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

VERSION 1.3

VUE D'ENSEMBLE REGROUPÉE

Version du document : 0.2

État du document : Ébauche aux fins de consultation

Date : 2021-04-21

Classification de sécurité : NON CLASSIFIÉ

CONTRÔLE DES VERSIONS DU DOCUMENT

Numéro de version	Date de l'émission	Auteurs	Courte description
0.1	2021-01-14	ISDE et SCT	Ébauche aux fins de consultation
0.2	2021-04-21	ISDE et SCT	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 12** présentent diverses annexes portant sur les termes et les définitions, des renseignements sur certains sujets liés au CCP, une liste de questions qui seront résolues dans les versions futures du document et une bibliographie.

Le Cadre de confiance pancanadien permettra de faciliter la transition vers un écosystème numérique pour les citoyens et les résidents du Canada. Un écosystème numérique canadien viendra accroître l'efficacité des processus opérationnels, comme les services bancaires ouverts, l'octroi de licences d'exploitation et la prestation de service du secteur public.

Le CCP est simple et intégré; pour être technologiquement agnostique; pour compléter les cadres existants; et pour être 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 définit deux types de *représentations numériques* essentielles au développement de l'écosystème numérique :

1. les *identités numériques* d'entités (comme les personnes et organisations);
2. les *relations numériques* entre les entités.

Le CCP facilite une approche commune entre tous les ordres de gouvernement et le secteur privé, répondant ainsi aux besoins des diverses communautés qui ont besoin de faire confiance aux identités numériques. Le Cadre est défini de manière à permettre l'utilisation de différents services, plateformes, architectures et technologies. Le CCP ne recommande pas une solution technologique plutôt qu'une autre.

Le CCP facilite l'acceptation d'identités numériques et de relations numériques en définissant un ensemble de modèles de processus discrets, appelés *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 et certifiés comme étant dignes de confiance dans l'écosystème numérique.

1 AVANT-PROPOS

Le présent document vise à décrire le profil du secteur public du Cadre de confiance pancanadien (CCP)[1].

Le public cible de ce document comprend :

- les chefs opérationnels et les gestionnaires de programmes — 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.

La définition des divers termes utilisés dans le présent document se trouve à l'*annexe A : Termes et définitions*.

[1] Le développement du profile du secteur public du cadre de confiance pancanadien est le résultat d'une collaboration dirigée par les conseils mixtes du Canada, 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 du profil du secteur public du CCP (GT PSP 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 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[2]. 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 méthodologie d'évaluation convenue. 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, lorsque possible (p. ex., la sécurité, la protection des renseignements personnels, la prestation des services) et qui précise les critères applicables aux domaines où les normes et les politiques n'existent pas.

Le CCP permet l'harmonisation et l'évaluation des processus opérationnels, ce qui accroît ainsi la confiance envers des solutions d'identité qui sont conçues pour fonctionner au-delà des frontières organisationnelles. Le CCP définit un ensemble de modèles de processus discrets (appelés processus atomiques) qui peuvent être mis en correspondance avec les processus d'exploitation. Cette mise en correspondance permet une évaluation structurée d'une solution d'identité et cerne toute dépendance vis-à-vis des organisations externes.

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

- les identités numériques des entités;
- les relations numériques entre les entités.

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

Le CCP est technologiquement indépendant : il est défini de manière à permettre l'utilisation de différents services, plateformes, architectures et technologies. Le CCP ne recommande pas une solution technologique plutôt qu'une autre.

En outre, le CCP est conçu pour tenir compte des cadres internationaux d'identité numérique, tels que :

- 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 noter que le CCP n'est pas un *cadre de gouvernance*.

2.1.3 La portée du CCP

À l'heure actuelle, la portée du Cadre de confiance pancanadien est la suivante :

- les personnes se trouvant au Canada, qu'on définit comme 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, qu'on définit comme 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.

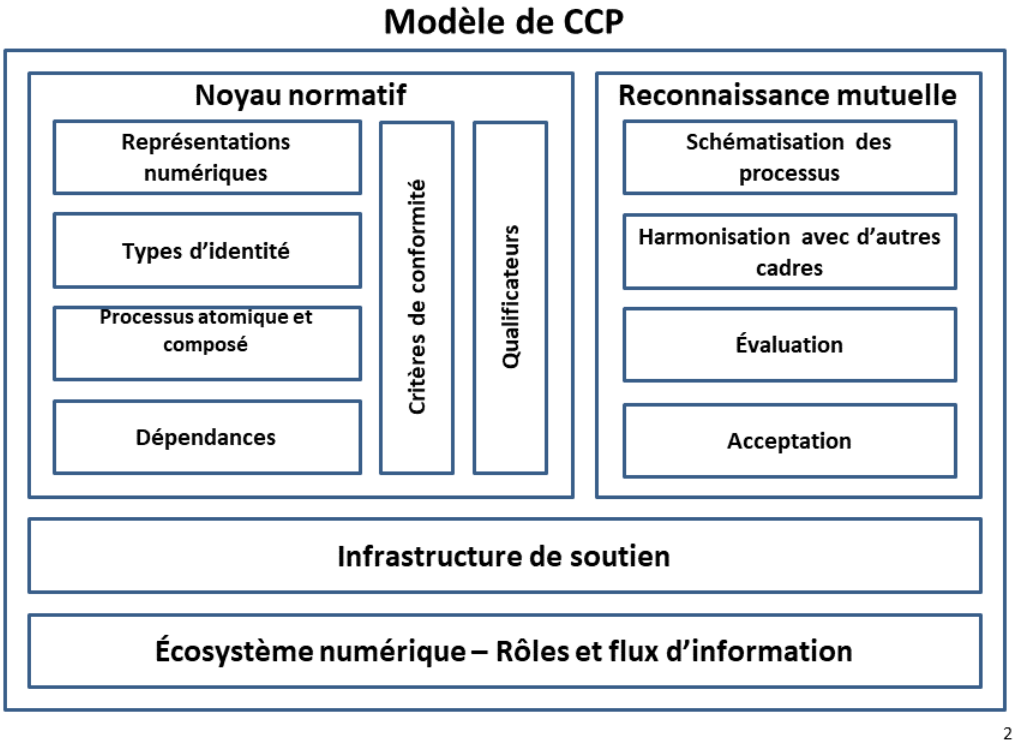


Figure 1 : Modèle de cadre de confiance pancanadien

Le modèle de CCP comprend quatre composantes principales :

1. une composante du **noyau normatif**, qui englobe les concepts clés du CCP;
2. une composante de la **reconnaissance mutuelle**, qui décrit la méthodologie actuelle servant à évaluer et à certifier les acteurs de l'écosystème numérique;
3. une 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. une 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 Représentations numériques

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

Actuellement, le CCP reconnaît deux types de représentations numériques :

- l'**identité numérique**, qui est une représentation électronique d'une entité employée exclusivement par celle-ci, dans le but d'accéder à des services appréciables et d'effectuer des transactions en toute confiance et avec assurance;
- la **relation numérique**, qui est une représentation électronique de la relation entre deux entités ou plus.

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

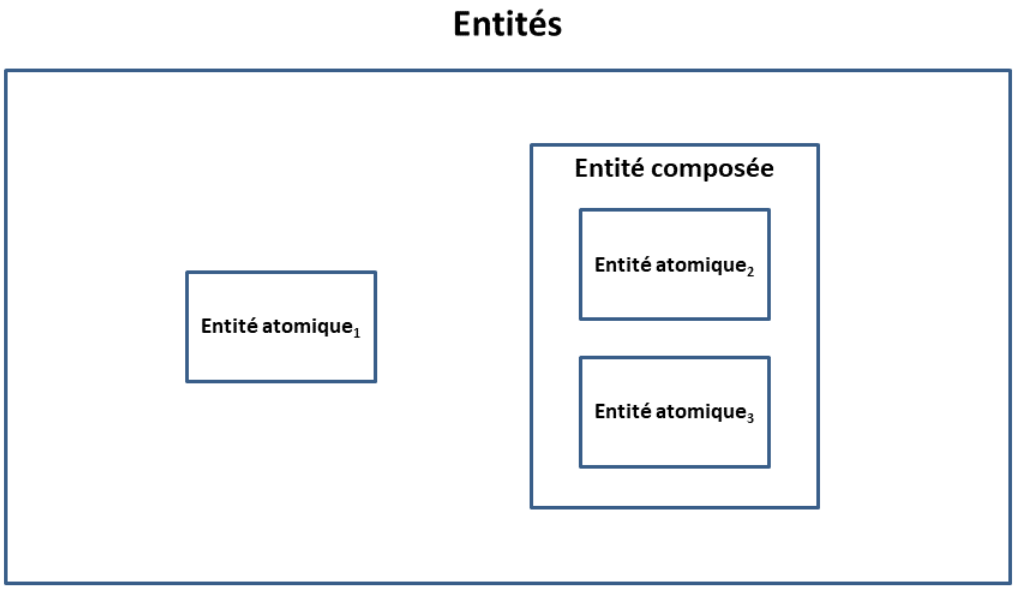
Au fur et à mesure que le CCP évolue, ces représentations numériques seront étendues à d'autres types d'entités, comme les actifs numériques. On prévoit également qu'à l'avenir, le CCP sera utilisé pour faciliter la reconnaissance mutuelle des représentations numériques entre les pays.

2.3.1.1 Entités

Une entité a une existence distincte et indépendante, comme une personne ou une organisation, qui peut être assujettie à des lois, des politiques ou des règlements dans un contexte, et qui peut avoir certains droits, devoirs et obligations. Une entité peut

remplir un ou plusieurs des quatre rôles (c'est-à-dire *Sujet*, *Émetteur*, *Titulaire* ou *Vérificateur*) dans l'écosystème numérique[3].

Il existe deux types d'entités : entités atomiques et entités composées. Une entité atomique est une entité qui ne peut pas être décomposée en unités plus petites. Les personnes sont des entités atomiques. Une entité composée est une entité qui comprend une ou plusieurs entités atomiques. Les organisations sont des entités composées. La figure 2 illustre les deux types d'entités.



3

Figure 2 : Entités atomiques et entités composées

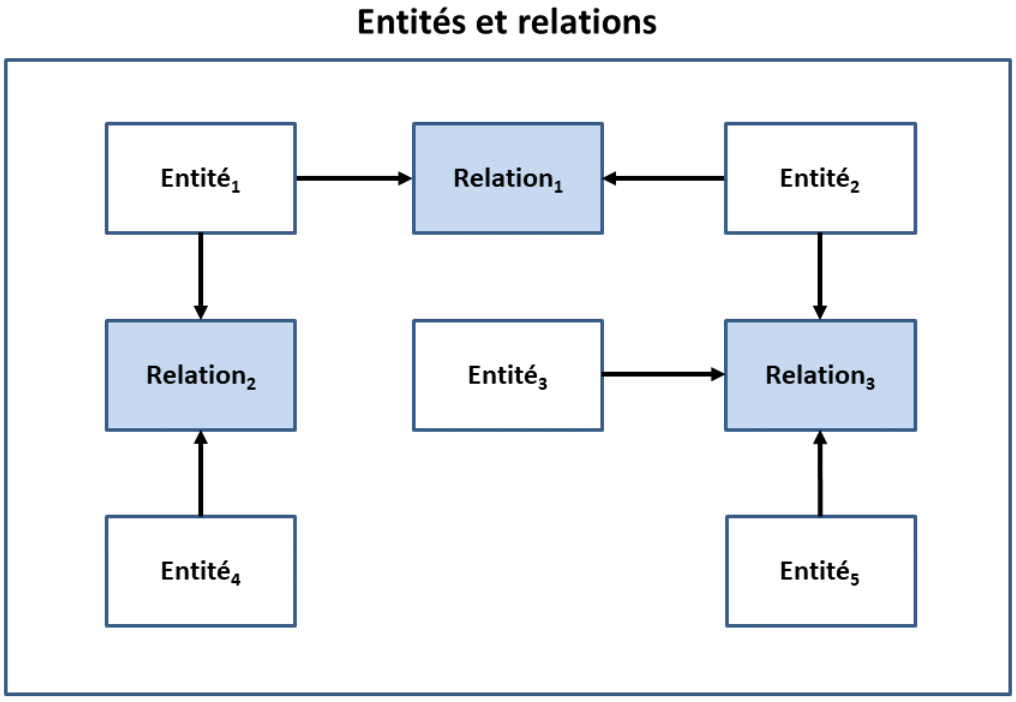
[3] Voir la section 2.6.1 pour plus d'informations sur les rôles de l'écosystème numérique.

2.3.1.2 Relations numériques entre les entités

Une relation[4] est une association entre deux entités ou plus. Les entités de la relation peuvent être n'importe quelle combinaison d'entités atomiques et d'entités composées[5]. Voici quelques exemples de relations :

- de personne à personne (p. ex., un couple marié);
- de personne à organisation (p. ex., un employé d'une société);
- d'organisation à organisation (p. ex., une filiale d'une société mère).

La figure 3 illustre un réseau de relations entre les entités. Veuillez noter que les entités dans ce diagramme pourraient être n'importe quelle combinaison d'entités atomiques et d'entités composées.



[4] Pour plus de détails sur les relations, voir l'annexe D.

[5] **Remarque** : Les relations entre les entités doivent être différenciées des interactions entre les entités (c.-à-d. l'exécution des transactions). Ce concept sera examiné plus en détail dans une version ultérieure du PSP du CCP.

Figure 3 : Un réseau d'entités et de relations

La figure 4 présente une vue détaillée d'un réseau de relations entre deux entités composées. Veuillez prendre note que l'une des entités composées possède un réseau interne de relations entre deux entités atomiques.

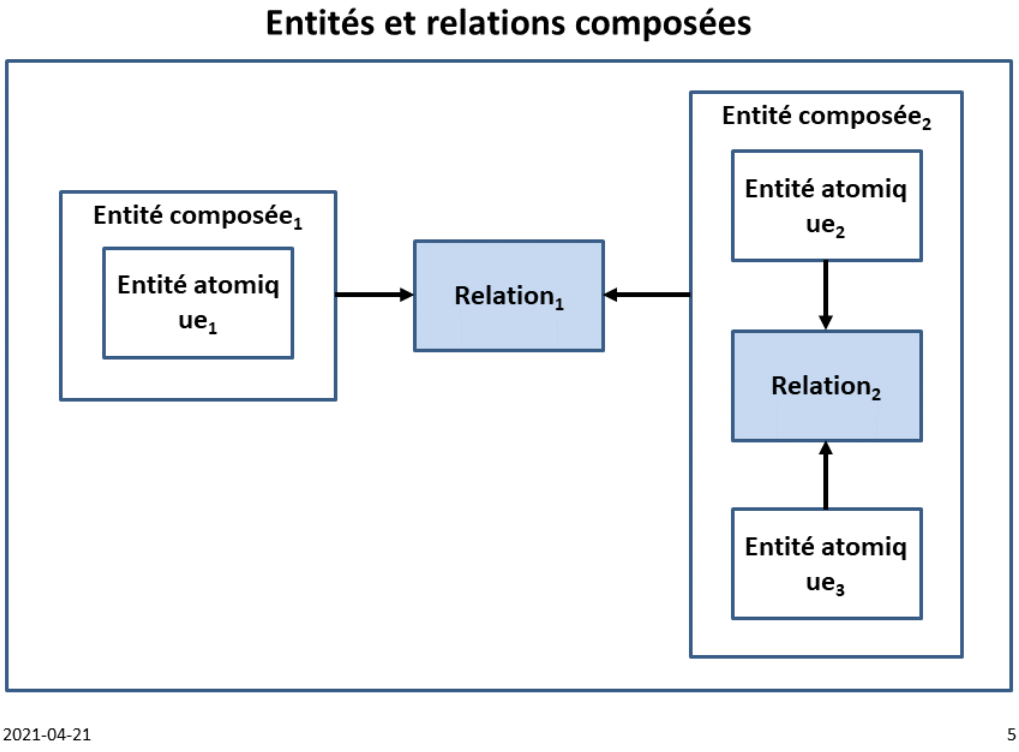


Figure 4 : Un réseau d'entités et de relations composées

Pour plus de détails sur les relations, voir l'annexe D.

2.3.1.3 Attributs

Un attribut est défini comme une propriété ou une caractéristique d'élément[6]. Le CCP reconnaît trois types d'attributs : attributs d'entité, attributs de relation et attributs de justificatif. Les attributs d'entité et les attributs de relation sont utilisés pour exprimer les revendications[7].

Un attribut d'entité est une propriété ou une caractéristique d'entité. Voici quelques exemples d'attributs d'entité :

- le nom complet d'une personne;
- le nom légal d'une société;
- la date de naissance d'une personne;
- la date de constitution d'une société;
- l'adresse de résidence d'une personne;
- l'adresse de l'entreprise d'une société;
- le numéro de permis de conduire d'une personne;
- le numéro du permis d'exploitation forestière d'une société;

Un attribut de relation est une propriété ou une caractéristique d'une association entre deux ou plusieurs entités. Voici quelques exemples d'attributs de relation :

- le type de relation (p. ex., mariage, partenariat, parent d'un enfant, propriétaire d'une entreprise);
- le sous-type de la relation (p. ex., propriétaire unique d'une entreprise);
- l'autorité déclarante;
- la date d'entrée en vigueur;
- la date d'expiration;
- le statut de la relation (p. ex., active, révoquée).

