LE PROFIL DU SECTEUR PUBLIC DU CADRE DE CONFIANCE PANCANADIEN (CCP)

VERSION 1.1

Version du document :	0.4
État du document :	Ébauche aux fins de consultation
Date :	2020-06-02
Classification de sécurité :	NON CLASSIFIÉ

CONTRÔLE DES VERSIONS DU DOCUMENT

Numéro de version	Date de l'émission	Auteurs	Courte description
0.1	2019-10-10	Groupe de travail sur le PSP du CCP	Ébauche aux fins de consultation
0.2	2019-10-31	Groupe de travail sur le PSP du CCP	Ébauche aux fins de consultation
0.3	2020-02-20	Groupe de travail sur le PSP du CCP	Ébauche aux fins de consultation
0.4	2020-06-02	Groupe de travail sur le PSP du CCP	Ébauche aux fins de consultation

TABLE DES MATIÈRES

LISTE DES FIGURES

RÉSUMÉ

Le présent document décrit la **version 1.1** du profil du secteur public du ***Cadre de confiance pancanadien (CCP)***. Le présent document est structuré de la façon suivante :

- la **section 1** décrit l'objet et le public du document;
- la **section 2** décrit les principaux éléments du CCP;
- les **sections 3 à 9** présentent diverses annexes portant sur les termes et les définitions, des analyses de certains sujets liés au CCP, une liste des questions qui seront résolues dans les versions futures du document et une bibliographie.

Le Cadre de confiance pancanadien facilitera la transition vers un écosystème numérique pour les citoyens et les résidents du Canada. Un écosystème numérique canadien augmentera l'efficience et garantira l'interopérabilité entre les processus opérationnels existants, comme le système bancaire ouvert, les permis d'exploitation d'entreprise et la prestation de services dans le secteur public.

Le CCP est simple et intégré et technologiquement agnostique; il complète les cadres existants; et il est clairement mis en correspondance avec des politiques, des règlements et des lois. Il est également conçu pour appliquer les normes pertinentes aux processus et aux capacités clés.

Le CCP facilite l'adoption d'une approche commune entre les divers ordres de gouvernements et le secteur privé, répondant ainsi aux besoins des diverses collectivités qui doivent faire confiance aux identités numériques. Le CCP a été défini de façon à encourager l'innovation et l'évolution de l'écosystème numérique. Le CCP permet l'interopérabilité des différentes plates-formes, des services, des architectures et des technologies.

Le CCP définit deux types de *représentations numériques* essentielles au développement de l'écosystème numérique :

1. les *identités numériques* d'entités comme des personnes, des organisations et des appareils;
2. les *relations numériques* entre les entités.

Le CCP appuie l'acceptation des identités numériques et des relations numériques en définissant un ensemble de modèles de processus discrets, que l'on appelle *processus atomiques*. Ces processus atomiques peuvent être mis en correspondance avec des processus opérationnels existants, évalués de façon indépendante à l'aide de critères de conformité[1] et certifiés comme étant dignes de confiance et interopérables dans l'écosystème numérique.

[1] Les critères de conformité sont conservés dans un document à part.

1 AVANT-PROPOS

Le présent document vise à décrire le profil du secteur public du Cadre de confiance pancanadien (CCP)[2].

Le public cible de ce document comprend :

- les propriétaires d'entreprise et les gestionnaires de programme – afin de rendre possibles des solutions d'identité numérique permettant d'atteindre les objectifs opérationnels ou les résultats de programme;
- les organismes de réglementation et de surveillance – afin de comprendre les conséquences pour leur rôle dans l'écosystème numérique;
- les fournisseurs de services et de technologies d'identité numérique – afin de leur montrer où ils cadrent dans l'écosystème numérique et de les aider à définir les exigences relatives à leurs produits et services;

On trouvera les définitions de divers termes et expressions utilisés dans ce document dans l'Annexe A : Termes et définitions.

[2] L'élaboration du profil du secteur public udu Cadre de confiance pancanadien est un effort de collaboration dirigé par les conseils mixtes du Canada. Les conseils mixtes du Canada sont un forum composé du Conseil de la prestation des services du secteur public (CPSSP) et du Conseil des dirigeants principaux de l'information du secteur public (CDPISP). Le présent document a été élaboré par le Groupe de travail sur le profil du secteur public du CCP (GT sur le PSP du CCP) aux fins de discussion et de consultation, et son contenu n'a pas encore été approuvé par les conseils mixtes. Ce document est publié en vertu de la Licence du gouvernement ouvert – Canada, qui se trouve à l'adresse suivante : https://ouvert.canada.ca/fr/licence-du-gouvernement-ouvert-canada.

2 LE CADRE DE CONFIANCE PANCANADIEN

2.1 Survol

2.1.1 Contexte

L'écosystème de gestion de l'identité du Canada est composé de multiples fournisseurs d'identité qui s'appuient sur des registres de sources faisant autorité qui s'étendent aux administrations provinciales, territoriales et fédérales. Par conséquent, l'écosystème canadien utilise actuellement un modèle d'identité fédéré.

Le Cadre de confiance pancanadien (CCP) est le résultat de l'approche pancanadienne pour la fédération de l'identité, une entente sur les principes et les normes à appliquer au moment de développer des solutions d'identité[3]. Cette approche, intégrée au CCP, vise à faciliter la transition vers un écosystème numérique qui permettra la mise au point de solutions transformatrices de prestation de services numériques pour les citoyens et les résidents du Canada.

2.1.2 Qu'est-ce que le CCP?

Le CCP est un modèle qui comprend un ensemble de concepts, de définitions, de processus, de critères de conformité et une approche d'évaluation convenus. Il ne s'agit pas d'une « norme » en tant que telle, mais plutôt d'un cadre qui relie et applique les normes, politiques, lignes directrices et pratiques existantes, et qui, en l'absence de telles normes et politiques, précise des critères supplémentaires. Le rôle du CCP est de compléter les normes et les politiques existantes comme celles concernant la sécurité, la protection des renseignements personnels et la prestation de services.

Le CCP facilite une approche commune entre le secteur public et le secteur privé. L'utilisation du CCP assure l'harmonisation, l'interopérabilité et la confiance des solutions d'identité numérique qui sont conçues pour fonctionner au-delà des frontières organisationnelles, sectorielles et des administrations. De plus, le CCP complète les lois, les règlements et les politiques en place.

Le CCP soutient l'acceptation et la reconnaissance mutuelle des éléments suivants :

- les identités numériques d'entités comme des personnes et des organisations;
- les relations numériques entre les entités.

Le CCP définit un ensemble de modèles de processus discrets (appelés processus atomiques) qui peuvent être mis en correspondance avec des processus opérationnels.

[3] Voir : *Ligne directrice sur l'assurance de l'identité* [SCT, 2017].

Cette cartographie permet une évaluation et une évaluation structurées d'une solution d'identité numérique et cerne les dépendances à l'égard d'organisations et de fournisseurs externes, s'il y a lieu.

Le CCP est technologiquement agnostique et a été défini de façon à encourager l'innovation et la participation à l'écosystème numérique. Il rend possible l'interopérabilité des différentes plates-formes, des services, des architectures et des technologies. De plus, le CCP est conçu pour tenir compte des cadres internationaux de l'identité numérique, comme les suivants :

- l'Identification électronique et services de confiance pour les transactions électroniques (eIDAS);
- le Groupe d'action financière (GAFI);
- la Commission des Nations Unies sur le droit commercial international (CNUDCI).

Enfin, il convient de faire remarquer que le profil du secteur public du CCP, en soi, n'est pas un cadre de *gouvernance*. Il s'agit plutôt d'un outil qui facilite l'évaluation d'un programme ou d'un service d'identité numérique.

2.1.3 Portée du CCP

Voici la portée actuelle du Cadre de confiance pancanadien :

- les personnes se trouvant au Canada : tous les citoyens et résidents du Canada (y compris les personnes décédées) pour qui une identité a été établie au Canada;
- les organismes au Canada : tous les organismes enregistrés et en activité au Canada (y compris les organismes inactifs), dont une identité a été établie au Canada;
- les relations au Canada : de personnes à personnes, d'organismes à organismes et de personnes à organismes.

2.2 Modèle de CCP

Le modèle de CCP, comme le montre la figure 1, est un aperçu de haut niveau du CCP sous forme de diagramme.

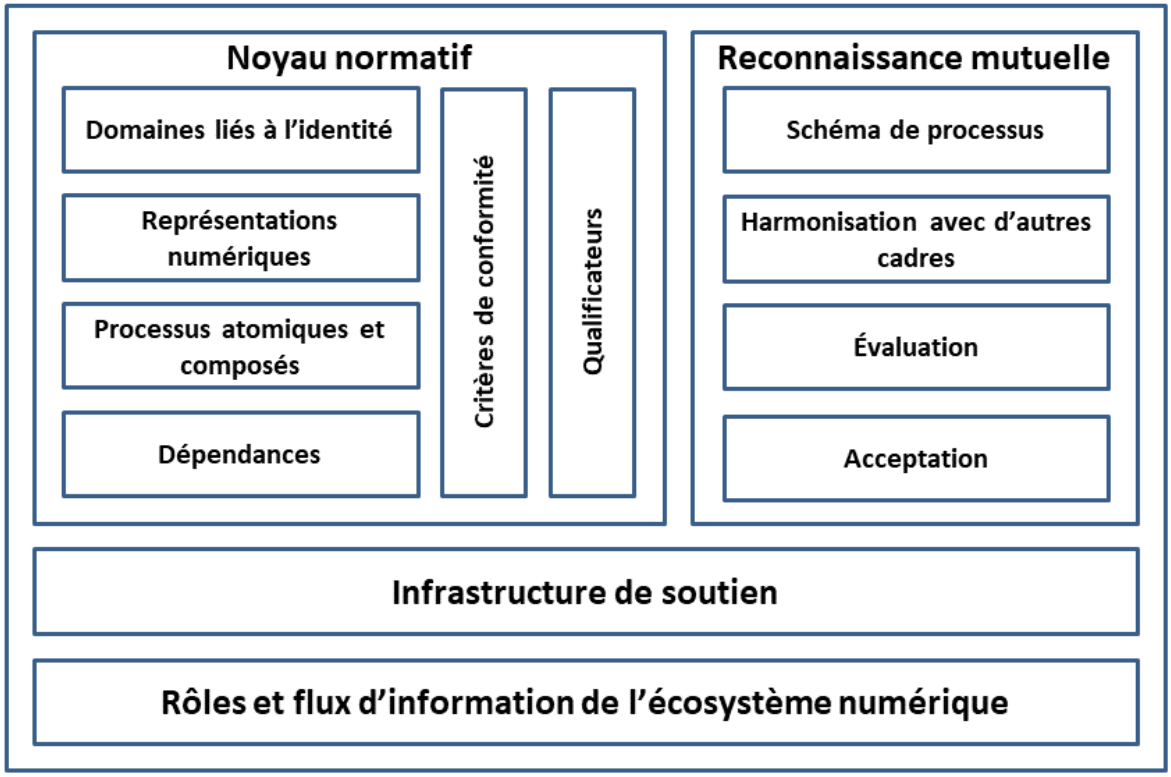

Figure 1 : Modèle de cadre de confiance pancanadien

Le modèle de CCP comprend quatre composantes principales :

1. la composante du **noyau normatif**, qui englobe les concepts clés du CCP;
2. la composante de la **reconnaissance mutuelle**, qui décrit la méthodologie actuelle servant à évaluer et à certifier les acteurs de l'écosystème numérique;
3. la composante de l'**infrastructure de soutien**, qui décrit l'ensemble de politiques, de règles et de normes opérationnelles et techniques qui constituent les principaux catalyseurs d'un écosystème numérique;

4. la composante des **rôles et flux d'information de l'écosystème numérique**, qui définit les rôles et les flux d'information au sein de l'écosystème numérique.

Tous les éléments de la composante du « noyau normatif » sont normatifs. La section sur la composante de la « reconnaissance mutuelle » décrit une méthodologie recommandée, mais il n'est pas obligatoire de la suivre. Les sections sur les composantes de l'« infrastructure de soutien » et des « rôles et flux d'information de l'écosystème numérique » sont descriptives seulement et non normatives.

Les quatre composantes du CCP sont décrites plus en détail dans les quatre sections suivantes du présent document (les sections 2.3 à 2.6, inclusivement).

2.3 Noyau normatif

2.3.1 Domaines liés à l'identité

Le CCP établit une distinction claire entre l'*identité principale* et l'*identité contextuelle*.

- Une **identité principale** est une 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 naturalisée, décès, enregistrement de la dénomination sociale de l'organisation, changement de nom légal de l'organisation ou faillite).
- Une **identité contextuelle** est une identité qui est utilisée à des fins précises dans un contexte d'identité précis[4] (p. ex., services bancaires, permis d'exploitation d'entreprise, services de santé, permis de conduire ou médias sociaux). Selon le contexte identitaire, une identité contextuelle peut être reliée à une identité principale (p. ex., un permis de conduire) ou ne pas être reliée à identité principale (p. ex., un profil de médias sociaux).

L'établissement et la tenue à jour des identités principales relèvent exclusivement du secteur public; plus précisément :

- les bureaux de l'état civil (BEC) des provinces et des territoires;
- les registres des entreprises des provinces et des territoires;
- Immigration, Refugiés et Citoyenneté Canada (IRCC);
- Le registre fédéral des sociétés de Corporations Canada.

L'établissement et la tenue à jour d'identités contextuelles relèvent des secteurs public et privé.

2.3.2 Représentations numériques

Une représentation numérique est une représentation électronique d'une entité ou une représentation électronique de la relation entre deux entités. Les représentations numériques sont destinées à des acteurs du monde réel, comme des personnes, des organisations et des appareils.

[4] En fournissant leurs programmes et leurs services, les fournisseurs de programmes et de services fonctionnent au sein d'un environnement ou d'un ensemble de circonstances particulières. C'est ce qu'on appelle le contexte de l'identité dans le domaine de la gestion de l'identité. Le contexte de l'identité est déterminé par des facteurs comme le mandat, la population cible (c.-à-d. les clients, la clientèle), et les autres responsabilités établies en vertu d'une loi, d'un accord ou d'une entente. Pour plus d'information sur l'identité et les concepts de gestion de l'identité, voir l'annexe B.

Actuellement, le CCP reconnaît deux types de représentations numériques :

- l'**identité numérique** : une représentation électronique d'une entité, utilisée exclusivement par cette même entité, permettant d'accéder à des services et d'exécuter des opérations en toute confiance et confidentialité.
- la **relation numérique** : une représentation électronique de la relation entre une entité et une autre entité.

Une représentation numérique est le résultat final d'un ensemble de processus et peut donc être conceptualisée comme étant un ensemble de transitions d'état (voir la section 2.3.3).

Au fur et à mesure que le CCP évolue, ces représentations numériques seront étendues à d'autres types entités telles que les actifs numériques et les contrats intelligents. Il est également prévu qu'à l'avenir, le CCP soit utilisé pour faciliter la reconnaissance mutuelle des représentations numériques entre les pays.

2.3.3 Processus atomiques et composés

Le CCP définit un ensemble de processus atomiques qui peuvent être évalués de façon indépendante et certifiés comme interopérant l'un avec l'autre dans un écosystème numérique. Un processus atomique est un ensemble d'activités logiquement mis en correspondance qui entraîne un état de transition[5]. Le CCP reconnaît qu'en pratique, un processus opérationnel est souvent un ensemble de processus atomiques qui entraînent un ensemble de transitions d'état. Ces ensembles de processus atomiques sont appelées des processus composés.

Tous les processus atomiques ont été conçus de façon à pouvoir être mis en œuvre en tant que services modulaires et à être évalués de façon distincte aux fins de certification. Une fois qu'un processus atomique est attesté, on peut s'appuyer sur lui ou lui « faire confiance » et l'intégrer à d'autres plateformes de l'écosystème numérique. L'écosystème numérique vise une interopérabilité absolue entre les différents secteurs, organisations et territoires. Il vise également l'interopérabilité avec les autres cadres de fiabilité.

Il convient de noter que deux processus atomiques – la *détermination des renseignements sur l'identité* et la *détermination de la preuve d'identité* – ne sont effectués qu'une seule fois pour un programme ou un service.

[5] Une transition d'état est la transformation de l'état d'intrant d'un objet vers un état d'extrant.

2.3.3.1 Processus atomiques

Un processus atomique est un ensemble d'activités logiquement mis en correspondance qui entraînent un état de transition d'un objet. D'autres processus atomiques peuvent se fier à l'état de sortie de l'objet. La figure 2 illustre le modèle de processus atomique.

