Profil d'identité du secteur automobile du CCP

Statut du document : Recommandation finale V1.0

Conformément aux procédures opérationnelles du CCIAN, une recommandation finale est un livrable qui représente les conclusions d'un comité d'experts du CCIAN ayant été approuvées par un comité d'experts et ratifiées par un scrutin des membres bienfaiteurs du CCIAN.

Ce document a été préparé par l'équipe de conception du profil d'identité du secteur automobile du Comité d'experts du Cadre de confiance pancanadien du CCIAN. On s'attend à ce que le contenu de ce document soit examiné et mis à jour régulièrement afin de donner suite à la rétroaction reliée à la mise en œuvre opérationnelle, aux progrès technologiques, et aux changements de lois, règlements et politiques. Les avis concernant les changements apportés à ce document seront partagés sous la forme de communications électroniques, notamment par courriel et sur les réseaux sociaux. Les notifications seront également consignées dans le programme de travail du Cadre de confiance pancanadien.

Table des matières

1. Introduction au profil d'identité du secteur automobile du CCP

Le Conseil canadien de l'identité et de l'authentification numériques (CCIAN) est en train d'élaborer le profil d'identité du secteur automobile du CCP afin d'uniformiser et de sécuriser les pratiques de vérification de l'identité numérique à l'échelle de l'écosystème du financement et de la location automobiles.

Ce profil spécialisé est mené par la demande du marché et le besoin grandissant d'avoir un mécanisme d'assurance clair et vérifiable qui soutient son public clé : les concessionnaires automobiles et les entités de location et de financement qui, en tant qu'entités engagées dans la vente, le financement ou la location de véhicules, sont engagées dans la vente, le financement ou la location de véhicules, sont des entités déclarantes (ED) en vertu de la Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes (LRPCFAT), ont des obligations de conformité prévues par la loi en ce qui concerne la lutte contre le blanchiment d'argent et le besoin de bien connaître son client administrées par le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE), et requièrent de robustes pratiques de vérification de l'identité afin de lutter contre la fraude d'identité.

En réponse aux directives des grandes banques canadiennes obligeant les concessionnaires automobiles à instaurer une vérification robuste de l'identité pendant le financement, le profil d'identité du secteur automobile du CCP définira des critères transparents et vérifiables qui permettent aux fournisseurs de services d'être certifiés contre les normes de confiance. Cette certification, qui est reconnue par le biais du Programme de certification du CCP du CCIAN, donnera aux concessionnaires, prêteurs et partenaires technologiques confiance dans les outils d'identité numériques sûrs préservant la vie privée, qui protègent les données des consommateurs et répondent aux attentes réglementaires. En instaurant une couche de confiance uniforme pour l'identité numérique dans l'achat et le financement de véhicules, le profil réduira la fraude, la contrefaçon et la falsification des documents, tout en renforçant l'assurance de la conformité en matière de lutte contre le blanchiment d'argent à l'échelle du secteur.

2. Parties applicables par rapport aux parties intéressées

2.1 Parties intéressées

Secteur privé

- Concessionnaires et groupes de concessionnaires (concessionnaires franchisés; concessionnaires indépendants)
- Prêteurs et institutions financières (banques, caisses d'économie; filiales de financement)

Associations de l'industrie

- Association Canadienne de Financement & de Location (ACFL)
- Canadian Lenders Association (CLA)
- Corporation des associations de détaillants d'automobiles (CADA)
- Used Car Dealers Association (UCDA)
- Associations provinciales de concessionnaires

2.2 Parties applicables

Fournisseurs de solutions d'identité et d'authentification numériques

- Fournisseurs de solutions d'identité et d'authentification numériques souhaitant obtenir ou détenant la certification du CCIAN ou encore l'ayant eu par le passé.

2.3 Directives et procédures opérationnelles pour les concessionnaires

Ce document remplit deux fonctions essentielles. Les sections 1 à 6 expliquent le contexte : à qui ce profil est destiné, les parties impliquées et les termes utilisés. La section 7 établit les critères de conformité — les exigences techniques auditables qu'un fournisseur de services de vérification de l'identité (SVI) doit remplir pour obtenir la certification du CCIAN. Les critères de conformité s'appliquent au fournisseur de services, mais pas au concessionnaire. Le choix d'un fournisseur de SVI certifié donne à un concessionnaire l'assurance que l'aspect technique de la vérification de l'identité — vérifications des documents, concordance biométrique, traitement des données — satisfait une norme de confiance. Cela ne transfère pas les responsabilités du concessionnaire au fournisseur. Le concessionnaire reste responsable de la gouvernance entourant l'outil : maintenir une politique de vérification de l'identité écrite,

décider de la façon dont les non-concordances et les alertes de fraude sont traitées, obtenir le consentement du client, tenir les dossiers et remplir les obligations légales qui s'appliquent à ses activités. L'orientation numérotée ci-dessous décrit ces responsabilités. En bref, un fournisseur certifié procure la solution; le concessionnaire reste responsable de la façon dont elle est utilisée.

En tant qu'entités engagées dans la vente, le financement ou la location de véhicules, les concessionnaires sont des entités déclarantes en vertu de la LRPCFAT et ils ont des obligations législatives directes en ce qui concerne l'identification des clients, la tenue des dossiers et les rapports. L'orientation dans cette section soutient ces obligations; elle ne les énumère ou ne les remplace pas. Lorsque le prêteur est aussi une entité déclarante, il conserve la pleine responsabilité législative à l'égard de ses propres obligations d'identification du client et de tenue de dossiers en vertu de la LRPCFAT et ses règlements, peu importe qui effectue la vérification. Ni l'utilisation par une partie d'un SVI certifié ni la responsabilité du concessionnaire en vertu de ce profil écarte les autres obligations réglementaires indépendantes. Avant de dépendre d'un service de vérification de l'identité certifié, une partie dépendante devrait s'assurer, dans le cadre de son propre programme de conformité basé sur les risques, que la méthode de vérification et l'assurance qu'elle fournit sont appropriées pour le risque du produit, du client et de la transaction en cause; la certification atteste de la qualité du processus de vérification, non de sa suffisance pour chaque cas d'utilisation.

1. **Exigences en matière de gouvernance et de politiques**

- **Établissement des règles :** Le concessionnaire doit maintenir une politique écrite de vérification de l'identité, sous forme de document autonome ou en tant que composante d'une documentation de conformité plus vaste. Cette politique doit expliquer son processus pour vérifier les identités et définir le « cadre de risque » utilisé pour déterminer si un client est ce qu'il affirme être.
- **Non-concordances de données :** La politique doit décrire la façon dont le personnel traite les anomalies dans le nom, l'adresse ou la date de naissance d'un client quand les résultats numériques ne concordent pas exactement avec les renseignements déclarés par le client.
- **Harmonisation avec l'industrie :** En tant qu'entité déclarante, le concessionnaire doit s'assurer que ses seuils de risque internes répondent aux exigences qui s'appliquent à ses activités en vertu de la LRPCFAR et ses règlements.

2. **Gestion des fraudes et prise de décision**

- **Examiner les sonnettes d'alarme :** Quand un fournisseur de services ou un bureau de crédit renvoie une « alerte à la fraude », le concessionnaire doit avoir un processus opérationnel pour l'examiner et déterminer si la transaction représente un « risque acceptable » selon sa politique.

- **Examiner le recours hiérarchique et les interventions humaines :** Le processus du concessionnaire devrait identifier qui examine les vérifications signalées ou ayant échoué, quand une transaction est transférée à du personnel formé pour un examen secondaire et comment la vérification est traitée quand les systèmes ne sont pas disponibles.
- **Assurer l'indépendance des données :** Lorsqu'il utilise la méthode à processus double, le concessionnaire ne doit pas se servir de ses propres dossiers internes (par exemple une ancienne facture pour des services) comme source pour la vérification et il doit se fier à des sources fiables indépendantes.

