ses objectifs liés à l'*identité*.

identificateur attribué

Chaîne numérique ou alphanumérique automatiquement générée et permettant de faire la distinction entre des *entités* d'une population sans recourir à un autre *attribut d'identité*.

identificateur de relation

Ensemble d'*identificateurs* des *entités* dans la *relation* et de l'*attribut de relation* « type de relation ».

Identificateur

Ensemble d'*attributs d'identité* utilisés pour distinguer uniquement une *entité* particulière au sein d'une population.

identité contextuelle

Identité qui est utilisée à des fins particulières dans un *contexte de l'identité* spécifique.

NOTE : Cette fin peut être la prestation de services bancaires ou de soins de santé; l'octroi d'un permis d'affaires ou d'un permis de conduire; l'utilisation de médias sociaux; etc. Selon le contexte identitaire, une *identité contextuelle* peut être liée à une *identité principale* (p. ex. un permis de conduire) ou ne pas être liée à une *identité principale* (p. ex. un profil de médias sociaux). Voir aussi « preuve d'identité principale ».

identité numérique

Représentation électronique d'une *entité* qui est exclusive à ladite *entité*.

identité principale

Identité qui a été établie ou modifiée à la suite d'un *événement fondamental* (p. ex. naissance, changement de nom légal de la *personne*, immigration, résidence légale, citoyenneté, décès, enregistrement de la dénomination sociale de l'*organisation*, changement de nom légal de l'*organisation*, faillite). Voir aussi « identité contextuelle ».

identité

Référence ou désignation unique utilisée pour distinguer une *entité* en particulier au sein d'une population. Il y a deux catégories d'identité : principale et contextuelle. Voir « identité principale » et « identité contextuelle ».

justificatif

Affirmation d'identité, de qualification, de compétence, d'autorité, de droits, de privilèges, d'autorisations, d'état, d'admissibilité ou de propriété d'actifs (ou une combinaison de ces éléments). Un *justificatif* contient un ensemble d'une ou plusieurs *affirmations* faites sur un ou plusieurs *sujets*.

liaison justificatif-authentifiant

Processus qui consiste à associer un *justificatif* délivré à un *titulaire* avec un ou plusieurs *authentifiants*. Ce processus comprend également des activités liées au cycle de vie de l'*authentifiant*, telles que la suspension des *authentifiants* (en cas d'oubli de mot de passe ou de verrouillage en raison d'échecs successifs de la *vérification des justificatifs*, d'inactivité ou d'activité suspecte), la suppression d'*authentifiants*, la liaison d'autres *authentifiants* et la mise à jour d'*authentifiants* (p. ex. changement de mot de passe, mise à jour des questions et réponses de sécurité, nouvelle photo faciale).

maintien de l'identité

Processus qui consiste à veiller à ce que les *renseignements sur l'identité* d'un *sujet* soient exacts, complets et à jour.

maintien de la relation

Processus qui consiste à veiller à ce que les *renseignements sur la relation* entre deux *sujets* ou plus soient exacts, complets et à jour.

maintien du justificatif

Processus consistant à mettre à jour les *attributs* (p. ex. date d'expiration, état) d'un *justificatif* délivré.

mandataire

Entité qui agit pour le compte d'une autre *entité*.

métadonnées du justificatif

Un ou plusieurs *attributs* qui décrivent les propriétés ou les caractéristiques d'un *justificatif*.

méthodes

Ensembles de règles qui régissent la façon dont les acteurs de l'*écosystème numérique* interagissent directement ou indirectement entre eux. Les méthodes englobent des éléments comme les modèles et schémas de données, les protocoles de communication, les mécanismes de transmission, les algorithmes cryptographiques, les bases de données, les registres distribués, les registres de données vérifiables et les systèmes similaires et les combinaisons de celles-ci.

modèle d'identité

Représentation simplifiée (ou abstraite) d'une méthodologie de *gestion de l'identité* (également appelée *schéma d'identité*).

NOTE : Les *modèles d'identité* centralisés, fédérés et décentralisés en sont des exemples.

NIST

National Institute of Standards and Technology (*NIST*). C'est un organisme fédéral sans vocation réglementaire qui relève du département du Commerce des États-Unis. Sa mission est de promouvoir l'innovation et la compétitivité industrielle aux États-Unis par l'avancement des sciences, normes et technologies de la mesure.

niveau de confiance dans l'identité (d'une organisation)

Niveau de confiance que les *renseignements sur l'identité* de l'*organisation* sont exacts.

niveau de confiance dans l'identité (d'une personne)

Niveau de confiance que la *personne* est bien celle qu'elle affirme être.

niveau de confiance dans la relation

Niveau de confiance dans le fait que la ou les *personnes* sont bien celles qu'elles affirment être, dans l'exactitude des *renseignements sur l'identité* de la ou des *organisations*, et dans la *preuve de la relation*.

niveau de confiance dans le justificatif

Niveau de confiance qu'un *titulaire* a maintenu le contrôle d'un *justificatif* délivré et que ce *justificatif* est valide.

niveau de confiance

Niveau d'assurance qu'une déclaration est vraie et sur laquelle d'autres peuvent se fier.

nom de préférence

Nom qu'une *personne* préfère qu'on emploie informellement avec elle.

nom fondamental

Nom d'une *entité* tel qu'il est indiqué dans un dossier officiel identifiant l'*entité* (p. ex. dossier de statistiques d'état civil provincial ou territorial; dossier d'immigration fédéral; dossiers du registre fédéral, provincial ou territorial des sociétés).

nom principal

Nom utilisé par une *entité* à des fins officielles et légales (également appelé « nom légal »). Voir aussi « nom fondamental ».

organisation

Entité juridique qui n'est pas un être humain (appelée en droit « personne morale »).

personne

Être humain (appelé en droit « personne physique »), ce qui inclut les « mineurs » et autres individus qui pourraient ne peuvent être considérés comme des *personnes* aux yeux de la loi.

présence légale

Droit d'être ou de résider légalement au Canada.

présentation de l'avis de consentement

Processus de présentation d'un avis de consentement à une *personne*.

présentation

Renseignements dérivés d'un ou de plusieurs *justificatifs*. Ces *justificatifs* sources peuvent avoir été délivrés par différents *émetteurs*.