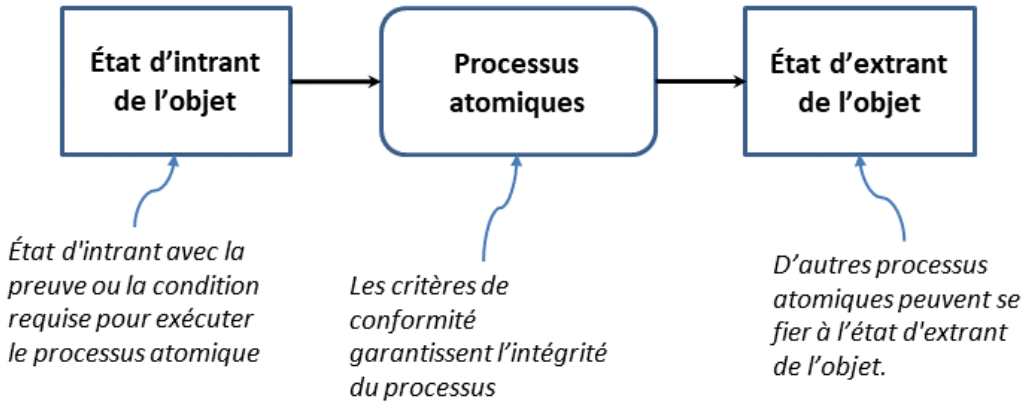

Figure 2 : Modèle de processus atomique

Les processus atomiques sont des constituants essentiels permettant de veiller à l'intégrité générale de la chaîne d'approvisionnement de l'identité numérique et, par extension, à l'intégrité des services numériques. L'intégrité du processus atomique relève de la plus haute importance, puisque le produit de ce processus est utilisé par de nombreux participants issus des secteurs public et privé et des administrations, et ce, à court et à long terme. Le CCP veille à l'intégrité des processus atomiques en établissant des critères de conformité convenus et bien définis qui facilitent la réalisation d'évaluations et d'attestations impartiales, transparentes et fondées sur les données probantes.

Les critères de conformité associés aux processus atomiques précisent les étapes à suivre pour faire passer un objet de son état d'entrée à son état de sortie. Les critères de conformité ont pour but de veiller à ce que les processus atomiques soient effectués avec intégrité. À titre d'exemple, le processus atomique peut consister à attribuer un identificateur à une personne ou à une organisation. Les critères de conformité pourraient indiquer qu'une partie responsable de gérer des processus atomiques doit veiller à ce que l'identificateur attribué à la personne ou à l'organisation soit unique au sein d'une population donnée.

Pour une description détaillée des processus atomiques, consulter la section 5.7.

La figure 3 illustre quelques modèles de diagrammes des trois processus atomiques.

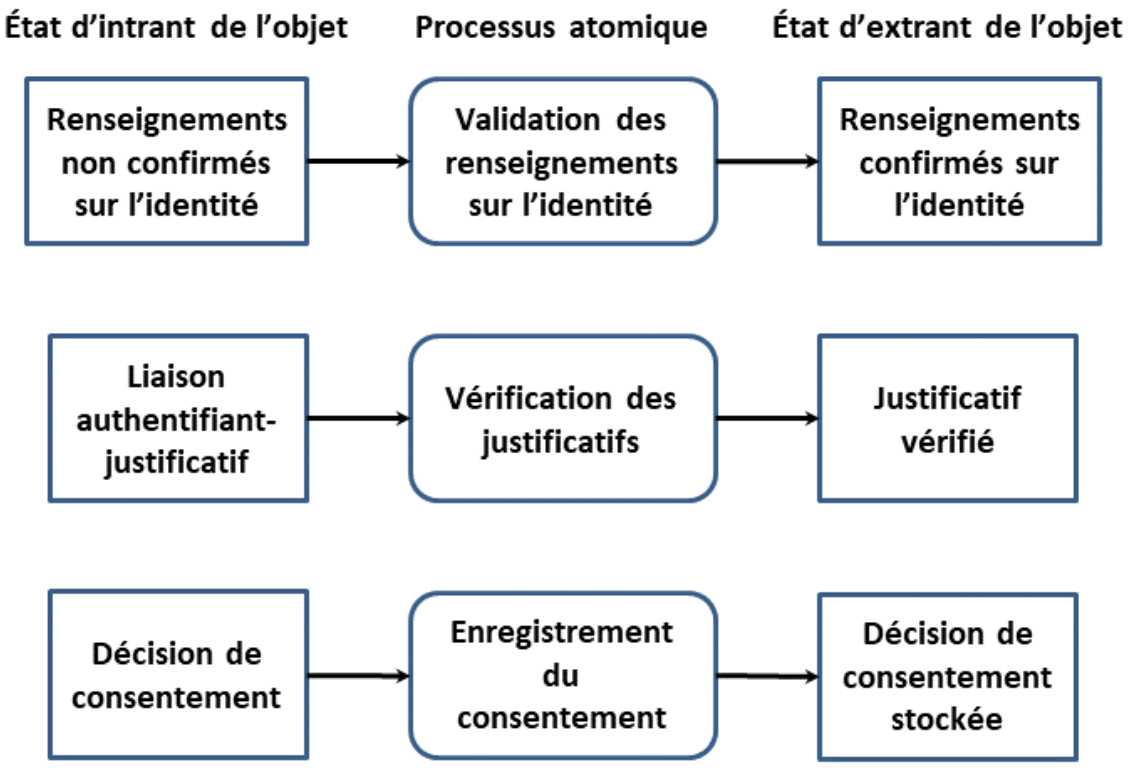

Figure 3 : Exemples de processus atomiques (modélisés)

2.3.3.2 Processus composés

La fonction principale du CCP est d'évaluer et de certifier les processus opérationnels existants. Lorsqu'ils sont analysés, ces processus opérationnels sont souvent composés de plusieurs processus atomiques. Un ensemble de processus atomiques regroupés forment un processus composé qui entraîne un ensemble de transitions d'état. Il se peut aussi qu'un processus composé soit constitué d'un ensemble d'autres processus composés qui peuvent eux-mêmes être décomposés en un ensemble de processus atomiques.

Par exemple, un processus opérationnel qu'une partie appelle la *confirmation d'identité* peut en fait se révéler être un processus composé comprenant 5 processus atomiques, comme le montre la figure 4.

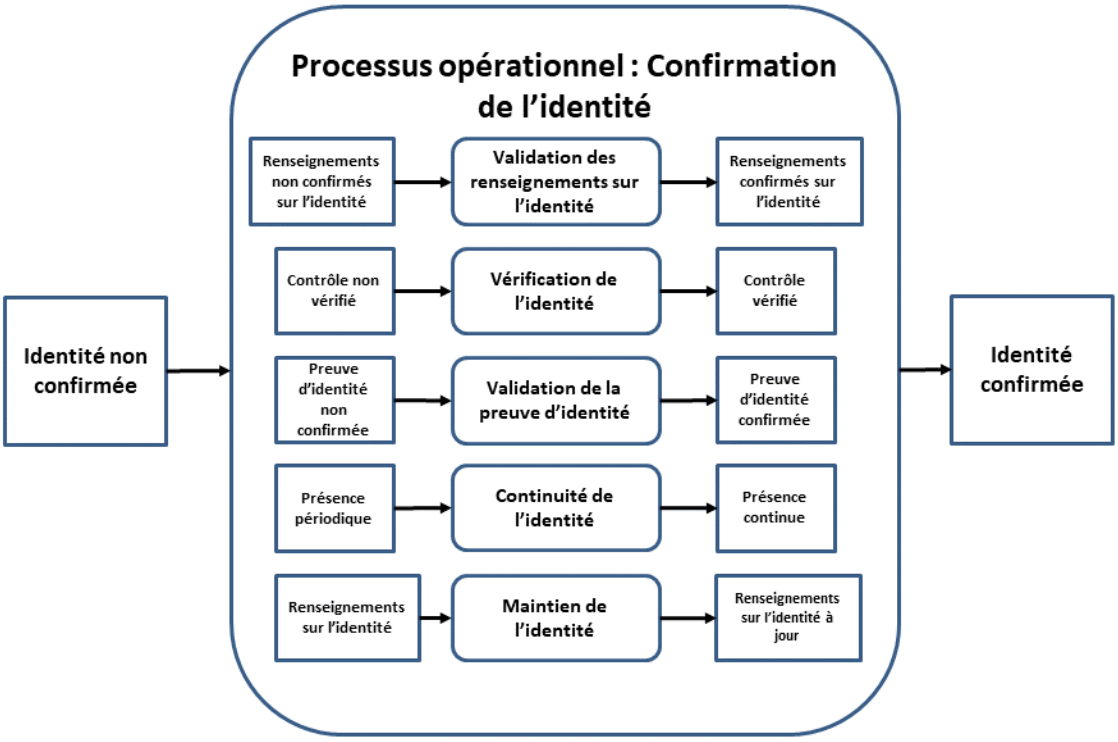

Figure 4 : Exemple de processus composé (modélisé)

Remarque : Il ne faut pas déduire un ordre particulier des processus atomiques à partir du diagramme.

2.3.4 Dépendances

Le modèle de CCP reconnaît deux types de dépendances. Le premier type est les dépendances qui existent entre les processus atomiques. Même si chaque processus atomique est fonctionnellement discret, pour produire une sortie acceptable, un processus atomique peut nécessiter qu'un autre processus atomique soit exécuté avec succès au préalable. Par exemple, même si l'*établissement de l'identité* d'une personne ou d'une organisation peut être effectué indépendamment à tout moment, il est logiquement exact de le faire seulement après que la *résolution de l'identité* de cette personne ou de cette organisation a été réalisée. Ce type de dépendance est précisé dans les critères de conformité (voir la section 2.3.5).

Le second type est celui des dépendances vis-à-vis des organisations externes pour assurer la prestation d'extrants de processus atomique (p. ex., un fournisseur de services commerciaux ou un service d'authentification des justificatifs). Ce type de dépendance est relevé et noté pendant le processus d'évaluation (voir la section 2.4.3).

2.3.5 Critères de conformité

Les critères de conformité sont un ensemble d'énoncés d'exigences définissant ce qu'il faut pour assurer l'intégrité d'un processus atomique. Les critères de conformité servent à appuyer une évaluation et un processus de certification réalisés de façon impartiale et transparente, et fondée sur des preuves.

À titre d'exemple, le processus atomique de la *résolution de l'identité* peut consister à attribuer un identificateur à une personne ou à une organisation. Le critère de conformité précise que le processus atomique doit garantir que l'identificateur attribué à la personne ou à l'organisation soit unique pour une population ou un contexte spécifique (p. ex., une province).

Les critères de conformité sont conservés dans un document à part. En ce moment, les critères de conformité sont regroupés dans une feuille de travail d'évaluation. Dans les versions futures, les critères de conformité pourront être intégrés à un outil d'évaluation automatisé.

2.3.6 Qualificateurs

Des qualificateurs peuvent être appliqués aux critères de conformité. Les qualificateurs visent à établir une correspondance entre des critères de conformité semblables ou identiques provenant de différents cadres de confiance et des exigences réglementaires ou des politiques des administrations. Par exemple, les critères de conformité de niveau 1 du CCP pour le processus atomique de la *vérification de l'identité* peuvent être mis en correspondance avec le niveau d'assurance de l'identité 1 tel qu'il est défini dans la *Norme sur l'assurance de l'identité et des justificatifs* émise par le Conseil du Trésor du gouvernement du Canada.

Les qualificateurs permettent de mieux décrire un niveau de confiance, la rigueur requise ou une exigence spécifique, en ce qui concerne un autre cadre de confiance, une exigence quant à un domaine lié à l'identité, ou une exigence stratégique ou réglementaire spécifique. Les qualificateurs peuvent être utilisés pour sélectionner les critères de conformité applicables à un processus d'évaluation. Les qualificateurs peuvent aussi être utilisés pour faciliter la mise en correspondance des équivalences de critères de conformité dans divers cadres de confiance.

Il est possible que les critères de conformité ne comprennent aucun qualificateur (applicable dans tous les cas) ou qu'ils comprennent un seul qualificatif (applicable dans certains cas), ou plusieurs qualificatifs (applicables dans plusieurs cas). Consultez la feuille de travail de l'évaluation pour obtenir des exemples de la façon dont les qualificateurs sont utilisés pour l'évaluation et dont ils peuvent être mis en correspondance avec d'autres cadres.

Les administrations voudront peut-être peuvent vouloir utiliser les qualificateurs qui sont déjà définis dans le CCP. Elles peuvent également définir de nouveaux

qualificateurs en fonction de leurs exigences particulières et ajouter de nouveaux critères de conformité, au besoin. De nouveaux qualificatifs peuvent être intégrés de nouveau à la composante du noyau normatif du CCP; toutefois, ces changements devraient être assujettis à un processus de gouvernance officiel ou à un processus de gestion du changement. Il convient également de noter que si de nouveaux qualificatifs et critères de conformité sont introduits dans le CCP, ils devront être mis en correspondance avec les critères de conformité existants et vérifiés par rapport à ceux-ci. Voir la section 2.8 pour de plus amples renseignements sur les qualificateurs.

2.4 Reconnaissance mutuelle

La reconnaissance mutuelle est une entente en vertu de laquelle au moins deux parties conviennent de reconnaître les résultats d'une évaluation de la conformité. Selon le contexte, la reconnaissance mutuelle peut être officialisée par l'émission d'une lettre d'acceptation ou faire partie d'une entente plus large.

Avant de commencer le processus de reconnaissance mutuelle du CCP, il est recommandé qu'un processus de planification et de mobilisation soit entrepris avec les principaux participants afin d'élaborer un régime de travail officiel.

À l'heure actuelle, le processus de reconnaissance mutuelle en est encore à ses débuts. Les sections qui suivent décrivent la reconnaissance mutuelle à un niveau élevé. Une orientation détaillée suivra dans les produits livrables subséquents.

2.4.1 Schéma de processus

Le schéma de processus consiste en un ensemble d'activités visant à mettre en correspondance les activités de programme, les processus opérationnels et les capacités techniques avec les processus atomiques définis dans le CCP.

Dans la plupart des cas, cette mise en correspondance est appliquée à un programme en cours d'exploitation. Le tableau ci-dessous illustre quelques exemples de mise en correspondance avec les processus opérationnels existants.

Processus atomique	Exemples de processus opérationnels existants
Résolution de l'identité	Un processus d'enregistrement à un service qui tente d'identifier de façon unique une personne en fonction de son nom et de sa date de naissance Un processus d'enregistrement des entreprises qui tente d'identifier de façon unique une organisation en fonction du nom légal de l'organisation, de sa date de création, de son adresse et du numéro d'identification ou du nom figurant dans un dossier faisant autorité
Établissement de l'identité	Un processus d'enregistrement de naissance qui consiste à créer un certificat de naissance faisant autorité Un processus d'enregistrement des entreprises qui crée un dossier d'entreprise faisant autorité
Validation des renseignements sur l'identité	Un processus de demande de permis de conduire qui confirme l'exactitude des renseignements présentés sur les documents physiques ou au moyen d'un service de validation électronique

Processus atomique	Exemples de processus opérationnels existants
	Un processus de délivrance de permis de cannabis qui confirme les renseignements sur l'identité présentés au sujet d'une entreprise au moyen d'une validation électronique avec le registre des entreprises applicable
Vérification de l'identité	Poser des questions à la personne qui présente les renseignements sur l'identité, dont les réponses ne sont connues (du moins en théorie) que de la personne et de son interrogateur (p. ex., renseignements financiers, antécédents en matière de crédit, secret partagé, code d'accès expédié par la poste, mot de passe, numéro d'identification personnel, identificateur attribué) Un processus de demande de passeport qui consiste à comparer les caractéristiques biologiques inscrites sur un document (par exemple, photographie du visage, couleur des yeux, taille) afin de s'assurer qu'il s'agit du demandeur en question La réalisation d'un audit sur place d'une entreprise
Maintien de l'identité	Un service de notification des renseignements sur l'identité Un service de récupération des renseignements sur l'identité
Émission d'un justificatif	Délivrer un document faisant autorité, notamment un certificat de naissance ou un permis de conduire Délivrer un document faisant autorité, notamment un certificat d'existence ou de conformité Émettre un justificatif vérifiable

2.4.2 Harmonisation avec d'autres cadres

L'harmonisation des processus, des systèmes et des solutions contribue à la reconnaissance mutuelle dans un contexte international où plusieurs cadres peuvent être utilisés.

Par exemple, une personne qui accède à des services numériques canadiens peut également avoir besoin d'avoir accès aux services numériques dans d'autres pays. Compte tenu de cette évolution vers le contexte international, le CCP est conçu pour s'appliquer conjointement avec les cadres mondiaux établis et émergents, comme les suivants :

- l'Identification électronique et services de confiance pour les transactions électroniques (eIDAS);

- le Groupe d'action financière (GAFI) – *Document d'orientation sur l'identité numérique*;
- la Commission des Nations Unies pour le droit commercial international (CNUDCI) – *Projet de dispositions relatives à la reconnaissance internationale de la gestion de l'identité et des services de confiance*.

La reconnaissance mutuelle internationale en est encore à ses débuts. Il faudrait envisager d'assurer l'harmonisation avec ces cadres avant de commencer le processus d'évaluation.

2.4.3 Évaluation

Le CCP définit un ensemble normatif de processus atomiques et les critères de conformité connexes[6]. Une fois que les processus opérationnels existants ont été mis en correspondance avec les processus atomiques, ils peuvent être évalués et une décision peut être prise par rapport à chacun des critères de conformité des processus atomiques connexes.