3. **Attribution de contrats et supervision des tierces parties**

- **Certification de la sécurité des fournisseurs :** Avant de passer un contrat avec un fournisseur de SVI, le concessionnaire devrait déterminer si le fournisseur détient une certification reconnue en matière de sécurité de l'information (par exemple SOC 2 Type II, SOC 3 ou ISO/IEC 27001). Si un fournisseur proposé ne détient pas une telle certification, le concessionnaire devrait évaluer, et être préparé à accepter et à documenter, le risque résiduel de traiter avec ce fournisseur.
- **Détermination du mécanisme juridique :** Avant qu'un concessionnaire se fie à la vérification de l'identité d'une autre partie — ou effectue la vérification à laquelle un prêteur se fiera — il doit déterminer et documenter le mécanisme en vertu duquel les règlements de la LRPCFAT régissent l'arrangement : vérification directe (art. 105), l'agent ou le mandataire (art. 106) ou la dépendance (art. 107). Ces mécanismes comportent des implications très différentes en termes de responsabilité, de passation de contrats et de tenue de dossiers. Le concessionnaire devrait solliciter un avis juridique lorsque la classification n'est pas claire.
- **Officialisation des ententes :** Lorsqu'un concessionnaire dépend d'une tierce partie pour vérifier les identités, un contrat écrit doit être en place avant de procéder à la vérification.
- **Principes essentiels des contrats :** De tels contrats doivent clairement définir la portée du travail, la façon dont les données sont partagées, qui tient les dossiers et qui est responsable des erreurs.
- **Vérification des partenaires :** Le concessionnaire doit confirmer que tout vérificateur tiers se conforme aux lois et règlements régissant l'identité au Canada et dans les territoires où le concessionnaire mène des activités.
- **Droit d'audit :** Les contrats devraient inclure des « droits d'audit » pour que le concessionnaire puisse confirmer que ses partenaires se conforment aux normes exigées.

4. **Vérification des entités du même groupe et des membres**

- **Vérifier le groupe :** Le concessionnaire ne doit pas se fier uniquement à la parole d'un client. Il doit utiliser une source indépendante (comme un registre

d'entreprise ou une base de données gouvernementale) pour confirmer que l'organisation à laquelle le client affirme appartenir existe réellement.
- **Confirmer le statut :** Le concessionnaire doit confirmer que la relation du client avec ce groupe est actuelle et en règle au moment de la transaction.
- **Recueillir des preuves :** Le concessionnaire devrait obtenir des preuves de la relation (p. ex. carte de membre, pièce d'identité d'employé ou confirmation numérique) pour soutenir la vérification.

5. **Confidentialité et documentation**

- **Obtenir le consentement :** Le concessionnaire doit obtenir un « consentement éclairé » (permission claire) de la personne avant de recueillir ou d'utiliser ses données d'identité numériques, et faire en sorte qu'un dossier prouvant ce consentement, incluant la date, est conservé. Cette attente est une exigence de conformité pour le processus de vérification certifiée en vertu des critères du sous-alinéa 102.1.0.10 (Exigences générales), qui s'applique à toutes les méthodes de vérification.
- **Réduire et protéger les données :** Le concessionnaire devrait recueillir uniquement les renseignements personnels que la vérification exige, et envisager des mesures pour préserver la confidentialité, comme la segmentation ou le hachage des données enregistrées, conformément aux orientations du Commissariat à la protection de la vie privée du Canada.
- **Tenir des dossiers clairs :** Le concessionnaire doit tenir ses propres dossiers de la vérification — incluant la date à laquelle elle a eu lieu, la source utilisée et les renseignements spécifiques obtenus — et les conserver pour la période exigée par la loi applicable.
- **Accessibilité :** Le concessionnaire devrait faire en sorte et être en mesure de démontrer que son processus de vérification de l'identité est accessible à tous les clients (référence aux normes WCAG 2.2 de niveau AA là où c'est applicable).

3. Processus de confiance

Le CCP promeut la confiance grâce à une série d'exigences opérationnelles et techniques vérifiables pour divers processus. Un processus est une activité commerciale ou technique (ou un ensemble de telles activités) qui transforme une condition d'intrant en condition d'extrant – un extrant sur lequel les autres se fient habituellement.

Dans le contexte du CCP, un processus appelé un processus de confiance est évalué selon des critères de conformité bien définis et convenus. L'intégrité d'un processus de confiance est de la plus haute importance parce que de nombreux participants – par-delà les frontières juridictionnelles, organisationnelles et sectorielles, et à court et long terme – dépendent du résultat de ce processus.

Remarque **:** Pour plus de renseignements sur les processus de confiance associés à l'identification et à la vérification des clients, veuillez vous reporter à la composante Personne vérifiée du CCP.

La composante Personne vérifiée du CCP est mentionnée ici uniquement comme corps de travail connexe. Elle ne fait pas partie du profil d'identité de l'industrie automobile du CCP et la conformité à ce profil est évaluée uniquement d'après les critères de la section 7 de ce document. La certification en vertu de la composante Personne vérifiée du CCP n'est pas requise pour - et ne confère pas - la certification en vertu de ce profil.

4. Exemple de transaction de vente d'automobile

Remarque : L'exemple d'ordinogramme qui suit est fourni uniquement à titre illustratif. Il vise non pas à être une représentation exhaustive ou exacte d'un processus réel quelconque, mais à montrer où des processus différents peuvent exister dans certains flux de transactions.

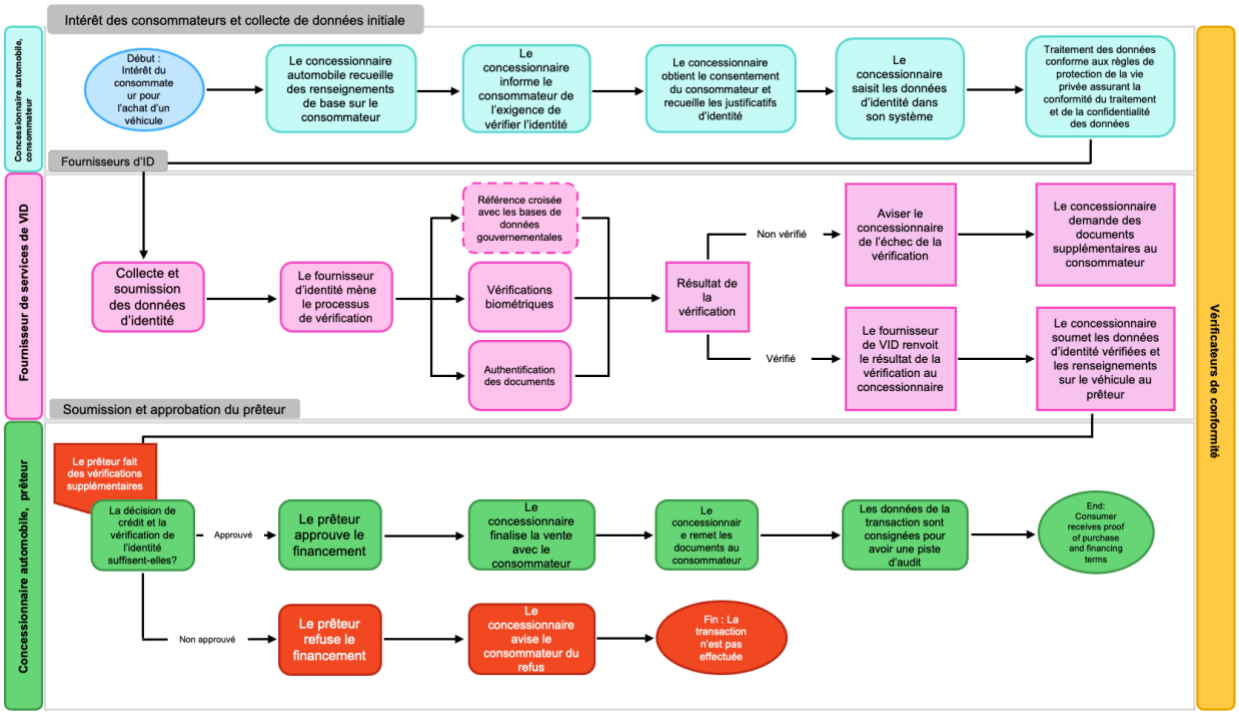

Figure 1. Exemple de processus de confiance (non normatif) : Transaction de vente d'automobile

5. Contexte du profil

Le profil d'identité du secteur automobile du CCP est un cadre spécialisé qui établit des critères clairs et vérifiables pour la vérification et la conformité de l'identité dans l'écosystème du financement et de la location d'automobiles au Canada.