preuve d'identité contextuelle (d'une organisation)

Preuve d'identité qui corrobore la *preuve d'identité principale* et aide à lier les *renseignements sur l'identité* à une *organisation*. Elle peut également fournir des renseignements supplémentaires comme l'activité sur les marchés, une signature ou une adresse. Par exemple, les registres des permis d'exploitation forestière ou minière ou de culture du cannabis et les enregistrements de statut d'organisme de bienfaisance.

preuve d'identité contextuelle (d'une personne)

Preuve d'identité qui corrobore la *preuve d'identité principale* et aide à lier les *renseignements sur l'identité* à une *personne*. Elle peut aussi offrir des renseignements

supplémentaires comme une photo, une signature ou une adresse. Par exemple, les dossiers d'assurance sociale; les dossiers sur le droit de voyager, de conduire ou d'obtenir des services de santé; les dossiers de mariage, de changement de nom ou de décès provenant d'une autorité compétente.

preuve d'identité principale (d'une *organisation*)

Preuve d'identité établissant les principaux *renseignements sur l'identité* d'une *organisation*, comme le nom légal, la date de l'événement, l'adresse, le statut et la personne-ressource principale. Par exemple, les dossiers d'enregistrement, les certificats de conformité et les dossiers de constitution en société d'une autorité compétente.

preuve d'identité principale (d'une *personne*)

Preuve d'identité établissant les principaux *renseignements sur l'identité* d'une *personne*, comme le(s) prénom(s), le nom de famille et la date et le lieu de naissance. Par exemple, les dossiers de naissance, d'immigration ou de citoyenneté provenant d'une autorité compétente.

preuve d'identité

Registre d'une *source faisant autorité* indiquant l'*identité* d'une *entité*. Il existe deux catégories de *preuves d'identité* : *preuve d'identité principale* et *preuve d'identité contextuelle*. Voir « preuve d'identité principale » et « preuve d'identité contextuelle ».

preuves des justificatifs

Une ou plusieurs méthodes ou mécanismes utilisés pour vérifier que l'*émetteur* est l'auteur du *justificatif* et que le *justificatif* n'a pas été altéré et est associé à un *titulaire*.

preuves électroniques ou numériques

Toute donnée enregistrée ou préservée sur n'importe quel support, par un système informatique ou tout autre appareil semblable. Exemples : enregistrements dans une base de données, journaux d'audit ou documents produits au moyen d'un logiciel de traitement de texte.

processus atomique

Ensemble d'activités logiquement mis en correspondance qui entraîne l'état de transition d'un objet. D'autres processus atomiques peuvent se fier à l'état de sortie de l'objet.

processus composé

Ensemble de *processus atomiques* et/ou d'autres *processus composés* qui entraînent un ensemble de transitions d'état.

recouvrement d'un justificatif

Processus qui consiste à transformer un *justificatif* suspendu en *justificatif* utilisable à nouveau (c'est-à-dire un *justificatif* délivré).

recupération des renseignements sur l'identité

Divulgence de *renseignements sur l'identité* d'une *entité* par une partie faisant autorité à une partie utilisatrice qui est déclenchée par une demande de la partie utilisatrice.

registre fondamental (d'organisations)

Registre qui conserve les dossiers permanents des *organisations* qui ont été créées et enregistrées au Canada. Il y a 14 registres de ce genre au Canada (les 13 registres provinciaux et territoriaux des entreprises et Corporations Canada [fédéral]).

registre fondamental (de personnes)

Registre qui conserve des dossiers permanents des *personnes* nées au Canada, de *personnes* nées à l'étranger d'un parent canadien ou de ressortissants étrangers ayant présenté une demande pour entrer au Canada. Il y a 14 registres de ce genre au Canada (les 13 registres provinciaux et territoriaux des bureaux de l'état civil et Immigration, Réfugiés et Citoyenneté Canada [fédéral]).

relation de mandataire

Cas particulier d'une *relation équilibrée* où les *entités* sont égales, mais où une *entité* (le mandant) nomme une autre *entité* (le *mandataire*) pour agir en son nom à une fin déterminée (p. ex. procuration, société comptable produisant des déclarations pour une société). Voir aussi « relation », « relation équilibrée » et « relation dirigée ».

relation dirigée

Relation dans laquelle les *entités* ne sont pas égales (p. ex. parent et enfant, société mère et filiale, gestionnaire et subordonné). Voir aussi « relation », « relation de mandataire » et « relation équilibrée ».

relation équilibrée

Relation dans laquelle les *entités* sont égales (p. ex. époux dans un mariage, partenaires dans une entreprise, sociétés dans une coentreprise). Voir aussi « relation », « relation de mandataire » et « relation dirigée ».

relation numérique

Représentation électronique d'une association entre deux *entités* ou plus.

relation

Association entre deux *entités* ou plus. Voir aussi « relation de mandataire », « relation équilibrée » et « relation dirigée ».

renouvellement du consentement

Processus qui consiste à prolonger la période de validité d'une décision d'affirmation de consentement en reportant la date d'expiration.

renseignements organisationnels

Renseignements sur une *organisation* identifiable.

renseignements personnels

Renseignements sur une *personne* identifiable.

renseignements sur l'entité

Renseignements sur une *entité* identifiable.

renseignements sur l'identité

Voir « identificateur ».

renseignements sur la relation

Ensemble d'*attributs de relation* qui décrit l'association entre deux *entités* ou plus.

représentation numérique

Représentation électronique d'une *entité* ou d'une association entre deux *entités* ou plus.

résolution de l'identité

Processus établissant l'unicité d'un *sujet* à l'intérieur de la population au moyen de *renseignements sur l'identité*.

résolution de la relation

Processus qui consiste à établir le caractère unique d'une instance de *relation* au sein d'une population par l'utilisation de *renseignements sur la relation* et de *renseignements sur l'identité*.

rétablissement de la relation

Processus par lequel on fait passer une *relation* suspendue à l'état actif.

révocation d'un justificatif

Processus permettant de garantir qu'un *justificatif* délivré est en permanence marqué comme inutilisable.

révocation de la relation

Processus qui consiste à signaler qu'un dossier de *relation* n'est plus en vigueur.