Une feuille de travail d'évaluation détaillée a été mise au point pour faciliter le processus d'évaluation du CCP. Cette feuille de travail consolide les processus atomiques et leurs critères de conformité connexes sur une seule feuille de calcul pour faciliter la mise en correspondance des processus opérationnels existants, et aider l'équipe d'évaluation à recouper les données aux fins d'analyse. Les critères de conformité sont également mis en correspondance avec les qualificateurs pour faciliter la sélection des critères de conformité s'appliquant au processus d'évaluation.

Les preuves recueillies à l'appui de l'analyse et de la justification de la décision doivent être recueillies et enregistrées de manière à être facilement recoupées par rapport aux critères de conformité applicables.

Il convient de relever que, de par sa conception, le CCP ne présume pas qu'un seul fournisseur soit l'unique responsable e l'exécution de tous les processus atomiques. Par conséquent, plusieurs organismes pourraient être impliqués dans le processus d'évaluation du CCP, en mettant l'accent sur les différents processus atomiques ou les différents aspects (p. ex., la sécurité, la protection de la vie privée, la prestation de services). Il faut tenir compte de la façon de coordonner plusieurs organisations qui pourraient avoir besoin de travailler ensemble pour produire une évaluation globale du CCP. L'organisation évaluée est responsable de toutes les parties visées par l'évaluation. L'organisation peut décider que cela n'est pas faisable, mais elle demeure néanmoins responsable. De tels cas seront notés pendant l'évaluation.

Au fur et à mesure que le processus d'évaluation du CCP évolue, il faudra déterminer quelles organisations ou quelles normes sont mieux indiquées pour répondre aux exigences des intervenants et mieux appliquées en ce qui concerne le CCP.

2.4.4 Acceptation

L'acceptation est le processus d'approbation officielle des résultats du processus d'évaluation. Le processus d'acceptation dépend de la gouvernance et tient compte des mandats, des lois, des règlements et des politiques applicables[7]. En fin de compte, le

[6] Les critères de conformité sont conservés dans un document à part.

[7] Site Web ISO : https://www.iso.org/certification.html.

processus d'acceptation du CCP peut comprendre des processus normalisés définis par l'Organisation internationale de normalisation (ISO)[1], comme suit :

- **Certification** : Assurance écrite (sous la forme d'un certificat) donnée par une tierce partie qu'un produit, service ou système est conforme à des exigences spécifiques.
- **Accréditation** : Reconnaissance formelle par un organisme indépendant (en général un organisme d'accréditation) qu'un organisme de certification se conforme aux normes internationales.

Des programmes de certification et d'accréditation officiels sont en cours d'élaboration. En principe, une fois que les programmes seront élaborés, des tiers indépendants seront autorisés à procéder aux évaluations du CCP. Plusieurs organismes de normalisation nationaux et internationaux ont reconnu les normes et programmes d'évaluation de la conformité. À titre d'exemple, le Conseil canadien des normes a pour mandat de promouvoir la normalisation volontaire au Canada, où la normalisation n'est pas expressément prévue par la loi.

2.5 Infrastructure de soutien

L'infrastructure de soutien est l'ensemble de politiques, de règles et de normes opérationnelles et techniques qui constituent les principaux catalyseurs d'un écosystème numérique. Les divers éléments de l'infrastructure de soutien ont établi des règles qui échappent à la portée du CCP. Le CCP ne fait aucune recommandation quant à la composition de l'infrastructure de soutien.

La figure 5 illustre certains éléments (avec des exemples) de ce qui pourrait constituer une infrastructure de soutien.

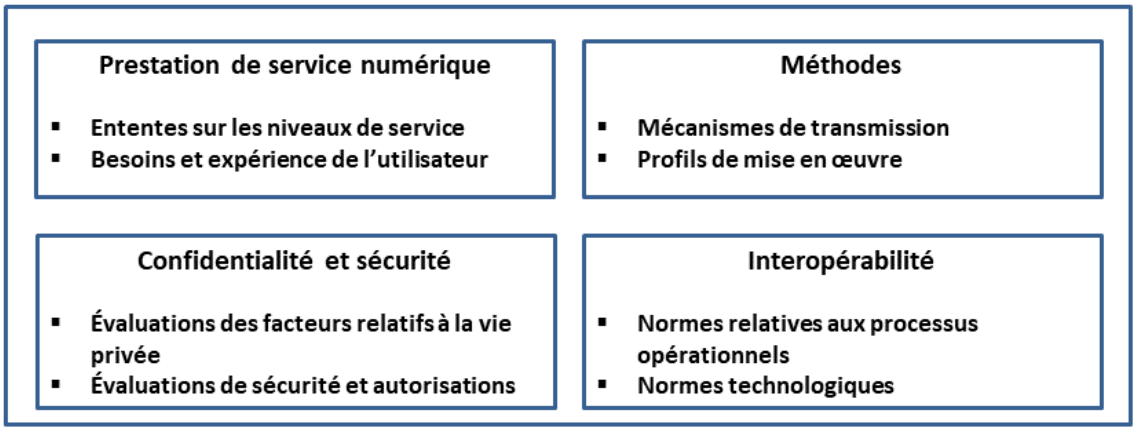

Figure 5 : Infrastructure de soutien

Les sections suivantes fournissent des détails sur deux éléments de l'infrastructure de soutien qui peuvent contribuer à relier les mises en œuvre existantes aux technologies et aux normes plus récentes.

2.5.1 Méthodes

Les méthodes englobent les ensembles de règles qui régissent des choses comme les modèles de données, les protocoles de communication, les algorithmes cryptographiques, les bases de données, les livres distribués, les registres de données vérifiables et les systèmes semblables, de même que leurs combinaisons. Les méthodes comprennent également les systèmes qui sont isolés ou ont une connectivité intermittente. Dans le contexte de l'écosystème numérique, les méthodes permettent aux acteurs d'interagir directement ou indirectement les uns avec les autres sans que l'une ou l'autre des parties soit liée à une solution ou à une technologie particulière.

2.5.2 Mécanismes de transmission

Les mécanismes de transfert sont les diverses méthodes par lesquelles l'extrant d'un processus atomique est rendu disponible pour être utilisé comme intrant dans un autre processus atomique. Comme on peut le constater dans la figure 6, les mécanismes de transmission se situent entre parties émettrices et destinataires des états d'extrant des processus atomiques.

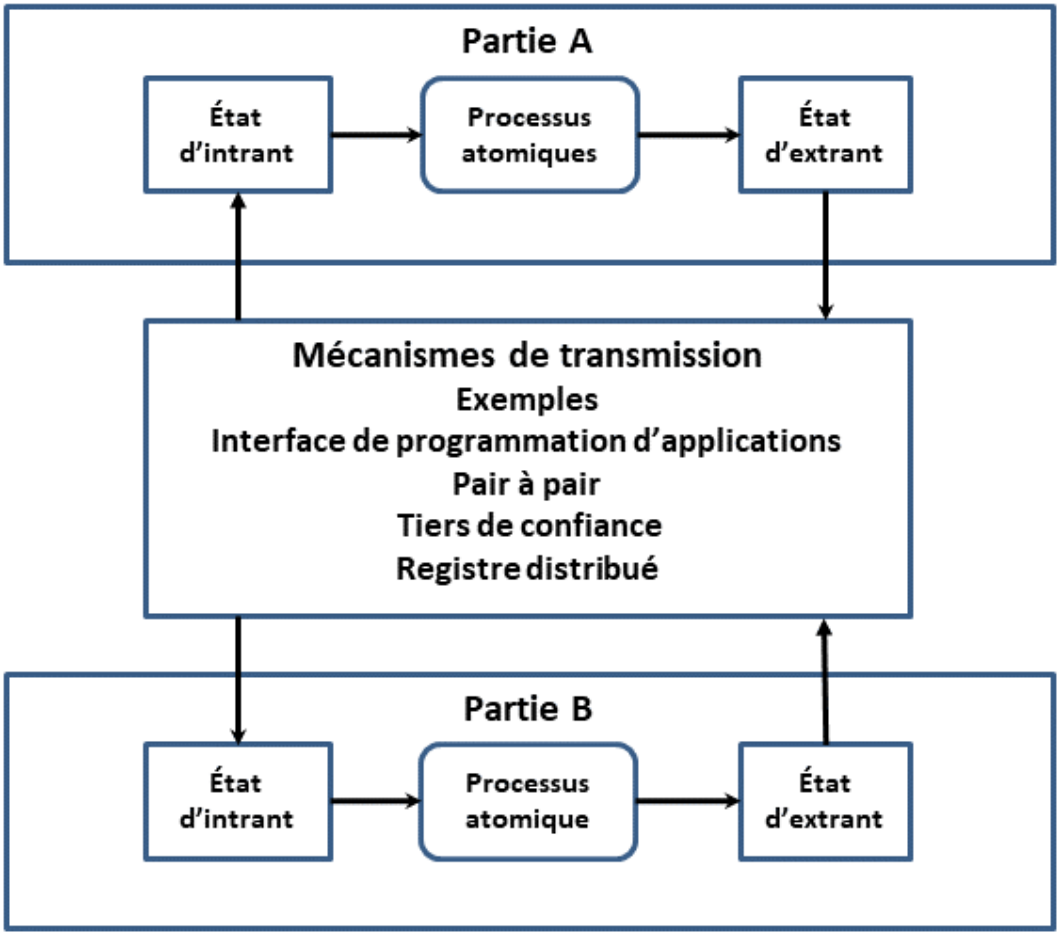

Figure 6 : Transmission d'états d'extrant entre parties

Le CCP ne limite pas la possibilité de recourir à plusieurs fournisseurs concurrents et on s'attend à ce que de nombreux fournisseurs coexistent pour répondre aux besoins en mécanismes de transmission des différentes collectivités dans l'ensemble du secteur public et du secteur privé.

2.6 Rôles et flux d'information de l'écosystème numérique

La figure 7 illustre un modèle conceptuel des rôles et des flux d'information de l'écosystème numérique. (Veuillez noter que les « méthodes » mentionnées dans le diagramme sont analysées dans la section 2.5.1.)

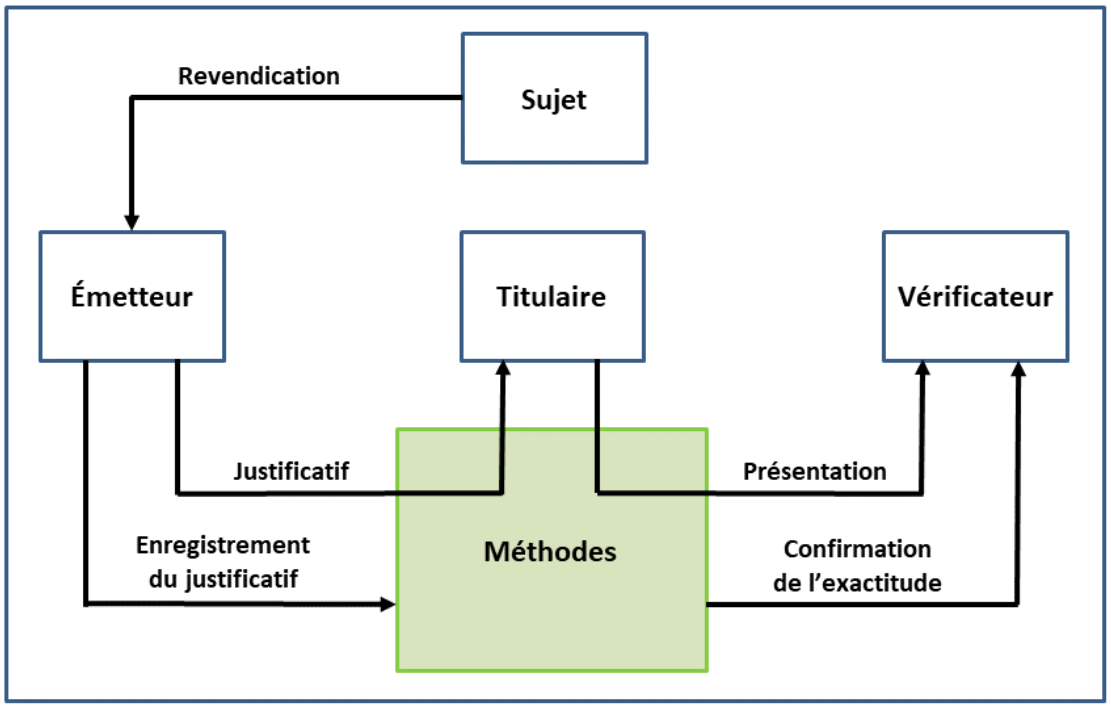

Figure 7 : Rôles et flux d'information de l'écosystème numérique

2.6.1 Rôles

Le modèle comporte quatre rôles :

1. **Sujet** : Entité[8] visée par des ***revendications*** présentées par un ***émetteur***.

[8] Une entité est définie comme une chose ayant une existence distincte et indépendante, comme une personne, une organisation ou un appareil, pouvant être assujettie aux lois, aux politiques ou aux règlements dans un contexte, et pouvant avoir certains droits, devoirs et obligations. Une entité peut jouer un ou plusieurs rôles dans l'écosystème numérique.

2. **Émetteur** : Entité qui présente une ou plusieurs ***revendications*** sur un ou plusieurs ***sujets***, crée un ***justificatif*** à partir de ces revendications et attribue le justificatif à un ***titulaire***.
3. **Titulaire** : Entité qui contrôle un ou plusieurs ***justificatifs*** à partir desquelles une ***présentation*** peut être exprimée à un ***vérificateur***. Un titulaire est habituellement, mais pas toujours, le ***sujet*** d'un justificatif[9].
4. **Vérificateur** : Entité qui accepte une ***présentation*** d'un ***titulaire*** aux fins de prestation de services ou d'administration de programmes.

Les rôles de l'écosystème numérique sont assumés par de nombreuses entités différentes qui remplissent des rôles particuliers sous diverses appellations. Ces rôles particuliers peuvent être classés dans les rôles de l'écosystème numérique, comme le montre le tableau suivant.

Rôle	Exemples
Émetteur	Partie faisant autorité, fournisseur d'assurance de l'identité, fournisseur de services d'assurance de l'identité, fournisseur d'identité, fournisseur d'assurance des justificatifs, fournisseur de services de justificatifs, fournisseur d'authentifiants, fournisseur d'identité numérique, fournisseur de services délégué
Sujet	Personne, organisation, appareil
Titulaire	Propriétaire d'identité numérique, titulaire de carte
Vérificateur	Partie utilisatrice, fournisseur de services de vérification des justificatifs, fournisseur de services d'authentification des justificatifs, fournisseur de services d'authentification, consommateur d'identité numérique, fournisseur de services délégué

Compte tenu de la variété de modèles opérationnels, de services et de technologies qui existent dans l'écosystème numérique, les rôles peuvent être assumés par plusieurs acteurs différents dans un contexte donné, ou encore un acteur peut jouer plusieurs rôles (p. ex., un acteur peut être à la fois une partie utilisatrice et un fournisseur de justificatifs).

[9] Exemples où le titulaire n'est pas le sujet d'un justificatif : un parent (le titulaire) qui détient le certificat de naissance (le justificatif) de son enfant (le sujet); un propriétaire de restaurant (le titulaire) qui détient un permis d'exploitation (le justificatif) d'une entreprise (le sujet).

En plus des quatre rôles décrits ci-dessus, les acteurs de l'écosystème numérique comprennent les fournisseurs d'infrastructure de soutien, comme les exploitants de réseaux.

2.6.2 Flux d'information

Le modèle comprend également cinq flux d'information :

1. **Revendication** : Une déclaration sur un ***sujet***.
2. **Justificatif** : Un ensemble d'une ou de plusieurs ***revendications*** présentées à propos d'un ou de plusieurs sujets[10].
3. **Présentation** : Renseignements tirés d'un ou de plusieurs ***justificatifs***. Les données d'une présentation portent souvent sur le même ***sujet***, mais les justificatifs auraient pu être émis par différents ***émetteurs***.
4. **Enregistrement de justificatif** : Une indication[11] de l'existence d'un justificatif.
5. **Confirmation de l'exactitude[12]** : Une indication de l'exactitude de la ***présentation*** elle-même et de l'exactitude des renseignements associés à la ***présentation***.

[10] Un certificat de mariage est un exemple d'un justificatif ayant plus d'un sujet.

[11] L'indication peut être un schéma de justificatif ou le justificatif lui-même.

[12] La confirmation de l'exactitude est souvent obtenue en reliant un vérificateur à un émetteur au moyen d'un système entre pairs ou d'un système intermédiaire.

2.7 Processus atomiques en détail

2.7.1 Détermination des renseignements sur l'identité

Description du processus	Le processus de détermination des renseignements sur l'identité consiste à déterminer le contexte de l'identité[13], les exigences en matière de renseignements sur l'identité[14] et l'identificateur[15]. Le processus de détermination des renseignements sur l'identité consiste à déterminer le contexte de l'identité
État d'intrant	**Aucune détermination n'a été faite** : Le contexte de l'identité, les exigences en matière de renseignements sur l'identité et l'identificateur n'ont pas été déterminés.
État d'extrant	**Détermination effectuée** : Le contexte de l'identité, les exigences en matière de renseignements sur l'identité et l'identificateur ont été déterminés.