[6] Il existe un type spécial d'attribut appelé *prédicat dérivé*. Un prédicat dérivé est un attribut qui prend la forme d'une valeur booléenne (c'est-à-dire une valeur « Vrai » ou « Faux ») basée sur la ou les valeurs d'un ou plusieurs autres attributs. Par exemple, un attribut de prédicat dérivé comme « Âgé21ansouplus » contient une valeur « Vrai » ou « Faux » qui indique si une personne a vingt et un ans ou plus, par opposition à contenir l'âge ou la date de naissance réels de la personne. L'utilisation d'un prédicat dérivé protège mieux la vie privée d'une personne en ne divulguant que le minimum de renseignements personnels requis pour valider l'admissibilité d'une personne à un service.

[7] Pour en savoir plus sur les revendications, consultez la section 2.6.2 et l'annexe E (section 7.4).

Un attribut d'identité[8] est une propriété ou une caractéristique d'une identité. Voici quelques exemples d'attributs de justificatifs :

- le type de justificatif;
- l'émetteur de la pièce d'identité;
- la date d'émission;
- la date d'expiration;
- le statut du justificatif (p. ex., actif, suspendu, révoqué).

2.3.2 Types d'identité

Dans le domaine de l'identité, il existe deux types d'identité : *identité principale* et *identité contextuelle*.

- Une **identité principale** est une identité qui a été établie ou modifiée à la suite d'un événement important (p. ex., naissance, changement de nom légal de la personne, immigration, résidence légale, citoyenneté naturalisée, décès, enregistrement ou changement de nom légal de l'organisation ou faillite).
- Une **identité contextuelle** est une identité qui est utilisée à des fins spécifiques dans un contexte d'identité spécifique[9] (p. ex., banque, permis d'affaires, services de santé, permis de conduire ou médias sociaux). Selon le contexte identitaire, une identité contextuelle peut être liée à une identité principale (p. ex., un permis de conduire) ou ne pas être liée à une identité fondamentale (p. ex., un profil de médias sociaux).

L'établissement et le maintien des identités principales sont sous le contrôle exclusif du secteur public; spécifiquement :

- les organismes responsables des données de l'état civil (ORDEC) des provinces et des territoires;
- les registres des entreprises des provinces et des territoires;
- Immigration, Refugiés et Citoyenneté Canada (IRCC);

[8] Les attributs de justificatif sont également connus sous le nom de *métadonnées de justificatif*. Voir l'annexe E pour obtenir plus de renseignements.

[9] En fournissant leurs programmes et leurs services, les fournisseurs de programme et de service 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'informations sur l'identité et les concepts de gestion de l'identité, voir l'annexe B.

- le registre fédéral des sociétés de Corporations Canada.

L'identité contextuelle est établie et maintenue à la fois par les secteurs public et privé.

2.3.3 Processus atomique et composé

Le CCP définit un ensemble de processus atomiques pouvant être évalués de façon indépendante et certifiés comme étant compatibles 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[10]. Le CCP reconnaît qu'en pratique, un processus opérationnel est souvent un ensemble de processus atomiques qui aboutissent à un ensemble de transitions d'état. Ces regroupements de processus atomiques sont appelés 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 indépendante 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 quatre processus atomiques — la *détermination des renseignements sur l'identité* et la *détermination de la preuve d'identité*, la *détermination des renseignements sur la relation* et la *détermination des preuves de la relation* — ne sont effectués qu'une seule fois pour un programme ou un service.

2.3.3.1 Processus atomiques

Un processus atomique est un ensemble d'activités logiquement mis en correspondance qui entraîne l'état de transition d'un objet. D'autres processus atomiques peuvent se fier à l'état de sortie de l'objet. La figure 5 illustre le modèle de processus atomique.

[10] Une transition d'état est la transformation d'un état d'entrée d'objet en état de sortie.

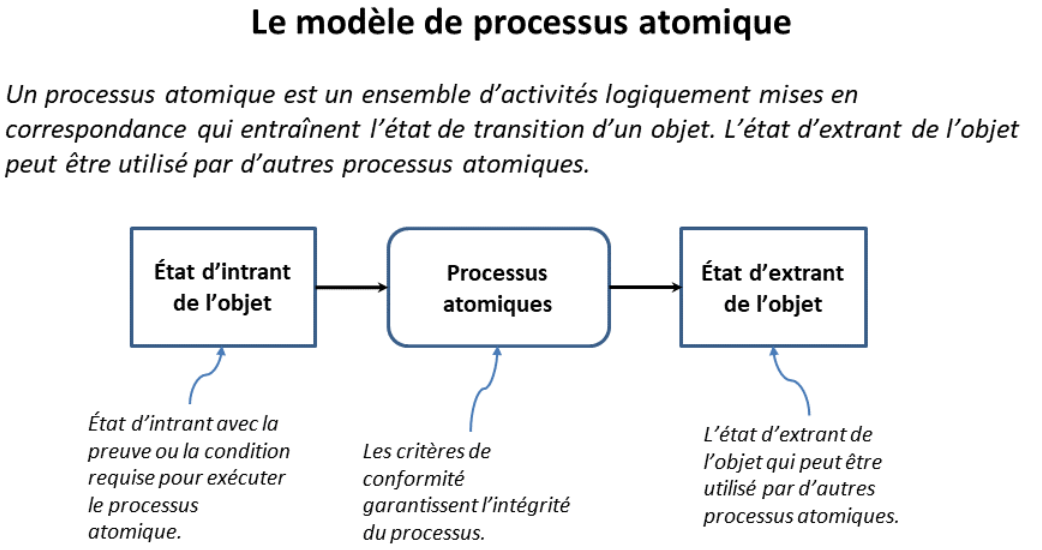


Figure 5 : Le modèle de processus atomique

Les processus atomiques sont des constituants essentiels permettant de veiller à l'intégrité générale de la chaîne d'approvisionnement d'identité numérique et, par extension, à l'intégrité des services numériques. L'intégrité d'un processus atomique relève de la plus haute importance, puisque le produit d'un processus atomique 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 d'un processus atomique 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 à un processus atomique 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 le processus atomique soit effectué avec intégrité. À titre d'exemple, un processus atomique peut consister à attribuer un identificateur à une entité. Les critères de conformité pourraient indiquer qu'un parti responsable de gérer le processus atomique doit veiller à ce que le code d'identification en question soit unique au sein d'une population donnée.

Pour une description détaillée des processus atomiques, consulter la section 2.7.

La figure 6 illustre quelques modèles de diagrammes des trois processus atomiques.

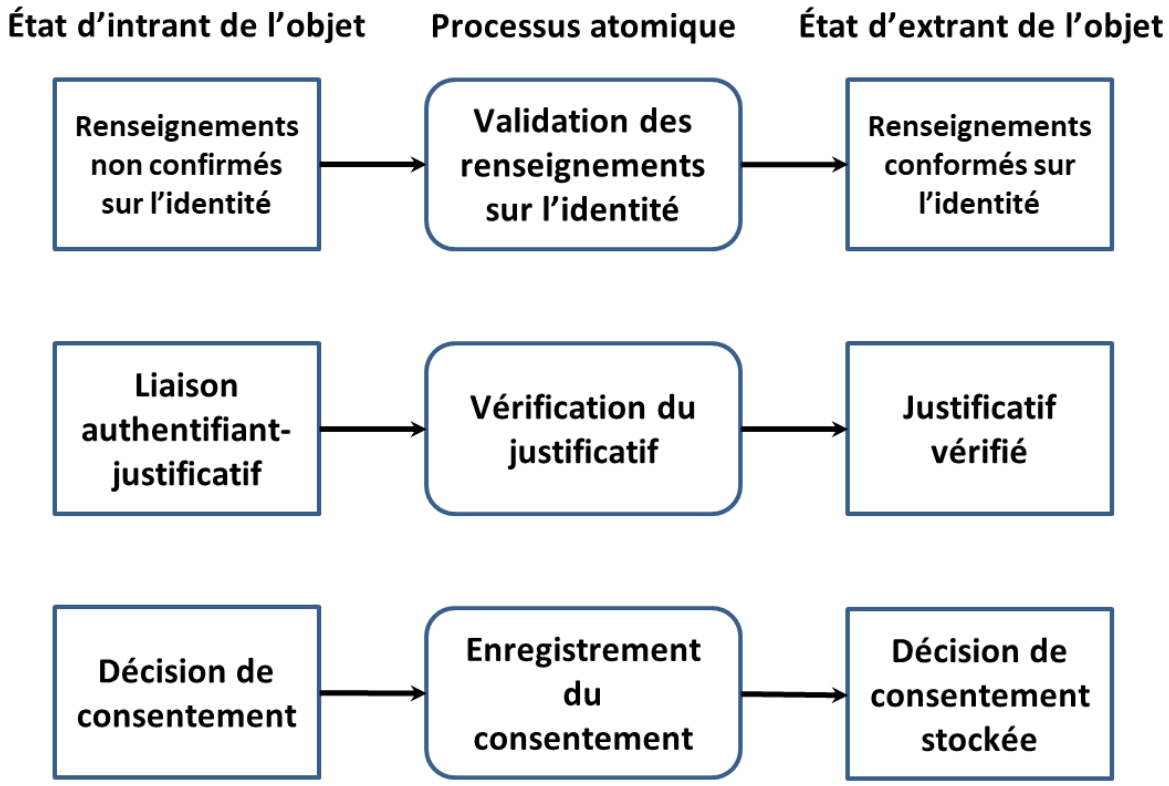


Figure 6 : Exemples de processus atomiques (modélisés)

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. Des processus atomiques sont regroupés pour former un processus composé qui entraîne un ensemble de transitions d'état. Il peut également arriver qu'un processus composé soit un regroupement d'autres processus composés qui, à leur tour, peuvent 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 de cinq processus atomiques, comme le montre la figure 7.

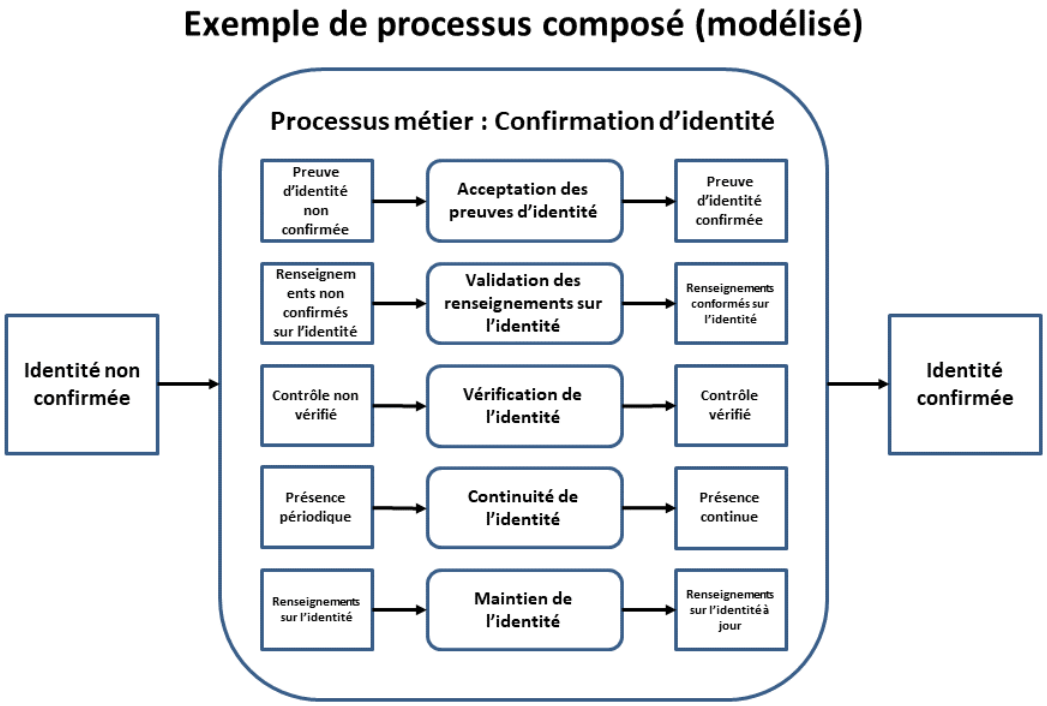


Figure 7 : Exemple de processus composé (modélisé)

Remarque : Tout ordre des processus atomiques ne doit pas être déduit du diagramme.

2.3.4 Dépendances

Le modèle de CCP reconnaît deux types de dépendances. Le premier type représente 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 entité peut être exécuté de manière indépendante en tout temps, il est logiquement exact de ne le faire qu'après la résolution de l'identité de cette entité. Ce type de dépendance est spécifié dans les critères de conformité (voir la section 2.3.5).

Le deuxième type est celui des dépendances d'organisations externes pour la fourniture des extrants de processus atomique (p. ex., un fournisseur de services d'accréditation). Ce type de dépendance est défini et noté dans 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 résolution de l'identité peut consister à attribuer un identificateur à une entité. Le critère de conformité précise que le processus atomique doit garantir que l'identificateur attribué à l'entité soit unique pour une population ou un contexte spécifique.

Les critères de conformité sont conservés dans un document distinct — le classeur sur le PSP du CCP. À l'avenir, les critères de conformité peuvent être intégrés à un outil d'évaluation automatisé.

2.3.6 Qualificateurs

Les qualificateurs sont affectés aux critères de conformité. Les qualificateurs peuvent permettre de mieux décrire un niveau de confiance ou la rigueur requise, ou peuvent indiquer une exigence spécifique, en ce qui concerne un domaine lié à l'identité, une exigence stratégique ou réglementaire spécifique ou un autre cadre de confiance. Les qualificateurs sont 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. De plus, on peut utiliser des qualificatifs pour établir des critères de conformité semblables ou identiques à partir de différents cadres de confiance, en fonction des politiques ou des exigences réglementaires des administrations. Par exemple, les critères de conformité du niveau 1 du CCP pour le processus atomique de *vérification de l'identité* peuvent être

mis en correspondance au niveau 1 de l'assurance de l'identité, selon la définition dans la *Norme sur l'assurance de l'identité et des justificatifs*, émise par le Secrétariat du Conseil du Trésor du Canada.

Un critère de conformité peut comprendre un qualificatif (applicable dans certains cas) ou plusieurs (applicables dans plusieurs cas). Consultez le classeur sur le PSP du CCP (un document distinct) pour obtenir des exemples de la façon dont les qualificatifs sont utilisés pour l'évaluation et de la façon dont ils peuvent être mis en correspondance avec d'autres cadres.

Voir la section 2.8 pour plus de détails sur les qualificatifs.

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 Schématisation des processus

La schématisation des 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 organisationnel faisant autorité.
Validation des renseignements sur l'identité	Un processus de demande de permis de conduire qui confirme l'exactitude des renseignements sur l'identité présentés sur les documents physiques ou au moyen d'un service de validation

Processus atomique	Exemples de processus opérationnels existants
	électronique. 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 (p. ex., photographie du visage, couleur des yeux, taille) afin de veiller à ce qu'il s'agisse 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 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. 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.

Le classeur sur le PSP du CCP (un document distinct) a été rédigé pour aider dans le processus d'évaluation du CCP. Ce classeur regroupe les processus atomiques et les critères de conformité qui les accompagnent dans un ensemble de feuilles de calcul destinées à aider à cartographier les processus opérationnels existants et à aider l'équipe d'évaluation à recouper les données pour l'analyse de l'évaluation. Les qualificateurs sont attribués à des critères de conformité pour faciliter la sélection des critères de conformité s'appliquant au processus d'évaluation[11].

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

Il convient de noter que le CCP ne présume pas qu'un vérificateur ou un émetteur unique est le seul responsable de tous les processus atomiques. Une organisation peut choisir de sous-traiter ou de déléguer la responsabilité d'un processus atomique à une autre partie. 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 organismes qui pourraient avoir besoin de travailler ensemble pour produire une

[11] Voir la section 2.3.6 pour plus de détails sur les qualificatifs.

évaluation globale du CCP. L'organisation évaluée est responsable de toutes les parties qui entrent dans le champ d'application de l'évaluation. Elle peut décider que cela n'est pas faisable, mais demeure néanmoins responsable. Ces cas seront pris en compte dans l'évaluation.

Au fur et à mesure que le processus d'évaluation du CCP évolue, il faudra déterminer quels organismes ou quelles normes sont mieux indiqués pour répondre aux exigences des intervenants et mieux appliqués 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.

Finalement, le processus d'acceptation du CCP peut comprendre des processus normalisés définis par l'Organisation internationale de normalisation (ISO)[12] 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 officiels de certification et d'accréditation sont en cours d'élaboration. En principe, une fois qu'ils sont élaborés, des tiers indépendants seront autorisés à procéder aux évaluations du CCP. De nombreux 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.