révocation du consentement

Processus qui consiste à suspendre la validité d'une décision d'affirmation de consentement à la suite du retrait explicite du consentement par la *personne* (c'est-à-dire qu'une

affirmation de consentement est convertie en refus de consentement).

schéma d'identité

Voir « modèle d'identité ».

sexe

Caractéristiques biologiques, comme le fait d'être de sexe masculin ou féminin, ou encore d'être intersexué.

signature

Représentation électronique dans laquelle, à tout le moins, la *personne* qui signe les données peut être associée aux représentations électroniques, il est clair que la *personne* avait l'intention de signer, la raison ou le but de la *signature* est communiqué et l'intégrité des données de la transaction signée est maintenue, y compris l'original.

source faisant autorité

Ensemble de dossiers conservés par une autorité qui respecte les critères établis.

sujet

Entité visée par des *affirmations* avancées par un *émetteur*.

suspension d'un justificatif

Processus qui consiste à transformer un *justificatif* délivré en un *justificatif* suspendu en marquant ce *justificatif* comme temporairement inutilisable.

suspension de la relation

Processus qui consiste à signaler qu'un dossier de *relation* n'est temporairement plus en vigueur.

titulaire

Entité qui contrôle un ou plusieurs *justificatifs* à partir desquels une *présentation* peut être exprimée à un *vérificateur*. Un *titulaire* est habituellement, mais pas toujours, le *sujet* d'un *justificatif*.

NOTE : Si le *titulaire* n'est pas le *sujet* d'un *justificatif*, alors le *titulaire* doit avoir le statut juridique nécessaire pour pouvoir représenter ce *sujet* (p. ex. tuteur légal, avocat).

utilisateur

Voir « titulaire ».

validation des justificatifs

Processus qui consiste à confirmer la validité du *justificatif* délivré (p. ex. non violé, corrompu, modifié, suspendu ou révoqué). La validité du *justificatif* délivré peut servir à établir un certain niveau de confiance.

validation des renseignements sur l'identité

Processus qui consiste à confirmer l'exactitude des *renseignements sur l'identité* d'un *sujet* comme établis par l'*émetteur*.

validation des renseignements sur la relation

Processus de confirmation de l'exactitude des *renseignements sur une relation* entre deux *sujets* ou plus, tel qu'il est établi par l'*émetteur*.

vérificateur

Entité qui accepte une *présentation* de la part d'un *titulaire* aux fins de prestation de services ou d'administration de programmes.

vérification de l'identité

Processus qui consiste à confirmer que les *renseignements sur l'identité* se trouvent sous le contrôle du *sujet*.

vérification de la relation

Processus de confirmation que les *renseignements sur la relation* se trouvent sous le contrôle du *sujet*.

vérification de la signature

Processus qui consiste à confirmer que la *signature* est valide.

vérification des justificatifs

Processus qui consiste à confirmer qu'un *titulaire* exerce un contrôle sur un *justificatif* délivré. Le contrôle d'un *justificatif* délivré est vérifié par un ou plusieurs *authentifiants*. Le degré de contrôle sur le *justificatif* délivré peut servir à établir un certain niveau de confiance.

4 Cadre de confiance

4.1 Notions fondamentales

4.1.1 Généralités

4.1.1.1 Quand une *organisation* délivre ou utilise une *identité* ou des *justificatifs* dans le cadre d'un *contexte de l'identité*, y compris dans le cadre d'une fédération, elle *doit* fixer et appliquer des critères pour créer le *cadre de confiance*¹ qui régira le fonctionnement de son système de *gestion de l'identité* ainsi que les droits et obligations des participants de la fédération, de manière à assurer la fiabilité de son propre système et de ceux des participants de la fédération. L'*organisation doit* tenir compte de ce qui suit lorsqu'elle formule les critères pour son *cadre de confiance* :

- a. Son contexte organisationnel, dont ses obligations contractuelles et sa position de risque;
- b. Son secteur d'activité, avec ses politiques et règles d'application générales;
- c. Les lois, règlements et politiques applicables;
- d. Les normes applicables, dont la présente norme.

NOTE : Un *cadre de confiance* est un ensemble de règles, de politiques et de lignes directrices qui facilitent l'établissement et le maintien d'un lien de confiance entre différentes *entités* dans un domaine en particulier. Dans le cadre de la gestion d'*identités numériques*, il peut s'agir d'un accord volontaire ou d'un document ayant force exécutoire définissant les modalités convenues, comme des *niveaux de confiance*, les *critères de conformité* et l'approche d'évaluation. Voici des exemples de *cadres de confiance* : le profil du secteur public du Cadre de confiance pancanadien (CCP), l'UK Digital Identity and Attributes Trust Framework du Royaume-Uni, et le règlement sur l'identification électronique et les services de confiance pour les opérations électroniques (*eIDAS*) de l'Union européenne.

4.1.1.2 L'*organisation doit* accepter des *identités* ou des *justificatifs* par l'intermédiaire d'un *cadre de confiance* approuvé au lieu de passer par un service ou la fourniture d'une ressource en personne, à la condition de vérifier ce qui suit :

- a. L'*identité* et les renseignements propres au service ou à la ressource, à savoir, vérifier s'il est nécessaire ou pertinent de demander des *preuves d'identité principale* ou *contextuelle* pour identifier une *entité* (voir l'article 8.2.1.1), et quels autres *renseignements sur l'entité* sont nécessaires à l'offre d'un service ou d'une ressource;
- b. Les *niveaux de confiance dans l'identité* et du *justificatif* figurant à l'annexe B;
- c. L'enregistrement de l'*identité*, à savoir, vérifier si l'*identité*, l'*organisation*

- et les *renseignements personnels* ont bien été associés à un *justificatif* délivré à une *organisation* ou à une *personne* et si le tout est exact;
- d. Les avis et consentements, à savoir, vérifier si le contenu de l'avis donné ainsi que la collecte, l'utilisation et la divulgation des *renseignements personnels* obtenus concordent bien avec la nature et la durée du consentement accordé.