2.7.2 Détermination de la preuve d'identité

Description du processus	Le processus de détermination de la preuve d'identité consiste à déterminer la preuve d'identité acceptable (matérielle ou électronique).
État d'intrant	**Aucune détermination n'a été faite** : La preuve d'identité acceptable n'a pas été déterminée.
État d'extrant	**Détermination effectuée** : La preuve d'identité acceptable a été déterminée.

[13] Voir la section 4.3 pour en savoir plus.

[14] Voir la section 4.4 pour en savoir plus.

[15] Voir la section 4.4.1 pour en savoir plus.

2.7.3 Résolution de l'identité

Description du processus	La résolution de l'identité est le processus établissant l'unicité d'un sujet à l'intérieur de la population d'un programme ou d'un service au moyen de renseignements sur l'identité. Le programme ou le service en question définit les exigences relatives à la résolution de l'identité, au sens des attributs d'identité; en d'autres mots, il détermine l'ensemble d'attributs d'identité requis pour assurer la résolution de l'identité au sein de la population en question.
État d'intrant	**Renseignements sur l'identité** : Les renseignements sur l'identité peuvent ou non être propre à un seul sujet.
État d'extrant	**Renseignements uniques sur l'identité** : Les renseignements sur l'identité se rapportent uniquement à un seul sujet.

2.7.4 Établissement de l'identité

Description du processus	Le processus d'établissement de l'identité consiste à créer le dossier d'identité d'un sujet appartenant à la population d'un programme ou d'un service, sur lequel peuvent s'appuyer d'autres programmes, services ou activités.
État d'intrant	**Aucun dossier d'identité** : Il n'existe aucun dossier d'identité.
État d'extrant	**Dossier d'identité** : Il existe un dossier d'identité.

2.7.5 Validation des renseignements sur l'identité

Description du processus	Le processus de validation des renseignements consiste à confirmer l'exactitude des renseignements sur l'identité d'un sujet tels qu'établis par l'émetteur.
État d'intrant	**Renseignements sur l'identité non confirmés** : Les renseignements sur l'identité n'ont pas été confirmés auprès de l'émetteur.
État d'extrant	**Renseignements sur l'identité confirmés** : Les renseignements sur l'identité ont été confirmés auprès de l'émetteur.

2.7.6 Vérification de l'identité

Description du processus	Le processus de vérification de l'identité consiste à confirmer que les renseignements sur l'identité sont subordonnés au contrôle du sujet. Il convient de noter que ce processus peut s'appuyer sur des renseignements personnels ou organisationnels qui ne relèvent pas de l'identité.
État d'intrant	**Contrôle non vérifié** : Il n'est pas confirmé que les renseignements sur l'identité sont subordonnés au contrôle du sujet.
État d'extrant	**Contrôle vérifié** : Il est confirmé que les renseignements sur l'identité sont subordonnés au contrôle du sujet.

2.7.7 Validation de la preuve d'identité

Description du processus	Le processus de validation de la preuve d'identité consiste à confirmer que la preuve d'identité présentée (qu'elle soit matérielle ou électronique) est acceptable.
État d'intrant	**Preuve d'identité non confirmée** : La preuve d'identité n'a pas été confirmée comme étant acceptable.
État d'extrant	**Preuve d'identité confirmée** : La preuve d'identité a été confirmée comme étant acceptable.

2.7.8 Continuité de l'identité

Description du processus	Le processus de continuité de l'identité consiste à confirmer dynamiquement que le sujet a une existence continue au fil du temps (c.-à-d. une « présence authentique »). Ce processus peut être utilisé afin de veiller à ce qu'aucune activité frauduleuse ou malveillante n'ait été effectuée (dans le présent ou par le passé).
État d'intrant	**Présence périodique** : L'identité existe seulement de façon sporadique et souvent uniquement en association avec un événement vital ou d'une entreprise (p. ex., naissance, décès, faillite).
État d'extrant	**Présence continue** : L'identité existe de façon permanente en association avec de nombreuses transactions.

2.7.9 Maintien de l'identité

Description du processus	Le processus de maintien de l'identité consiste à s'assurer que les renseignements sur l'identité d'un sujet sont exacts, complets et à jour.
État d'intrant	**Renseignements sur l'identité** : Les renseignements sur l'identité ne sont pas à jour.
État d'extrant	**Renseignements sur l'identité à jour** : Les renseignements sur l'identité sont à jour.

2.7.10 Établissement de liens pour déterminer l'identité

Description du processus	L'établissement de liens pour déterminer l'identité est le processus de mise en correspondance entre deux identifiants ou plus et le même sujet.
État d'intrant	**Identifiant non lié** : L'identifiant n'est pas associé à un autre identifiant du même sujet.
État d'extrant	**Identifiant lié** : L'identifiant est associé à un ou plusieurs autres identifiants du même sujet.

2.7.11 Liaison justificatif-identité

Description du processus	Le processus de liaison justificatif-identité consiste à présenter une ou plusieurs revendications concernant un ou plusieurs sujets.
État d'intrant	**Aucune revendication** : Il n'existe aucune revendication.
État d'extrant	**Revendication présentée** : Une ou plusieurs revendications présentées ont été associées à un ou plusieurs sujets.

2.7.12 Émission d'un justificatif

Description du processus	Le processus d'émission d'un justificatif consiste à créer un justificatif à partir d'une ensemble de revendications et d'attribuer le justificatif à un titulaire.
État d'intrant	**Revendication présentée** : Une ou plusieurs revendications présentées ont été associées à un ou plusieurs sujets.
État d'extrant	**Justificatif émis** : Un justificatif a été attribué à un titulaire.

2.7.13 Liaison justificatif-authentifiant

Description du processus	Le processus de liaison justificatif-authentifiant consiste à associer un justificatif émis 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 (causée par un mot de passe oublié ou un verrouillage en raison d'authentifications défaillantes successives, 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).
État d'intrant	**Justificatif émis** : Un justificatif a été attribué à un titulaire.
État d'extrant	**Liaison authentifiant-justificatif** : Un justificatif émis a été associé à un ou plusieurs authentifiants.

2.7.14 Validation des justificatifs

Description du processus	Le processus de validation des justificatifs consiste à confirmer la validité du justificatif émis (p. ex., non violé, corrompu, modifié, suspendu ou révoqué). La validité du justificatif émis peut servir à générer un certain niveau d'assurance.
État d'intrant	**Liaison authentifiant-justificatif** : Un justificatif émis a été associé à un ou plusieurs authentifiants.
État d'extrant	**Justificatif validé** : Le justificatif émis est valide.

2.7.15 Vérification des justificatifs

Description du processus	Le processus de vérification des justificatifs consiste à confirmer qu'un titulaire exerce un contrôle sur un justificatif émis. Le contrôle d'un justificatif émis est vérifié par un ou plusieurs authentifiants. Le degré de contrôle sur le justificatif émis peut servir à générer un certain niveau d'assurance.
État d'intrant	**Liaison authentifiant-justificatif** : Un justificatif émis a été associé à un ou plusieurs authentifiants.
État d'extrant	**Justificatif vérifié** : Le titulaire a prouvé qu'il contrôle le justificatif émis.

2.7.16 Maintien du justificatif

Description du processus	Le processus de maintien du justificatif consiste à mettre à jour les attributs (p. ex., date d'expiration, portée du service, autorisations) d'un justificatif émis.
État d'intrant	**Justificatif émis** : Un justificatif a été attribué à un titulaire.
État d'extrant	**Justificatif émis à jour** : Le justificatif émis a été mis à jour.

2.7.17 Suspension d'un justificatif

Description du processus	La suspension d'un justificatif est un processus qui consiste à transformer un justificatif émis en un justificatif suspendu en marquant le justificatif émis comme temporairement inutilisable.
État d'intrant	**Justificatif émis** : Un justificatif a été attribué à un titulaire.
État d'extrant	**Justificatif suspendu** : Le titulaire n'est pas en mesure d'utiliser le justificatif.

2.7.18 Recouvrement d'un justificatif

Description du processus	Le recouvrement d'un justificatif est un processus qui consiste à transformer à nouveau un justificatif suspendu en justificatif utilisable (c.-à-d. un justificatif utilisable).
État d'intrant	**Justificatif suspendu** : Le titulaire n'est pas en mesure d'utiliser le justificatif.
État d'extrant	**Justificatif émis à jour** : Le justificatif émis a été mis à jour.

2.7.19 Révocation d'un justificatif

Description du processus	La révocation d'un justificatif est le processus permettant de garantir qu'un justificatif émis est en permanence marqué comme inutilisable.
État d'intrant	**Justificatif émis** : Un justificatif a été attribué à un titulaire.
État d'extrant	**Justificatif révoqué :** Le titulaire n'est pas en mesure d'utiliser le justificatif.

2.7.20 Formulation d'avis

Description du processus	La formulation d'avis est le processus consistant à produire un énoncé d'avis décrivant les renseignements personnels qui sont recueillis ou qui peuvent l'être; les parties auxquelles les renseignements personnels sont transmis, et le type de renseignements personnels transmis (tels qu'ils sont connus 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; et la personne ou l'entité ayant compétence ou autorité pour l'énoncé d'avis émis. Ce processus devrait être mené conformément aux exigences des lois et des règlements applicables.
État d'intrant	**Aucun énoncé d'avis** : Aucun énoncé d'avis n'existe.
État d'extrant	**Énoncé d'avis** : Un énoncé d'avis existe.

2.7.21 Présentation de l'avis

Description du processus	Le processus de présentation de l'avis consiste à présenter un avis à une personne.
État d'intrant	**Énoncé d'avis** : Un énoncé d'avis existe.
État d'extrant	**Énoncé d'avis présenté :** Un énoncé d'avis a été présenté à une personne.

2.7.22 Demande de consentement

Description du processus	Le processus de demande de consentement consiste à demander à une personne de donner son consentement (« Oui ») ou de refuser de donner son consentement (« Non ») en fonction du contenu de l'énoncé d'avis présenté, ce qui entraîne une décision de consentement par « oui » ou par « non ».
État d'intrant	**Énoncé d'avis présenté** : Un énoncé d'avis a été présenté à une personne.
État d'extrant	**Décision de consentement** : Une décision de consentement existe.

2.7.23 Enregistrement du consentement

Description du processus	Le processus d'enregistrement du consentement consiste à stocker de manière persistante un énoncé d'avis et la décision de consentement connexe de la personne. Plus d'information peut également être stockée. Par exemple : des renseignements sur la personne, la version de l'avis qui lui a été présentée, la date et l'heure à laquelle l'avis a été présenté et, le cas échéant, la date d'expiration relative à la décision de consentement. Une fois les renseignements relatifs au consentement stockés, une notification sur la décision de consentement prise par le sujet est envoyée aux parties concernées.
État d'intrant	**Décision de consentement** : Une décision de consentement existe.
État d'extrant	**Décision de consentement stockée :** Une décision de consentement stockée existe.

2.7.24 Examen du consentement

Description du processus	Le processus d'examen du consentement consiste à rendre les détails d'une décision de consentement stockée visibles pour le personne qui a donné le consentement.
État d'intrant	**Décision de consentement stockée** : Une décision de consentement stockée existe.
État d'extrant	**Décision de consentement stockée** : Une décision de consentement stockée existe.

2.7.25 Renouvellement du consentement

Description du processus	Le processus de renouvellement du consentement consiste à prolonger la validité d'une décision de consentement par « oui » en reportant la date d'expiration.
État d'intrant	**Décision de consentement stockée** : Une décision de consentement stockée existe.
État d'extrant	**Décision de consentement mise à jour** : Une décision de consentement stockée a été mise à jour.

2.7.26 Expiration du consentement

Description du processus	Le processus d'expiration du consentement consiste à suspendre la validité d'une décision de consentement par un « oui » en raison d'une date d'expiration dépassée.
État d'intrant	**Décision de consentement stockée :** Une décision de consentement stockée existe.
État d'extrant	**Décision de consentement mise à jour** : Une décision de consentement stockée a été mise à jour.

2.7.27 Révocation du consentement

Description du processus	Le processus de révocation du consentement consiste à suspendre la validité d'une décision de consentement par un « oui » à la suite du retrait explicite du consentement par la personne (c'est-à-dire qu'une décision de consentement par un « oui » est convertie en une décision de consentement par un « non »).
État d'intrant	**Décision de consentement stockée :** Une décision de consentement stockée existe.
État d'extrant	**Décision de consentement mise à jour** : Une décision de consentement stockée a été mise à jour.

2.7.28 Création de signature

Description du processus	Le processus de création de signature consiste à créer une signature.
État d'intrant	**Aucune signature** : Aucune signature n'existe.
État d'extrant	**Signature** : Il existe une signature.

2.7.29 Vérification de la signature

Description du processus	Le processus de vérification de la signature consiste à confirmer que la signature est valide.
État d'intrant	**Signature** : Il existe une signature.
État d'extrant	**Signature vérifiée** : La signature est valide.

2.8 Les qualificateurs en détail

2.8.1 Qualificateurs de domaines liés à l'identité

Pour refléter la responsabilité partagée de l'identité entre les administrations dans le contexte pancanadien, deux qualificatifs de domaines liés à l'identité ont été définis :

- **Domaine lié à l'identité principale** : Critères de conformité qui sont reliés à un événement fondamental en particulier (p. ex., naissance, changement de nom légal de la personne, immigration, résidence légale, citoyenneté naturalisée, décès, enregistrement de la dénomination sociale de l'organisation, changement de nom légal de l'organisation ou faillite). Les identités fondamentales relèvent exclusivement du secteur public (plus précisément, les bureaux de l'état civil [BEC] et les registres des entreprises des provinces et des territoires, Immigration, Réfugiés et Citoyenneté Canada [IRCC]; et le registre fédéral des sociétés de Corporations Canada).
- **Domaine lié à l'identité contextuelle** : Critères de conformité propres à un contexte d'identité (p. ex., services bancaires, permis d'exploitation d'entreprise, services de santé, permis de conduire ou médias sociaux). Selon le contexte identitaire, une identité contextuelle peut être reliée à une identité principale (par exemple, un permis de conduire) ou ne pas être reliée à identité principale (par exemple, un profil de médias sociaux). L'identité contextuelle relève à la fois des secteurs public et privé.

2.8.2 Qualificateurs de niveaux d'assurance (NA) à l'échelle pancanadienne

La version actuelle des critères de conformité au CCP utilise les quatre niveaux d'assurance (NA) à l'échelle pancanadienne :

- **Niveau 1 :** Peu ou pas de confiance requise.
- **Niveau 2 :** Un certain niveau de confiance requis.
- **Niveau 3 :** Un niveau élevé de confiance requis.
- **Niveau 4 :** Un niveau très élevé de confiance requis.

2.8.3 Qualificateurs de signatures électroniques sécurisées

La partie 2 de la *Loi fédérale sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) définit une signature électronique comme « une signature constituée d'une ou de plusieurs lettres, ou d'un ou de plusieurs caractères, nombres ou autres symboles sous forme numérique incorporée, jointe ou associée à un document électronique ».

La partie 2 de la LPRPDE aborde certains cas spécifiques à la technologie et exige l'utilisation d'une catégorie particulière de signatures électroniques (appelée ***signature électronique sécurisée***, une expression définie dans le *Règlement sur les signatures électroniques sécurisées* [RSE] annexé). Des signatures électroniques sécurisées peuvent être utilisées comme qualificateurs.

2.8.4 Autres qualificateurs de cadre de confiance

Les qualificateurs peuvent être fondés sur les trois niveaux d'assurance définis par le Règlement européen nº 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques :

- **Faible :** Faible degré de confiance.
- **Important :** Degré de confiance important.
- **Élevé :** Degré de confiance élevé.

Les qualificateurs peuvent être fondés sur les niveaux d'assurance définis dans les *directives sur l'identité numérique énoncées dans la publication spéciale 800-63* de la NIST :

- **Niveau d'assurance de l'identité :** Désigne le niveau de vérification de l'identité.
- **Niveau d'assurance de l'authentification :** Fait référence au processus d'authentification.
- **Niveau d'assurance de la fédération** : Désigne la force d'une affirmation dans un environnement fédérée, utilisée pour communiquer les renseignements liés à l'authentification et aux attributs (le cas échéant) à une partie utilisatrice.

3 ANNEXE A : TERMES ET DÉFINITIONS

Les définitions qui suivent sont des définitions qui font autorité, tirées de la Norme sur l'assurance de l'identité et des justificatifs, des définitions provenant de lignes directrices et de documents de référence de l'industrie ainsi que des définitions créées par le Groupe de travail pour les besoins de ce document.

Terme	Définition
appareil	Une machine, en particulier du matériel électronique.
assurance	Confiance qu'une déclaration est véridique.
assurance de l'identité	La confiance qu'une personne, une organisation ou un appareil est bel et bien la personne, l'organisation ou l'appareil qu'il ou elle prétend être.
assurance du justificatif	La confiance qu'un titulaire a maintenu le contrôle d'un justificatif émis et que ce justificatif est valide.
attribut	Propriété ou caractéristique associée à une entité. Voir également « attribut d'identité ».
attribut d'identité	Une propriété ou une caractéristique associée à une personne, une organisation, ou un appareil identifiable (également appelé « élément de donnée sur l'identité »).
authentifiant	Élément qu'un titulaire contrôle (p. ex., un module cryptographique ou un mot de passe) et qui sert à prouver que le titulaire a conservé le contrôle d'un justificatif émis.
authentification	Voir « vérification des justificatifs ».
biométrique	Terme général utilisé pour décrire une caractéristique ou un processus. Il s'agit d'une caractéristique biologique (anatomique et physiologique) ou comportementale mesurable, qui peut être utile à la reconnaissance automatisée. « Biométrique » peut aussi désigner des méthodes automatisées de reconnaissance des personnes fondées sur des caractéristiques biologiques (anatomiques et physiologiques) ou comportementales mesurables.