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

2.5 Infrastructure de soutien

L'infrastructure de soutien décrit 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 ne relèvent pas du CCP. Le CCP ne fait aucune recommandation quant à la composition de l'infrastructure de soutien.

La figure 8 illustre certains éléments (avec des exemples) de ce qui pourrait constituer l'infrastructure de soutien.

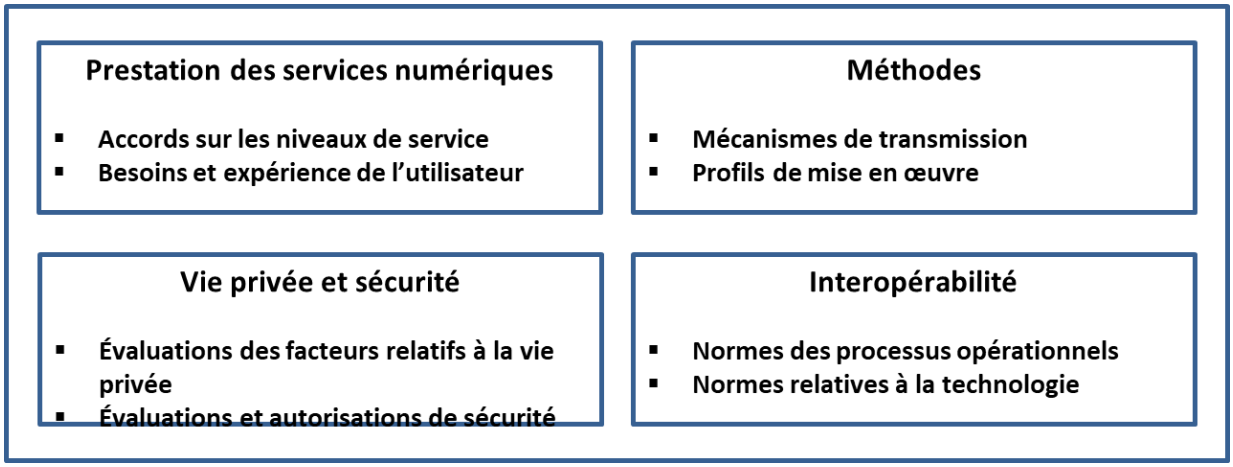


Figure 8 : Infrastructure de soutien

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

2.5.1 Méthodes

Les méthodes sont les ensembles de règles qui régissent la façon dont les acteurs de l'écosystème numérique interagissent directement ou indirectement entre eux. Les méthodes englobent des éléments comme les modèles et schémas de données, les protocoles de communication, les mécanismes de transport[13], les algorithmes cryptographiques, les bases de données, les registres distribués, les registres de

[13] Voir la section 2.5.2.

données vérifiables et les systèmes similaires; et les combinaisons de celles-ci. Les méthodes peuvent également comprendre des systèmes isolés ou intermittents.

Le CCP ne recommande pas une méthode plutôt qu'une autre.

2.5.2 Mécanismes de transmission

Les mécanismes de transport sont les différentes méthodes par lesquelles la sortie d'un processus atomique est disponible pour être utilisée comme entrée dans un autre processus atomique. Comme le montre la figure 9, les mécanismes de transport sont situés entre les parties produisant et consommant les états de sortie des processus atomiques.

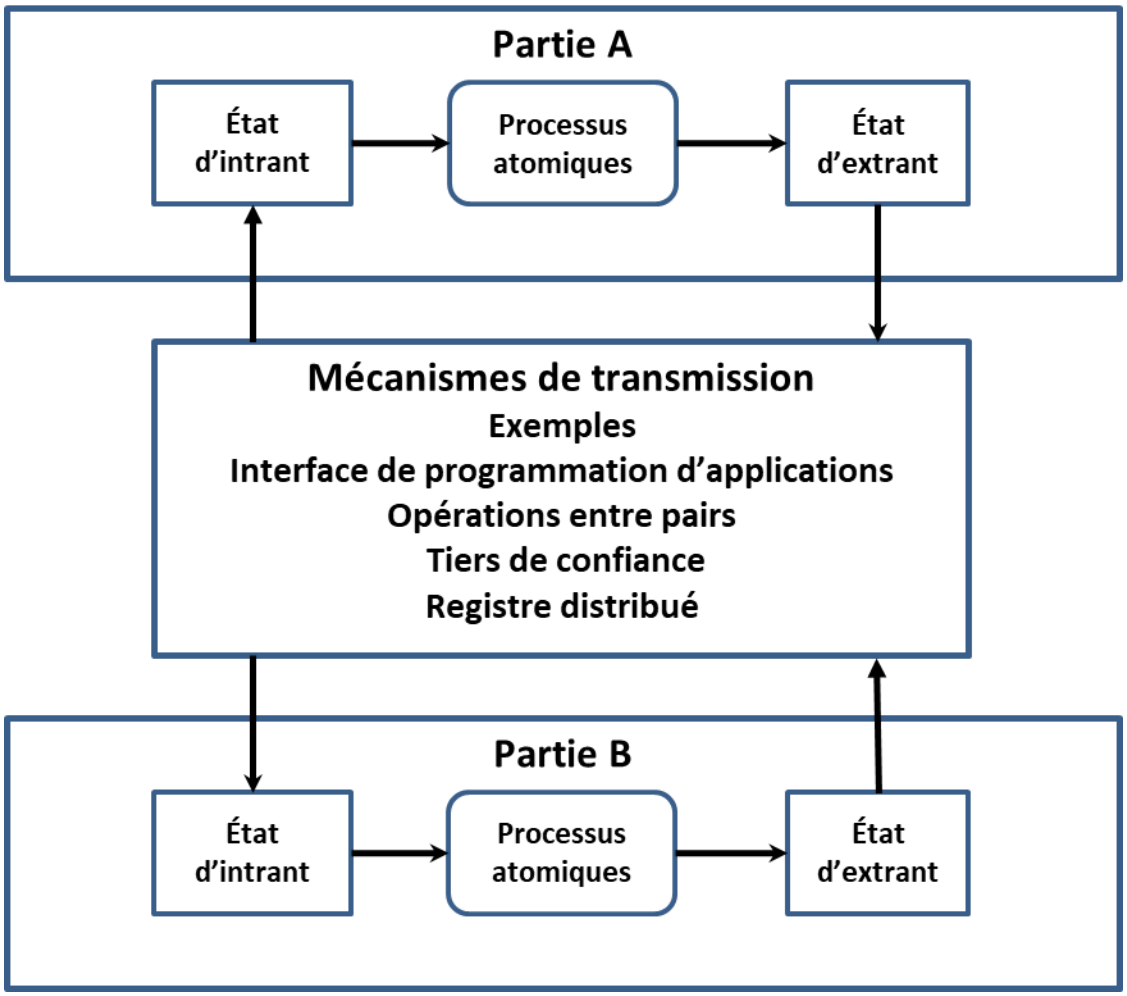


Figure 9 : Communication d'états de sortie entre les parties

Le CCP ne recommande pas un moyen de transport plutôt qu'un autre. De plus, le CCP permet à des fournisseurs concurrents de coexister pour répondre aux besoins des différentes collectivités du secteur public et du secteur privé en matière de mécanismes de transport.

2.6 Écosystème numérique — Rôles et flux d'information

La figure 10 illustre un modèle conceptuel des rôles et des flux d'information de l'écosystème numérique. (Il est à noter que les « méthodes » du diagramme sont abordées à la section 2.5.1.)

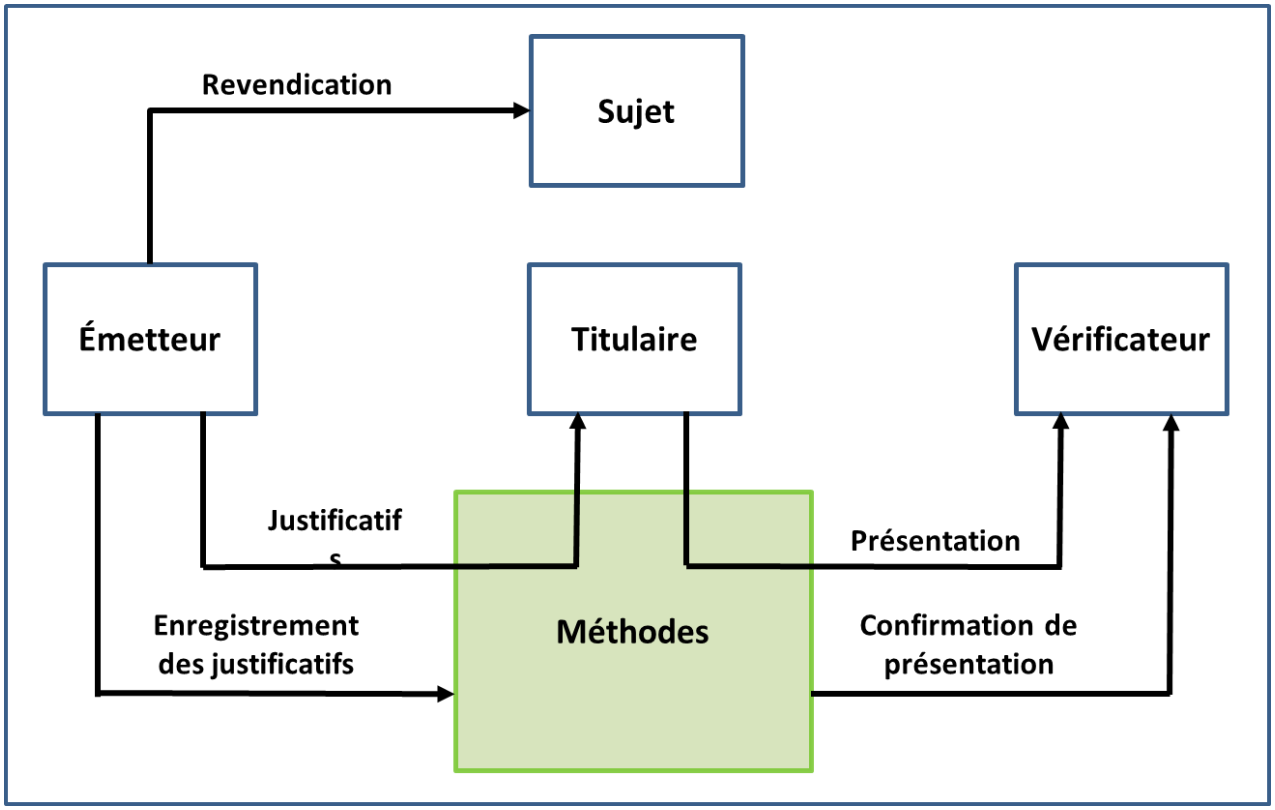


Figure 10 : Rôles et flux d'information de l'écosystème numérique

2.6.1 Rôles

Le modèle comporte quatre rôles :

1. **Sujet** : Entité visée par des revendications présentées par un émetteur.
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[14].
4. **Vérificateur** : Entité qui accepte une présentation d'un titulaire aux fins de prestation de services ou d'administration de programmes.

Traditionnellement, les rôles de l'écosystème numérique sont assumés (en tout ou en partie) par de nombreuses entités différentes agissant sous diverses appellations. Ces acteurs et leurs rôles traditionnels peuvent être assignés aux rôles de l'écosystème numérique comme le montre le tableau suivant.

Rôle	Acteurs
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.
Titulaire	Propriétaire d'identité numérique, titulaire de carte.
Vérificateur	Partie utilisatrice, fournisseur de services de vérification des justificatifs, consommateur d'identité numérique, fournisseur de services délégué, consommateur.

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).

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.

[14] Par exemple, lorsque le titulaire n'est pas l'objet d'un titre de créance, il s'agit d'un parent (le titulaire) qui détient le certificat de naissance (le justificatif) de son enfant (le sujet) ou d'un propriétaire de restaurant (le titulaire) qui détient un permis d'exploitation (le justificatif) d'une entreprise (le sujet).

2.6.2 Flux d'information

En outre, le modèle comprend cinq flux d'information :

1. **Revendication :** Une déclaration sur un sujet ou une déclaration sur une association qui existe entre deux sujets ou plus. Les émetteurs font valoir leurs revendications.
2. **Justificatif** : Une affirmation d'identité, de qualification, de compétence, d'autorité, de droits, de privilèges, d'autorisations, d'état, d'admissibilité ou de propriété d'actifs (ou une combinaison de ces éléments). Un justificatif contient un ensemble d'une ou plusieurs revendications faites sur un ou plusieurs sujets. ***15***
3. **Présentation** : Renseignements tirés d'un ou de plusieurs justificatifs. Les justificatifs sources peuvent avoir été émis par différents émetteurs.
4. **Enregistrement de justificatif** : Déclaration de l'émetteur selon laquelle l'émetteur émet un type de justificatif. La déclaration peut comprendre une définition du format des justificatifs.
5. **Confirmation de présentation :** Une détermination par le vérificateur de l'exactitude[16] de la présentation.

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

[16] La détermination de l'exactitude implique l'acceptation par le vérificateur de l'autorité des émetteurs des justificatifs qui constituent la base de la présentation et de veiller à ce que les justificatifs d'identité source n'aient pas été falsifiés.

2.7 Processus atomiques en détail

2.7.1 Processus des domaines liés à l'identité

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[17], les exigences en matière de renseignements sur l'identité[18] et l'identificateur[19].
État d'intrant	**Aucune décision n'a été prise :** 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.

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.

[17] Voir la section 4.3 pour obtenir de plus amples renseignements.

[18] Voir la section 4.4 pour obtenir de plus amples renseignements.

[19] Voir la section 4.4.1 pour obtenir de plus amples renseignements.

Acceptation des preuves d'identité

Description du processus	L'acceptation de la preuve d'identité est le processus qui consiste à confirmer que la preuve d'identité présentée (physique ou électronique) est acceptable.
État d'intrant	**Preuve d'identité non confirmée** : La preuve d'identité n'a pas été confirmée comme acceptable.
État d'extrant	**Preuve d'identité confirmée : La preuve d'identité a été confirmée comme acceptable.**

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, tel qu'il est établi 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.

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[20].
État d'intrant	**Renseignements sur l'identité** : Les renseignements sur l'identité peuvent ou non être propres à un seul sujet.
État d'extrant	**Renseignements uniques sur l'identité** : Les renseignements sur l'identité se rapportent uniquement à un seul sujet.

[20] Voir la section 4.5 pour obtenir de plus amples renseignements.

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.

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. [21]
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.

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.

[21] Pour de plus amples renseignements sur la vérification de l'identité, voir l'annexe F.

Maintien de l'identité

Description du processus	Le processus de maintien de l'identité consiste à veiller à ce que les renseignements sur l'identité d'un sujet soient 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.

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.

2.7.2 Processus des domaines liés aux relations

Détermination des renseignements sur la relation

Description du processus	La détermination des renseignements sur la relation est le processus de détermination du contexte de la relation, des exigences en matière renseignements sur la relation et de l'identificateur de la relation.
État d'intrant	**Aucune décision n'a été prise** : Le contexte de la relation, les exigences en matière de renseignements sur la relation et l'identificateur de relation n'ont pas été déterminés.
État d'extrant	**Détermination effectuée** : Le contexte de la relation, les exigences en matière de renseignements sur la relation et l'identificateur de relation ont été déterminés.

Détermination de la preuve de relation

Description du processus	Preuve de relation : La détermination est le processus visant à déterminer la preuve acceptable d'une relation (physique ou électronique).
État d'intrant	**Aucune détermination n'a été faite** : La preuve d'une relation acceptable n'a pas été déterminée.
État d'extrant	**Détermination effectuée** : La preuve d'une relation acceptable a été déterminée.

Acceptation des preuves de relation

Description du processus	Preuve de relation : L'acceptation est le processus qui consiste à confirmer que la preuve d'une relation présentée (physique ou électronique) est acceptable.
État d'intrant	**Preuve de relation non confirmée** : La preuve d'une relation n'a pas été confirmée comme acceptable.
État d'extrant	**Preuve de relation confirmée : La preuve d'une relation a été confirmée comme acceptable.**

Validation des renseignements sur la relation

Description du processus	La validation des renseignements sur les relations est le processus de confirmation de l'exactitude des renseignements sur une relation entre deux sujets ou plus, comme établi par l'émetteur.
État d'intrant	**Renseignements sur les relations non confirmés** : Les renseignements sur la relation n'ont pas été confirmés auprès de l'émetteur.
État d'extrant	**Renseignements sur les relations confirmés** : Les renseignements sur la relation ont été confirmés auprès de l'émetteur.

Résolution des relations

Description du processus	La résolution des relations est le processus qui consiste à établir le caractère unique d'une instance de relation au sein d'une population de programmes et de services par l'utilisation de renseignements sur les relations et de renseignements sur l'identité.
État d'intrant	**Renseignements sur la relation et l'identité** : Les renseignements sur la relation et l'identité peuvent ou non être propres à une seule relation.
État d'extrant	**Renseignements uniques sur la relation et l'identité** : Les renseignements sur la relation et les renseignements sur l'identité sont uniques à une seule relation.