4.2 Gestion de l'identité

4.2.1 Généralités

- 4.2.1.1 En l'absence de prescriptions légales, l'*organisation doit* choisir des *attributs d'identité* servant à distinguer une *identité* unique qui répondent à ses besoins et exigences tout en équilibrant le risque, la flexibilité et l'inclusivité.
- 4.2.1.2 L'*organisation doit* évaluer les risques associés à la *vérification de l'identité* et des *justificatifs* en étudiant les répercussions potentielles sur une *personne*, une activité, un service, une transaction ou un secteur donnés.
- 4.2.1.3 L'*organisation doit*, en ce qui concerne les processus liés à l'*identité* et aux *justificatifs*, appliquer les *niveaux de confiance dans l'identité* et du *justificatif* requis et les mesures de contrôle connexes.
- 4.2.1.4 L'*organisation doit* surveiller ses systèmes et ses processus de *gestion de l'identité* pour en garantir la confidentialité, l'intégrité et la continuité, et évaluer dans la même optique le *cadre de confiance* de sa fédération.
- 4.2.1.5 Sur demande, l'*organisation doit* fournir les politiques applicables rapidement, en respectant les critères.

5 Direction

5.1 Rôle de la direction de l'organisation

5.1.1 Généralités

5.1.1.1 La haute direction *doit* montrer le souci qu'elle accorde aux systèmes et services d'*identité numérique* de l'organisation :

- a. en se dotant, pour ces systèmes et services, de politiques et d'objectifs qui sont harmonisés à son orientation stratégique;
- b. en véhiculant l'importance de la sécurité et de l'efficacité des systèmes et services d'*identité numérique* et en assurant la disponibilité des ressources essentielles à ces systèmes et services;
- c. en assurant la conformité des systèmes et services d'*identité numérique* aux exigences des politiques, objectifs et programmes de cybersécurité;
- d. en mettant en place des indicateurs pour les systèmes et services d'*identité numérique*, et en faisant un suivi des progrès et de l'efficacité;
- e. en aidant les autres gestionnaires concernés à faire preuve de leadership dans leurs domaines de responsabilité.

6 Planification

6.1 Gestion des risques et des mesures d'atténuation

6.1.1 Généralités

6.1.1.1 Lorsqu'elle planifie ses systèmes et services d'*identité numérique*, l'organisation *doit* tenir compte des exigences et des enjeux mentionnés à l'article 4, et déterminer les risques et les mesures d'atténuation qu'il faut gérer pour :

- garantir que les systèmes et services peuvent produire les résultats escomptés;
- prévenir ou réduire le plus possible les effets indésirables;
- assurer une amélioration continue;
- évaluer les risques conformément aux pratiques de gestion du risque généralement reconnues et consigner les résultats.

6.1.1.2 L'organisation *doit* planifier :

- a) les actions à poser pour gérer ces risques et ces mesures d'atténuation;
- b) la manière dont elle :
 - intégrera et appliquera ces actions aux processus associés aux systèmes et services d'*identité numérique*;
 - évaluera l'efficacité de ces actions.

6.2 Objectifs et planification

6.2.1 Généralités

6.2.1.1 *L'organisation doit* déterminer les objectifs de ses systèmes et services d'*identité numérique*.

6.2.1.2 Ces objectifs *doivent* :

- a. cadrer avec les politiques existantes;
- b. être mesurables (dans la mesure du possible);
- c. tenir compte des exigences applicables;
- d. faire l'objet d'un suivi;
- e. être communiqués;
- f. être mis à jour au besoin;
- g. être disponibles à l'écrit.

6.2.1.3 Lorsqu'elle planifie comment réaliser ces objectifs, *l'organisation doit* déterminer :

- les mesures à prendre;
- les ressources requises;
- les responsables des mesures;
- l'échéancier;
- la méthode d'évaluation des résultats.

6.3 Planification de changements

6.3.1 Généralités

6.3.1.1 Quand *l'organisation* détermine qu'il faut changer ses systèmes et services d'*identité numérique*, elle *doit* réaliser les changements de manière planifiée.

7 Soutien

7.1 Ressources

7.1.1 Généralités

7.1.1.1 *L'organisation doit* déterminer les ressources nécessaires à l'établissement, à la mise en œuvre, à la maintenance et à l'amélioration continue des systèmes et services d'*identité numérique*.

7.2 Compétences

7.2.1 Généralités

- 7.2.1.1 *L'organisation doit* déterminer les compétences que doivent avoir les personnes exécutant les tâches touchant au fonctionnement des systèmes et services d'*identité numérique*.
- 7.2.1.2 *L'organisation doit* s'assurer que les compétences envisagées à l'article 7.2.1.1 se fondent sur une éducation, une formation et une expérience appropriées.
- 7.2.1.3 *L'organisation doit*, s'il y a lieu, prendre des mesures pour obtenir les compétences nécessaires, et évaluer l'efficacité de ces mesures.

7.3 Connaissances

7.3.1 Généralités

- 7.3.1.1 Pour que la mise en œuvre respecte les objectifs énoncés à l'article 8, *l'organisation doit* s'assurer que les *personnes* exécutant des tâches liées aux systèmes et services d'*identité numérique* connaissent :
- les mesures de contrôle manuelles et automatisées;
 - les politiques et procédures à suivre;
 - les implications du non-respect des exigences du présent document, surtout pour les sujets des systèmes et services d'*identité numérique*.

7.4 Communication

7.4.1 Généralités

- 7.4.1.1 *L'organisation doit* déterminer quelles communications internes et externes doivent être transmises dans la mise en œuvre des systèmes et services d'*identité numérique*, et établir notamment :
- l'objet de ces communications;
 - le moment où elles doivent avoir lieu;
 - les interlocuteurs;
 - les modes de communication.

7.5 Documentation

7.5.1 Généralités

- 7.5.1.1 La documentation sur les systèmes et services d'*identité numérique* de l'*organisation* doit présenter l'information qu'exige le présent document.
- 7.5.1.2 La documentation sur les systèmes et services d'*identité numérique* de l'*organisation* doit comprendre l'information que l'*organisation* juge nécessaire pour assurer l'efficacité de ces systèmes et services.

7.5.2 Création et mise à jour de la documentation

- 7.5.2.1 La documentation préparée et mise à jour sur les systèmes et services d'*identité numérique* de l'*organisation* doit être bien identifiée (p. ex. titre, date, auteur, numéro de référence).
- 7.5.2.2 L'adéquation de la documentation préparée et mise à jour concernant les systèmes et services d'*identité numérique* de l'*organisation* doit faire l'objet d'un examen et d'une approbation en bonne et due forme.