Terme	Définition
cadre de confiance	Un ensemble de principes, de définitions, de normes, de spécifications, de critères de conformité et d'approche d'évaluation dont on convient.
CANAFE	Centre d'analyse des opérations et déclarations financières du Canada Le CANAFE est l'unité canadienne du renseignement financier. Il a pour mandat de faciliter la détection, la prévention et la dissuasion du blanchiment d'argent et du financement des activités terroristes.
client	Le destinataire prévu d'un extrant de service. Les clients externes sont généralement des personnes (citoyens canadiens, résidents permanents, etc.) ou des entreprises (organisations des secteurs public et privé). Les clients internes sont généralement des employés et des entrepreneurs.
CNUDCI	Commission des Nations Unies sur le droit commercial international Le mandat de la CNUDCI est de promouvoir l'harmonisation et l'unification progressives du droit commercial international au moyen de conventions, de lois types et d'autres instruments qui traitent de domaines clés du commerce, englobant le règlement des différends, l'approvisionnement et la vente de biens.
confirmation de l'exactitude	Une indication de l'exactitude de la présentation elle-même et de l'exactitude de l'information associée à la présentation.
confirmation de possession matérielle	Une méthode de vérification de l'identité qui exige la possession ou la présentation d'éléments de preuve pour prouver que la personne ou l'organisation qui présente les renseignements sur l'identité contrôle l'identité.

Terme	Définition
confirmation des caractéristiques biologiques ou comportementales	Une méthode de vérification de l'identité qui utilise des caractéristiques biologiques (anatomiques et physiologiques) (p. ex., visage, empreintes digitales, rétines) ou des caractéristiques comportementales (p. ex., rythme de frappe au clavier, démarche) pour prouver que la personne qui présente les renseignements sur l'identité contrôle l'identité. 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 à la personne qui présente les renseignements sur l'identité.
confirmation fondée sur les connaissances	Une méthode de vérification de l'identité qui utilise des renseignements personnels ou organisationnels ou des secrets partagés pour prouver que la personne ou l'organisation qui présente les renseignements sur l'identité contrôle l'identité. La confirmation fondée sur les connaissances est obtenue au moyen du modèle de défi-réponse : on pose des questions à la personne ou à l'organisme qui présente les renseignements sur l'identité, dont les réponses ne sont connues (du moins en théorie) que de la personne et de son interrogateur (p. ex., renseignements financiers, antécédents en matière de crédit, secret partagé, code d'accès expédié par la poste, mot de passe, numéro d'identification personnel, identificateur attribué).
confirmation par un arbitre de confiance	Une méthode de vérification de l'identité qui fait appel à un répondant de confiance pour prouver que la personne ou l'organisation qui présente les renseignements sur l'identité contrôle l'identité. Le type d'arbitre de confiance et l'acceptabilité de l'arbitre sont déterminés par des critères propres au programme. Les garants, notaires, comptables et agents accrédités sont des exemples d'arbitres de confiance.
contexte de l'identité	L'environnement ou l'ensemble de circonstances où une organisation fonctionne et où elle exécute ses programmes et ses services. Le contexte de l'identité est

Terme	Définition
	déterminé par des facteurs comme le mandat, la population cible (c.-à-d. les clients, la clientèle), et les autres responsabilités établies en vertu d'une loi, d'un accord ou d'une entente.
continuité de l'identité	Le processus qui consiste à confirmer dynamiquement que le sujet a une existence continue au fil du temps (c.-à-d. une « présence authentique »). Ce processus peut être utilisé afin de veiller à ce qu'aucune activité frauduleuse ou malveillante n'ait été effectuée (dans le présent ou par le passé).
création de signature	Le processus qui consiste à créer une signature.
critères de conformité	Un ensemble d'énoncés d'exigences définissant ce qu'il faut pour assurer l'intégrité d'un processus atomique.
demande de consentement	Le processus consistant à demander à une personne de donner son consentement (« Oui ») ou de refuser de donner son consentement (« Non ») en fonction du contenu de l'énoncé d'avis présenté, ce qui entraîne une décision de consentement par « oui » ou par « non ».
détermination de la preuve d'identité	Le processus de détermination de la preuve d'identité consiste à déterminer la preuve d'identité acceptable (matérielle ou électronique).
détermination des renseignements sur l'identité	Le processus qui consiste à déterminer le contexte de l'identité, les exigences en matière de renseignements sur l'identité et l'identificateur.
écosystème numérique	Un 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	Identification électronique et services de confiance pour les transactions électroniques (eIDAS) eIDAS 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 réglemente les signatures électroniques, les transactions électroniques, les organismes concernés et leurs

Terme	Définition
	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 sur l'identité	Voir « attribut d'identité ».
émetteur	Une entité qui présente une ou plusieurs revendications sur un ou plusieurs sujets, crée un justificatif à partir de ces revendications et attribue le justificatif à un titulaire.
émission d'un justificatif	Le processus consistant à créer un justificatif à partir d'un ensemble de revendications et d'attribuer le justificatif à un titulaire.
enregistrement du consentement	Le processus consistant à stocker de manière persistante un énoncé d'avis et la décision de consentement connexe de la personne. De plus, les renseignements sur la personne, la version de l'avis qui a été présenté, la date et l'heure de la présentation de l'avis et, le cas échéant, la date d'expiration de la décision de consentement peuvent être stockés. Une fois les renseignements relatifs au consentement stockés, une notification sur la décision de consentement prise par le sujet est envoyée aux parties concernées.
enregistrement du justificatif	Enregistrement de justificatif : Une indication de l'existence d'un justificatif.
entité	Une chose ayant une existence distincte et indépendante, comme une personne, une organisation ou un appareil, qui peut être assujettie aux lois, aux politiques ou aux règlements dans un contexte, et pouvant avoir certains droits, devoirs et obligations. Une entité peut jouer un ou plusieurs rôles dans l'écosystème numérique.
établissement de l'identité	Le processus qui consiste à créer le dossier d'identité d'un sujet appartenant à la population d'un programme ou d'un service, sur lequel peuvent s'appuyer d'autres programmes, services ou activités.

Terme	Définition
établissement de liens pour déterminer l'identité	Le processus de mise en correspondance entre deux identifiants ou plus et le même sujet.
événement d'entreprise	Un événement important se produisant durant la vie d'une entreprise. En vertu de la loi, un événement d'entreprise doit être enregistré auprès d'une entité gouvernementale et est assujetti à la loi et aux règlements. Parmi les événements d'entreprise, on peut citer l'enregistrement de la charte, la fusion, le regroupement, l'abandon de charte, et la dissolution.
événement fondamental	Un événement fondamental est soit un événement d'entreprise, soit un événement vital. Les événements d'entreprise et les événements vitaux sont des épisodes distincts importants qui se produisent dans la vie des entreprises et des personnes, respectivement. En vertu de la loi, les événements d'entreprise et les événements vitaux doivent être enregistrés auprès d'une entité gouvernementale et sont assujettis à la législation et à la réglementation. Voir « événement d'entreprise » et « événement vital ».
événement vital	Un épisode discret important qui se produit durant la vie d'une personne. En vertu de la loi, un événement vital doit être enregistré auprès d'une entité gouvernementale et est assujetti à la législation et à la réglementation. Des exemples d'événements vitaux sont la naissance vivante, l'accouchement d'un mort-né, l'adoption, la légitimation, la reconnaissance de la parentalité, l'immigration, la résidence légale, la citoyenneté naturalisée, le changement de nom, le mariage, l'annulation du mariage, la séparation légale, le divorce et la mort.
examen du consentement	Le processus consistant à rendre les détails d'une décision de consentement stockée visibles pour la personne qui a donné le consentement.
expiration du consentement	Le processus consistant à suspendre la validité d'une décision de consentement par un « oui » en raison d'une date d'expiration dépassée.

Terme	Définition
formulation d'avis	Le processus consistant à produire un énoncé d'avis décrivant les renseignements personnels qui sont recueillis ou qui peuvent l'être; les parties auxquelles les renseignements personnels sont transmis, et le type de renseignements personnels transmis (tels qu'ils sont connus 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; et la personne ou l'entité ayant compétence ou autorité pour l'énoncé d'avis émis. Ce processus devrait être mené conformément aux exigences des lois et des règlements applicables.
GAFI	Groupe d'action financière Le GAFI 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	Désigne une identité sociale, comme le fait d'être un homme, une femme, une personne non binaire ou une personne bispirituelle.
gestion de l'identité	L'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	L'ensemble d'attributs d'identité qui sont utilisés uniquement pour distinguer une personne, une organisation ou un appareil en particulier dans une population.
identificateur attribué	Chaîne numérique ou alphanumérique automatiquement générée et permettant de faire la

Terme	Définition
	distinction entre des personnes ou des organisations sans recourir à un autre attribut d'identité.
identité	Une référence ou une désignation unique utilisée pour distinguer une personne, organisation, ou un dispositif particulier. Il existe deux types d'identité : principale et contextuelle. Voir « identité principale » et « identité contextuelle ».
Identité contextuelle	Une identité utilisée à des fins précises dans un contexte d'identité précis (p. ex., services bancaires, permis d'exploitation d'entreprise, services de santé, permis de conduire ou médias sociaux). Selon le contexte identitaire, une identité contextuelle peut être reliée à une identité principale (par exemple, un permis de conduire) ou ne pas être reliée à identité principale (par exemple, un profil de médias sociaux.
identité numérique	Une représentation électronique d'une entité, utilisée exclusivement par cette même entité, permettant d'accéder à des services et d'exécuter des opérations en toute confiance et confidentialité.
identité principale	Une 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).
infrastructure de soutien	L'ensemble de politiques, de règles et de normes opérationnelles et techniques qui constituent les principaux catalyseurs d'un écosystème numérique.
justificatif	Un ensemble d'une ou de plusieurs revendications présentées à propos d'un ou de plusieurs sujets.
justificatif anonyme	Justificatif qui, tout en faisant une affirmation au sujet d'un bien, d'un statut ou d'un droit d'une personne, ne révèle pas son identité. Un justificatif peut comprendre des attributs d'identité, mais être toujours considéré comme un justificatif anonyme si les attributs d'identité ne sont pas reconnus ou utilisés aux fins de validation

Terme	Définition
	des renseignements sur l'identité. Les justificatifs anonymes permettent aux personnes de prouver des affirmations à leur sujet et au sujet de leurs relations avec d'autres personnes ou organisations tout en maintenant leur anonymat.
liaison justificatif-authentifiant	Le processus qui consiste à associer un justificatif émis à un titulaire à un ou plusieurs authentifiants. Ce processus comprend également des activités liées au cycle de vie de l'authentifiant, telles que la suspension des authentifiants (causée par un mot de passe oublié ou un verrouillage en raison d'authentifications défaillantes successives, 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.
liaison justificatif-identité	Le processus consistant à présenter une ou plusieurs revendications concernant un ou plusieurs sujets.
maintien de l'identité	Le processus qui consiste à s'assurer que les renseignements sur l'identité d'un sujet sont exacts, complets et à jour.
maintien du justificatif	Le processus consistant à mettre à jour les attributs (p. ex., date d'expiration, portée du service, autorisations) d'un justificatif émis.
méthodes	Les ensembles de règles qui régissent des choses comme les modèles de données, les protocoles de communication, les algorithmes cryptographiques, les livres distribués, les bases de données et les systèmes semblables, de même que leurs combinaisons.
modèle d'identité	Une représentation simplifiée (ou abstraite) d'une méthodologie de gestion de l'identité (aussi appelée « schéma d'identité »). Les modèles d'identité centralisés, fédérés et décentralisés en sont des exemples.

Terme	Définition
NIST	National Institute of Standards and Technology Le NIST 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, des normes et des technologies de la mesure.
niveau d'assurance	Niveau de confiance qu'une déclaration est véridique et que d'autres peuvent s'y fier.
niveau d'assurance de l'identité	Le niveau de confiance qu'une personne, une organisation ou un appareil est bel et bien la personne, l'organisation ou l'appareil qu'il ou elle prétend être.
niveau d'assurance du justificatif	Le niveau de confiance qu'un titulaire a maintenu le contrôle d'un justificatif émis et que ce justificatif est valide.
nom fondamental	Le nom d'une personne ou d'une organisation tel qu'il est indiqué dans un dossier officiel identifiant la personne ou l'organisation (p. ex., dossier de statistiques d'état civil provincial ou territorial, dossier d'immigration fédéral, dossiers du registre fédéral des sociétés).
nom légal	Voir « nom fondamental », « nom principal ».
nom principal	Le nom qu'une personne ou une organisation utilise à des fins officielles et légales (aussi appelé « nom légal »). Voir aussi « nom fondamental ».

Terme	Définition
notification des renseignements sur l'identité	La divulgation de renseignements sur l'identité sur une personne ou une organisation par une partie faisant autorité à une partie utilisatrice et qui est déclenchée par un événement vital ou un événement d'entreprise, un changement aux renseignements sur l'identité, ou une indication que ses renseignements sur l'identité ont été exposés à un facteur de risque (p. ex., le décès de la personne, une renonciation à la charte, l'utilisation de documents expirés, une atteinte à la vie privée, une utilisation frauduleuse des renseignements sur l'identité).
organisation	Une personne juridique qui n'est pas un être humain (en termes juridiques, une « personne juridique »).
personne	Un être humain (en termes juridiques, une « personne physique »), y compris les « mineurs » et d'autres personnes qui pourraient ne pas être considérées comme des personnes en vertu de la loi.
prénom d'usage	Le prénom par lequel une personne préfère être adressée de façon informelle.
présence légale	Le droit légal de se trouver ou de résider au Canada.
présentation	Renseignements tirés d'un ou de plusieurs justificatifs. Les données d'une présentation portent souvent sur le même sujet, mais les justificatifs auraient pu être émis par différents émetteurs.
présentation de l'avis	Le processus qui consiste à présenter un avis à une personne.
preuve d'identité	Un registre d'une source faisant autorité indiquant l'identité d'une entité. Il existe deux catégories de preuve d'identité : principal et contextuel. Voir « preuve d'identité principale » et « preuve d'identité contextuelle ».
preuve d'identité contextuelle	Une preuve d'identité qui corrobore la preuve d'identité principale et aide à relier les renseignements sur l'identité à une personne. Elle peut également fournir des renseignements supplémentaires comme une

Terme	Définition
	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; et les dossiers de mariage, de changement de nom ou de décès provenant d'une autorité compétente. Une preuve d'identité qui corrobore la preuve d'identité principale et aide à relier les renseignements sur l'identité à une personne ou 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 principale	Une preuve établissant les principaux renseignements liés à l'identité sur 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 d'une autorité compétente. Une preuve établissant les principaux renseignements liés à l'identité sur 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 électronique ou numérique	Toute donnée enregistrée ou préservée sur n'importe quel support, par un système informatique ou tout autre appareil semblable. Par exemple, les dossiers de base de données, les journaux d'audit et les documents électroniques de traitement de texte.
processus atomique	Ensemble d'activités logiquement mis en correspondance qui entraîne un état de transition d'un objet. D'autres processus atomiques peuvent se fier à l'état d'extrant de l'objet.

Terme	Définition
processus composé	Un ensemble de processus atomiques et/ou d'autres processus composés qui entraînent un ensemble de transitions d'état.
recouvrement d'un justificatif	Le processus consistant à transformer à nouveau un justificatif suspendu en justificatif utilisable (c.-à-d. un justificatif utilisable).
récupération des renseignements sur l'identité	La divulgation de renseignements sur l'identité sur une personne ou une organisation par une partie faisant autorité à une partie utilisatrice et qui est déclenchée par une demande faite par la partie utilisatrice.
registre fondamental	Un 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 BEC et Immigration, Réfugiés et Citoyenneté Canada [fédéral]). Un 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]).
relation numérique	Une représentation électronique de la relation entre une entité et une autre entité.
renouvellement du consentement	Le processus consistant à prolonger la validité d'une décision de consentement par « oui » en reportant la date d'expiration.
renseignements organisationnels	Renseignements sur une organisation identifiable.
renseignements personnels	Renseignements sur une personne identifiable.
renseignements sur l'identité	L'ensemble d'attributs d'identité qui est suffisant pour distinguer une entité de toutes les autres entités au sein d'une population de programmes ou de services et qui est suffisant pour décrire l'entité comme l'exige le programme ou le service. Selon le contexte, les

Terme	Définition
	renseignements sur l'identité constituent soit un sous-ensemble de renseignements personnels, soit un sous-ensemble de renseignements organisationnels.
représentation numérique	Une représentation électronique d'une entité ou une représentation électronique de la relation entre deux entités.
résolution de l'identité	Le processus établissant l'unicité d'un sujet à l'intérieur de la population d'un programme ou d'un service au moyen de renseignements sur l'identité.
revendication	Une déclaration sur un sujet.
révocation d'un justificatif	Le processus permettant de garantir qu'un justificatif émis est en permanence marqué comme inutilisable.
révocation du consentement	Le processus consistant à suspendre la validité d'une décision de consentement par un « oui » à la suite du retrait explicite du consentement par la personne (c'est-à-dire qu'une décision de consentement par un « oui » est convertie en une décision de consentement par un « non »).
schéma d'identité	Voir « modèle d'identité ».
sexe	Renvoie aux caractéristiques biologiques, comme le fait d'être de sexe masculin ou féminin, ou intersexuel.
signature	Une 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 communiquée; et l'intégrité des données de la transaction signée est maintenue, y compris l'original.
source faisant autorité	Un ensemble ou un registre de dossiers conservés par une autorité qui respecte les critères établis.
sujet	Une entité visée par des revendications présentées par un émetteur.