Établissement des relations

Description du processus	L'établissement de relations est le processus de création d'un enregistrement d'une relation entre deux sujets ou plus.
État d'intrant	**Aucun dossier de relation** : Aucun dossier d'une relation n'existe.
État d'extrant	**Dossier de relation** : Il existe un dossier d'une relation.

Vérification de la relation

Description du processus	La vérification de la relation est le processus de confirmation que les renseignements sur la relation sont subordonnés au contrôle du sujet.
État d'intrant	**Contrôle non vérifié** : Il n'est pas confirmé que les renseignements sur la relation sont subordonnés au contrôle des sujets.
État d'extrant	**Contrôle vérifié** : Il est confirmé que les renseignements sur la relation sont subordonnés au contrôle des sujets.

Continuité des relations

Description du processus	Le processus de continuité des relations consiste à confirmer dynamiquement qu'une relation entre deux sujets ou plus a une existence continue au fil du temps.
État d'intrant	**Présence périodique** : La relation existe seulement de façon sporadique et souvent uniquement en association avec un événement vital ou d'une entreprise (p. ex., naissance, mariage, acquisition)**.**
État d'extrant	**Présence continue** : La relation existe de façon permanente en association avec de nombreuses transactions.

Maintien de la relation

Description du processus	Le maintien des relations est le processus qui consiste à veiller à ce que les renseignements sur une relation entre deux sujets ou plus soient exacts, complets et à jour.
État d'intrant	**Renseignements sur la relation** : Les renseignements sur la relation ne sont pas à jour.
État d'extrant	**Renseignements de relation mis à jour** : Les renseignements sur la relation sont à jour.

Suspension de la relation

Description du processus	La suspension de la relation est le processus qui consiste à signaler qu'un dossier de relation n'est plus temporairement en vigueur.
État d'intrant	**Dossier de relation** : Il existe un dossier d'une relation.
État d'extrant	**Relation suspendue** : La relation n'est plus en vigueur temporairement.

Rétablissement de la relation

Description du processus	Le rétablissement de la relation est le processus de transformation d'une relation suspendue en état actif.
État d'intrant	**Relation suspendue** : Le dossier d'une relation n'est plus en vigueur temporairement.
État d'extrant	**Compte rendu de la relation mis à jour** : Le dossier d'une relation a été mis à jour.

Révocation de la relation

Description du processus	La révocation de la relation est le processus qui consiste à signaler qu'un dossier de relation n'est plus temporairement en vigueur.
État d'intrant	**Dossier de relation** : Il existe un dossier d'une relation.
État d'extrant	**Relation révoquée** : La relation n'est plus en vigueur.

2.7.3 Processus des domaines liés aux justificatifs

Émission d'un justificatif

Description du processus	Le processus d'émission d'un justificatif consiste à créer un justificatif à partir d'un ensemble de revendications et d'attribuer le justificatif à un titulaire.
État d'intrant	**Aucun justificatif** : Aucune revendication n'a été associée aux renseignements du justificatif.
État d'extrant	**Émission d'un justificatif** : Une ou plusieurs revendications concernant un ou plusieurs sujets ont été associées aux renseignements d'identification et les renseignements d'identification ont été attribués à un titulaire.

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.

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	**Justificatif émis** : Un justificatif a été attribué à un titulaire.
État d'extrant	**Justificatif validé : Le justificatif émis est valide.**

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[22]. 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.

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.

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.

[22] Pour de plus amples renseignements sur le justificatif, voir l'annexe G.

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.

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.

2.7.4 Processus des domaines liés au consentement

Formulation de l'avis de consentement

Description du processus	La formulation d'avis de consentement est le processus consistant à produire un énoncé d'avis de consentement décrivant les renseignements personnels qui sont recueillis ou qui peuvent l'être; les parties auxquelles les renseignements personnels sont transmis (connus au moment de la présentation), et le type de renseignements personnels transmis; les fins auxquelles les renseignements personnels sont recueillis, utilisés ou divulgués; le risque de préjudice et d'autres conséquences de la collecte, de l'utilisation ou de la divulgation; la façon dont les renseignements personnels seront traités et protégés; la période d'application de l'avis de consentement; et la personne ou l'entité ayant compétence ou autorité pour l'énoncé d'avis de consentement émis. Ce processus devrait être effectué conformément à toute exigence de la législation et de la réglementation de compétence.
État d'intrant	**Aucun énoncé d'avis de consentement** : Aucun énoncé d'avis de consentement n'existe.
État d'extrant	**Énoncé d'avis de consentement** : Un énoncé d'avis de consentement existe.

Présentation de l'avis de consentement

Description du processus	La présentation de l'avis de consentement est le processus de présentation d'un avis de consentement à une personne.
État d'intrant	**Énoncé d'avis de consentement** : Un énoncé d'avis de consentement existe.
État d'extrant	**Énoncé d'avis de consentement présenté** : Un avis de consentement a été présenté à une personne.

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 de consentement présenté** : Un avis de

	consentement a été présenté à une personne.
État d'extrant	**Décision de consentement** : Une décision de consentement existe.

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. De plus, les renseignements sur la personne peuvent également être stockés. Par exemple : des renseignements sur la personne, la version de l'avis de consentement qui lui a été présentée, la date et l'heure auxquelles l'avis de consentement a été présenté et, le cas échéant, la date d'expiration 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.

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 la 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.

Renouvellement du consentement

Description du processus	Le processus de renouvellement du consentement consiste à prolonger la période de 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 stocké a été mise à jour

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 stocké a été mise à jour.

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 stocké a été mise à jour

2.7.5 Processus des domaines liés aux signatures

Création d'une 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

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). L'établissement et le maintien des 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]; 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 liée à une identité principale (p. ex., un permis de conduire) ou ne pas être liée à une identité fondamentale (p. ex., un profil de médias sociaux). L'identité contextuelle est établie et maintenue à la fois par les secteurs public et privé.

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

Qualificateurs de niveaux d'assurance (NA) à l'échelle pancanadienne	
Qualificateur	**Description**
IP1	Niveau 1 : Besoin d'un faible niveau de confiance que la personne est bien celle qu'elle affirme être.
IP2	Besoin d'un certain niveau de confiance que la personne est bien celle qu'elle affirme être.
IP3	Besoin d'un niveau élevé de confiance que la personne est bien celle qu'elle affirme être.
IP4	Besoin d'un niveau très élevé de confiance que la personne est bien celle qu'elle affirme être.

Qualificateurs de niveaux d'assurance de l'identité à l'échelle pancanadienne	
Qualificateur	**Description**
IO1	Besoin d'un faible niveau de confiance que l'organisation est bien celle qu'elle

	affirme être.
IO2	Besoin d'un certain niveau de confiance que l'organisation est bien celle qu'elle affirme être.
IO3	Besoin d'un niveau élevé de confiance que l'organisation est bien celle qu'elle affirme être.
IO4	Besoin d'un niveau très élevé de confiance que l'organisation est bien celle qu'elle affirme être.

Qualificateurs de niveaux d'assurance de la relation à l'échelle pancanadienne	
Qualificateur	**Description**
R1	Besoin d'un faible niveau de confiance que la ou les personnes sont bien celles qu'elles affirment être, quant à l'exactitude des renseignements sur l'identité de la ou des organisations et à la preuve de la relation.
R2	Besoin d'un certain niveau de confiance que la ou les personnes sont bien celles qu'elles affirment être, quant à l'exactitude des renseignements sur l'identité de la ou des organisations et à la preuve de la relation.
R3	Besoin d'un niveau élevé de confiance que la ou les personnes sont bien celles qu'elles affirment être, quant à l'exactitude des renseignements sur l'identité de la ou des organisations et à la preuve de la relation.
R4	Besoin d'un niveau très élevé de confiance que la ou les personnes sont bien celles qu'elles affirment être, quant à l'exactitude des renseignements sur l'identité de la ou des organisations et à la preuve de la relation.

Niveaux d'assurance des justificatifs à l'échelle pancanadienne	
Qualificateur	**Description**
C1	Besoin d'un faible niveau de confiance qu'un titulaire exerce un contrôle sur un justificatif émis et que le justificatif émis est valide.
C2	Besoin d'un certain niveau de confiance qu'un titulaire exerce un contrôle sur un justificatif émis et que le justificatif émis est valide.
C3	Besoin d'un niveau élevé de confiance qu'un titulaire exerce un contrôle sur un justificatif émis et que le justificatif émis est valide.
C4	Besoin d'un niveau très élevé de confiance qu'un titulaire exerce un contrôle sur un justificatif émis et que le justificatif émis est valide.

2.8.3 Qualificateurs de domaine de signature

La partie 2 de la *Loi fédérale sur la protection des renseignements personnels et les documents électroniques 7* (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*** qui est définie en détail dans le *Règlement sur les signatures électroniques sécurisées* [RSES] ci-joint). Des signatures électroniques sécurisées peuvent être utilisées comme qualificateurs de domaine de signature.

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** : Fait référence aux processus du domaine d'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
relation de mandataire	Cas particulier d'une relation équilibrée où les entités sont égales, mais où une entité (le principal) nomme une autre entité (le mandataire) pour agir au nom du mandant à une fin déterminée (p. ex., procuration, société comptable qui produit des déclarations pour une société). Voir également « relation équilibrée ».
agent	Personne agissant pour le compte d'une entité.
identificateur attribué	Chaîne numérique ou alphanumérique automatiquement générée et permettant de faire la distinction entre des entités d'une population sans recourir à un autre attribut d'identité.
assurance	Confiance qu'une déclaration est vraie.
Niveau d'assurance	Un niveau de confiance qu'une déclaration est vraie et sur laquelle d'autres peuvent se fier.
entité atomique	Une entité qui ne peut pas être décomposée en unités plus petites. Les personnes sont des entités atomiques. Voir également « entité composée ».
processus atomique	Il s'agit d'un ensemble d'activités logiquement mis en correspondance qui entraînent l'état de transition d'un objet. D'autres processus atomiques peuvent se fier à l'état de sortie de l'objet.
attribut	Une propriété ou une caractéristique d'élément. Voir également « attribut d'entité », « attribut de relation », « attribut d'identification » et « attribut d'identité ».
authentifications	Voir « vérification des justificatifs ».

Terme	Définition
authentificateur	Quelque chose qu'un titulaire contrôle et qui est utilisé pour prouver que le titulaire a conservé le contrôle sur un justificatif émis.
source faisant autorité	Un ensemble ou un registre de dossiers conservés par une autorité qui respecte les critères établis.
relation équilibrée	Une relation dans laquelle les entités sont égales (p. ex., les époux dans un mariage, les partenaires dans une entreprise, les sociétés dans une coentreprise). Voir également « relation de mandataire ».
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.
biométrique	Terme général utilisé pour décrire une caractéristique ou un processus. Il peut s'agir d'une caractéristique biologique (anatomique et physiologique) ou comportementale mesurable, qui peut être utile à la reconnaissance automatisée. Elle peut également faire référence à des méthodes automatisées de reconnaissance d'une personne en fonction de caractéristiques biologiques (anatomiques et physiologiques) et comportementales mesurables.
événement organisationnels	Un événement discret important se produisant durant la vie d'une entreprise. En vertu de la loi, un événement organisationnel doit être enregistré auprès d'une entité gouvernementale et est assujetti à la loi et aux règlements. Parmi les événements organisationnels, on peut citer l'enregistrement de la charte, la fusion, le

Terme	Définition
	regroupement, l'abandon de charte, et la dissolution.
revendication	Une déclaration sur un sujet ou une déclaration sur une association qui existe entre deux sujets ou plus. Une revendication est exprimée au moyen d'un ou de plusieurs attributs. Les émetteurs font valoir leurs revendications. Voir aussi « Revendication du sujet » et « Revendication de la relation ».
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.
entité composée	Une entité qui comprend une ou plusieurs entités atomiques. Les organisations sont des entités composées. Voir également « entité atomique ».
processus composé	Un ensemble de processus atomiques et/ou d'autres processus composés qui entraînent un ensemble de transitions d'état.
critères de conformité	Un ensemble d'énoncés d'exigences définissant ce qu'il faut pour assurer l'intégrité d'un processus atomique.
expiration du consentement	Le processus qui consiste à suspendre la validité d'une décision de consentement par un « oui » en raison d'une date d'expiration dépassée.
formulation d'avis de consentement	Le processus consistant à produire un énoncé d'avis de consentement décrivant les renseignements personnels qui sont recueillis ou qui peuvent l'être; les parties auxquelles les renseignements personnels sont transmis (connus au moment de la présentation), et le type de renseignements personnels transmis; 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

Terme	Définition
	divulgation; la façon dont les renseignements personnels seront traités et protégés; la période d'application de l'avis de consentement; et la personne ou l'entité ayant compétence ou autorité pour l'énoncé d'avis de consentement émis. Ce processus devrait être effectué conformément à toute exigence de la législation et de la réglementation de compétence.
Présentation de l'avis de consentement	Le processus de présentation d'un avis de consentement à une personne.
enregistrement du consentement	Le processus qui consiste 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 de consentement 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.
renouvellement du consentement	Le processus qui consiste à prolonger la période de validité d'une décision de consentement par « oui » en reportant la date d'expiration.
demande de consentement	Le processus qui 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 ».
examen du consentement	Le processus qui consiste à rendre les détails d'une décision de consentement stockée visibles pour la personne qui a donné le consentement.
révocation du consentement	Le processus qui 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

Terme	Définition
	« non »).
identité contextuelle	Une identité qui est utilisée à des fins particulières dans un contexte d'identité spécifique (p. ex., banque, permis d'affaires, services de santé, permis de conduire ou médias sociaux). Selon le contexte identitaire, une identité contextuelle peut être liée à une identité principale (p. ex., un permis de conduire) ou ne pas être liée à une identité fondamentale (p. ex., un profil de médias sociaux).
justificatifs	Une affirmation d'identité, de qualification, de compétence, d'autorité, de droits, de privilèges, d'autorisations, d'état, d'admissibilité ou de propriété d'actifs (ou une combinaison de ces éléments). Un justificatif contient un ensemble d'une ou plusieurs revendications faites sur un ou plusieurs sujets.
assurance du justificatif	Niveau de confiance requis qu'un titulaire exerce un contrôle sur un justificatif émis et que le justificatif émis est valide.
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.
attribut du justificatif	Une propriété ou une caractéristique d'un justificatif.
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.

Terme	Définition
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.
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.
Métadonnées du justificatif	Un ou plusieurs attributs de justificatifs qui décrivent les propriétés ou les caractéristiques des charges utiles d'un justificatif.
Charge utile d'un justificatif	Un ensemble d'une ou plusieurs revendications faites sur un ou plusieurs sujets.
Preuves des justificatifs	Une ou plusieurs méthodes ou mécanismes utilisés pour vérifier que l'émetteur est l'auteur du justificatif et que le justificatif n'a pas été altéré.
recouvrement d'un justificatif	Le processus qui consiste à transformer à nouveau un justificatif suspendu en justificatif utilisable (c.-à-d. un justificatif utilisable).
Enregistrement des justificatifs	Déclaration de l'émetteur selon laquelle l'émetteur émet un type de justificatif. La déclaration peut comprendre une définition du format des justificatifs.
révocation d'un justificatif	Le processus permettant de garantir qu'un justificatif émis est en permanence marqué comme inutilisable.
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.
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.
vérification du justificatif	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.

Terme	Définition
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.
identité numérique	Une représentation électronique d'une entité employée exclusivement par celle-ci, dans le but d'accéder à des services appréciables et d'effectuer des transactions en toute confiance et avec assurance.
relation numérique	Une représentation électronique de la relation entre deux entités ou plus.
représentation numérique	Une représentation électronique d'une entité ou de la relation entre deux entités ou plus.
relation dirigée	Une relation dans laquelle les entités ne sont pas égales (p. ex., le parent et l'enfant, la société mère et la société filiale, le gestionnaire et le subordonné).
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 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.
preuves électroniques ou numériques	Toute donnée enregistrée ou préservée sur n'importe quel support, par un système informatique ou tout autre appareil semblable. Exemples : enregistrements dans une base de données, journaux d'audit ou documents produits au moyen d'un logiciel de traitement de texte.
entité	Une existence distincte et indépendante, comme une personne ou une organisation, qui peut être assujettie à des lois, des politiques ou des règlements dans un contexte, et qui peut avoir certains droits, devoirs et obligations. Une entité peut remplir un ou plusieurs des

Terme	Définition
	quatre rôles (c'est-à-dire Sujet, Émetteur, Titulaire ou Vérificateur) dans l'écosystème numérique.
attribut d'entité	Une propriété ou une caractéristique d'entité.
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 aussi offrir des renseignements supplémentaires comme une photo, une signature ou une adresse. Par exemple, les dossiers d'assurance sociale; les dossiers sur le droit de voyager, de conduire ou d'obtenir des services de santé; les dossiers de mariage, de changement de nom ou de décès provenant d'une autorité compétente. Une preuve d'identité qui corrobore la preuve d'identité principale et aide à relier les renseignements sur l'identité à une organisation. Elle peut également fournir des renseignements supplémentaires comme l'activité sur les marchés, une signature ou une adresse. Par exemple, les registres des permis d'exploitation forestière ou minière ou de culture du cannabis et les enregistrements de statut d'organisme de bienfaisance.
preuve d'identité 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 d'identité	Un registre d'une source faisant autorité indiquant l'identité d'une entité. Il existe deux catégories de preuve d'identité : principale et contextuelle.