7.5.3 Gestion de la documentation

- 7.5.3.1 L'*organisation* doit gérer sa documentation sur les systèmes et services d'*identité numérique* pour que celle-ci puisse être utilisée là où elle est requise.
- 7.5.3.2 L'*organisation* doit gérer sa documentation sur les systèmes et services d'*identité numérique* de manière à bien la protéger (p. ex. contre un bris de confidentialité, une mauvaise utilisation ou une atteinte à son intégrité).
- 7.5.3.3 L'*organisation* doit gérer la documentation sur les systèmes et services d'*identité numérique* en encadrant les activités suivantes :
- Distribution, accès, récupération et utilisation;
 - Stockage et préservation, y compris le maintien de la lisibilité;
 - Gestion des changements (p. ex. versions);
 - Conservation et élimination.

- 7.5.3.4 Si la documentation sur les systèmes et services d'*identité numérique* de l'*organisation* est d'origine externe, cette origine *doit* être indiquée, et la documentation faire l'objet d'un contrôle.

7.5.4 Documentation sur les systèmes et services d'*identité numérique*

- 7.5.4.1 L'*organisation doit* créer, mettre à jour et gérer la documentation sur la portée des systèmes et services d'*identité numérique* pour évaluer la conformité aux présentes.
- 7.5.4.2 L'*organisation doit* créer, mettre à jour et gérer la documentation sur les systèmes et services d'*identité numérique* de manière à réaliser les objectifs du programme.

NOTE : Par exemple, l'*organisation* a créé, mis à jour et géré la documentation sur les critères pour un *cadre de confiance* qu'exige l'article **Error! Reference source not found.** de la présente norme.

- 7.5.4.3 L'*organisation doit* créer, mettre à jour et gérer la documentation sur les mesures de contrôle nécessaires à l'obtention des résultats énoncés à l'article 8 ainsi qu'à l'évaluation de l'efficacité des systèmes et services d'*identité numérique*.

8 Processus opérationnels

8.1 Processus de détermination des renseignements sur l'identité

8.1.1 But

- 8.1.1.1 Le processus de *détermination des renseignements sur l'identité* vise à déterminer le *contexte de l'identité*, les exigences en matière de *renseignements sur l'identité* et l'*identificateur*.

8.1.2 Résultats

- 8.1.2.1 À l'issue du processus de *détermination des renseignements sur l'identité*, le *contexte de l'identité*, les exigences en matière de *renseignements sur l'identité* et l'*identificateur* sont établis.

8.2 Processus de détermination de la preuve d'identité

8.2.1 But

- 8.2.1.1 Le processus de *détermination de la preuve d'identité* vise à déterminer ce qui

constitue une *preuve d'identité* (physique ou électronique) acceptable.

8.2.2 Résultats

8.2.2.1 À l'issue du processus de *détermination de la preuve d'identité*, il est déterminé ce qui constitue une *preuve d'identité* acceptable.

8.3 Processus d'acceptation de la preuve d'identité

8.3.1 But

8.3.1.1 Le processus d'*acceptation de la preuve d'identité* vise à confirmer que la *preuve d'identité* (physique ou électronique) présentée est acceptable.

8.3.2 Résultats

8.3.2.1 À l'issue du processus d'*acceptation de la preuve d'identité*, il est confirmé que la *preuve d'identité* est acceptable.

8.4 Processus de validation des renseignements sur l'identité

8.4.1 But

8.4.1.1 Le processus de *validation des renseignements sur l'identité* vise à confirmer l'exactitude des *renseignements sur l'identité* d'un *sujet* comme établis par l'*émetteur*.

8.4.2 Résultats

8.4.2.1 À l'issue du processus de *validation des renseignements sur l'identité*, l'exactitude des *renseignements sur l'identité* est validée auprès de l'*émetteur*.

8.5 Processus de résolution de l'identité

8.5.1 But

8.5.1.1 Le processus de *résolution de l'identité* vise à établir l'unicité d'un *sujet* à l'intérieur de la population.

8.5.2 Résultats

8.5.2.1 À l'issue du processus de *résolution de l'identité*, il est établi que les *renseignements sur l'identité* sont propres à un seul *sujet* dans une population.

8.6 Processus d'établissement de l'identité

8.6.1 But

8.6.1.1 Le processus d'*établissement de l'identité* vise à créer le dossier d'*identité* d'un *sujet* au sein d'une population.

8.6.2 Résultats

8.6.2.1 À l'issue du processus d'*établissement de l'identité*, il existe un dossier d'*identité* propre au *sujet*.

8.7 Processus de vérification de l'identité

8.7.1 But

8.7.1.1 Le processus de *vérification de l'identité* vise à confirmer que les *renseignements sur l'identité* se trouvent sous le contrôle du *sujet*.

8.7.2 Résultats

8.7.2.1 À l'issue du processus de *vérification de l'identité*, il est confirmé que le *sujet* a le contrôle des *renseignements sur l'identité*.

8.8 Processus de continuité de l'identité

8.8.1 But

8.8.1.1 Le processus de *continuité de l'identité* vise à confirmer que le *sujet* a une existence continue durant un cycle de vie défini (c'est-à-dire une « présence authentique »).

NOTE : Ce processus peut être utilisé afin de veiller à ce qu'aucune activité frauduleuse ou malveillante n'est ou n'a été effectuée et de lutter contre la mystification.

8.8.2 Résultats

8.8.2.1 À l'issue du processus de *continuité de l'identité*, il est confirmé que l'*identité* a une existence continue durant le cycle de vie, associable à plusieurs transactions.

8.9 Processus de maintien de l'identité

8.9.1 But

8.9.1.1 Le processus de *maintien de l'identité* vise à veiller à ce que les *renseignements sur*

l'identité d'un sujet soient exacts, complets et à jour.