Terme	Définition
suspension d'un justificatif	Le processus qui consiste à transformer un justificatif émis en un justificatif suspendu en marquant le justificatif émis comme temporairement inutilisable.
titulaire	Une entité qui contrôle un ou plusieurs justificatifs à partir desquelles une présentation peut être exprimée à un vérificateur. Un titulaire est habituellement, mais pas toujours, le sujet d'un justificatif.
validation de la preuve d'identité	Le processus qui consiste à confirmer que la preuve d'identité présentée (qu'elle soit matérielle ou électronique) est acceptable.
validation des justificatifs	Le processus qui consiste à confirmer la validité du justificatif émis (p. ex., non violé, corrompu, modifié, suspendu ou révoqué). La validité du justificatif émis peut servir à générer un certain niveau d'assurance.
validation des renseignements sur l'identité	Le processus qui consiste à confirmer l'exactitude des renseignements sur l'identité d'un sujet tels qu'établis par l'émetteur.
vérificateur	Une entité qui accepte une présentation d'un titulaire aux fins de prestation de services ou d'administration de programmes.
vérification de l'identité	Le processus qui consiste à confirmer que les renseignements sur l'identité sont subordonnés au contrôle du sujet. Il convient de noter que ce processus peut s'appuyer sur des renseignements personnels ou organisationnels qui ne relèvent pas de l'identité.
vérification de la signature	Le processus qui consiste à confirmer que la signature est valide.
vérification des justificatifs	Le processus qui consiste à confirmer qu'un titulaire exerce un contrôle sur un justificatif émis. Le contrôle d'un justificatif émis est vérifié par un ou plusieurs authentifiants. Le degré de contrôle sur le justificatif émis peut servir à générer un certain niveau d'assurance.

4 ANNEXE B : APERÇU DE LA GESTION DE L'IDENTITÉ

La présente annexe fait le survol général d'aspects particuliers de la gestion d'identité. Des renseignements supplémentaires sont disponibles dans la *Ligne directrice sur l'assurance de l'identité* [SCT, 2015].

4.1 Identité

4.1.1 Identité réelle

> [Traduction] « L'identité est la façon dont nous reconnaissons des personnes et des choses données, dont nous nous souvenons d'elles et dont nous y réagissons en fin de compte [...] Elle nous aide à reconnaître nos amis et nos familles, et à distinguer les menaces; elle nous permet de nous souvenir des anniversaires, des préférences et des histoires; elle nous donne la capacité de répondre à chaque individu en tant que personne unique.
>
> [...] Nos identités sont plus larges que nos incarnations numériques. Nos identités existaient avant elles, et elles continuent d'exister en toute indépendance. Les identités numériques sont simplement des outils permettant aux personnes et aux organisations de mieux gérer leur identité réelle. »
>
> – *A Primer on Functional Identity*, par Joe Andrieu[16]

4.1.2 L'identité dans la gestion de l'identité

L'identité, dans le domaine de la gestion de l'identité, renvoie à une notion beaucoup plus étroite que celle que l'on trouve dans le monde réel. Dans le domaine de la gestion de l'identité, l'identité est définie comme une référence ou une désignation unique utilisée pour distinguer une personne, organisation, ou un dispositif particulier.

Une identité doit être unique[17]. Cela signifie que chaque personne et chaque organisation peuvent être distinguées de toutes les autres personnes et organisations et qu'au besoin, chaque personne et chaque organisation peuvent être identifiées de façon unique. L'exigence d'unicité permet de s'assurer qu'un programme ou un service peut être offert à une personne ou à une organisation en particulier et qu'un programme ou un service est offert à la bonne personne ou à la bonne organisation.

[16] Le texte intégral de cet article est disponible à : http://bit.ly/FunctionalIdentityPrimer.

[17] Il s'agit d'une des exigences à respecter pour établir le niveau d'assurance de l'identité. Voir l'annexe C de la *Norme sur l'assurance de l'identité et des justificatifs* (SCT, 2013).

4.2 Définir la population

Dans le contexte canadien, l'univers des personnes est défini comme tous les citoyens et résidents du Canada (y compris les personnes décédées) pour qui une identité a été établie au Canada. L'univers des organisations est défini comme toutes les organisations enregistrées et en activité au Canada (y compris les organisations inactives) dont une identité a été établie au Canada. Les personnes ou les organisations visées par un programme ou un service constituent la population du programme ou du service[18].

Voici quelques exemples de populations visées par des programmes et des services du secteur public canadien :

- les personnes nées en Alberta;
- les personnes qui doivent remplir une déclaration de revenus destinée au gouvernement fédéral;
- les personnes qui sont autorisées à conduire un véhicule au Québec;
- les personnes qui sont des anciens combattants;
- les personnes qui sont assurées par le régime d'assurance-santé de l'Ontario;
- les organisations autorisées à cultiver du cannabis au Canada;
- les organisations tenues de s'enregistrer auprès de CANAFE;
- les organisations autorisées à couper du bois en Colombie-Britannique;
- les organisations assujetties à la surveillance du Bureau du surintendant des institutions financières;
- les organisations autorisées à construire et à exploiter des installations pétrolières et gazières en Saskatchewan.

4.3 Définir le contexte de l'identité

En fournissant leurs programmes et leurs services, les fournisseurs de programmes et de services fonctionnent au sein d'un environnement ou d'un ensemble de circonstances particulières. C'est ce qu'on appelle le contexte de l'identité dans le domaine de la gestion de l'identité. Le contexte de l'identité est déterminé par des facteurs comme le mandat, la population cible (c.-à-d. les clients, la clientèle), et les autres responsabilités établies en vertu d'une loi, d'un accord ou d'une entente.

[18] Les caractéristiques d'une population de programme/service constituent le facteur clé pour déterminer le contexte de l'identité. Voir la prochaine section.

Comprendre et définir le contexte de l'identité aide les fournisseurs de programmes et de services à déterminer quels renseignements sur l'identité sont requis ou non. Le contexte de l'identité aide également à déterminer les points en commun avec d'autres fournisseurs de programmes et de services. Il permet de déterminer si les renseignements sur l'identité ou les processus d'assurance peuvent être utilisés dans d'autres contextes.

Les facteurs suivants devraient être pris en considération au moment de définir le contexte de l'identité d'un programme ou d'un service donné :

- le destinataire prévu d'un programme ou d'un service : le destinataire peut ne pas faire partie du fournisseur de programmes et de services (p. ex., un citoyen, une personne non canadienne, une entreprise, un organisme à but non lucratif) ou en faire partie (p. ex., un employé, un ministère);
- la taille, les caractéristiques et la composition de la clientèle;
- les points communs avec d'autres programmes et services (c.-à-d. entre fournisseurs de programmes et de services);
- les fournisseurs de programmes et de services ayant des mandats semblables;
- l'utilisation de services partagés lorsque le contexte de la prestation de services partagés peut différer du contexte du programme.

4.4 Déterminer les exigences en matière de renseignements sur l'identité

Une propriété ou une caractéristique associée à une personne ou une organisation identifiable est appelée *attribut d'identité* ou *élément de donnée sur l'identité*. Des exemples d'attributs d'identité d'une personne sont le *nom* et la *date de naissance*. Des exemples d'attributs d'identité d'une organisation sont le *nom légal* et la *date de création*. Dans le cadre d'un programme ou d'un service, quel qu'il soit, les renseignements sur l'identité constituent l'ensemble des attributs d'identité qui est à la fois :

- suffisant pour faire la distinction entre les différentes personnes ou organisations appartenant à la population d'un programme ou d'un service (c.-à-d., qui permet de satisfaire à l'exigence d'unicité de l'identité);
- suffisant pour décrire une personne ou une organisation en fonction des exigences du programme ou du service.

Les renseignements sur l'identité constituent un sous-ensemble strict de l'ensemble beaucoup plus vaste de renseignements appelés soit les renseignements personnels (« renseignements sur une personne identifiable »), soit les renseignements organisationnels (« renseignements sur une organisation identifiable »). Les

renseignements personnels ou organisationnels qui sont recueillis et utilisés dans le but précis d'administrer un programme ou d'offrir un service sont appelés les renseignements personnels *propres au programme* ou les *renseignements organisationnels propres au programme*. Les renseignements personnels propres au programme se limitent habituellement au programme et limités par la loi sur la protection des renseignements personnels afin d'assurer une utilisation uniforme pour laquelle ils ont été recueillis (p. ex., pour déterminer l'admissibilité au programme), à quelques exceptions près.

[19] Au moment de déterminer les exigences en matière de renseignements sur l'identité pour un programme ou un service, les fournisseurs de programmes et de services doivent faire la distinction entre les renseignements sur l'identité et les renseignements personnels propres au programme, car ils peuvent se chevaucher. Par exemple, la date de naissance peut être utilisée pour déterminer l'unicité de l'identité (et dans ce cas, elle est utilisée à titre de renseignement sur l'identité), mais elle peut également être utilisée comme critère d'admissibilité en fonction de l'âge (et dans ce cas, elle est utilisée comme renseignement personnel propre à un programme). Lorsqu'il y a un chevauchement entre les renseignements sur l'identité et les renseignements personnels propres au programme, une bonne pratique consiste à décrire les deux utilités. On veille ainsi à ce que l'utilisation des renseignements sur l'identité soit cohérente avec le but initial, en vertu duquel lesdits renseignements ont été collectés. On veille également à ce que les renseignements obtenus puissent être gérés séparément, ou faire l'objet d'une protection accrue au moyen des contrôles de sécurité et de protection de la vie privée appropriés. Il est recommandé aux fournisseurs de programmes et de services de réduire, autant que possible, le chevauchement entre les renseignements sur l'identité et les renseignements propres à un programme.

4.4.1 Identificateur

Un *identificateur* désigne l'ensemble d'attributs d'identité qui sont utilisés uniquement pour distinguer une personne ou une organisation donnée dans une population de programme ou de service. Cet ensemble d'attributs d'identité est habituellement un sous-ensemble des renseignements sur l'identité requis par un programme ou un service.

Différents ensembles d'attributs d'identité peuvent être désignés à titre d'identificateur selon les exigences du programme ou du service, voire parfois de lois et de règlements. Par exemple, un programme peut définir le nom et la date de naissance comme ensemble d'attributs d'identité constituant l'identificateur. Un autre programme pourrait définir le nom, la date de naissance et le sexe comme ensemble d'attributs

[19] Il ne s'agit habituellement pas d'un problème pour les renseignements organisationnels.

d'identité constituant l'identificateur. Un troisième programme pourrait utiliser un identificateur attribué[20] (comme le numéro d'assurance-maladie ou le numéro d'entreprise) à titre d'attribut d'identité constituant l'identificateur.

Au moment de déterminer l'ensemble d'attributs d'identité qui sera utilisé à titre d'identificateur, les facteurs suivants doivent être pris en considération :

- **Universalité** – Chaque personne ou organisation faisant partie de la population du programme ou du service doit posséder l'ensemble d'attributs d'identité constituant l'identificateur. Cependant, même quand un attribut d'identité est universel, un grand nombre de valeurs manquantes ou incomplètes peut le rendre inutile comme élément de l'identificateur. Par exemple, pour de nombreuses personnes nées hors du Canada, la date de naissance comprend seulement l'année et le mois de naissance.
- **Unicité** – Les valeurs associées aux attributs d'identité doivent être suffisamment différentes pour que chaque personne ou organisation faisant partie de la population du programme ou du service puisse être distinguée des autres. Par exemple, la date de naissance à elle seule n'est pas suffisante pour distinguer une personne d'une autre puisque de nombreuses personnes ont la même date de naissance.
- **Constance** – Les valeurs données aux attributs d'identité doivent varier aussi peu que possible (voire pas du tout) au fil du temps. Par exemple, l'adresse comme attribut pose problème, puisque les gens ont tendance à déménager plusieurs fois au cours de leur vie.
- **Facilité d'obtention** – Il devrait être relativement facile d'obtenir l'attribut d'identité. Par exemple, les séquences d'ADN des êtres humains sont universelles, uniques et très stables dans le temps, mais elles sont quelque peu difficiles à obtenir.

Ces quatre facteurs ne sont pas une liste exhaustive. Un autre facteur qui pourrait être pris en considération est la question de savoir si le programme ou le service a le pouvoir légal de recueillir l'attribut d'identité. Un autre facteur pourrait être le caractère envahissant de la collecte d'un attribut d'identité lorsque d'autres attributs d'identité pourraient être suffisants à cette fin (p. ex., les échantillons d'ADN ne devraient pas être recueillis lorsque le nom suffirait).

[20] Voir la prochaine section.

4.4.2 Identificateur attribué

Il est généralement convenu que le nom et la date de naissance constituent l'ensemble d'attributs d'identité minimal nécessaire pour constituer un identificateur pour une personne. Des analyses[21] ont démontré qu'une combinaison de nom (nom de famille + premier prénom) et de date de naissance complète fera une différence de plus de 96 % des personnes dans toute population. L'ajout d'autres attributs d'identité (p. ex., le *sexe*, le *lieu de naissance*) permet d'améliorer marginalement l'unicité au sein d'une population, mais aucune combinaison d'attributs d'identité ne peut garantir à 100 % l'unicité au sein d'une population donnée.

Par conséquent, afin d'éviter que des identités se chevauchent au sein du pourcentage résiduel de la population dont l'unicité n'est pas garantie, les fournisseurs de programmes et de services ont recours aux *identificateurs attribués*. Un identificateur attribué est un attribut d'identité artificiel dont la seule utilité est de garantir l'unicité des identités. L'identificateur attribué se composera d'une chaîne numérique ou alphanumérique automatiquement générée et attribuée à une personne ou une organisation au moment où elle s'inscrit ou s'enregistre.

Toutefois, avant d'associer une personne ou une organisation à un identificateur attribué, il faut établir l'unicité de l'identité de la personne ou de l'organisation au sein de la population visée (en d'autres mots, il faut effectuer une résolution de l'identité [voir la prochaine section]) en utilisant d'autres attributs d'identité (p. ex., *nom*, *date de naissance*). Par conséquent, l'utilisation d'un identificateur attribué n'élimine pas la nécessité des méthodes traditionnelles de résolution de l'identité, mais elle réduit cette nécessité à une occurrence ponctuelle isolée pour chaque personne ou organisation au sein d'une population.

Une fois associé à une personne ou une organisation, un identificateur attribué permet d'établir l'unicité de cette personne ou organisation parmi toutes les autres personnes ou organisations au sein de la population sans qu'il soit nécessaire de recourir à d'autres attributs d'identité. Le numéro d'enregistrement de naissance, le numéro d'entreprise, le numéro du permis de conduire, le numéro d'assurance sociale et le numéro de compte client sont tous des exemples d'identificateurs attribués. Les éléments suivants doivent être pris en considération au moment d'utiliser des identificateurs attribués :

- L'accès aux identificateurs attribués peut être réservé à l'utilisation interne du programme qui les gère.
- Les identificateurs attribués entretenus dans le cadre d'un programme peuvent être fournis à d'autres programmes, afin que ceux-ci puissent également y

[21] Projet de vérification de l'identité de la NASPO, Rapport sur le projet de résolution de l'identité (vérification de l'identité), 17 février 2014

recourir pour faire la distinction entre les différentes personnes ou organisations au sein de leurs propres populations ou services. Il se peut toutefois que des restrictions soient mises en place sur cette pratique en raison de lois ou de considérations relatives à la protection de la vie privée.

- Certains identificateurs attribués peuvent être assujettis à des restrictions juridiques et stratégiques qui peuvent varier entre les secteurs et les administrations. Par exemple, le gouvernement du Canada impose des restrictions sur la collecte, l'utilisation, la conservation, la divulgation et l'élimination du numéro d'assurance sociale.

4.5 Résolution de l'identité

La résolution de l'identité est la détermination de l'unicité d'une personne ou organisation à l'intérieur de la population d'un programme ou d'un service au moyen de renseignements sur l'identité. Le programme ou le service en question définit les exigences relatives à la résolution de l'identité, au sens des attributs d'identité; en d'autres mots, il détermine l'ensemble d'attributs d'identité requis pour assurer la résolution de l'identité au sein de la population en question. Comme l'identificateur est l'ensemble d'attributs d'identité qui sert à distinguer une personne ou organisation en particulier à l'intérieur de la population d'un programme ou d'un service, l'identificateur est le moyen qui permet d'assurer la résolution de l'identité.