Terme	Définition
	Voir « preuve d'identité principale » et « preuve d'identité contextuelle ».
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.
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.
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).
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]].

Terme	Définition
événement fondamental	Un événement fondamental est soit un événement organisationnel, soit un événement vital. Les événements organisationnels 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 organisationnels et les événements vitaux doivent être enregistrés auprès d'une entité gouvernementale et sont assujettis à la législation et à la réglementation. Voir « événement organisationnel » et « événement vital ».
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).
genre	désigne une identité sociale, comme le fait d'être un homme, une femme, une personne non binaire ou une personne bispirituelle.
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.
identificateur	Ensemble d'attributs d'identité utilisés pour distinguer uniquement une entité particulière au sein d'une population.
identité	Référence ou désignation utilisée pour distinguer de façon unique une entité donnée. Il existe deux types d'identité : identité principale et identité contextuelle. Voir « preuve d'identité principale » et « preuve d'identité contextuelle ».
assurance de l'identité (d'une organisation)	Besoin d'un niveau de confiance que l'organisation est bien celle qu'elle affirme être.
assurance de l'identité	Besoin d'un niveau de confiance que la personne est

Terme	Définition
(d'une personne)	bien celle qu'elle affirme être.
niveau d'assurance de l'identité (d'une organisation)	Le niveau de confiance que les renseignements sur l'identité de l'organisation sont exacts.
niveau d'assurance de l'identité (d'une personne)	Le niveau de confiance que la personne est bien celle qu'elle affirme être.
attribut d'identité	Propriété ou caractéristique associée à une entité identifiable (également appelée « élément de données d'identité »). Les attributs d'identité d'une entité sont un sous-ensemble des attributs d'entité de l'entité.
Contexte de l'identité	L'environnement ou l'ensemble des circonstances dans lesquelles une organisation exerce ses activités et dans lesquelles elle offre ses programmes et ses services. Le contexte de l'identité est déterminé par des facteurs comme le mandat, la population cible (c.-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) et d'aborder les préoccupations quant à la possibilité d'une usurpation d'identité.
élément de données d'identité	Voir « attribut d'identité ».
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.
détermination de la preuve d'identité	Le processus de détermination de la preuve d'identité acceptable (matérielle ou électronique).
acceptation de la preuve d'identité	Le processus qui consiste à confirmer que la preuve d'identité présentée (physique ou électronique) est acceptable.

Terme	Définition
renseignements sur l'identité	Ensemble d'attributs d'identité qui sont utilisés uniquement pour distinguer une entité donnée dans une population de programme ou de service et pour décrire cette entité conformément au programme ou au service. Selon le contexte, les renseignements d'identité sont soit un sous-ensemble de renseignements personnels, soit un sous-ensemble de renseignements organisationnels.
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.
avis des renseignements sur l'identité	La divulgation de renseignements sur l'identité d'une entité par une partie faisant autorité à une partie de confiance qui est déclenchée par un événement vital ou un événement commercial, un changement des renseignements d'identité ou une indication que les renseignements d'identité ont été exposés à un facteur de risque (p. ex., décès de la personne, abandon de la charte, utilisation de documents expirés, atteinte à la vie privée, utilisation frauduleuse des renseignements d'identification).
récupération des renseignements sur l'identité	La divulgation de renseignements sur l'identité d'une entité par une partie faisant autorité à une partie de confiance qui est déclenchée par une demande de la partie faisant autorité.
Validation des renseignements sur l'identité	Le processus qui consiste à confirmer l'exactitude des renseignements sur l'identité d'un sujet comme établis par l'émetteur.
Établissement de liens pour déterminer l'identité	Le processus de mise en correspondance entre deux identifiants ou plus et le même sujet.
maintien de l'identité	Le processus qui consiste à veiller à ce que les renseignements sur l'identité d'un sujet soient exacts, complets et à jour.
gestion de l'identité	Ensemble de principes, de pratiques, de processus et de procédures utilisés pour réaliser le mandat d'une organisation et ses objectifs liés à l'identité.

Terme	Définition
modèle d'identité	Une représentation simplifiée (ou abstraite) d'une méthodologie de gestion de l'identité (également appelée « schéma d'identité »). Les modèles d'identité centralisés, fédérés et décentralisés en sont des exemples.
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.
schéma d'identité	Voir « modèle d'identité ».
vérification de l'identité	Le processus qui consiste à confirmer que les renseignements sur l'identité sont subordonnés au contrôle du sujet.
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.
confirmation fondée sur les connaissances	Méthode de vérification de l'identité qui utilise des renseignements personnels ou organisationnels ou des secrets partagés pour prouver que l'entité qui présente les renseignements identificateurs contrôle l'identité. La confirmation fondée sur les connaissances est obtenue au moyen du modèle défi-réponse : l'entité qui présente les renseignements d'identité se voit poser des questions, réponses auxquelles (en théorie du moins) seuls elle et l'interrogateur seraient au courant (p. ex., renseignements financiers, historique de crédit, secret partagé, clé cryptographique, code d'accès envoyé par la poste, mot de passe, numéro d'identification personnel, identificateur attribué).
dénomination sociale	Voir « nom fondamental », « nom principal ».
présence légale	Droit d'être ou de résider légalement au Canada.
méthodes	Les ensembles de règles qui régissent la façon dont les acteurs de l'écosystème numérique interagissent directement ou indirectement entre eux. Les méthodes englobent des éléments comme les modèles et schémas de données, les protocoles de communication, les

Terme	Définition
	mécanismes de transport, les algorithmes cryptographiques, les bases de données, les registres distribués, les registres de données vérifiables et les systèmes similaires et les combinaisons de celles-ci.
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.
organisation	Une entité juridique qui n'est pas un être humain (appelée en droit « personne morale »).
renseignements organisationnels	renseignements sur une organisation identifiable.
personne	Un être humain (appelé en droit « personne physique »), y compris des « mineurs » et d'autres personnes qui ne peuvent être considérées comme des personnes en vertu de la loi.
renseignements personnels	renseignements sur une personne identifiable.
confirmation de possession matérielle	méthode de vérification de l'identité qui exige la possession physique ou la présentation d'éléments de preuve pour prouver que l'entité qui présente les renseignements sur l'identité contrôle l'identité.
prénom d'usage	Le nom par lequel une personne préfère qu'on s'adresse à elle de façon informelle.
présentation	Renseignements tirés d'un ou de plusieurs justificatifs. Les justificatifs sources peuvent avoir été émis par différents émetteurs.
confirmation de présentation	Une détermination par le vérificateur de l'exactitude de la présentation.
nom principal	Nom utilisé par une personne ou une organisation à des fins officielles et légales (également appelé « nom légal »).

Terme	Définition
	Voir aussi « nom fondamental ».
relation	Une relation est une association entre deux entités ou plus.
assurance de la relation	Niveau de confiance que la ou les personnes sont bien celles qu'elles affirment être, quant à l'exactitude des renseignements sur l'identité de la ou des organisations et à la preuve de la relation.
niveau d'assurance de la relation	Niveau de confiance que la ou les personnes sont bien celles qu'elles affirment être, quant à l'exactitude des renseignements sur l'identité de la ou des organisations et à la preuve de la relation.
attribut de la relation	Une propriété ou une caractéristique d'une association entre deux ou plusieurs entités.
Revendication de relation	Une déclaration sur une association qui existe entre deux sujets ou plus. Une revendication de relation est exprimée au moyen d'un ou de plusieurs attributs de relation.
continuité des relations	Le processus qui consiste à confirmer dynamiquement qu'une relation entre deux sujets ou plus a une existence continue au fil du temps.
établissement des relations	Le processus de création d'un enregistrement d'une relation entre deux sujets ou plus.
détermination de la preuve de relation	Le processus visant à déterminer la preuve acceptable d'une relation (physique ou électronique).
acceptation des preuves de relation	Le processus qui consiste à confirmer que la preuve d'une relation présentée (physique ou électronique) est acceptable.
identificateur de relation	Ensemble d'identificateurs des parties dans la relation et l'attribut de relation *type de relation*.
renseignements sur les relations	Ensemble d'attributs de relation qui décrit l'association entre deux entités ou plus.
détermination des renseignements sur la relation	Le processus de détermination du contexte de la relation, des exigences en matière renseignements sur la relation et de l'identificateur de la relation.

Terme	Définition
validation des renseignements liés à la relation	Le processus de confirmation de l'exactitude des renseignements sur une relation entre deux sujets ou plus, tel qu'il est établi par l'émetteur.
maintien de la relation	Le processus qui consiste à veiller à ce que les renseignements sur une relation entre deux sujets ou plus soient exacts, complets et à jour.
rétablissement de la relation	Le processus de transformation d'une relation suspendue en état actif.
résolution des relations	Le processus qui consiste à établir le caractère unique d'une instance de relation au sein d'une population de programmes et de services par l'utilisation de renseignements sur les relations et de renseignements sur l'identité.
révocation de la relation	Le processus qui consiste à signaler qu'un dossier de relation n'est plus temporairement en vigueur.
suspension de la relation	Le processus qui consiste à signaler qu'un dossier de relation n'est plus temporairement en vigueur.
vérification de la relation	Le processus de confirmation que les renseignements sur la relation sont subordonnés au contrôle du sujet.
sexe	Renvoie aux caractéristiques biologiques, comme le fait d'être de sexe masculin ou féminin, ou intersexuel.
signature	Le processus qui consiste à créer 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 communiqué et l'intégrité des données de la transaction signée est maintenue, y compris l'original.
vérification de la signature	Le processus qui consiste à confirmer que la signature est valide.
création d'une signature	Le processus qui consiste à créer une signature.
sujet	Entité visée par des revendications présentées par un émetteur.

Terme	Définition
revendication présentée à un sujet	Une déclaration sur un sujet. Une revendication présentée à un sujet est exprimée au moyen d'un ou de plusieurs attributs d'entité.
cadre de confiance	Un ensemble de principes, de définitions, de normes, de spécifications, de critères de conformité et d'approche d'évaluation convenus.
confirmation par un arbitre de confiance	Méthode de vérification de l'identité qui s'appuie sur un arbitre de confiance pour prouver que l'entité présentant les renseignements d'identité contrôle l'identité. Le type d'arbitre de confiance et leur acceptabilité sont déterminés par des critères propres au programme. Les répondants de confiance comprennent les garants, les notaires, les comptables et les agents certifiés.
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 par le biais de conventions, de lois types et d'autres instruments qui traitent de domaines clés du commerce, du règlement des différends à la passation et à la vente de biens.
utilisateur	Voir « Titulaire ».
vérificateur	Une entité qui accepte une présentation d'un titulaire aux fins de prestation de services ou d'administration de programmes.

Terme	Définition
événement vital	Un événement discret important se produisant 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.

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

> « L'identité, c'est la façon dont nous reconnaissons, nous nous souvenons et, en fin de compte, nous répondons à des personnes et à des choses en particulier. Elle **nous aide** à garder le suivi des personnes et des choses… elle nous donne la capacité de **répondre** à chaque individu en tant que personne unique.
>
> [Traduction] 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[23]

4.1.2 L'identité dans la gestion de l'identité

Le concept d'identité dans la gestion de l'identité a une définition beaucoup plus stricte que les notions d'identité 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 entité en particulier.

Une identité doit être unique. [24] Cela signifie que chaque entité peut être distinguée de toutes les autres entités d'une population d'intérêt et que, au besoin, chaque entité peut être identifiée de manière unique. L'exigence d'unicité garantit qu'un programme ou un service peut être livré à une entité en particulier et qu'un programme ou service est livré à la bonne entité.

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

[24] C'est l'une des exigences pour l'établissement d'un niveau d'assurance de l'identité. Voir l'annexe C de la Norme sur l'assurance de l'identité et des justificatifs [SCT c., 2013].

4.2 Définir la population

Les entités visées par un programme ou un service constituent la population du programme ou du service[25].

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

1. les personnes nées en Alberta;
2. les personnes qui doivent remplir une déclaration de revenus destinée au gouvernement fédéral;
3. les personnes qui sont autorisées à conduire un véhicule au Québec;
4. les personnes qui sont des anciens combattants;
5. les personnes qui sont assurées par le régime d'assurance maladie de l'Ontario;
6. les organisations autorisées à cultiver du cannabis au Canada;
7. Les organisations tenues de s'enregistrer auprès de CANAFE;
8. les organisations autorisées à couper du bois en Colombie-Britannique;
9. les organisations assujetties à la surveillance du Bureau du surintendant des institutions financières;
10. 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.

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 communs entre les différents fournisseurs de programmes et de services. Il permet de déterminer si les

[25] Les caractéristiques d'une population de programme ou de service constituent le facteur clé pour déterminer le contexte de l'identité. Voir la section 4.3.

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., citoyens, entreprises, organismes à but non lucratif) ou en faire partie (p. ex., exemple, employés, ministères).
- 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 entité 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*. Parmi les attributs d'identité d'une organisation, mentionnons 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 entités 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 entité 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 sont habituellement limités au programme et limités par la législation 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.

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[26]. 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. Cela permet de veiller à ce que l'utilisation des renseignements sur l'identité soit conforme à l'objectif initial pour lequel les renseignements sur l'identité ont été obtenus et qu'ils puissent être gérés séparément ou protégés en plus par des mesures de sécurité et de protection des renseignements personnels appropriées. 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 entité 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 la législation et de la réglementation. 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 d'identité constituant l'identificateur. Un autre programme pourrait utiliser un identificateur attribué[27] (comme le numéro d'assurance maladie ou un numéro d'entreprise) à titre d'attribut d'identité constituant l'identificateur.

[26] Ce n'est généralement pas un problème pour les renseignements organisationnels.

[27] Voir la section 4.4.2;

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 entité faisant partie de la population du programme ou du service doit posséder l'ensemble d'attributs d'identité constituant l'identificateur. Toutefois, 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 entité 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 un 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 constituent pas une liste exhaustive. Un autre facteur qui pourrait être pris en considération est de savoir si le programme ou le service a le pouvoir légal de recueillir l'attribut identité. Un autre facteur pourrait être le degré d'invasivité de la collecte d'un attribut d'identité lorsque d'autres attributs d'identité pourraient suffire à l'objectif (p. ex., les échantillons d'ADN ne devraient pas être prélevés là où le nom suffirait).

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[28] 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

[28] 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

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 entité au moment où elle s'inscrit.

Toutefois, avant d'associer une personne à un identificateur attribué, il faut établir l'unicité de l'identité de l'entité au sein de la population visée (en d'autres mots, il faut effectuer une résolution de l'identité [voir la prochaine section]) par l'intermédiaire d'autres attributs d'identité (p. ex., le *nom*, la *date de naissance*, etc.). 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 entité au sein d'une population.

Une fois associé à une personne, un identificateur attribué permet d'établir l'unicité de cette entité parmi toutes les autres entités au sein de la population sans qu'il soit nécessaire de recourir à d'autres attributs d'identité. Les numéros d'enregistrement de naissance, les numéros d'entreprise, les numéros de permis de conduire, les numéros d'assurance sociale et les numéros de compte client sont 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 recourir pour faire la distinction entre les différentes entités 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 assignés peuvent être assujettis à des restrictions juridiques et politiques qui peuvent varier d'un secteur à l'autre. 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 entité 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 entité 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[29]. La qualité des renseignements sur l'identité se mesure par leur exactitude. Elle garantit la véracité des renseignements fournis au sujet d'une entité, 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 :

5. **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., décès d'une personne, dissolution d'une société). C'est pourquoi il faut toujours mettre à jour les renseignements sur l'identité lorsque le besoin survient, sans quoi ils deviennent inexacts.
6. Les renseignements sur l'identité se rapportent à une entité réelle. Les renseignements sur l'identité doivent être associés à une entité qui existe ou existait réellement à un moment donné.
7. **Les renseignements d'identité se rapportent à l'entité correcte.** Dans les grandes populations, certaines entités 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 entité.

Les fournisseurs de programmes et de services sont eux-mêmes responsables de veiller à l'exactitude des renseignements sur l'identité fournis dans le cadre de leurs

[29] C'est l'une des exigences pour l'établissement d'un niveau d'assurance de l'identité. Voir l'annexe C de la *Norme sur l'assurance de l'identité et des justificatifs* [SCT c., 2013].

programmes et de leurs services. L'exactitude des renseignements d'identité peut être assurée en les comparant à une source faisant autorité. Il y a deux façons d'y arriver :

8. 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.
9. 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 : ENTITÉS JURIDIQUES

5.1 Types d'entités juridiques.

Le droit canadien reconnaît deux types d'entités juridiques : les êtres humains appelés personnes physiques et les entités non humaines telles que les sociétés, les partenariats, les fonds, les fiducies, les coopératives, les organismes de bienfaisance enregistrés, les gouvernements, entre autres, qui sont traités en droit comme s'ils étaient des personnes physiques. Le Cadre de confiance pancanadien fait référence à ces deux types d'entités juridiques comme des personnes et des organisations, respectivement.