Cette initiative répond à la demande grandissante du marché et au besoin pour un mécanisme d'assurance crédible qui répond aux attentes de son auditoire : les concessionnaires automobiles et les entités de location et de financement qui, en tant qu'entités engagées dans la vente, le financement ou la location de véhicules, sont des entités déclarantes en vertu du CANAFE avec des obligations législatives de conformité à la lutte contre le blanchiment d'argent et au besoin de bien connaître son client pour prévenir et déceler la fraude d'identité.

Veuillez noter que le profil d'identité actuel ne s'aligne pas sur des méthodes d'identification spécifiques ou des exigences connexes prescrites en vertu de la LRPCFAT et ses règlements connexes, décrits plus avant dans les directives du CANAFE.

Plusieurs grandes institutions financières du Canada ont adressé à leurs réseaux de concessionnaires des directives leur demandant des processus de vérification de l'identité plus rigoureux pour les transactions de financement et de location afin de s'attaquer à ce qui suit :

- Augmentation du vol d'identité;
- Menaces de fraude synthétique;
- Fraude facilitée par l'IA;
- Attaques par hypertrucage; et
- Élevage de comptes.

Ce virage a créé une demande croissante pour des directives claires alignées sur l'industrie et des outils de vérification de l'identité numérique fiables qui préservent la confidentialité.

Le profil d'identité du secteur automobile du CCP s'attaque directement à ce besoin en définissant des critères vérifiables pour une vérification de l'identité numérique spécifique aux transactions de financement automobiles. Ces critères serviront de base pour un programme de certification de l'industrie, ce qui permettra aux fournisseurs de services d'être évalués et certifiés d'après des exigences uniformisées et transparentes.

Les fournisseurs de services certifiés obtiendront la marque de confiance du profil d'identité du secteur automobile du CCP, ce qui signifie que leur solution répond aux plus hautes normes de sécurité, de confidentialité, d'interopérabilité et de conformité. Pour les concessionnaires et leur personnel, cette marque de confiance donne l'assurance que leur service choisi répond aux attentes opérationnelles et

réglementaires, ce qui assure que les transactions sont sûres et conformes, et que les données des consommateurs restent protégées.

En établissant ce profil, le secteur du financement automobile obtient une méthode uniforme, fondée sur des preuves, pour évaluer les services de vérification de l'identité numérique. Cela aide alors à réduire les obstacles à l'adoption, améliore la résilience à la fraude et soutient une confiance à plus grande échelle dans l'écosystème de l'identité numérique du Canada

Note juridictionnelle : Au Québec, la *Loi sur la protection des renseignements personnels dans le secteur privé* (comme amendée par la Loi 25) impose des obligations directement pertinentes aux méthodes de vérification dans ce profil, incluant l'obligation de déclarer les bases de données et les systèmes biométriques à la Commission d'accès à l'information du Québec (CAI). Les participants menant des activités au Québec demeurent responsables de la conformité à ces exigences, qui sont déclenchées par le traitement biométrique dans la méthode basée sur les pièces d'identité avec photo.

Remarque : Les critères de conformité du CCP ne remplacent ou ne substituent pas des règlements existants; on s'attend à ce que les organisations et les personnes se conforment à la législation, à la politique et aux règlements pertinents de leur territoire de compétence.

6. Conventions du document

6.1 Mots-clés des critères de conformité

Les mots clés suivants indiquent la priorité et la rigidité générale d'un critère de conformité donné, et ils doivent être interprétés de la façon suivante :

- **DOIT** signifie que l'exigence est impérative en ce qui concerne les critères de conformité.
- **NE DOIT PAS** signifie que l'exigence est une interdiction absolue des critères de conformité.

- **DEVRAIT** signifie qu'on s'attend à ce que l'exigence soit remplie, sauf dans des cas limités où le demandeur fournit des raisons ou des circonstances valables pour ignorer l'exigence. Toutes les implications d'une telle exception doivent être comprises et soupesées avec soin avant de choisir de ne pas se conformer aux critères de conformité tels que décrits.

- **NE DEVRAIT PAS** signifie qu'il peut exister une raison valable de faire une exception dans des circonstances particulières lorsque l'exigence est acceptable ou même utile, mais les pleines implications devraient être comprises et le cas

devrait être soigneusement soupesé avant de choisir de ne pas se conformer à l'exigence telle que décrite.

- **PEUT** signifie que l'exigence est discrétionnaire mais recommandée.

Les mots-clés sont en caractères gras et en MAJUSCULES dans les critères de conformité.

6.2 Termes et définitions

Pour la liste complète des termes et définitions utilisés dans le CCP, veuillez vous reporter au glossaire du CCP.

- **Entité du même groupe :** Entité reliée à une autre si une possède entièrement l'autre, les deux appartiennent entièrement à la même entité ou leurs états financiers sont consolidés.
- **Bureau Canadien du Crédit :** Entreprise privée (p. ex., Equifax ou Transunion) qui recueille, entrepose et vend des renseignements sur le crédit à la consommation (p. ex., paiements de prêts, historique des cartes de crédit, faillites) à des prêteurs et autres, ce qui crée un rapport de crédit détaillé et une note pour aider à évaluer la solvabilité pour les prêts et les services, même si elle ne prend pas elle-même de décisions concernant les prêts. Elle compile les données des banques, créanciers et dossiers publics, ce qui fournit des connaissances sur les habitudes d'emprunt d'une personne pour l'usage des institutions financières.
- **Partie dépendante** : Rôle qu'assume une organisation ou personne pour consommer des renseignements sur l'identité numérique créés et gérés par des participants afin d'effectuer des transactions numériques avec des sujets. Dans le contexte de ce profil, une partie dépendante est un prêteur.
- **Entités déclarantes :** Cela fait généralement référence à une organisation qui est tenue ou qui choisit de préparer des états financiers ou encore qui a des obligations juridiques spécifiques de déclarer certaines transactions à un organe réglementaire. En vertu de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* fédérale, les entités déclarantes sont des entreprises et des organisations légalement tenues de remplir des obligations spécifiques, notamment de déclarer des transactions suspectes et importantes au CANAFE.
- **Autorité responsable** : Rôle que joue un participant pour fournir un ou plusieurs des processus de confiance de la personne vérifiée ou de l'organisation vérifiée afin de déterminer si un sujet est réel, unique et identifiable, et qui protège les renseignements connexes contre la compromission. Dans le contexte de ce profil, une autorité responsable est un concessionnaire.
- **Ligne de crédit :** Terme associé au dossier de crédit pour un compte spécifique figurant dans le dossier de crédit d'une personne ou d'une entreprise. Chaque compte de crédit distinct (p. ex. carte de crédit, hypothèque ou prêt auto) a sa

propre ligne de crédit correspondante qui détaille l'historique et le statut de ce compte.

7. Critères de conformité

Portée de ces critères. Les critères de conformité dans cette section définissent le processus de confiance pour vérifier l'identité d'une personne, et les dossiers que ce processus doit produire et rendre disponible. Ils ne couvrent pas les obligations juridiques plus générales d'un participant — incluant la rétention et l'élimination des dossiers, les rapports réglementaires, les sanctions ou le filtrage des personnes politiquement exposées (PPE), la détermination de la propriété bénéficiaire ou la surveillance continue. Ces obligations sont régies par la législation et les règlements applicables à chaque participant ,et elles demeurent la responsabilité de ce participant indépendamment de la certification. Ces critères ne remplacent pas les lois, politiques ou règlements existants ou ne les substituent pas.