NOTE : Le processus de *maintien de l'identité* englobe la tenue des dossiers, ce qui peut comprendre leur suppression. En effet, il peut être indiqué de supprimer des dossiers d'*identité* pour des raisons d'exactitude (p. ex. inclusion par erreur dans un registre faisant autorité, comme un duplicata de l'attestation de naissance), des raisons de politique (p. ex. politique de conservation des dossiers limitant à trois ans la rétention des renseignements sur les anciens clients) ou des motifs juridiques (p. ex. ordonnance d'un commissariat à la protection de la vie privée).

8.9.2 Résultats

8.9.2.1 À l'issue du processus de *maintien de l'identité*, les *renseignements sur l'identité* sont exacts, complets et à jour.

8.10 Processus d'établissement de liens pour déterminer l'identité

8.10.1 But

8.10.1.1 Le processus d'*établissement de liens pour déterminer l'identité* vise à mettre en correspondance un ou des *identificateurs attribués* et un *sujet* donné.

8.10.2 Résultats

8.10.2.1 À l'issue du processus d'*établissement de liens pour déterminer l'identité*, un ou plusieurs *identificateurs attribués* sont associés au *sujet*.

8.11 Processus de détermination des renseignements sur la relation

8.11.1 But

8.11.1.1 Le processus de *détermination des renseignements sur la relation* vise à déterminer le contexte de la *relation*, les exigences en matière de *renseignements sur la relation* et l'*identificateur de relation*.

8.11.2 Résultats

8.11.2.1 À l'issue du processus de *détermination des renseignements sur la relation*, le contexte de la *relation*, les exigences en matière de *renseignements sur la relation* et l'*identificateur de relation* sont établis.

8.12 Processus de détermination de la preuve de relation

8.12.1 But

8.12.1.1 Le processus de *détermination de la preuve de relation* vise à déterminer ce qui est la preuve (physique ou électronique) acceptable d'une *relation*.

8.12.2 Résultats

8.12.2.1 À l'issue du processus de *détermination de la preuve de relation*, il est établi une preuve de *relation* acceptable.

8.13 Processus d'acceptation de la preuve de relation

8.13.1 But

8.13.1.1 Le processus d'*acceptation de la preuve de relation* vise à confirmer que la preuve (physique ou électronique) présentée pour attester une *relation* est acceptable.

8.13.2 Résultats

8.13.2.1 À l'issue du processus d'*acceptation de la preuve de relation*, il est confirmé que la preuve de *relation* est acceptable.

8.14 Processus de validation des renseignements sur la relation

8.14.1 But

8.14.1.1 Le processus de *validation des renseignements sur la relation* vise à confirmer l'exactitude des renseignements sur une *relation* entre deux *sujets* ou plus, tel qu'il est établi par l'*émetteur*.

8.14.2 Résultats

8.14.2.1 À l'issue du processus de *validation des renseignements sur la relation*, les *renseignements sur la relation* sont validés auprès de l'*émetteur*.

8.15 Processus de résolution de la relation

8.15.1 But

8.15.1.1 Le processus de *résolution de la relation* vise à établir le caractère unique d'une instance de *relation* au sein d'une population par l'utilisation de *renseignements sur la relation* et de *renseignements sur l'identité*.

8.15.2 Résultats

8.15.2.1 À l'issue du processus de *résolution de la relation*, il est établi que les *renseignements sur la relation* et *l'identité* sont propres à une seule *relation*.

8.16 Processus d'établissement de la relation

8.16.1 But

8.16.1.1 Le processus d'*établissement de la relation* vise à consigner l'existence d'une *relation* entre deux *sujets* ou plus

8.16.2 Résultats

8.16.2.1 À l'issue du processus d'*établissement de la relation*, il existe un enregistrement de la *relation*.

8.17 Processus de vérification de la relation

8.17.1 But

8.17.1.1 Le processus de *vérification de la relation* vise à confirmer que les *renseignements sur la relation* se trouvent sous le contrôle du *sujet*.

8.17.2 Résultats

8.17.2.1 À l'issue du processus de *vérification de la relation*, il est confirmé que les *sujets* ont le contrôle des *renseignements sur la relation*.

8.18 Processus de continuité de la relation

8.18.1 But

8.18.1.1 Le processus de *continuité de la relation* vise à confirmer dynamiquement qu'une *relation* entre deux *sujets* ou plus a une existence continue dans le temps.

8.18.2 Résultats

8.18.2.1 À l'issue du processus de *continuité de la relation*, il est confirmé que la *relation* a une existence continue dans le temps associable à plusieurs transactions.

8.19 Processus de maintien de la relation

8.19.1 But

8.19.1.1 Le processus de *maintien de la relation* vise à veiller à ce que les *renseignements sur la relation* entre deux *sujets* ou plus soient exacts, complets et à jour.

8.19.2 Résultats

8.19.2.1 À l'issue du processus de *maintien de la relation*, les *renseignements sur la relation* sont à jour.

8.20 Processus de suspension de la relation

8.20.1 But

8.20.1.1 Le processus de *suspension de la relation* vise à signaler qu'un dossier de *relation* n'est temporairement plus en vigueur.

8.20.2 Résultats

8.20.2.1 À l'issue du processus de *suspension de la relation*, la *relation* n'est temporairement plus en vigueur.

8.21 Processus de rétablissement de la relation

8.21.1 But

8.21.1.1 Le processus de *rétablissement de la relation* vise à faire passer une *relation* suspendue à l'état actif.

8.21.2 Résultats

8.21.2.1 À l'issue du processus de *rétablissement de la relation*, le dossier d'une *relation* est à jour.

8.22 Processus de révocation de la relation

8.22.1 But

8.22.1.1 Le processus de *révocation de la relation* vise à signaler qu'un dossier de *relation* n'est plus en vigueur.

8.22.2 Résultats

8.22.2.1 À l'issue du processus de *révocation de la relation*, la *relation* n'est plus en vigueur.

8.23 Processus de délivrance d'un justificatif

8.23.1 But

8.23.1.1 Le processus de *délivrance d'un justificatif* vise à créer un *justificatif* à partir d'un ensemble d'*affirmations* sur un ou plusieurs *sujets* et à attribuer le *justificatif* à un *titulaire*.

8.23.2 Résultats

8.23.2.1 À l'issue du processus de *délivrance d'un justificatif*, une ou plusieurs *affirmations* sur un ou plusieurs *sujets* sont associées au *justificatif*, lequel a été attribué à un *titulaire*.