4.6 Assurer l'exactitude des renseignements sur l'identité

Les renseignements sur l'identité doivent être exacts, complets et à jour[22]. La qualité des renseignements sur l'identité se mesure par leur exactitude. Elle garantit la véracité des renseignements fournis au sujet d'une personne ou organisation, en plus de garantir que ces renseignements sont complets et tenus à jour.

Pour que les renseignements sur l'identité soient considérés comme étant exacts, trois exigences doivent être respectées :

- **Les renseignements sur l'identité sont exacts et à jour.** Les renseignements sur l'identité peuvent changer au fil du temps, à la suite de certains événements de la vie (p. ex., le mariage). C'est pourquoi il faut toujours mettre à jour les renseignements sur l'identité lorsque le besoin survient, sans quoi ils deviennent inexacts.
- **Les renseignements sur l'identité se rapportent à une personne ou une organisation réelle.** Les renseignements sur l'identité doivent être associés à une

[22] Il s'agit d'une des exigences à respecter pour établir le niveau d'assurance de l'identité. Voir l'annexe C de la *Norme sur l'assurance de l'identité et des justificatifs* (SCT, 2013).

personne ou une organisation qui existe ou a existé vraiment à un moment donné.

- **Les renseignements sur l'identité se rapportent à la bonne personne ou organisation.** Dans les grandes populations, certaines personnes ou organisations peuvent présenter les mêmes renseignements sur l'identité que d'autres, ou des renseignements semblables. L'exigence d'unicité permet de régler la situation, mais elle n'élimine pas la possibilité que des renseignements sur l'identité soient associés à la mauvaise personne ou organisation.

Il incombe aux fournisseurs de programmes et de services de veiller à l'exactitude des renseignements sur l'identité fournis dans le cadre de leurs programmes et de leurs services. Il est possible de veiller à l'exactitude des renseignements sur l'identité au moyen d'une source faisant autorité. Il y a deux façons d'y arriver :

- Au besoin, demander les renseignements sur l'identité à une source qui fait autorité. C'est ce qu'on appelle l'extraction des renseignements sur l'identité. Par exemple, le lieu de naissance d'une personne peut être extrait électroniquement du registre fédéral des personnes nées à l'étranger.
- Souscrire à un service de notification offert par une source qui fait autorité. C'est ce qu'on appelle les notifications relatives aux renseignements sur l'identité. Par exemple, des avis de décès pourraient être transmis par un registraire de l'état civil provincial.

Ces méthodes peuvent être utilisées indépendamment les unes des autres ou en combinaison, et une stratégie efficace nécessite généralement le recours aux deux méthodes.

S'il est impossible de vérifier l'exactitude des renseignements sur l'identité au moyen d'une source qui fait autorité, on peut recourir à d'autres méthodes, comme la corroboration des renseignements sur l'identité à l'aide d'une ou de plusieurs preuves d'identité.

5 ANNEXE C : PERSONNES ET ORGANISATIONS

La présente annexe fournit des renseignements généraux supplémentaires sur la nature des personnes et des organisations d'un point de vue strictement juridique.

5.1 Entités juridiques

En droit, il existe deux types d'entités juridiques : les êtres humains, appelés *personnes physiques*, et les *personnes juridiques* non humaines – aussi appelées *personnes juridiques*, *personnes civiles*, *personnes artificielles* et *personnes fictives* (latin : *persona ficta*) – telles qu'une société, une entreprise, un groupement d'entreprises ou d'autres entités, un organisme gouvernemental, etc. –, qui sont traitées en droit comme si elles étaient des personnes physiques. Il convient toutefois de noter que l'emploi de l'expression *personne juridique* pour représenter uniquement une entité juridique non humaine est fautif. En droit, les entités juridiques, tant humaines que non humaines, sont reconnues comme des personnes juridiques qui ont certains privilèges et certaines obligations, comme la capacité juridique de conclure des contrats, d'intenter des poursuites et d'être poursuivies.

Les êtres humains acquièrent la *personnalité juridique* à leur naissance (ou même avant [c.-à-d. un fœtus] dans certaines administrations). Les personnes juridiques acquièrent la personnalité juridique lorsqu'elles sont constituées conformément à la loi. L'expression *personnalité juridique* sert à décrire le fait d'avoir acquis le statut de personne juridique.

La personnalité juridique est une condition préalable à la *capacité juridique*, c'est-à-dire la capacité de toute personne juridique de négocier (conclure, modifier, transférer, etc.) des droits et obligations. Par exemple, en droit international, la personnalité juridique est une condition préalable pour qu'une organisation internationale puisse signer des traités internationaux en son nom propre.

5.2 Personnes juridiques

Une personne juridique a une dénomination sociale et des droits, protections, privilèges, responsabilités et comptes à rendre en droit, semblables à ceux d'une personne physique. Le concept de personne juridique est une *fiction juridique* fondamentale. Il est pertinent pour la philosophie du droit, étant essentiel aux lois qui touchent une société (c.-à-d., le droit des sociétés).

La personnalité juridique est le fait d'une entité juridique non vivante qui est considérée par la loi comme ayant le statut de personne juridique.

La personnalité juridique permet à une ou plusieurs personnes physiques (*universitas personarum*) d'agir comme une seule entité (une personne morale) à des fins juridiques. Dans de nombreuses administrations, la personnalité juridique permet à cette entité d'être considérée en vertu de la loi séparément de ses membres individuels (par

exemple, dans une société limitée par des actions, ses actionnaires). Une personne juridique peut intenter des poursuites et être poursuivie, conclure des contrats, contracter des dettes et posséder des biens. Une personne juridique peut également être soumise à certaines obligations légales, telles que le paiement d'impôts. Une entité dotée de la personnalité juridique peut protéger ses membres de toute responsabilité personnelle.

Dans certaines administrations de common law, une distinction est établie entre une *personne morale composée* (comme une société, qui est composée d'un certain nombre de membres) et une *personne morale individuelle*, qui est une charge publique ayant la personnalité juridique qui est distincte de la personne qui remplit la charge. D'un point de vue historique, la plupart des personnes morales individuelles simples étaient de nature ecclésiastique (par exemple, le bureau de l'archevêque de Canterbury est une personne morale individuelle), mais d'autres charges publiques sont maintenant constituées en personne morale individuelle.

Le concept de la personnalité juridique n'est pas absolu. « Percer le voile corporatif » consiste à examiner les personnes physiques qui agissent à titre d'*agents* intervenant dans une action ou une décision de l'entreprise. Cela peut donner lieu à une décision juridique dans laquelle les droits ou les devoirs d'une société ou d'une société ouverte à responsabilité limitée sont traités comme les droits ou les responsabilités des membres ou des administrateurs de cette société.

5.3 Histoire des personnes juridiques

Le concept de la personnalité juridique pour les organisations de personnes (personnalité juridique) est au moins aussi ancien que la Rome antique : diverses institutions collégiales en bénéficiaient en vertu du droit romain.

La doctrine de la personnalité juridique a été attribuée au pape Innocent IV, qui a contribué à répandre l'idée de *persona ficta*. En droit canonique, la doctrine de *persona ficta* permettait aux monastères d'avoir une existence légale qui était à l'écart des moines, ce qui simplifiait la difficulté d'équilibrer la nécessité pour ces groupes d'avoir des infrastructures, alors que les moines eux-mêmes prenaient des vœux de pauvreté personnelle. Un autre effet était qu'en tant que personne fictive, un monastère ne pouvait être reconnu coupable d'actes délictuels[23] parce qu'il n'avait pas d'âme, ce qui aidait à protéger l'organisation contre les obligations non contractuelles envers les communautés environnantes. Cette responsabilité était effectivement transférée aux personnes qui intervenaient au sein de l'organisation tout en protégeant la structure

[23] Un acte délictuel désigne, dans les administrations de droit civil, un tort civil qui consiste en une violation intentionnelle ou par négligence de l'obligation de diligence qui inflige une perte ou un préjudice et qui entraîne la responsabilité juridique de l'auteur du tort.

même, puisque les personnes étaient considérées comme ayant une âme et donc capables d'être coupables de négligence.

Dans la tradition de common law, seule une personne physique peut intenter des poursuites ou être poursuivie. Ce n'était pas un problème à l'époque de la Révolution industrielle, où l'entreprise type était soit une entreprise à propriétaire unique, soit une société de personnes : les propriétaires étaient simplement responsables des dettes de l'entreprise. Une caractéristique de la société, cependant, est que les propriétaires et actionnaires jouissaient d'une responsabilité limitée : les propriétaires n'étaient pas responsables des dettes de la société. Ainsi, lorsqu'une société enfreint un contrat ou enfreint une loi, il n'y a pas de recours, car la responsabilité limitée protège les propriétaires et la société n'est pas une personne juridique soumise à la loi. Il n'y avait aucune responsabilité pour les actes répréhensibles commis par les sociétés.

Pour résoudre ce problème, la personnalité juridique d'une société a été établie de manière à inclure cinq droits juridiques : le droit à un trésor ou un coffre commun (y compris le droit de posséder des biens), le droit à un sceau d'entreprise (c.-à-d. le droit de conclure et de signer des contrats), le droit d'intenter des poursuites et d'être poursuivi (pour faire respecter les contrats), le droit d'embaucher des agents (employés) et le droit de prendre des règlements administratifs (auto-gouvernance).

Depuis le XIX^{e} siècle, la personnalité juridique d'une organisation a été interprétée de manière à en faire un citoyen, un résident ou un domiciliaire d'un État. Le concept de personne juridique est aujourd'hui au cœur du droit occidental, tant dans les pays de common law que dans les pays de droit civil, mais il se retrouve aussi dans pratiquement tous les systèmes juridiques.

5.4 Exemples de personnes juridiques

Voici des exemples de personnes juridiques.

- Société : Une personne morale constituée en vertu d'une loi ou d'une charte. Une personne morale composée est une société constituée par au moins deux personnes physiques. Une personne morale individuelle est une société constituée par une seule personne physique pour exécuter une certaine fonction – accomplie également par les successeurs de la personne – afin de lui donner un avantage juridique, notamment celui de la perpétuité, qu'une personne physique ne peut avoir. Des exemples de personnes morales individuelles sont un officiant religieux exécuter une telle fonction, ou la Couronne dans les royaumes du Commonwealth. Les sociétés municipales (municipalités) sont des « créatures législatives ». D'autres organisations peuvent être créées par la loi en tant que personnes juridiques, y compris les groupements européens d'intérêt économique (GEIE).

- Société de personnes : Ensemble de deux personnes physiques ou plus qui exploitent une entreprise commune à but lucratif créée d'un commun accord. Traditionnellement, les sociétés de personnes n'avaient pas la personnalité juridique permanente, mais de nombreuses administrations les considèrent maintenant comme ayant cette personnalité juridique.
- Entreprise : Une forme d'association commerciale qui exploite une entreprise industrielle. Une entreprise est souvent une société, bien qu'une société puisse prendre d'autres formes, comme un syndicat, une compagnie à responsabilité illimitée, une fiducie ou un fonds. Une société à responsabilité limitée – qu'il s'agisse d'une société privée limitée par une garantie, d'une société privée limitée par des actions ou d'une société ouverte à responsabilité limitée – est une association d'affaires ayant certaines caractéristiques d'une société et d'une société de personnes. Différents types d'entreprises présentent un ensemble complexe d'avantages et d'inconvénients.
- Coopérative : Organisation commerciale détenue et gérée démocratiquement par un groupe de personnes physiques dans leur intérêt mutuel.
- Association non constituée en société : Ensemble de deux personnes physiques ou plus qui sont traitées comme des personnes juridiques dans certaines administrations, mais non dans d'autres.
- Les États souverains sont des personnes juridiques.
- Dans le système juridique international, diverses organisations ont la personnalité juridique. Il s'agit notamment d'organisations intergouvernementales (p. ex., l'Organisation des Nations Unies, le Conseil de l'Europe) et d'autres organisations internationales (dont l'Ordre souverain et militaire de Malte, un ordre religieux).
- L'Union européenne (UE) a la personnalité juridique depuis l'entrée en vigueur du traité de Lisbonne le 1er décembre 2009. L'adhésion de l'UE à la Convention européenne des droits de l'homme (CEDH) exige que l'UE ait la personnalité juridique. Toutefois, en 2014, l'UE a décidé de ne pas être liée par les décisions de la Cour européenne des droits de l'homme.
- Les temples, dans certains systèmes juridiques, ont une personnalité juridique distincte.

Toutes les organisations n'ont pas la personnalité juridique. Par exemple, le conseil d'administration d'une société, d'une législature ou d'un organisme gouvernemental n'est généralement pas une personne juridique en ce sens qu'il n'est pas en mesure d'exercer des droits juridiques indépendants de la société ou de l'organisme politique dont il fait partie.

5.5 Renseignements sur l'entité juridique

Au Canada, le traitement et la manipulation des renseignements personnels (renseignements sur une personne identifiable) et des renseignements organisationnels (renseignements sur une organisation identifiable) diffèrent considérablement. Le tableau suivant illustre cette situation :

Dispositions législatives et réglementaires	**Portée et application**	
	Renseignements personnels	**Renseignements organisationnels**
Vie privée	Tous	S.O.
Protection	Tous	Certaines

Dans ce tableau, on peut constater que si tous les renseignements personnels sont assujettis à des garanties de vie privée et de protection, les renseignements organisationnels ne sont pas considérés comme des renseignements privés. Cependant, certains renseignements organisationnels peuvent être protégés par des ententes de confidentialité.

6 ANNEXE D : VÉRIFICATION DE L'IDENTITÉ ET DES JUSTIFICATIFS

La présente annexe fournit des renseignements généraux supplémentaires sur la nature de la vérification de l'identité et de la vérification des justificatifs.

6.1 Vérification de l'identité

Le processus de vérification de l'identité consiste à confirmer que les renseignements sur l'identité sont subordonnés au contrôle du sujet. Il convient de noter que ce processus peut s'appuyer sur des renseignements personnels ou organisationnels qui ne relèvent pas de l'identité. Quatre méthodes sont employées pour effectuer la vérification de l'identité :

Confirmation fondée sur les connaissances : Une méthode de vérification de l'identité qui utilise des renseignements personnels ou organisationnels ou des secrets partagés pour prouver que la personne ou l'organisation qui présente les renseignements sur l'identité contrôle l'identité. La confirmation fondée sur les connaissances est obtenue au moyen du modèle de défi-réponse : on pose des questions à la personne ou à l'organisme qui présente les renseignements sur l'identité, dont les réponses ne sont connues (du moins en théorie) que de la personne et de son interrogateur (p. ex., renseignements financiers, antécédents en matière de crédit, secret partagé, clé cryptographique, code d'accès expédié par la poste, mot de passe, numéro d'identification personnel, identificateur attribué).

Confirmation fondée sur les caractéristiques biologiques ou comportementales : Une méthode de vérification de l'identité qui utilise des caractéristiques biologiques (anatomiques et physiologiques) (p. ex., visage, empreintes digitales, rétines) ou des caractéristiques comportementales (p. ex., rythme de frappe au clavier, démarche) pour prouver que la personne qui présente les renseignements sur l'identité contrôle l'identité. La confirmation des caractéristiques biologiques ou comportementales est obtenue au moyen du modèle de défi-réponse : les caractéristiques biologiques ou comportementales enregistrées sur un document ou dans un magasin de données sont comparées à la personne qui présente les renseignements sur l'identité.

Confirmation fondée sur la possession physique : Une méthode de vérification de l'identité qui exige la possession ou la présentation d'éléments de preuve pour prouver que la personne ou l'organisation qui présente les renseignements sur l'identité contrôle l'identité.

Confirmation par un arbitre de confiance : Méthode de vérification de l'identité qui fait appel à un arbitre de confiance pour prouver que la personne ou l'organisation qui présente les renseignements sur l'identité contrôle l'identité.

Le type d’arbitre de confiance et l’acceptabilité de l’arbitre sont déterminés par des critères propres au programme. Les garants, notaires, comptables et agents accrédités sont des exemples d’arbitres de confiance.

6.2 Vérification des justificatifs

Le processus de vérification des justificatifs consiste à confirmer qu'un titulaire exerce un contrôle sur un justificatif émis. Le contrôle d'un justificatif émis est vérifié par un ou plusieurs authentifiants. Le degré de contrôle sur les justificatifs émis et le statut des justificatifs émis (c.-à-d., non violés, corrompus, modifiés, suspendus ou révoqués) peut servir à générer un niveau d'assurance. Le processus de vérification des justificatifs est également utilisé pour prouver que le titulaire est la même entité que l'entité de la transaction précédente.