5.2 Traitement des renseignements sur les entités juridiques

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 : RELATIONS EN DÉTAIL

6.1 Modèles de relation

6.1.1 Relation équilibrée

Une relation équilibrée est une relation où les entités sont égales (c.-à-d. que la répartition du pouvoir entre les entités est symétrique) (p. ex., les époux dans un mariage, les associés dans une entreprise, les sociétés dans une coentreprise).

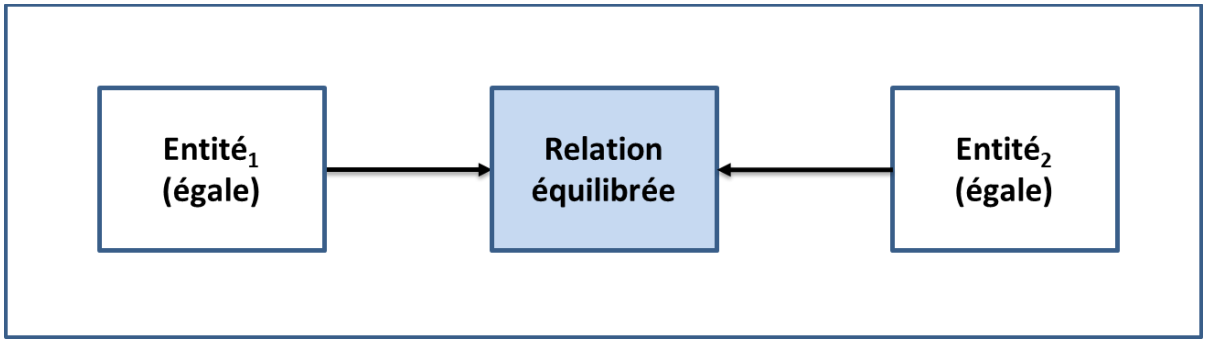


Figure 11 : Modèle de relation équilibrée

6.1.2 Relation de mandataire

Une relation de mandataire est un cas particulier d'une relation équilibrée où les entités sont égales, mais où une entité (le principal) nomme une autre entité (le mandataire) pour agir au nom du mandant à une fin déterminée (p. ex., procuration, société comptable qui produit des déclarations pour une société).

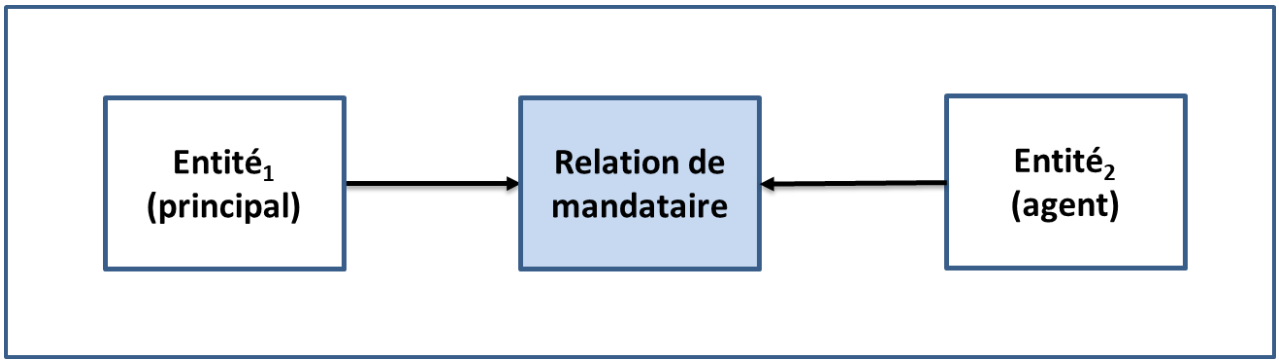


Figure 12 : **Modèle de relation de mandataire**

La relation entre un mandant et un mandataire est contractuelle. Par conséquent, les droits et les obligations du mandataire et du mandant sont conformes au contrat d'agence. Pour établir une agence, il faut obtenir le consentement du mandant et du mandataire, même si ce consentement peut être implicite plutôt qu'exprimé.

L'autorisation par laquelle le mandant nomme un autre mandataire et donne à celui-ci le pouvoir d'accomplir certains actes pour le compte du mandant peut être tout type de contrat ou d'accord. L'embauche d'un agent immobilier, d'un avocat, d'un assistant administratif représente des formes d'établissement de mandataire.

6.1.3 Relation dirigée

Une relation dirigée est une relation dans laquelle les entités ne sont pas égales (c.-à-d. que la répartition du pouvoir entre les entités est asymétrique) (p. ex., la société mère et l'enfant, la société mère et la filiale, le gestionnaire et le subalterne).

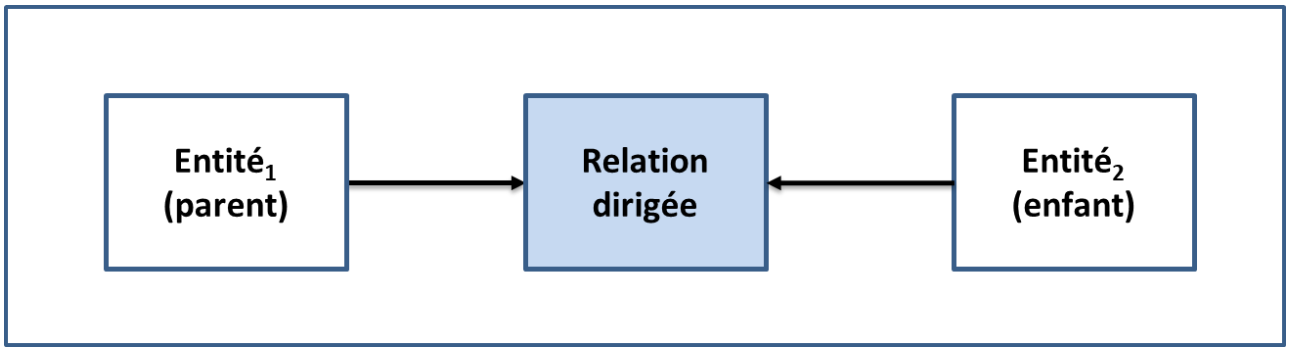


Figure 13 : Modèle de relation dirigée

6.2 Relations au sein d'une organisation

Les relations entre les entités atomiques (personnes) qui existent au sein d'une entité composée (une organisation) peuvent former un réseau complexe. Chaque relation du réseau peut être identifiée comme une relation équilibrée ou dirigée[30]. Cela est illustré dans la figure 14.

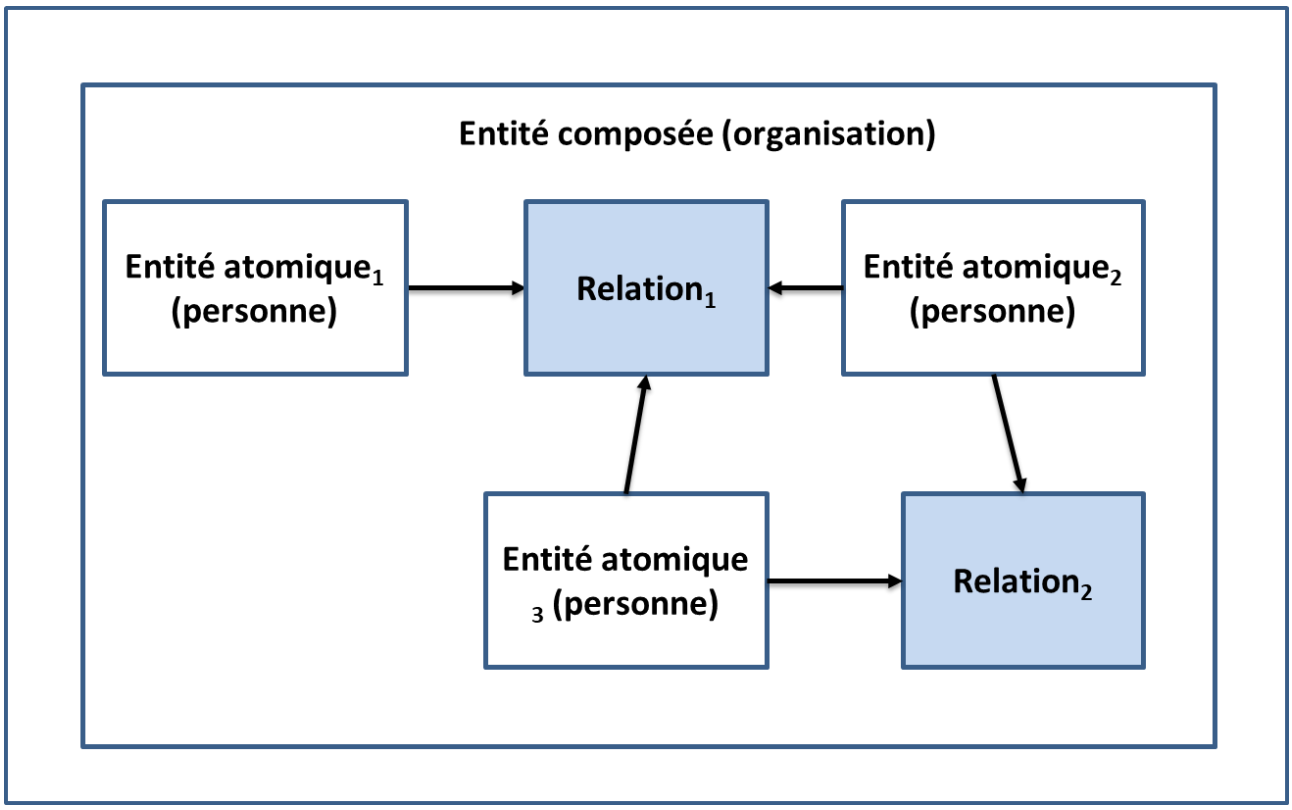


Figure 14 : Un réseau de relations internes au sein d'une organisation

[30] Les relations de mandataire peuvent exister au sein d'une organisation, mais elles sont probablement rares. On pourrait soutenir qu'un gestionnaire pourrait être considéré comme le principal et son subordonné comme l'agent. Toutefois, si l'on effectue une analyse de près, cet exemple de relation de mandataire acquiert probablement l'aspect de l'inégalité d'entité d'une relation dirigée et devrait être considéré comme tel.

6.3 Relations organisation-organisation

Les entités composées comme les organisations peuvent avoir des relations avec d'autres organisations et le réseau que ces relations forment peut être assez complexe. En outre, ces réseaux contiennent souvent les trois modèles de relation et, par conséquent, une organisation peut assumer plus d'un rôle de relation. Cela est illustré dans la figure 15.

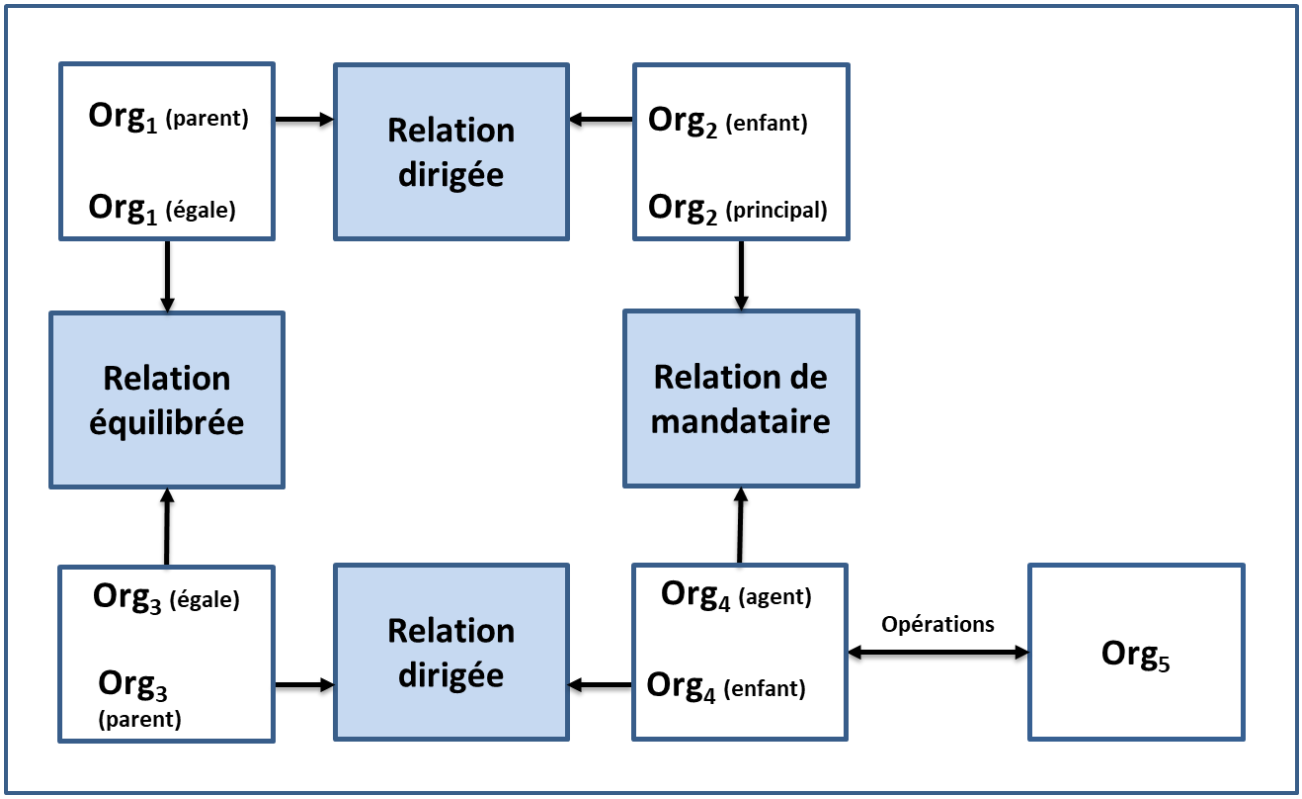


Figure 15 : Relations organisation-organisation

Il convient de noter que les relations entre les entités doivent être différenciées des interactions entre les entités (c.-à-d. l'exécution des transactions). Dans la figure 15 ci-dessus, **Org4** a des interactions avec **Org5**, mais **Org4** n'a pas de relation avec **Org5**. Ce concept sera examiné plus en détail dans une version ultérieure du PSP du CCP.

7 ANNEXE E : APERÇU DES JUSTIFICATIFS

7.1 Qu'est-ce qu'un « justificatif »?

Le fondement de toute transaction est la confiance. La confiance repose sur l'assurance que toute réclamation faite par une entité négociatrice peut être invoquée comme étant vraie. À titre d'exemple, une entité qui transige peut avoir besoin de confirmer l'identité de l'autre entité avec laquelle elle traite, que cette autre entité ait le pouvoir de mener une certaine activité ou que cette autre entité possède un actif particulier.

Au fil du temps, de nombreux types de justificatifs[31] ont été élaborés et émis afin de résoudre le problème de confiance entre les entités. Ces références permettent de répondre à des questions telles que : « cette personne est-elle autorisée à conduire une voiture en Ontario? », « cette personne satisfait-elle aux exigences requises pour recevoir des prestations d'assurance-emploi? », « cette entreprise est-elle autorisée à couper du bois en Colombie-Britannique? » ou « cette entreprise est-elle admissible à un prêt pour une petite entreprise? »

Dans le sens le plus général, un titre d'identité est une affirmation d'identité, de qualification, de compétence, d'autorité, de droits, de privilèges, d'autorisations, d'état, d'admissibilité ou de propriété d'actifs (ou une combinaison de ces éléments). Plus précisément, un justificatif contient un ensemble d'une ou de plusieurs revendications revendiquées sur un ou plusieurs sujets[32]. Les renseignements d'identification sont délivrés par une entité, *l'émetteur*, à une autre entité, le *titulaire*. L'émetteur possède l'autorité de jure de délivrer les justificatifs, ou se voit accorder par convention et par consensus l'autorité de facto et a assumé la compétence de délivrer le justificatif.

Les renseignements d'identification contiennent deux types de renseignements de base. Le premier type de renseignements porte sur le justificatif lui-même[33] :

1. les renseignements qui spécifient le type de justificatifs;
2. les renseignements qui identifient l'émetteur du justificatif;
3. les renseignements qui précisent la date à laquelle le justificatif a été délivré;
4. les renseignements qui précisent toute contrainte sur le justificatif (p. ex., une date d'expiration, les conditions d'utilisation);
5. les renseignements sur l'état du justificatif (c.-à-d. si le justificatif est actif, suspendu ou révoqué).

[31] Voir la section 7.2.

[32] Pour de plus amples renseignements sur les rôles et les flux d'information de l'écosystème numérique, voir la section 2.6.