8.24 Processus de liaison justificatif-authentifiant

8.24.1 But

8.24.1.1 Le processus de *liaison justificatif-authentifiant* vise à associer un *justificatif* délivré à un *titulaire* avec un ou plusieurs *authentifiants*.

NOTE : Ce processus comprend également des activités liées au cycle de vie de l'*authentifiant*, telles que la suspension des *authentifiants* (en cas d'oubli de mot de passe ou de verrouillage en raison d'échecs successifs de la *vérifications des justificatifs*, d'inactivité ou d'activité suspecte), la suppression d'*authentifiants*, la liaison d'autres *authentifiants* et la mise à jour d'*authentifiants* (p. ex. changement de mot de passe, mise à jour des questions et réponses de sécurité, nouvelle photo faciale).

8.24.2 Résultats

8.24.2.1 À l'issue du processus de *liaison justificatif-authentifiant*, un *justificatif* délivré est associé à un ou plusieurs *authentifiants*.

8.25 Processus de validation des justificatifs

8.25.1 But

8.25.1.1 Le processus de *validation des justificatifs* vise à confirmer la validité du *justificatif* délivré (p. ex. non violé, expiré, corrompu, modifié, suspendu ou révoqué).

NOTE : La validité du *justificatif* délivré peut alors servir de base pour établir le *niveau de confiance*.

8.25.2 Résultats

8.25.2.1 À l'issue du processus de *validation des justificatifs*, le *justificatif* délivré est validé.

8.26 Processus de vérification des justificatifs

8.26.1 But

8.26.1.1 Le processus de *vérification des justificatifs* vise à confirmer qu'un *titulaire* exerce un contrôle sur un *justificatif* délivré.

NOTE : Le degré de contrôle exercé sur le *justificatif* délivré peut alors servir de base pour établir le *niveau de confiance*. Le contrôle exercé sur un *justificatif* délivré *doit* être vérifié au moyen d'un ou de plusieurs *authentificateurs*.

8.26.2 Résultats

8.26.2.1 À l'issue du processus de *vérification des justificatifs*, le *titulaire* a prouvé qu'il a le contrôle du *justificatif* délivré.

8.27 Processus de maintien du justificatif

8.27.1 But

8.27.1.1 Le processus de *maintien du justificatif* vise à mettre à jour les *attributs* (p. ex. date d'expiration, état) d'un *justificatif* délivré.

8.27.2 Résultats

8.27.2.1 À l'issue du processus de *maintien du justificatif*, le *justificatif* délivré est mis à jour.

8.28 Processus de suspension d'un justificatif

8.28.1 But

8.28.1.1 Le processus de *suspension d'un justificatif* vise à suspendre un *justificatif* délivré de manière reconnue en marquant ce *justificatif* comme temporairement inutilisable.

NOTE : Ce processus vise à mettre à l'épreuve la confiance dans le *justificatif*. Il peut être indiqué quand il y a lieu de croire qu'une *affirmation* est inexacte (p. ex. il y a une

faute de frappe dans un nom) ou encore qu'un *titulaire* n'a pas conservé le contrôle d'un *justificatif* (p. ex. son mot de passe a été volé).

8.28.2 Résultats

8.28.2.1 À l'issue du processus de *suspension d'un justificatif*, la suspension du *justificatif* est reconnue

8.29 Processus de recouvrement d'un justificatif suspendu

8.29.1 But

8.29.1.1 Le processus de *recouvrement d'un justificatif* vise à rendre le *justificatif* suspendu de nouveau actif (c'est-à-dire un *justificatif* délivré).

NOTE : Ce processus vise à confirmer la confiance dans le *justificatif*. Il peut être indiqué quand il y a suffisamment lieu de croire qu'une *affirmation* est inexacte (p. ex. la graphie du nom est incorrecte) ou encore que le *titulaire* a repris le contrôle d'un *justificatif* suspendu (p. ex. le *titulaire* a changé son mot de passe).

8.29.2 Résultats

8.29.2.1 À l'issue du processus de *recouvrement d'un justificatif* suspendu, le *justificatif* délivré est redevenu actif.

8.30 Processus de révocation d'un justificatif

8.30.1 But

8.30.1.1 Le processus de *révocation d'un justificatif* vise à révoquer de façon permanente un *justificatif* délivré.

8.30.2 Résultats

8.30.2.1 À l'issue du processus de *révocation d'un justificatif*, il est clairement indiqué que le *justificatif* est révoqué.

8.31 Processus de formulation de l'avis de consentement

8.31.1 But

8.31.1.1 Le processus de *formulation de l'avis de consentement* vise à produire un énoncé d'avis de consentement.

8.31.2 Résultats

8.31.2.1 À l'issue du processus de *formulation de l'avis de consentement*, il existe un énoncé d'avis de consentement.

NOTE : L'énoncé d'avis de consentement *doit* indiquer :

- a. quels *renseignements personnels* sont ou peuvent être recueillis;
- b. les parties à qui sont communiqués les renseignements personnels (connues au moment de la présentation de l'avis);
- c. dans quels buts les *renseignements personnels* sont recueillis, utilisés ou divulgués;
- d. quels sont les risques de préjudice et autres conséquences découlant de la collecte, de l'utilisation ou de la divulgation des renseignements;
- e. comment les *renseignements personnels* seront gérés et protégés;
- f. quelle est la durée d'application de l'avis;
- g. de quelle autorité relève l'avis;
- h. quelles sont les modalités de révocation de tout consentement donné, en tout ou en partie, en vertu de l'avis.

8.32 Processus de présentation de l'avis de consentement

8.32.1 But

8.32.1.1 Le processus de *présentation de l'avis de consentement* vise à remettre un avis de consentement à une *personne*.

8.32.2 Résultats

8.32.2.1 À l'issue du processus de *présentation de l'avis de consentement*, un avis de consentement est remis à une *personne*.

8.33 Processus de demande de consentement

8.33.1 But

8.33.1.1 Le processus de *demande de consentement* vise à demander à une *personne* si elle consent ou ne consent pas – selon la forme de l'énoncé d'avis présenté – à quelque chose, ce qui entraîne une décision d'affirmation (« oui ») ou de refus (« non ») de consentement.