Les critères de conformité dans cette section spécifient les résultats qu'une solution certifiée doit réaliser et la preuve que ces résultats sont vérifiés. Ils n'imposent pas, ne favorisent pas ou n'excluent pas un produit, un fournisseur, une technique ou une architecture de système en particulier. Lorsqu'une technologie spécifique est nommée dans un critère ou les directives qui l'accompagnent, elle est citée comme moyen illustratif et acceptable de remplir l'exigence, et non comme une méthode exigée; une solution qui donne le résultat voulu par d'autres moyens, soutenu par une preuve équivalente, est également conforme. Cela garde les critères technologiquement neutres, vérifiables d'après les résultats plutôt que les mises en œuvre, et ouverts à de nouveaux intrants et méthodes émergentes.

Les critères de conformité sont organisés selon les méthodes suivantes pour vérifier l'identité d'une personne.

Méthode d'identification à l'aide du dossier de crédit

- Méthode utilisée pour vérifier l'identité d'une personne en se référant aux renseignements contenus dans un dossier de crédit canadien qui existe depuis au moins trois ans. Le nom, l'adresse et la date de naissance dans le dossier de crédit doivent concorder avec ce qu'a fourni la personne.

Méthode d'identification à processus double

- Méthode pour vérifier l'identité d'une personne en se référant à deux des renseignements suivants :
  - renseignements provenant d'une source fiable qui comprennent le nom et l'adresse de la personne;
  - renseignements provenant d'une source fiable qui comprennent le nom et la date de naissance de la personne;

- renseignements comportant le nom de la personne et confirmant qu'elle détient un compte de dépôt, une carte de crédit ou un autre compte de prêt auprès d'une institution financière.

Méthode d'identification à l'aide d'un document d'identité avec photo

Méthode pour vérifier l'identité d'une personne à l'aide d'un document d'identité délivré par un gouvernement valide, authentique et à jour (non expiré) contenant le nom et la photographie de la personne (p. ex. permis de conduire, passeport, certificat sécurisé de statut indien, carte de résident permanent ou certaines cartes d'assurance santé provinciales ou territoriales).Seuls des documents d'identité délivrés par le gouvernement fédéral canadien, un gouvernement provincial ou territorial canadien (ou un gouvernement étranger si le document d'identité est l'équivalent d'un document d'identité délivré au Canada) peuvent être utilisés. Un document émis à l'étranger est équivalent uniquement s'il est délivré par un gouvernement national ou par une autorité d'État, provinciale ou territoriale d'un gouvernement étranger; porte le nom et la photographie de la personne et un numéro d'identification unique; et contient des caractéristiques de sécurité dont l'authenticité peut être vérifiée. Les documents d'identité délivrés par des gouvernements municipaux (canadiens ou étrangers) **NE DOIVENT PAS** être utilisés.

Remarque : La détermination de l'équivalence est faite par la solution de vérification de l'identité de l'autorité responsable d'après les critères ci-dessus et elle est évaluée dans le cadre de la certification. Cela n'enlève pas la responsabilité qu'a le concessionnaire ou le prêteur de remplir ses propres obligations en matière d'identification du client en vertu de la loi applicable. Pour soutenir cette responsabilité, ce profil exige que chaque résultat de la vérification retourné à la partie dépendante identifie le document utilisé, son type, son numéro d'identification unique, et le territoire et le pays de délivrance — de sorte que les décisions concernant l'acceptation des documents puissent être examinées.

Méthode d'identification liée aux entités du même groupe ou entités financières membres

Cette méthode permet à l'autorité responsable de vérifier l'identité d'une personne en confirmant qu'elle a déjà été vérifiée par une entité admissible avec laquelle la personne a une relation d'entité du même groupe ou d'entité financière membre — par

exemple, une banque qui vérifie qu'une personne a déjà été identifiée par son entité du même groupe réglementée. La méthode dépend de trois confirmations, à savoir : que l'entité admissible existe, que la relation de la personne avec elle est actuelle, et que l'entité a vérifié auparavant l'identité de la personne en utilisant une méthode acceptable. Les catégories d'entités admissibles sont définies à l'alinéa 102.1.4

Méthode d'identification liée aux entités du même groupe ou entités financières membres (voir 102.1.4.10.1, qui contient la restriction s.5(a)–5(g) de la LRPCFAT).

Méthode d'identification consistant à se fier aux renseignements fournis par une autre entité

Cette méthode porte sur les arrangements en vertu de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* (LRPCFAT, art. 107 (dépendance)) uniquement. Une méthode basée sur un agent ou un mandataire (LRPCFAT, art. 106) n'est pas incluse dans cette version du profil et est reportée à une version future. L'inclusion de la méthode d'identification consistant à se fier aux renseignements fournis par une autre entité n'implique pas que l'article 107 est la bonne classification pour un arrangement entre concessionnaire et prêteur; voir la section 2.3 pour avoir des directives sur la façon de déterminer et de documenter le mécanisme applicable.

L'identité d'une personne peut être vérifiée en se fiant aux mesures qui ont déjà été prises par :

- Une autre entité déclarante mentionnée dans l'un ou l'autre des paragraphes 5(a) à (g) de la LRPCFAT énumérées ci-dessous :

  (5a) banques étrangères autorisées au sens que donne l'article 2 de la *Loi sur les banques* en ce qui concerne leurs activités au Canada, ou banques auxquelles cette Loi s'applique;

  (5b) coopératives de crédit, caisses d'épargne et de crédit et caisses populaires régies par une loi provinciale, et associations régies par la *Loi sur les associations coopératives de crédit*;

  (5c) sociétés d'assurance-vie ou sociétés d'assurance-vie étrangères auxquelles s'applique la *Loi sur les sociétés d'assurances* ou encore sociétés d'assurance-vie régies par une loi provinciale;

  (5d) entreprises auxquelles la *Loi sur les sociétés de fiducie et de prêt* s'applique;

  (5e) sociétés de fiducie régies par une loi provinciale;

  (5e.1) sociétés de fiducie incorporées ou constituées par ou en vertu d'une loi provinciale qui ne sont pas régies par une loi provinciale;

  (5f) sociétés de prêt régies par une loi provinciale;

  (5g) personnes et entités autorisées en vertu de la législation provinciale à mener des activités de négoce de valeurs mobilières ou d'autres instruments financiers ou à fournir des services-conseils en gestion de portefeuille ou placements, autres que des personnes qui agissent exclusivement pour le compte d'une telle personne ou entité autorisée;

- Une entité qui est affiliée à vous ou à une autre entité déclarante et qui mène des activités à l'extérieur du Canada qui sont similaires à celles d'une personne ou d'une entité visée à l'un ou l'autre des alinéas 5 a) à g) de la Loi (une entité étrangère du même groupe).

Méthode d'identification liée aux justificatifs numériques

Le CANAFE a mis à jour ses directives pour permettre la vérification de l'identité numérique, ce qui facilite l'utilisation de technologies numériques avancées. Toutefois, il n'existe pas actuellement de définition explicite pour cette méthode dans leur documentation officielle. La modernisation des directives de vérification de l'identité du CANAFE inclut la reconnaissance et l'autorisation des technologies de vérification de l'identité à distance pour l'identification des clients. Les entités déclarantes sont tenues de se conformer aux règlements du CANAFE lorsqu'elles instaurent une méthode de vérification de l'identité. Pour obtenir les renseignements les plus exacts et à jour sur les méthodes de vérification de l'identité approuvées, les entités déclarantes devraient se référer aux directives officielles du CANAFE.