Le processus de vérification des justificatifs dépend du processus de **liaison justificatif-authentifiant** :

> **Liaison justificatif-authentificateur :** Le processus qui consiste à associer un justificatif émis à un titulaire avec un ou plusieurs authentificateurs.
>
> Un authentifiant est un élément qu'un titulaire contrôle et qui sert à prouver que le titulaire a conservé le contrôle d'un justificatif émis. On trouve trois types d'authentifiants :
>
> - Quelque chose dont dispose le titulaire (p. ex., une clé cryptographique ou un mot de passe unique). Cela est semblable à la confirmation de possession physique utilisée par la vérification de l'identité.
> - Quelque chose que le titulaire sait (c.-à-d., des authentifiants fondés sur les connaissances [AFC]) (p. ex., un mot de passe, une réponse à une question de défi). Cela est semblable à la confirmation fondée sur les connaissances utilisée par la vérification de l'identité.
> - Quelque chose que le titulaire est ou fait (p. ex., visage, empreintes digitales, rétines, rythme de frappe au clavier, démarche). Cela est semblable à la confirmation fondée sur les caractéristiques biologiques ou comportementales utilisée par la vérification de l'identité.
>
> Le processus de liaison justificatif-authentifiant comprend également des activités liées au cycle de vie de l'authentificateur, telles que la suspension des authentificateurs (causée par un mot de passe oublié ou un verrouillage en raison d'authentifications défaillantes successives, 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).

7 ANNEXE E : LIGNES DIRECTRICES SUR LA RECONNAISSANCE MUTUELLE

À l'heure actuelle, le processus de reconnaissance mutuelle en est encore à ses débuts. Les sections qui suivent exposent des lignes directrices sur la reconnaissance mutuelle à un niveau élevé. Une orientation détaillée suivra dans les produits livrables subséquents.

7.1 Planification et mobilisation

L'étape de planification et de mobilisation devrait comprendre les éléments suivants :

- **Définir la portée de l'évaluation.** La portée de l'évaluation peut comprendre une ou plusieurs parties qui remplissent les rôles définis au sein de l'écosystème numérique. Bien que l'évaluation porte principalement sur une administration en tant qu'« émetteur », l'évaluation peut englober d'autres parties qui se sont vus déléguer des fonctions ou des rôles opérationnels particuliers. Le modèle du CCP peut également servir à clarifier les rôles et les responsabilités qui sont pertinents, mais pas nécessairement dans le cadre du processus d'évaluation officiel.
- **Officialiser l'équipe.** Officialiser l'équipe du projet de reconnaissance mutuelle qui sera responsable du processus et des produits livrables. L'équipe de projet devrait être composée de l'équipe d'évaluation et des membres des organisations participantes qui ont une connaissance opérationnelle détaillée du programme.
- **Visite des lieux.** L'équipe d'évaluation devrait effectuer une visite des lieux. Le résultat souhaité est de veiller à ce que les membres de l'équipe d'évaluation puissent acquérir une connaissance directe du programme et établir des relations de travail étroites avec les autres membres de l'équipe de projet de reconnaissance mutuelle afin de faciliter le transfert des connaissances et la compréhension commune.
- **Définir un volet de travail distinct.** Bien que l'équipe du projet de reconnaissance mutuelle puisse être intégrée à une initiative de projet plus vaste, le processus de reconnaissance mutuelle devrait être maintenu en tant que volet de travail distinct. Toutefois, le volet de travail devrait être étroitement synchronisé avec les autres volets de travail, comme les évaluations des facteurs relatifs à la vie privée, l'évaluation de sécurité et l'autorisation ainsi que l'intégration technique.
- **Faire participer le conseiller juridique dès le début.** Il est recommandé de faire participer les conseillers juridiques de toutes les parties dès le début du processus. Étant donné que le processus d'évaluation et les ententes qui en

découlent peuvent être nouveaux par rapport aux ententes existantes, il peut y avoir des conséquences pour les ententes et les pouvoirs respectifs.

- **Faire participer les responsables de la protection de la vie privée et de la sécurité dès le début.** Il est recommandé de faire participer les responsables de la protection de la vie privée et de la sécurité de toutes les parties dès le début du processus, car il faudra effectuer des évaluations des facteurs relatifs à la vie privée et des évaluations de la sécurité.
- **Gestion des dossiers.** Veiller à ce l'ensemble des preuves reçues, des documents d'évaluation et des ébauches de travail soient déposés dans un système de gestion des dossiers approprié dans la catégorie de sécurité appropriée. À la fin de l'évaluation, tous les documents devraient être mis au pont comme dossiers aux fins d'audit.

7.2 Schéma de processus

Voici quelques recommandations pour l'étape du schéma de processus.

- **Définir la portée de la mise en correspondance.** Typiquement, la mise en correspondance sera celle d'un programme ou d'un secteur d'activité établi. La portée de la mise en correspondance peut comprendre des programmes en amont comme des statistiques de l'état civil ou des fournisseurs de services commerciaux externes. Celles-ci peuvent être incluses dans la portée de l'évaluation ou être désignées comme étant des *dépendances*.
- **Se préparer aux variations terminologiques.** De nombreux programmes en cours d'évaluation seront bien établis et utiliseront la terminologie propre à leur contexte. Le but du schéma de processus n'est pas d'introduire une nouvelle terminologie, mais plutôt de mettre en correspondance les termes existants avec les éléments à évaluer au moyen du CCP.
- **Travailler en étroite collaboration avec tous les membres de l'équipe.** Une grande partie de la mise en correspondance du processus est un processus de découverte par l'équipe. Bien que la documentation existante puisse être la principale source d'information, des entrevues avec des experts en la matière et des membres du personnel opérationnel pourraient être nécessaires. Il faudra peut-être aussi organiser des ateliers pour parvenir à une compréhension et à une mise en correspondance communes.
- **Clarifier les responsabilités entre les parties.** Des processus semblables peuvent être exécutés ou reproduits entre les différentes parties. Par exemple, l'« inscription » à un programme d'identité numérique peut être la même chose qu'une « inscription » différente à un service qui a accepté l'identité numérique, ou elle peut être différente. La mise en correspondance des processus atomiques peut contribuer à clarifier ce qui peut être un processus en double (c.-à-d.

redondant) pour l'utilisateur et ce qui peut être spécifiquement requis pour le service.

7.3 Évaluation

L'évaluation nécessite un jugement rendu par un expert impartial en utilisant l'information la meilleure et la plus complète possible. Dans sa forme la plus simple, l'évaluation peut avoir un simple résultat de réussite ou d'échec. Toutefois, dans la pratique, l'évaluateur peut exiger des évaluations supplémentaires pour exprimer les préoccupations soulevées au moment de la décision ou pour indiquer que certains renseignements peuvent être incomplets ou inaccessibles pour l'évaluateur.

Voici les décisions d'évaluation qui ont été élaborées jusqu'à présent et qui pourront être ajustées au fil du temps. Il est à noter que les décisions d'évaluation qui comportent trop de classements peuvent rendre le processus d'évaluation moins transparent.

Voici les décisions d'évaluation qui sont actuellement utilisées.

- **Accepter** – Les critères de conformité sont respectés.
- **Accepter en faisant une observation –** Les critères de conformité sont respectés, mais une dépendance ou un risque sur lequel la partie faisant l'objet d'une évaluation n'a peut-être pas de contrôle direct a été relevé.
- **Accepter en émettant une recommandation –** Les critères de conformité sont respectés, mais une amélioration ou un perfectionnement doit être constaté à l'avenir.
- **Accepter en posant une condition –** Les critères de conformité ne sont pas respectés, mais le processus atomique est accepté en raison de la démonstration des mesures de sauvegarde, des facteurs compensatoires ou d'autres garanties mises en place. Ne pas accepter – Les critères de conformité ne sont pas respectés. Sans objet – Les critères de conformité ne s'appliquent pas.
- **Ne pas accepter –** Les critères de conformité ne sont pas respectés.
- **Sans objet –** Les critères de conformité ne s'appliquent pas.

7.4 Acceptation

À la fin du processus d'évaluation, une *lettre d'acceptation* est émise à l'administration. Cette lettre devrait :

- être adressée à la personne/l'organisation/l'instance agissant à titre d'émetteur de l'identité numérique;

- être signée par la personne, l'organisation ou l'administration acceptant l'identité numérique, à un niveau de qualificateur donné;
- inclure la portée ou à quelle fin spécifique l'identité numérique sera utilisée, y compris la durée d'utilisation;
- comporter une annexe énumérant les qualificateurs spécifiques (p. ex., niveaux d'assurance), et indiquant toute observation, condition ou recommandation découlant du processus d'évaluation.

8 ANNEXE F : ENJEUX THÉMATIQUES

Le Groupe de travail sur le PSP du CCP a déterminé plusieurs enjeux thématiques de haut niveau qu'il abordera à court ou à moyen terme.

Enjeu thématique 1 : Relations numériques

Nous devons travailler à élargir notre modélisation et notre discussion sur les relations numériques – à l'heure actuelle, il n'y a guère plus qu'une définition.

Enjeu thématique 2 : L'état en évolution des justificatifs

Nous nous trouvons au milieu de faits récents très intéressants dans les domaines des justificatifs numériques. Un changement radical se produit dans l'industrie : on passe de l'« échange de renseignements » à la « présentation de preuves numériques ». De plus, un travail solide lié aux normes est en cours au Consortium World Wide Web (W3C) en ce qui concerne les justificatifs vérifiables et les identificateurs décentralisés.

En raison de cette évolution des faits, nous entrevoyons maintenant la possibilité que les services intermédiés traditionnels (comme les fournisseurs de services d'ouverture de session centralisés ou fédérés) puissent disparaître en raison des nouvelles avancées technologiques. Cela peut ne pas arriver dans un avenir rapproché, mais nous ajustons actuellement le modèle du CCP pour y intégrer l'idée générale d'un « justificatif vérifiable » et la généraliser de manière à permettre aux justificatifs physiques (par exemple, le certificat de naissance, le permis de conduire) d'évoluer numériquement dans le modèle.

Nous ne sommes pas (encore) certains que le modèle que nous envisageons soit tout à fait juste. Quoi qu'il en soit, le Canada semble se diriger vers le peloton de tête pour ce qui est de comprendre les conséquences de l'application de ces technologies à l'échelle écosystémique (autant publique que privée). Ainsi, nous recevons des demandes de renseignements sur la façon dont le CCP pourrait faciliter la migration vers les écosystèmes numériques et vers de nouveaux justificatifs fondés sur des normes, des systèmes de vérification de source ouverte et l'interopérabilité internationale.

Enjeu thématique 3 : Consentement éclairé

Le consentement éclairé est un domaine en évolution, et nous ne croyons pas que le CCP englobe actuellement tous les enjeux et toutes les nuances gravitant autour de ce sujet, surtout en ce qui concerne le secteur public. Nous avons intégré du contenu du DIACC et l'avons adapté aux considérations relatives au secteur public, mais nous estimons qu'il reste encore beaucoup à faire. Entre-temps, nous estimons que le CCP est suffisamment clair pour que l'on procède à des évaluations – mais nous sommes prêts à apporter des changements au besoin.

Enjeu thématique 4 : Portée du CCP

Certaines personnes ont suggéré que la portée du CCP soit élargie de manière à inclure la qualification scolaire, les titres professionnels, etc. Nous menons actuellement des projets pilotes expérimentaux dans ces domaines avec d'autres pays. Nous avons anticipé l'extensibilité par la généralisation du modèle du CCP et l'ajout possible de nouveaux processus atomiques. Il faut toutefois garder à l'esprit que l'identité numérique représente un cas d'utilisation très précis, mais d'une importance énorme que nous devons d'abord établir correctement. Nous ne sommes pas encore prêts à envisager d'étendre la portée du CCP à d'autres domaines, mais nous le serons bientôt.

Enjeu thématique 5 : Autres détails

Un grand nombre de questions ont été posées à propos de la version actuelle du présent document en ce qui concerne l'application précise du CCP. Même si nous en avons une bonne idée, nous n'avons pas encore toutes les réponses. Ces détails seront tirés en grande partie de l'application réelle du CCP (comme on l'a fait précédemment avec l'Alberta et la Colombie-Britannique). Le CCP sera complété par un document d'orientation détaillé distinct.

Enjeu thématique 6 : Organisations non enregistrées

À l'heure actuelle, la portée du CCP englobe « toutes les organisations enregistrées et en activité au Canada (y compris les organisations inactives) dont une identité a été établie au Canada ». Il existe également de nombreux types d'organisations non enregistrées au Canada, comme les entreprises individuelles, les syndicats, les coopératives, les organisations non gouvernementales, les organismes de bienfaisance non enregistrés et les fiducies. Il faut entreprendre une analyse de ces organisations non enregistrées sous l'angle du CCP.

Enjeu thématique 7: Évaluation des processus atomiques externalisés

L'article 2.4.3 précise ceci :

> de par sa conception, le CCP ne présume pas qu'un seul fournisseur soit l'unique responsable e l'exécution de tous les processus atomiques. Par conséquent, plusieurs organismes pourraient être impliqués dans le processus d'évaluation du CCP, en mettant l'accent sur les différents processus atomiques ou les différents aspects (p. ex., la sécurité, la protection de la vie privée, la prestation de services). Il faut tenir compte de la façon de coordonner plusieurs organisations qui pourraient avoir besoin de travailler ensemble pour produire une évaluation globale du CCP. L'organisation évaluée est responsable de toutes les parties visées par l'évaluation. L'organisation peut décider que cela n'est pas faisable, mais elle demeure néanmoins responsable. De tels cas seront notés pendant l'évaluation.

Dans ce modèle, l'émetteur est l'autorité responsable en dernier ressort. Bien qu'un émetteur puisse choisir d'externaliser ou de déléguer la responsabilité du processus atomique d'*émission de justificatifs* à un autre organisme, la responsabilité incombe toujours à l'émetteur.

Nous devons déterminer comment les évaluations entre plusieurs acteurs seront menées. Il a été suggéré que l'organisation évaluée ait le pouvoir d'exposer le rendement d'autres organisations qui exécutent des processus atomiques en son nom.

Enjeu thématique 8: Le processus atomique de la *continuité de l'identité*

Le processus atomique de la *continuité de l'identité* est défini comme suit :

> confirmer dynamiquement que le sujet a une existence continue au fil du temps (c.-à-d. une « présence authentique »). Ce processus peut être utilisé afin de veiller à ce qu'aucune activité frauduleuse ou malveillante n'ait été effectuée (dans le présent ou par le passé).

Il a été noté que la notion de « confirmation dynamique » de l'existence continue d'un sujet au fil du temps soulève des préoccupations en matière de protection de la vie privée. Nous devons élaborer une définition du processus atomique de la *continuité de l'identité* qui soit plus précise et plus respectueuse de la vie privée.

Enjeu thématique 9 : Signature

L'annexe A définit la *signature* comme suit :

> une 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 sont communiqués; et l'intégrité des données de la transaction signée est maintenue, y compris l'original.

Nous devons examiner comment le concept de signature doit être appliqué dans le contexte CCP.

Enjeu thématique 10 : Nom fondamental, nom principal, nom légal

L'annexe A contient des définitions de *nom fondamental*, *nom principal* et *nom légal*.

Les trois expressions signifient plus ou moins la même chose. Nous devons choisir l'expression privilégiée et l'employer de manière plus cohérente.

Enjeu thématique 11 : Examen des annexes

À un moment donné, nous devrions entreprendre un examen complet des annexes actuelles. Pour chaque annexe, nous devons évaluer son utilité, son applicabilité et sa pertinence, ainsi que déterminer si elle doit continuer d'être incluse dans le document du CCP. Certaines annexes demeureront; certaines pourront être déplacées dans un

document de lignes directrices; tandis que d'autres pourraient être complètement rejetées. Certaines des annexes qui demeureront devront peut-être être modifiées.

9 ANNEXE G : BIBLIOGRAPHIE

Organisations

1. Conseils mixtes du Canada (CMC)
    a. Priorité des conseils mixtes du Canada en matière d'identité numérique : recommandations en matière de politique publique (2018)
2. Centre de la sécurité des télécommunications Canada (CST)
    a. Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (2018)
3. Conseil de l'identification et de l'authentification numériques du Canada (CIANC)
    a. Aperçu du modèle de cadre de confiance pancanadien (février 2019)
    b. Aperçu de la composante notification et consentement (avril 2019)
    c. Modèle de cadre de confiance pancanadien (juin 2019)
    d. Aperçu de la composante vérification de l'organisation (novembre 2019)
    e. Aperçu de la composante vérification des identifiants de connexion (novembre 2019)
    f. Aperçu de la composante vérification de la personne (novembre 2019)
4. Sous-comité sur la gestion de l'identité (SCGI)
    a. Modèle pancanadien d'assurance (2010)
    b. Approche pancanadienne de la confiance dans l'identité (2011)
5. Commissariat à la protection de la vie privée du Canada (CPVP)
    a. Lignes directrices pour l'obtention d'un consentement valable (mai 2018)
6. Secrétariat du Conseil du Trésor du Canada (SCT)
    a. Fédérer la gestion de l'identité au gouvernement du Canada (2011)
    b. Ligne directrice sur la définition des exigences en matière d'authentification (2012)
    c. Norme sur l'assurance de l'identité et des justificatifs (2013)
    d. Ligne directrice sur l'assurance de l'identité (2017)
    e. Directive sur la gestion de l'identité (2019)
7. Banque mondiale (BM)
    a. Guide du praticien de l'ID4D (2019)

8. World Wide Web Consortium (W3C)
    a. Verifiable Credentials Data Model 1.0 (2019)

Personnes

1. Joe Andrieu
    a. A Primer on Functional Identity (2018)