8.33.2 Résultats

8.33.2.1 À l'issue du processus de *demande de consentement*, une décision de consentement

est prise.

8.34 Processus d'enregistrement du consentement

8.34.1 But

8.34.1.1 Le processus d'*enregistrement du consentement* vise à stocker de manière persistante un énoncé d'avis et la décision de consentement connexe de la *personne*.

8.34.2 Résultats

8.34.2.1 À l'issue du processus d'*enregistrement du consentement*, il existe une décision de consentement enregistrée aux dossiers.

NOTE : L'*organisation doit* consigner ce qui suit en lien avec la décision de consentement :

- a. les *renseignements sur l'identité* de la *personne*;
- b. la version de l'avis qui a été présentée;
- c. la date et l'heure de présentation de l'avis;
- d. la teneur de la décision (affirmation ou refus de consentement) et la date et l'heure de cette décision;
- e. le cas échéant, la date et l'heure d'expiration ou de révocation de la décision de consentement.

8.34.2.2 Une fois ces renseignements consignés, l'*organisation doit* informer les parties concernées de la décision de consentement.

8.35 Processus d'examen du consentement

8.35.1 But

8.35.1.1 Le processus d'*examen du consentement* vise à rendre visibles pour la *personne* qui a donné le consentement les détails d'une décision de consentement enregistrée.

8.35.2 Résultats

8.35.2.1 À l'issue du processus d'*examen du consentement*, il existe une décision de consentement enregistrée.

NOTE : L'*organisation doit* définir son processus d'*examen du consentement* de façon à exposer les données minimales requises pour confirmer la teneur de la décision (affirmation ou refus de consentement) prise par le *sujet* devant l'avis reçu, ainsi qu'une copie de l'avis en question. Si l'examineur autorisé relève du *cadre de confiance* d'une fédération, une trace écrite de la requête *doit* également être conservée dans le cadre des processus d'*acceptation de la preuve d'identité* et de *demande de consentement*. En outre, s'il y a *renouvellement, expiration* ou *révocation du consentement* par la suite, cette information *doit* être rendue accessible dans le cadre du processus d'*examen du consentement* et expressément communiquée sous forme d'avis à l'examineur autorisé.

8.36 Processus de renouvellement du consentement

8.36.1 But

8.36.1.1 Le processus de *renouvellement du consentement* vise à prolonger la période de validité d'une décision d'affirmation de consentement en reportant la date d'expiration.

8.36.2 Résultats

8.36.2.1 À l'issue du processus de *renouvellement du consentement*, une décision de consentement est mise à jour.

8.37 Processus d'expiration du consentement

8.37.1 But

8.37.1.1 Le processus d'*expiration du consentement* vise à suspendre la validité d'une décision d'affirmation de consentement en raison du dépassement de la date d'expiration.

8.37.2 Résultats

8.37.2.1 À l'issue du processus d'*expiration du consentement*, la décision de consentement est mise à jour.

8.38 Processus de révocation du consentement

8.38.1 But

8.38.1.1 Le processus de *révocation du consentement* vise à suspendre la validité d'une décision d'affirmation de consentement à la suite du retrait explicite du consentement par la *personne* (c'est-à-dire qu'une affirmation de consentement est convertie en refus de consentement).

8.38.2 Résultats

8.38.2.1 À l'issue du processus de *révocation du consentement*, la décision de consentement est mise à jour.

8.39 Processus de création d'une signature

8.39.1 But

8.39.1.1 Le processus de *création d'une signature* vise à créer une *signature*.

8.39.2 Résultats

8.39.2.1 À l'issue du processus de *création d'une signature*, il existe une *signature*.

8.40 Processus de vérification de la signature

8.40.1 But

8.40.1.1 Le processus de *vérification de la signature* vise à confirmer que la *signature* est valide.

8.40.2 Résultats

8.40.2.1 À l'issue du processus de *vérification de la signature*, la signature est valide.

Bibliographie

- [1] Australie, Trusted Digital Identity Framework.
- [2] BSI PAS 499:2019, *Code of practice for digital identification and strong customer authentication.*
- [3] Union européenne, *Règlement n° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.*
- [4] *Good Practice Guide n° 43 – Requirements for Secure Delivery of Online Public Services.*
- [5] *Good Practice Guide n° 44 – Authentication Credentials in Support of HMG Online Services.*
- [6] *Good Practice Guide n° 45 – Identity Proofing and Verification of an Individual.*
- [7] *Good Practice Guide n° 53 – Transaction Monitoring for HMG Online Service Providers.*
- [8] ISO/IEC 24760-1:2019, *Sécurité IT et confidentialité — Cadre pour la gestion de l'identité — Partie 1 : Terminologie et concepts.*
- [9] ISO/IEC 24760-2:2015, *Technologies de l'information — Techniques de sécurité — Cadre pour la gestion de l'identité — Partie 2 : Architecture de référence et exigences.*
- [10] ISO/IEC 24760-3:2016, *Technologies de l'information — Techniques de sécurité — Cadre pour la gestion de l'identité — Partie 3 : Mise en œuvre.*
- [11] ISO/IEC 27018, *Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII.*
- [12] ISO/IEC 29100, *Technologies de l'information — Techniques de sécurité — Cadre privé.*
- [13] ISO/IEC 29115:2013, *Technologies de l'information — Techniques de sécurité — Cadre d'assurance de l'authentification d'entité.*
- [14] ITSP.30.031, *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information.*
- [15] Gouvernement de la Nouvelle-Zélande, Digital Identity New Zealand.
 - i) Norme sur les preuves d'identité
 - ii) Normes d'authentification

iii) Gestion de l'identification

- [16] NIST, *Digital Identity Guidelines*, Special Publication 800-63.
- [17] *Le profil du secteur public du Cadre de confiance pancanadien (CCP)*, version 1.4, 2021.
- [18] Secrétariat du Conseil du Trésor du Canada, *Ligne directrice sur la définition des exigences en matière d'authentification*, 2012.
- [19] Secrétariat du Conseil du Trésor du Canada, *Ligne directrice sur l'assurance de l'identité*, 2016.
- [20] Secrétariat du Conseil du Trésor du Canada, *Directive sur la gestion de l'identité*, 2019.
- [21] UK Digital Identity and Attributes Trust Framework.