Référence et critères de conformité

Référence	Critères de conformité
102	**Profil d'identité du secteur automobile du CCP**
102.1	**Identification et vérification du client**
102.1.0	**Exigences générales**
102.1.0.10	L'autorité responsable **DOIT** obtenir le consentement éclairé de la personne à la vérification de son identité avant de recueillir ou d'utiliser les renseignements sur son identité, et **DOIT** conserver un dossier suffisant pour prouver que le consentement a été obtenu, incluant la date. Cette exigence s'applique à toutes les méthodes de vérification en 102.1.1 à 102.1.6.
102.1.0.20	L'autorité responsable **DOIT** avoir des procédures documentées pour revérifier l'identité d'une personne conformément aux critères de conformité applicables lorsqu'il y a des doutes à propos de la validité, de l'état à jour ou de l'exactitude des renseignements sur l'identité recueillis auparavant, conformément au paragraphe 155(1) de la LRPCFAT. Les déclencheurs de revérification **DOIVENT** être documentés dans la politique de vérification de l'identité de l'autorité responsable.

102.1.0.30	L'autorité responsable et tout fournisseur de services de vérification de l'identité agissant pour son compte **DOIVENT** divulguer à la partie dépendante : • Les territoires où les données d'identité (incluant les modèles biométriques, les images de documents et les registres de vérification) sont traitées, enregistrées et consultées; et • Les relations avec les sous-traitants comportant la même divulgation. (Ce critère concerne uniquement la divulgation; il n'impose pas l'endroit où résident les données.)
102.1.1	**Méthode d'identification à l'aide du dossier de crédit**
102.1.1.10	Le nom complet, l'adresse résidentielle et la date de naissance fournis par la personne dont l'identité est vérifiée **DOIVENT** concorder avec le nom, l'adresse et la date de naissance contenus dans les dossiers d'une agence d'évaluation du crédit canadienne (par exemple, Equifax et Transunion).
102.1.1.20	Les renseignements d'un dossier de crédit utilisés pour mener un processus de vérification de l'identité **DOIVENT** exister depuis au moins trois ans à partir de la date de la vérification.
102.1.1.30.2	Les renseignements d'un dossier de crédit utilisés pour mener un processus de vérification de l'identité **DOIVENT** contenir de l'information provenant de deux lignes de crédit indépendantes, chacune confirmant une des deux catégories de renseignements nécessaires pour vérifier l'identité d'une personne selon cette méthode. Dans ce cas-ci, chaque ligne de crédit est une source distincte; l'agence d'évaluation du crédit n'est pas la source.
102.1.1.40.1	Les renseignements d'un dossier de crédit utilisés pour mener un processus de vérification de l'identité **DOIVENT** être obtenus directement d'une agence d'évaluation du crédit canadienne ou par l'entremise d'une autorité responsable (fournisseur tiers) autorisée par une agence d'évaluation du crédit canadienne.

102.1.1.60	Les renseignements d'un dossier de crédit utilisés pour mener un processus de vérification de l'identité **DOIVENT**: • Être obtenus au moment où le processus de vérification est mené; • Être valides et à jour au moment où le processus de vérification est mené. (Autrement dit, une personne ne peut pas fournir une image de son dossier de crédit et un dossier de crédit obtenu précédemment ne peut pas être utilisé).
102.1.1.70.1	L'autorité responsable **DOIT** recueillir tous les points de données suivants et les redonner à la partie dépendante (p. ex., à confirmer en fonction des détails de l'introduction) : • Le nom de la personne; • Le nom de l'agence d'évaluation du crédit qui détient le dossier de crédit; • Le numéro du dossier de crédit de la personne; • La date à laquelle le dossier de crédit a été consulté; • Le résultat de la vérification, notamment si l'identité de la personne a été vérifiée ou non, la fiabilité des résultats et tous les autres points de données qui peuvent influencer la décision du prêteur d'interagir avec la personne ou de la représenter.
102.1.1.80	L'autorité responsable **DOIT** développer et documenter une politique de vérification de l'identité qui décrit le cadre d'évaluation des risques utilisé pour évaluer les écarts entre les renseignements dans le dossier de crédit actuel et l'identité revendiquée.
102.1.1.90	Une politique de vérification de l'identité **DOIT** décrire l'approche utilisée pour évaluer les différences de nom, d'adresse et de date de naissance entre le dossier de crédit et l'identité revendiquée, soit individuellement ou dans le cadre d'un ensemble de données plus vaste.
102.1.1.100.1	Quand un bureau de crédit renvoie des signaux de lutte contre la fraude de quelque genre que ce soit en réponse à une vérification d'identité, l'autorité responsable **DOIT** avoir des processus en place pour évaluer ces signaux pour déterminer un risque acceptable selon la politique documentée.

102.1.1.120.1	L'autorité responsable qui utilise la méthode d'identification à l'aide du dossier de crédit **DOIT** recueillir le nom légal, la date de naissance et l'adresse résidentielle de la personne faisant l'objet d'une vérification et fournir ces données à une agence d'évaluation du crédit pour qu'elles soient traitées, notamment : • Au moins deux adresses résidentielles si la partie a déménagé au cours des trois dernières années; • Jusqu'à six adresses résidentielles maximum.
102.1.2	**Méthode d'identification à processus double**
102.1.2.10	En vérifiant le nom, l'adresse et la date de naissance fournis par la personne qui revendique une identité, l'autorité responsable **DOIT** s'assurer que les renseignements qu'elle reçoit sont valides et à jour, qu'ils proviennent de deux sources fiables différentes et qu'ils contiennent au moins deux des éléments suivants : • Renseignements provenant d'une source fiable qui contiennent le nom et l'adresse de la personne; • Renseignements provenant d'une source fiable qui contiennent le nom et la date de naissance de la personne; • Renseignements qui contiennent le nom de la personne et qui confirment qu'elle a un compte de dépôt, un compte pour des produits prépayés ou une carte de crédit ou encore un autre prêt avec une institution financière. (Par exemple, une source fiable pourrait être des ordres de gouvernement fédéral, provincial, territorial ou municipal, des sociétés d'État, des institutions financières sous réglementation fédérale ou des fournisseurs de services publics.)
102.1.2.20	Les renseignements obtenus par l'autorité responsable ou l'agent de l'autorité responsable à partir de sa propre ligne d'activités **NE DOIVENT PAS** servir à vérifier l'identité, même s'ils étaient autrement considérés comme une source fiable à cette fin.
102.1.2.30	Les renseignements provenant d'une personne revendiquant l'identité **NE DOIVENT PAS** servir aussi à vérifier l'identité. (Les renseignements recueillis auprès d'une personne sont utilisés pour résoudre l'identité revendiquée à une seule personne juridique qui est ensuite vérifiée d'après des sources fiables pour s'assurer que l'identité résolue existe et est valide.)

102.1.2.40	Si les données du dossier de crédit sont utilisées comme une des sources pour répondre aux exigences de la méthode d'identification à processus double, l'autorité responsable **DOIT** confirmer que le dossier de crédit d'où les données sont extraites existe depuis au moins six mois.
102.1.2.50.2	Si les données du dossier de crédit sont utilisées comme une des sources servant à répondre aux exigences de la méthode d'identification à processus double, l'autorité responsable **DOIT** vérifier que le dossier de crédit a été établi et qu'il est actif au moment de la vérification.
102.1.2.51.1	Si l'autorité responsable dépend de deux lignes de crédit, elle **DOIT** contenir des renseignements provenant de deux lignes de crédit indépendantes dans le même dossier de crédit, chaque ligne de crédit confirmant une des deux catégories de renseignements exigés pour vérifier l'identité d'une personne selon cette méthode. Dans ce cas-ci, chaque ligne de crédit est une source distincte; l'agence d'évaluation du crédit n'est pas la source.
102.1.2.60.2	L'autorité responsable **DOIT** s'assurer que les documents utilisés pour répondre aux exigences de la méthode d'identification à processus double (p. ex., facture d'une société de services publics) sont évalués en utilisant une solution qui est capable de déceler les preuves d'altération, de manipulation ou de falsification ou d'autres indicateurs qui remettraient raisonnablement en question l'authenticité ou l'intégrité d'un document et identifierait les documents qui ne satisfont pas aux exigences applicables en matière de validité et de fiabilité.
102.1.2.80	Le niveau de risque acceptable résultant des différences entre les renseignements fournis par la source fiable et les renseignements sur l'identité revendiquée **DOIVENT** se conformer aux exigences des services de l'industrie réglementée, le cas échéant.
102.1.2.90.1	L'autorité responsable **DOIT** développer et documenter des politiques qui énoncent le processus et l'approche utilisés pour évaluer les anomalies dans les données d'identité présentées à l'intérieur de différentes sources fiables.