[33] Ce type de renseignements est exprimé au moyen d'attributs de justificatif. Voir la section 2.3.1.3.

Le deuxième type de renseignement contenu dans un justificatif consiste en un ensemble d'attributs qui décrivent les propriétés ou les caractéristiques des entités qui sont les sujets des justificatifs. Ces attributs d'entité sont une combinaison d'attributs[34] d'identité des objets et d'attributs non liés à l'identité des sujets[35]. Voici quelques exemples d'attributs non liés à l'identité d'un sujet : la langue de préférence du sujet, l'adresse de résidence du sujet et le total des actifs du sujet. En outre, les attributs non liés à l'identité d'un sujet contenus dans un titre de compétence fournissent souvent des renseignements non liés à l'identité propre au sujet, directement ou indirectement (p. ex., la nationalité du sujet, le sujet a obtenu une maîtrise en génie électrique de l'Université ABC, les catégories de véhicules à moteur que le sujet est autorisé à exploiter). Si un justificatif affirme qu'il existe une relation entre les sujets, il inclut également des attributs de relation[36]. Tous ces différents attributs sont utilisés pour exprimer une ou plusieurs revendications concernant un sujet.

7.2 Types de justificatif

Voici la liste des nombreux types de justificatifs qui existent, ainsi que quelques exemples de leur *documentation*[37] :

1. Citoyenneté et justificatif du statut de résidence légale (p. ex., certificat de naissance, certificat de citoyenneté, certificat de résidence permanente, passeport).
2. Justificatif d'inscription au service (p. ex., carte des services de santé provinciaux/territoriaux, carte d'assurance de services de santé privés, carte d'assurance de services dentaires privés, carte d'assurance voyage privée, carte de programme de récompense de fidélité, carte d'adhésion à un groupe ou à un club).

[34] Un *justificatif pseudonyme* (aussi appelé *justificatif anonyme*) est un justificatif qui, tout en faisant une affirmation au sujet d'une entité, ne révèle pas son identité. Un justificatif d'identité peut contenir des attributs d'identité (comme un identifiant attribué), mais il doit être traité comme un pseudonyme si les attributs d'identité ne sont pas destinés à être utilisés à des fins de résolution d'identité. Les références pseudonymes fournissent aux entités un moyen de prouver leurs déclarations sur elles-mêmes et leurs relations avec d'autres entités tout en préservant leur anonymat.

[35] Pour plus de renseignements sur la distinction entre les attributs d'identité et les attributs non liés à l'entité, voir l'annexe B (section 4.4).

[36] Pour une discussion générale sur les entités, les relations et les attributs, voir la section 2.3.1.

[37] Voir la section 7.3.

3. Justificatif d'obtention d'un agrément pour les exploitants (p. ex., permis de conduire automobile, permis d'exploitation d'équipement lourd).
4. Justificatifs organisationnels (p. ex., licences, permis, certificats d'inspection)
5. Justificatif des services financiers (p. ex., carte de débit bancaire, carte de crédit).
6. Justificatif lié à des titres de propriété (p. ex., l'immatriculation d'un véhicule automobile, l'acte de propriété, la preuve de l'assurance d'un véhicule automobile).
7. Diplômes universitaires (p. ex., diplôme, certificat, accréditation, certification, relevé de notes).
8. Justificatif d'emploi (p. ex., lettre d'emploi)
9. Justificatif d'une adhésion professionnelle (p. ex., carte de membre du Syndicat des électriciens).
10. Justificatif diplomatique (p. ex., lettres d'introduction d'ambassadeurs).
11. Justificatif des journalistes (p. ex., carte de presse).
12. Justificatif d'une cote de sécurité (p. ex., laissez-passer d'accès au bâtiment, laissez-passer d'accès à une zone sécurisée).
13. Justificatif d'authentification[38] (p. ex., combinaison du nom d'utilisateur et du mot de passe).

[38] Les systèmes de renseignements utilisent généralement des justificatifs d'authentification pour contrôler l'accès aux renseignements, aux applications ou à d'autres ressources système. La combinaison classique du numéro de compte ou du nom d'un utilisateur associé à un mot de passe secret (l'authentificateur) est un exemple largement utilisé de justificatif d'identification. Certains systèmes de renseignements utilisent d'autres formes d'authentificateurs, comme les caractéristiques biologiques (p. ex., photo faciale, empreintes digitales, voix, rétines) ou les certificats de clé publique.

7.3 Modèle de renseignements d'identification du CCP

La figure 16 illustre le modèle de renseignements d'identification du CCP.

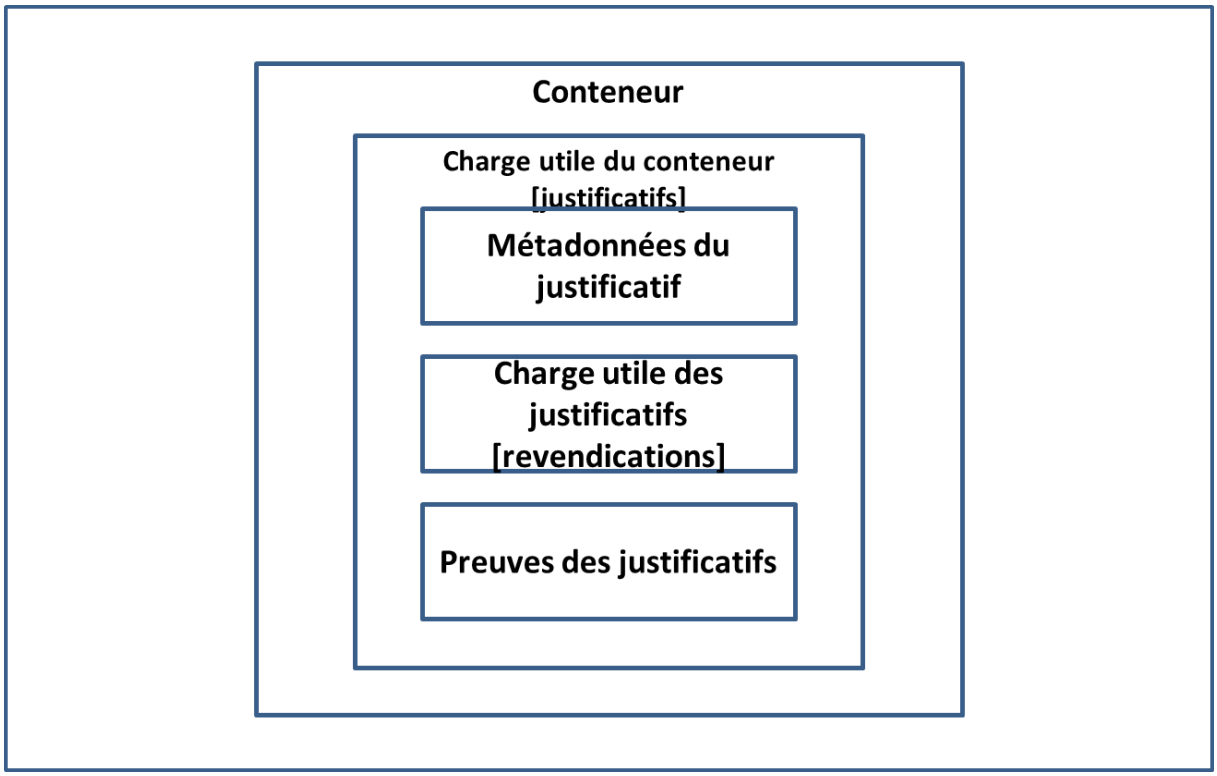


Figure 16 : Modèle de renseignements d'identification du CCP

Dans le modèle de renseignements d'identification du CCP, un justificatif se compose de trois composants :

1. **Métadonnées des justificatifs** : Un ou plusieurs attributs de justificatif qui décrivent les propriétés ou les caractéristiques des justificatifs.
2. **Charge utile d'un justificatif** : Un ensemble d'une ou plusieurs revendications faites sur un ou plusieurs sujets.
3. **Preuves du justificatif** : Une ou plusieurs méthodes ou mécanismes utilisés pour vérifier que l'émetteur est l'auteur du justificatif et que le justificatif n'a pas été altéré.

Il convient de noter que, même si un vérificateur peut *vérifier* l'auteur d'un justificatif et peut inspecter un justificatif à des fins de preuve de falsification, la véracité de la charge utile des justificatifs d'identité elle-même ne peut pas être vérifiée par un vérificateur (c.-à-d., le fait d'une revendication [p. ex., « le ciel est vert »]. En acceptant un justificatif, un vérificateur déclare essentiellement qu'il fait confiance à l'émetteur du justificatif pour avoir correctement vérifié les demandes avant de créer la charge utile des justificatifs.

Le *titulaire* d'une pièce d'identité se voit habituellement remettre une forme de documentation comme preuve de possession du justificatif. Pendant de nombreuses années, la documentation d'accréditation consistait principalement en un morceau de papier ou une carte plastique. Au fil du temps, des fonctions d'authentification (y compris des fonctions d'authentification électronique) ont été intégrées à la carte plastique. De plus en plus, les titres de justificatif sont émis sous forme électronique[39]. La preuve documentaire d'un justificatif peut être considérée comme un *contenant*[40] ou comme un substrat pour le transport du justificatif. Les justificatifs sont placés à l'intérieur du conteneur et deviennent la *charge utile du conteneur.*

[39] La spécification la plus récente des références électroniques est des références vérifiables. Voir [W3C, 2021].

[40] Ruff, 2020

7.4 Modèles de présentation de revendications

7.4.1 Modèle de présentation des revendications d'une revendication d'un sujet

Une revendication présentée à un sujet est une déclaration à propos d'un sujet. Une revendication présentée à un sujet est exprimée au moyen d'un ou de plusieurs *attributs d'entité*. La figure 17 illustre le modèle de présentation des revendications d'une revendication d'un sujet.

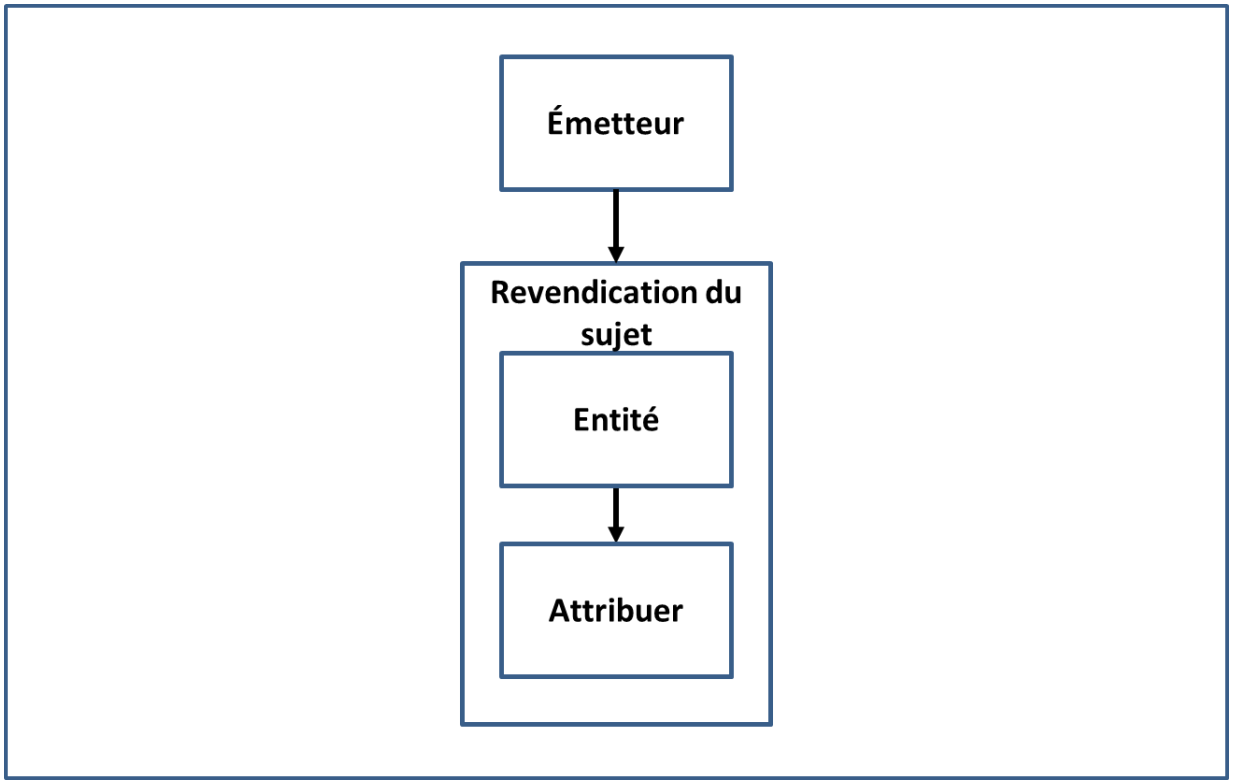


Figure 17 : Modèle de présentation des revendications d'une revendication d'un sujet

7.4.2 Modèle de présentation des revendications d'une revendication de relation

Une revendication de relation est une déclaration au sujet d'une association qui existe entre deux sujets ou plus. Une revendication de relation est exprimée au moyen d'un ou de plusieurs *attributs de relation*. La figure 18 illustre le modèle de présentation des revendications d'une revendication de relation.

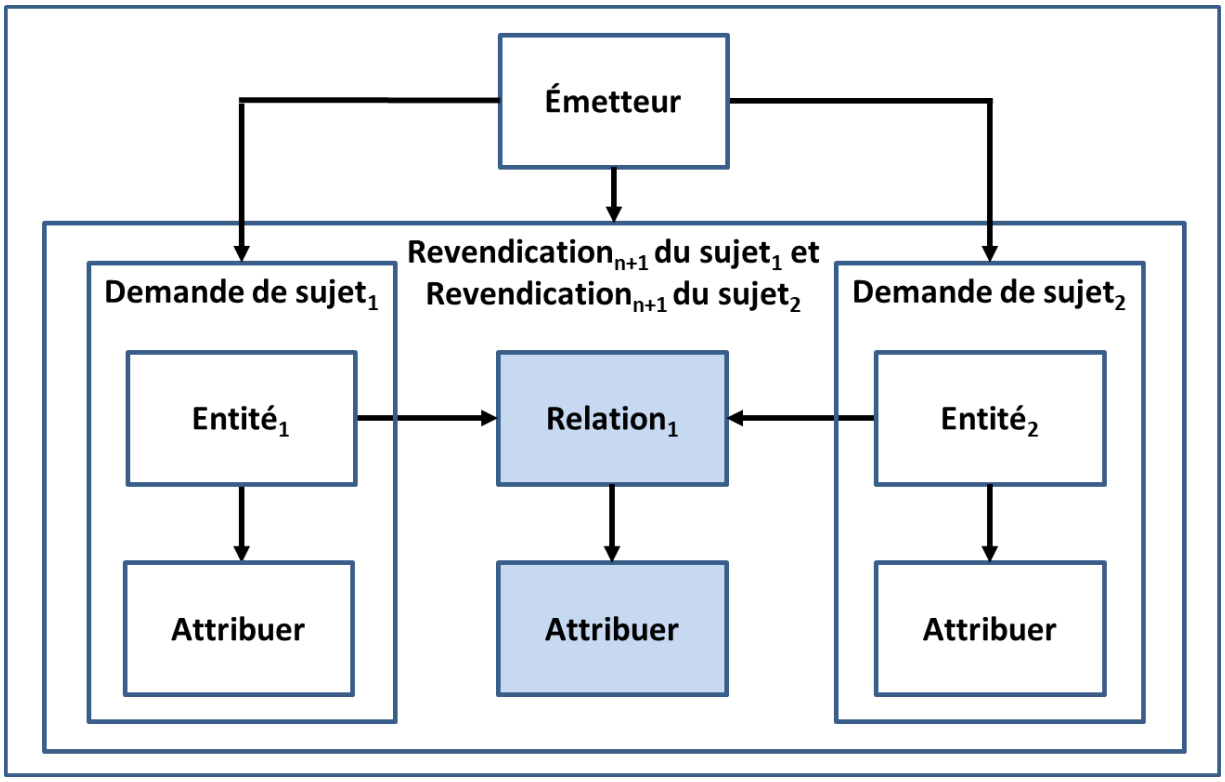


Figure 18 : Modèle de présentation des revendications d'une revendication de relation

7.5 Modèle d'émission d'un justificatif

Un émetteur 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. La figure 19 illustre le modèle d'émission des justificatifs.