102.1.2.110.1	L'autorité responsable **DOIT** recueillir tous les points de données suivants et les retourner à la partie dépendante (p. ex., prêteur) : • Le nom de la personne; • La date à laquelle les renseignements ont été vérifiés; • Les noms de deux sources fiables qui ont été utilisées pour vérifier l'identité de la personne; • Le type de renseignements auxquels il a été fait référence; • Le numéro associé aux renseignements recueillis (par exemple, numéro de compte ou, s'il n'y en a pas, un numéro associé aux renseignements, qui pourrait être un numéro de référence ou un numéro de certificat, etc.); • Le résultat de la vérification, notamment si l'identité de la personne a été vérifiée ou non, la fiabilité des résultats et tous les autres points de données qui peuvent affecter la décision du prêteur à interagir avec la personne ou à la représenter.
102.1.3	**Méthode d'identification à l'aide d'un document d'identité avec photo**
102.1.3.10.1	L'autorité responsable **DOIT** recueillir et redonner à la partie dépendante (c.-à-d. le prêteur) tous les points de données suivants provenant de la pièce d'identité avec photo délivrée par un gouvernement : • Imagerie du ou des documents utilisés pour la vérification; • Nom de la personne; • Date à laquelle l'identité de la personne a été vérifiée; • Type de document utilisé pour la vérification (p. ex., permis de conduire, passeport, etc.); • Numéro d'identification unique du document utilisé; • Juridiction (province ou État) et pays de délivrance du document; • Date d'expiration du document, si disponible (c.-à-d., si cette information figure sur le document, elle doit être recueillie et redonnée); • Résultat de la vérification, notamment si l'identité a été vérifiée ou non, fiabilité des résultats et tous les autres points de données qui peuvent influencer la décision du prêteur d'interagir avec la personne ou de la représenter.

102.1.3.20.1	L'autorité responsable **DOIT** vérifier que le document d'identité avec photo délivré par le gouvernement est authentique et délivré de façon valide par la source faisant autorité (p. ex., un gouvernement fédéral, provincial, territorial ou étranger) en : a) utilisant une technologie capable d'évaluer les caractéristiques de sécurité du document lorsque la vérification est effectuée à distance (la personne n'est pas présente physiquement); ou b) lorsque la vérification est effectuée en personne, en inspectant physiquement les caractéristiques de sécurité du document en présence de la personne ou en utilisant une technologie qui fournit un niveau d'assurance équivalent. (Directives : La validation judiciaire du document, incluant les contre-vérifications du code barres et de la bande MRZ, la lecture de la puce NFC et la validation du certificat de l'émetteur, est encouragée lorsque le document et le dispositif de saisie la soutiennent. La saisie OCR seule qui n'effectue pas de vérification de l'authenticité ne remplit pas ce critère. La lecture de la puce NFC demeure souhaitable (DEVRAIT); voir 102.1.3.110.)
102.1.3.30.1	Pour les documents avec des zones de lecture automatique (ZLA) ou des codes-barres, l'autorité responsable **DOIT**, conformément à la pratique exemplaire acceptée, comparer le contenu de la ZLA ou du code-barres avec les données imprimées sur le document et mettre en évidence les non-concordances. (Un code ZLA est une série de caractères qui apparaît au bas de la page de données personnelles d'un passeport. Il s'agit d'une combinaison de lettres, de chiffres et de symboles arrangés sur trois lignes.)
102.1.3.40.1	L'autorité responsable **DOIT** saisir en temps réel les documents d'identité avec photo délivrés par le gouvernent et empêcher le téléversement d'un fichier d'images. Cette exigence s'applique uniquement à la méthode d'identification à l'aide d'un document d'identité avec photo décrite en 102.1.3 et n'empêche pas d'utiliser des documents numérisés ou photographiés comme information de source fiable en vertu de la méthode d'identification à processus double (102.1.2), conformément à l'annexe 5 des Directives sur les méthodes de CANAFE.

102.1.3.50.4	L'autorité responsable **DOIT** soutenir, à tout le moins, la présentation de toute pièce d'identité avec photo délivrée par le gouvernement qui inclut un nom complet, un numéro d'identification unique et une photo si : • Elle est délivrée par un gouvernement provincial, territorial ou fédéral au Canada ou par un gouvernement étranger équivalent; • Elle est valide (non échue); • Elle porte un numéro d'identification unique (comme un numéro de permis de conduire); • Elle porte le nom de la personne en train d'être identifiée; • Elle porte une photo de la personne que nous sommes en train d'identifier.
102.1.3.60.1	L'autorité responsable **DOIT** documenter ses revendications de conformité aux WCAG 2.0 de niveau AA au minimum, en notant les planchers réglementaires juridictionnels qui font référence à une version antérieure (p. ex., la législation sur l'accessibilité qui fait référence au niveau AA des WCAG 2.0). (Les Règles pour l'accessibilité des contenus Web [WCAG] sont élaborées par le biais du processus W3C en coopération avec des personnes et des organisations du monde entier, dans le but de fournir une seule norme commune pour l'accessibilité des contenus Web qui répond aux besoins des personnes, des organisations et des gouvernements à l'échelle internationale.)
102.1.3.70.1	L'autorité responsable **DOIT** utiliser une technologie fiable comme déterminée acceptable et basée sur les normes de l'industrie, pour comparer les caractéristiques de l'égoportrait en temps réel avec la photo sur le document d'identité avec photo authentique délivré par un gouvernement.
102.1.3.71	L'autorité responsable qui suit la méthode d'identification à l'aide d'un document d'identité avec photo délivré par un gouvernement **DOIT** faire une détection active ou passive de la vivacité sur l'égoportrait.

102.1.3.72	Pour la vérification à distance (sans personnel), la solution de l'autorité responsable **DOIT** résister à l'injection de médias synthétiques ou préenregistrés dans le flux de données de vérification, évaluée d'après la norme CEN/TS 18099:2025 (détection d'attaque par injection de données biométriques) ou la norme ISO/IEC 25456 qui lui succédera une fois publiée, par un laboratoire indépendant compétent, atteignant au moins le niveau 2. (La détection d'attaques par injection concerne les médias synthétiques ou préenregistrés, comme les hypertrucages, la substitution de caméra virtuelle et l'injection de flux de données, envoyées directement dans le pipeline de vérification, contournant la caméra. Les techniques spécifiques comme l'attestation des points de terminaison ou capteurs, la détection par caméra virtuelle et l'analyse des médias capturés pour le contenu généré par l'IA sont des moyens illustratifs de remplir cette exigence, et non des méthodes obligatoires.)
102.1.3.73	La preuve du résultat de l'évaluation de la détection d'attaques par injection obtenue en vertu de 102.1.3.72 **DOIT** être disponible pour être vérifiée par un auditeur externe.
102.1.3.80.1	Les solutions de concordance faciale utilisées par une autorité responsable **DOIVENT** être testées par une tierce partie qualifiée et indépendante pour évaluer la performance de l'algorithme de reconnaissance faciale dans un scénario de concordance un à un. (L'existence, mais non le contenu, de ces résultats de tests doit être disponible pour être vérifiée par un auditeur externe.)
102.1.3.100.1	La vérification de la vivacité de l'autorité responsable **DOIT** être évaluée pour la détection d'attaques de présentation conformément à la norme ISO/IEC 30107-3 par un laboratoire accrédité pour la norme ISO/IEC 17025 pour ces essais et atteindre au moins le niveau 2 de la norme ISO/IEC 30107-3. (La détection d'attaques de présentation est une détection automatisée d'une tentative pour fausser une détection de la vivacité au moyen de la mesure et l'analyse des caractéristiques anatomiques ou des réactions involontaires ou volontaires, dans le but de déterminer si un échantillon biométrique est en train d'être saisi à partir d'un sujet vivant présent au point de saisie.)
102.1.3.101	Le résultat de l'évaluation de la preuve de détection d'attaque contre la présentation obtenu en 102.1.3.100.1 **DOIT** être disponible pour être vérifié par un auditeur externe.

102.1.3.110	Lorsqu'on utilise une application mobile pour numériser des documents d'identité avec photo à lecture NFC, une lecture de puce NFC fournissant un plus haut niveau d'assurance **DEVRAIT** être utilisée pour vérifier d'une manière cryptographique l'authenticité et l'origine du certificat de l'émetteur. (La communication en champ proche ou *Near-field communication* (NFC) est un ensemble de protocoles de communication qui permet la communication entre deux appareils électroniques sur de très courtes distances.)
102.1.4	**Méthode d'identification liée aux entités du même groupe ou entités financières membres**
102.1.4.10.1	L'autorité responsable **DOIT** vérifier que la personne est une entité du même groupe ou membre qui : (a) est une entité déclarante mentionnée dans n'importe lequel des paragraphes 5(a) à 5(g) de la LRPCFAT; (b) est une entité du même groupe étrangère qui mène des activités à l'extérieur du Canada similaires à celles d'une entité mentionnée aux paragraphes 5(a) à 5(g); ou (c) est une entité financière assujettie à la loi qui est membre de la coopérative de services financiers ou de la centrale de caisse de crédit de l'autorité responsable, et dont l'autorité responsable a confirmé l'existence au moyen d'une vérification indépendante.
102.1.4.20	L'autorité responsable **DOIT** confirmer l'existence de l'entité liée aux entités du même groupe ou entités financières membres en se référant à une source indépendante et fiable, comme des registres d'entreprises, des organes de délivrance de permis professionnels ou des bases de données gouvernementales.
102.1.4.30	L'autorité responsable **DOIT** recueillir au minimum les renseignements suivants auprès de la personne : • Nom légal complet; • Adresse de la personne; • Nom de l'entité liée aux entités du même groupe ou entités financières membres; • Nature de la relation de la personne avec l'entité.
102.1.4.31	L'autorité responsable **DOIT** confirmer que les renseignements de la personne (nom, adresse et date de naissance de la personne) concordent avec ceux trouvés dans les dossiers de l'entité liée ou membre.

102.1.4.40	L'autorité responsable **DOIT** vérifier l'existence de l'entité liée aux entités du même groupe ou entités financières membres avant ou au moment de confirmer l'identité de la personne au moyen de cette méthode.
102.1.4.50.1	L'autorité responsable **DOIT** vérifier que le statut d'entité du même groupe ou entité financière membre de la personne est à jour et en règle au moment de la vérification de l'identité.
102.1.4.60	L'autorité responsable **DOIT** obtenir une preuve documentaire qui confirme la relation de la personne avec l'entité vérifiée, comme des cartes de membre, des cartes d'identité d'employés ou de la correspondance officielle.
102.1.4.70	L'autorité responsable **NE DOIT PAS** se fier uniquement aux renseignements fournis par la personne pour confirmer l'existence de l'entité du même groupe ou l'entité financière membre.
102.1.4.90.2	L'autorité responsable **DOIT** produire et rendre disponibles les dossiers de vérification de l'entité, à savoir : • La source consultée; • La date of vérification; • Les renseignements obtenus; • Le nom de la personne; • La date à laquelle les renseignements ont été vérifiés au moyen de cette méthode; • Le nom de l'entité du même groupe ou de l'entité financière membre; • La méthode utilisée pour vérifier l'identité; • Tous les renseignements qui ont été enregistrés au moment de la vérification.
102.1.4.100	L'autorité responsable **DEVRAIT** compléter cette méthode avec une vérification supplémentaire de l'adresse de la personne par des moyens indépendants lorsque les renseignements de l'entité du même groupe ou de l'entité financière membre n'incluent pas la confirmation de l'adresse résidentielle de la personne.
102.1.4.110	L'autorité responsable **PEUT** instaurer une revérification périodique du statut individuel de l'entité du même groupe ou de l'entité financière membre dans le cadre des procédures de diligence raisonnable continues du client.
102.1.4.120	L'autorité responsable **DOIT** confirmer que l'entité du même groupe ou l'entité financière membre a vérifié auparavant l'identité d'une personne et a consigné la méthode spécifique qu'elle a utilisée.

102.1.5	**Méthode d'identification consistant à se fier aux renseignements fournis par une autre entité**
102.1.5.10	L'autorité responsable **DOIT** avoir une entente écrite avec un agent ou un mandataire (vérificateur tiers) sur qui elle compte pour les activités de vérification de l'identité.
102.1.5.20	L'autorité responsable **DOIT** confirmer que le vérificateur tiers sur lequel elle compte a vérifié l'identité de la personne au moyen d'une des méthodes acceptables prescrites par les règlements applicables.
102.1.5.30	L'autorité responsable **DOIT** obtenir du vérificateur tiers tous les renseignements qui ont servi à vérifier l'identité de la personne, notamment : • La méthode utilisée pour la vérification; • La date à laquelle la vérification a été faite; • Les renseignements d'identité recueillis; • Des copies des documents examinés.
102.1.5.40	L'autorité responsable **DOIT** s'assurer que le vérificateur tiers sur lequel elle compte est assujetti à des obligations en vertu du même cadre réglementaire ou d'un cadre sensiblement similaire pour la vérification de l'identité.
102.1.5.50	L'autorité responsable **DOIT** établir la dépendance à la vérification du vérificateur tiers avant que l'autorité responsable soit tenue de vérifier l'identité de la personne ou au moment où elle est tenue de le faire, et non rétroactivement.
102.1.5.60	L'autorité responsable **DEVRAIT** faire son devoir de diligence raisonnable envers le vérificateur tiers pour confirmer sa capacité, sa fiabilité et sa conformité aux exigences applicables en matière de vérification de l'identité.
102.1.5.70	Une entente écrite avec le vérificateur tiers **DOIT** spécifier : • La portée des activités de vérification; • Les obligations en termes de partage de l'information; • Les responsabilités en ce qui concerne la rétention des dossiers; • Les dispositions en matière de responsabilité et de décharge de responsabilité.
102.1.5.80.1	L'autorité responsable **NE DOIT PAS** compter sur un vérificateur tiers pour la vérification de l'identité si le tiers lui-même a compté sur une autre entité pour la vérification.