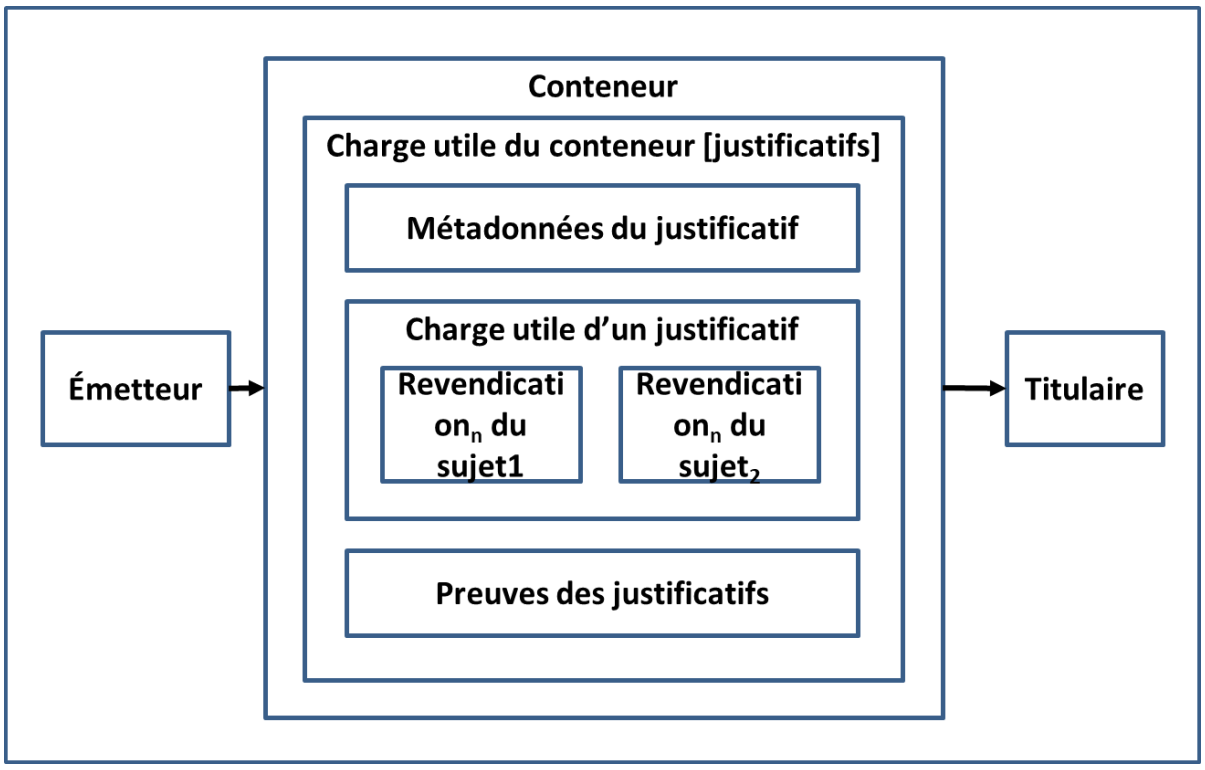


Figure 19 : Modèle d'émission d'un justificatif

8 ANNEXE F : VÉRIFICATION DE L'IDENTITÉ EN DÉTAIL

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 utiliser des renseignements personnels ou des renseignements organisationnels qui ne sont pas liés à l'identité. Quatre méthodes sont utilisées pour effectuer la vérification de l'identité :

Confirmation basée sur les connaissances : Méthode de vérification de l'identité qui utilise des renseignements personnels ou organisationnels ou des secrets partagés pour prouver que l'entité qui présente les renseignements identificateurs contrôle l'identité. La confirmation basée sur les connaissances est obtenue au moyen du modèle défi-réponse : l'entité qui présente les renseignements d'identité se voit poser des questions, réponses auxquelles (en théorie du moins) seuls elle et l'interrogateur seraient au courant (p. ex., renseignements financiers, historique de crédit, secret partagé, clé cryptographique, code d'accès envoyé par la poste, mot de passe, numéro d'identification personnel, identificateur attribué).

Confirmation 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 de possession physique : Méthode de vérification de l'identité qui exige la possession physique ou la présentation d'éléments de preuve pour prouver que l'entité qui présente les renseignements sur l'identité contrôle l'identité.

Confirmation de l'arbitre de confiance : Méthode de vérification d'identité qui s'appuie sur un arbitre de confiance pour prouver que l'entité présentant les renseignements d'identité contrôle l'identité. Le type d'arbitre de confiance et leur acceptabilité sont déterminés par des critères propres au programme. Les arbitres de confiance comprennent les garants, les notaires, les comptables et les agents certifiés.

9 ANNEXE G : VÉRIFICATION DES JUSTIFICATIFS EN DÉTAIL

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.

Le processus de vérification des justificatifs dépend du processus de **liaison justificatif-authentifiant** (c.-à-d. le processus d'association d'un justificatif émis à un titulaire avec un ou plusieurs authentificateurs). Le processus liaison justificatif-authentifiant 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).

9.1 Authentificateurs

Un authentificateur est quelque chose qu'un titulaire contrôle et qui est utilisé pour prouver que le titulaire a conservé le contrôle sur un justificatif émis. Il existe trois types d'authentificateurs :

1. Quelque chose que le titulaire a [41](p. ex., une clé cryptographique ou un mot de passe unique).
2. Quelque chose que le titulaire connaît[42] (p. ex., un mot de passe, une réponse à une question d'identification).
3. Quelque chose que le titulaire est ou fait[43] (p. ex., visage, empreintes digitales, rétines, temps de course au clavier, démarche).

Les authentificateurs, lorsqu'ils sont liés à un justificatif d'identité, seront ensuite utilisés pour prouver, avec un niveau d'assurance précis, que le justificatif d'identité fait référence au même titulaire qui était lié à l'origine au justificatif d'identité.

[41] Ceci est similaire à la méthode de confirmation de possession physique utilisée par la vérification d'identité.

[42] Ceci est similaire à la méthode de confirmation basée sur les connaissances utilisée par la vérification d'identité.

[43] Cette méthode est similaire à la méthode de confirmation biologique ou comportementale utilisée par la vérification d'identité.

Il convient de noter qu'étant donné l'irrévocabilité des caractéristiques biologiques (p. ex., le visage, les empreintes digitales, les rétines), les normes de l'industrie [44]sont généralement prudentes en ce qui concerne l'utilisation des caractéristiques biologiques comme authentificateurs pour les justificatifs d'authentification. Une caractéristique biologique n'est pas la même chose qu'un secret qui peut être changé périodiquement; une caractéristique biologique ne peut être modifiée. En outre, la caractéristique biologique d'un titulaire peut être reproduite. Par exemple, un acteur de la menace peut obtenir une copie de l'empreinte digitale du titulaire, construire une réplique et réussir la vérification des justificatifs d'identification (en supposant que le processus de vérification des justificatifs d'identification ne bloque pas de telles attaques en utilisant des techniques de détection de la résistance robustes).

Toutefois, une caractéristique biologique peut être utilisée pour déverrouiller l'accès à un authentificateur stocké dans un dispositif local afin de faciliter la vérification des justificatifs à distance à l'aide d'un service. Un exemple d'un tel scénario est l'utilisation d'un logiciel de reconnaissance faciale pour déverrouiller l'accès à un code d'accès mobile unique ou à un autre authentificateur mobile stocké et généré localement.

[44] Pour des exemples, voir NIST 800-63 et ITSP.30.031.

10 ANNEXE H : 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 décrivent certaines lignes directrices sur la reconnaissance mutuelle à un niveau élevé. Une orientation détaillée suivra dans les produits livrables subséquents.

10.1 Planification et mobilisation

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

1. **Définir la portée de l'évaluation.** La portée de l'évaluation peut comprendre une ou plusieurs parties agissant dans les rôles définis dans l'écosystème numérique. Bien que l'évaluation soit principalement axée sur la compétence en tant qu'émetteur, l'évaluation peut comprendre d'autres parties qui ont reçu une délégation de fonctions ou de 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 officiel d'évaluation.
2. **Officialiser l'équipe.** Officialiser l'équipe de 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 de membres des organisations participantes qui ont une connaissance opérationnelle détaillée du programme.
3. **Visite des lieux.** L'équipe d'évaluation devrait effectuer une visite sur place. Le résultat visé 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.
4. **Définir un flux 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 secteur de travail devrait être étroitement synchronisé avec les autres secteurs de travail, comme les évaluations des incidences sur la vie privée, l'évaluation et l'autorisation de la sécurité et l'intégration technique.
5. **Mobiliser le conseiller juridique dès le début.** Il est recommandé que les conseillers juridiques de toutes les parties soient mobilisés dès le début du processus. Étant donné que le processus d'évaluation et les dispositions qui en découlent peuvent être nouveaux par rapport aux dispositions existantes, il peut y avoir des incidences pour les autorités respectives et les accords respectifs.

6. **Susciter le respect de la vie privée et la sécurité dès le début.** Il est recommandé que les responsables de la protection de la vie privée et de la sécurité de toutes les parties soient mobilisés dès le début du processus, étant donné que les évaluations des facteurs relatifs à la vie privée et les évaluations de la sécurité devront être effectuées.
7. **Gestion des dossiers.** Veiller à ce que toutes les preuves reçues, les documents d'évaluation et les ébauches de travail soient déposés dans un système de gestion des documents approprié dans la catégorie de sécurité appropriée. Une fois l'évaluation terminée, tous les documents doivent être mis au point comme documents aux fins de vérification.

10.2 Schématisation des processus

Voici quelques recommandations pour l'étape de schématisation des processus :

1. **Définir l'étendue de la schématisation.** Habituellement, la schématisation sera faite à partir d'un programme ou d'un secteur d'activité établi. La portée de la schématisation peut inclure des programmes en amont tels que des statistiques de l'état civil ou des fournisseurs de services commerciaux externes. Ces éléments peuvent être inclus dans la portée de l'évaluation ou être identifiés comme des *dépendances*.
2. **Se préparer à la variation terminologique.** De nombreux programmes en cours d'évaluation seront bien établis et utiliseront la terminologie pour leur contexte. Le but du processus de cartographie n'est pas d'introduire une nouvelle terminologie, mais plutôt de cartographier ce qui existe en nom et ce qui doit être évalué à l'aide du CCP.
3. **Travailler en étroite collaboration avec tous les membres de l'équipe.** Une grande partie de la schématisation des 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 du personnel opérationnel peuvent être nécessaires. Il faudra peut-être aussi organiser des ateliers pour parvenir à une compréhension et à une schématisation commune.
4. **Préciser les responsabilités entre les parties.** Des processus similaires peuvent être mis en œuvre ou dupliqués entre les différentes parties. Par exemple, l'« inscription » dans un programme d'identité numérique peut être identique ou différente d'une « inscription » subséquente dans un service qui a accepté l'identité numérique. La schématisation des processus atomiques peut aider à clarifier ce qui peut être un processus en double (c.-à-d. redondant) pour l'utilisateur et ce qui peut être précisément requis pour le service.

10.3 Évaluation

L'évaluation exige un jugement d'un expert impartial qui utilise les renseignements les meilleurs et les plus complets disponibles. Pour le plus simple, la détermination de l'évaluation peut être simplement RÉUSSIE/ÉCHEC. Toutefois, dans la pratique, l'évaluateur peut exiger des gradations supplémentaires pour exprimer les préoccupations exprimées au moment de la détermination ou pour indiquer que certains renseignements peuvent être incomplets ou inaccessibles à l'évaluateur.

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

Les déterminations actuelles de l'évaluation utilisées sont les suivantes :

1. **Accepter** – Les critères de conformité sont respectés.
2. **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.
3. **Accepter en émettant une recommandation** – Les critères de conformité sont respectés, mais une amélioration ou un perfectionnement doit être constaté à l'avenir.
4. **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.
5. **Ne pas accepter** – Les critères de conformité ne sont pas respectés.
6. **Sans objet** – Les critères de conformité ne s'appliquent pas.

10.4 Acceptation

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

1. adressée à la personne, l'organisation, l'instance agissant à titre d'émetteur de l'identité numérique;
2. être signée par le personnel, l'organisation ou l'administration acceptant l'identité numérique, à un niveau de qualificateur donné;
3. Indiquer la portée ou à quelle fin précise l'identité numérique sera utilisée, y compris la durée d'utilisation;

4. comporter une annexe énumérant les qualificateurs spécifiques (p. ex., niveaux d'assurance), et indiquant toute observation, condition ou recommandation découlant du processus d'évaluation.

11 ANNEXE F : ENJEUX THÉMATIQUES

Le Groupe de travail sur le PSP du CCP a déterminé plusieurs enjeux thématiques de haut niveau qui doivent être abordés afin de faire progresser l'écosystème numérique.

Enjeu thématique 1 : Relations (priorité : élevée)

Il faut élaborer un modèle de relation.

État : Achevé.

Enjeu thématique 2 : justificatifs (priorité : élevée)

L'élaboration d'un modèle généralisé d'accréditation est nécessaire. Ce modèle devrait intégrer les références physiques traditionnelles et les références d'authentification à la notion plus large d'une identification vérifiable.

État : Achevé.

Enjeu thématique 3 : Organisations non enregistrées (priorité : élevée)

À l'heure actuelle, la portée du PSP du CCP comprend tous les organismes enregistrés au Canada (y compris les organismes inactifs) pour lesquels une identité a été établie au Canada. Il existe aussi de nombreux types *d'organismes non enregistrés* au Canada comme les entreprises individuelles, les syndicats, les coopératives, les ONG, les organismes de bienfaisance non enregistrés et les fiducies. Une analyse de ces organisations non enregistrées doit être entreprise.

Enjeu thématique 4 : Consentement éclairé (priorité : élevée)

La version actuelle du document Aperçu consolidé du PSP du CCP pourrait ne pas saisir adéquatement toutes les questions et nuances entourant le sujet du consentement éclairé, particulièrement dans le contexte du secteur public. Une étude plus rigoureuse de ce sujet doit être effectuée.

Enjeu thématique 5 : Préoccupations en matière de protection de la vie privée (priorité : moyenne)

En ce qui concerne les processus atomiques de *continuité de l'identité* et de *continuité des relations*, il a été noté que la notion de confirmation dynamique soulève des préoccupations en matière de confidentialité. Une analyse plus approfondie fondée sur les commentaires provenant de l'application du PSP du CCP est nécessaire pour déterminer si ces processus atomiques sont appropriés.

Enjeu thématique 6 : Évaluation des processus atomiques externalisés (priorité : moyenne)

Le PSP du CCP ne présume pas qu'un vérificateur ou un émetteur unique est le seul responsable de tous les processus atomiques. Une organisation peut choisir de sous-traiter ou de déléguer la responsabilité d'un processus atomique à une autre partie. Par conséquent, plusieurs organismes pourraient être impliqués dans le processus

d'évaluation du PSP 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 reste à déterminer comment ces évaluations à intervenants multiples seront menées.

Enjeu thématique 7 : Portée du PSP du CCP (priorité : faible)

Il a été suggéré d'élargir le champ d'application du PSP du CCP pour y inclure d'autres domaines tels que les qualifications universitaires, les désignations professionnelles, le statut vaccinal, entre autres. Le PSP du CCP prévoit l'extensibilité grâce à la généralisation du modèle PSP du CCP et à l'ajout éventuel de nouveaux processus atomiques. Il faut étudier l'élargissement de la portée du PSP du CCP à d'autres domaines.

Enjeu thématique 8 : Signature (priorité : faible)

Le concept de signature tel qu'il doit être appliqué dans le contexte du PSP du CCP doit être examiné.

Enjeu thématique 9 : *Nom fondamental*, *nom principal*, *nom légal* (priorité : faible)

Le PSP du CCP a des définitions pour le *nom fondamental*, le *nom principal* et le *nom légal*. Étant donné que les trois termes signifient la même chose, un terme préféré devrait être choisi et utilisé de façon uniforme dans tous les documents du PSP du CCP.

Enjeu thématique 10 : Renseignements supplémentaires (priorité : faible)

Il a été noté que le document de synthèse du PSP du CCP ne contient pas suffisamment de détails sur l'application précise du PSP du CCP. Le document de synthèse du PSP du CCP doit être complété par des directives détaillées dans un document distinct.

Enjeu thématique 11 : Examen des annexes (priorité : faible)

Il faut examiner les annexes actuelles du document de synthèse du PSP du CCP. Chaque annexe devrait être évaluée en fonction de son utilité, de son applicabilité et de son caractère approprié, et il faudrait déterminer s'il doit continuer d'être inclus dans le document.

12 ANNEXE J : BIBLIOGRAPHIE

Organisations

1. Conseils mixtes du Canada
    a. Priorité des conseils mixtes du Canada en matière d'identité numérique : recommandations en matière de politique publique (2018)
2. Centre de sécurité des télécommunications (CST)
    a. Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (2018).
3. Digital Identity and Authentication Council of Canada (DIACC)
    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. Vue d'ensemble du composant de connexion vérifié (novembre 2019)
    f. Aperçu de la composante vérification de la personne (novembre 2019)
    g. Justificatifs (relations et attributs) — Présentation de la composante (juillet 2020)
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 professionnel ID4D (2019)
8. World Wide Web Consortium (W3C) (en anglais seulement)
    a. Modèle de données des justificatifs 1.0 (Ébauche de la rédaction) (2021)

Personnes

5. Joe Andrieu
    a. A Primer on Functional Identity (2018)
6. Timothy Ruff
    a. Verifiable Credentials Aren't Credentials. They're Containers (2020)