102.1.5.90	L'autorité responsable **DEVRAIT** inclure dans l'entente écrite des dispositions qui accordent des droits d'audit pour vérifier la conformité du vérificateur tiers aux exigences de la vérification de l'identité.
102.1.5.100.1	L'autorité responsable **DOIT** produire et rendre disponible de la documentation sur la relation de dépendance, notamment l'accord, la preuve du statut réglementaire du vérificateur tiers et les dossiers des transferts de renseignements.
102.1.6	**Méthode liée aux justificatifs numériques**
102.1.6.10	L'autorité responsable **DOIT** vérifier l'authenticité du justificatif numérique en confirmant qu'il a été délivré par une source de confiance et vérifiable à l'aide de méthodes de validation cryptographiques ou d'autres méthodes de validation sûres.
102.1.6.20.1	L'autorité responsable **DOIT** confirmer que l'émetteur de justificatifs numériques fonctionne à l'intérieur d'un cadre de confiance reconnu ou qu'il a été évalué selon des normes établies pour l'attribution de justificatifs d'identité numériques. (Note de bas de page : Voir le Cadre de confiance pancanadien et ses critères de reconnaissance comme cadre de confiance : https://diacc.ca/trust-framework/)
102.1.6.30	Le justificatif numérique **DOIT** contenir au minimum les attributs de l'identité vérifiés suivants : • Nom légal complet; • Date de naissance; • Adresse ou renseignements sur un autre endroit; • Numéro d'identification unique du justificatif utilisé.
102.1.6.31	L'autorité responsable **DEVRAIT** faire en sorte que seuls les renseignements nécessaires pour les besoins de la transaction sont divulgués pendant la vérification des justificatifs.

102.1.6.40.1	L'autorité responsable **DOIT** vérifier que les justificatifs numériques sont à jour et n'avaient pas expiré au moment de la vérification de l'identité, et confirmer, si possible, le statut de validité actuel des justificatifs, incluant toute condition qui affecte la validité ou l'utilisation autorisée (expiration, révocation, suspension, restriction, rétablissement), en utilisant un mécanisme approprié au modèle de confiance des justificatifs. Les mécanismes acceptables incluent un service sur le statut publié par l'émetteur, un mécanisme sur le statut cryptographique (p. ex., listes de statuts, des registres de révocation, des schémas de justificatifs de courte durée) ou une preuve de statut présentée par le titulaire.
102.1.6.60.1	L'autorité responsable **DEVRAIT** vérifier que les justificatifs numériques et leurs processus de validation sont conformes aux normes techniques reconnues pour l'identité numérique (p. ex., ISO/IEC 18013-5 pour les permis de conduire mobiles (mDL), le modèle de données de justificatifs vérifiables W3C, d'autres normes, spécifications et cadres d'identité numérique nationale).
102.1.6.61	Lorsqu'un justificatif mobile délivré par un gouvernement (p. ex., mDL provincial canadien) est présenté, l'autorité responsable **DOIT** le valider conformément à la norme technique reconnue en vertu de laquelle il est délivré, incluant l'authentification des données de l'émetteur et l'association avec les appareils (p. ex., ISO/IEC 18013-5), plutôt que d'accepter un rendu visuel.
	L'autorité responsable **DOIT** instaurer des mécanismes pour confirmer le statut de validité actuel des justificatifs numériques pendant le processus de vérification, en utilisant un mécanisme approprié au modèle de confiance des justificatifs comme décrit en 102.1.6.40.1.
102.1.6.90	Lorsqu'un justificatif numérique est utilisé pour une vérification de l'identité à distance, la vérification **DEVRAIT** appliquer une validation cryptographique des justificatifs avec la comparaison biométrique, la vivacité et les protections anti-intrusion exigées en vertu de l'alinéa 102.1.3.
102.1.6.100	Les processus de vérification des justificatifs numériques **DEVRAIENT** réduire au minimum la divulgation inutile, à l'émetteur ou des parties non reliées, de l'endroit ou du moment où ou encore à qui un justificatif est présenté, sauf lorsque cela est exigé par la loi ou un besoin opérationnel.
102.1.6.110	Les processus de vérification **DEVRAIENT** réduire au minimum la capacité des entités participantes à faire une corrélation entre des transactions distinctes impliquant la même personne, sauf si une telle corrélation est exigée par la loi ou une raison commerciale légitime.

102.1.6.120	L'autorité responsable **DEVRAIT** s'assurer que les demandes d'attributs de l'identité sont limitées à celles pour lesquelles la partie demanderesse a une raison d'être commerciale, réglementaire ou opérationnelle légitime.
102.1.6.130	L'autorité responsable **DEVRAIT** soutenir la présentation de la divulgation sélective lorsque les justificatifs sous-jacents la soutiennent.

8. Historique des révisions

Version	Date de	Auteur(s)	Description des changements

	publication		
0.01	2025-09-23	Équipe de conception du profil d'identité du secteur automobile du CCP	Ébauche initiale préparée par l'équipe de conception du profil d'identité du secteur automobile du CCP pour inclure un contexte, des termes et des définitions, des critères de conformité, etc.
0.02	2026-04-07	Équipe de conception du profil d'identité du secteur automobile du CCP	Ébauche préparée pour l'examen du TFEC et l'appel public à commentaires, et les approbations de l'examen des droits de propriété intellectuelle.
1.0	2026-04-22	Équipe de conception du profil d'identité du secteur automobile du CCP	Approuvé par le TFEC en tant que recommandation préliminaire V1.0 en prévision de l'appel public à commentaires et de l'examen des droits de propriété intellectuelle.
1.1	2026-07-16	Équipe de conception du profil d'identité du secteur automobile du CCP	Commentaires sur la disposition de l'examen public appliqués sous forme d'annotations en rouge (123 commentaires; voir le registre de disposition des commentaires et la note de la rédaction ci-dessous).
1.0	2026-08-12	Équipe de conception du profil d'identité du secteur automobile du CCP	Approuvé par le TFEC en tant que candidat à une recommandation finale V1.0.
1.0	2026-09-11	Équipe de conception du profil d'identité du secteur automobile du CCP	Approuvé comme recommandation finale V1.0 par scrutin des membres bienfaiteurs du CCIAN.

9. Note du rédacteur sur les commentaires de la disposition de l'examen public

L'examen public s'est déroulé du 5 mai au 4 juin 2026 et a obtenu 123 commentaires. Au lieu de rendre une décision isolée sur chaque commentaire, le rédacteur a groupé les questions récurrentes dans des résumés de décisions et a présenté chaque résumé à l'équipe de conception pour discussion. Une entente a été conclue sur chaque résumé avant qu'une disposition soit finalisée, de sorte que les commentaires connexes ont reçu une réponse uniforme et chaque disposition dans le registre des commentaires ramène à une décision que l'équipe a prise collectivement.

Ces discussions ont donné les décisions qui façonnent cette révision :

- **Limite de la portée.** Le profil est une spécification des processus, et non un manuel de conformité. Il certifie le processus de confiance pour produire une identité vérifiée et les dossiers que ce processus doit produire et rendre disponibles. Les obligations juridiques qui lient les participants indépendamment de la certification (rétention et élimination des dossiers, sanctions et filtrage PEP, propriété bénéficiaire, surveillance continue, rapports réglementaires) restent en dehors des critères. Un énoncé de la portée débute à présent la section 7, et les termes « retenir et conserver » ont été remplacés par « produire et rendre disponible » (102.1.4.90.2, 102.1.5.100.1).
- **Résultats et non architecture.** Les critères spécifient les résultats qu'une solution doit obtenir et les preuves qui les confirment. Aucun produit ni fournisseur et aucune technique ni architecture de réseau ne sont imposés. Les technologies nommées sont illustratives. Ce principe débute aussi à présent la section 7 et a entraîné la réécriture technoneutre des critères de statut des justificatifs (102.1.6.40.1, 102.1.6.80.2).
- **Intégrité biométrique.** La présentation de la détection des attaques est passée de DEVRAIT à DOIT au niveau 2 en vertu de la norme ISO/IEC 30107-3, testée par un laboratoire accrédité par la norme ISO/IEC 17025 (102.1.3.100.1). Un nouveau critère de détection d'attaques par injection (102.1.3.72) est une OBLIGATION au niveau 2 par rapport à la norme CEN/TS 18099:2025 pour la vérification à distance. Les deux sont rédigés en fonction des résultats, avec des techniques comme exemples uniquement, et chacun comporte un critère de preuve d'auditeur distinct (102.1.3.101, 102.1.3.73).
- **Consentement.** Un critère de consentement horizontal unique (102.1.0.10) s'applique désormais à toutes les méthodes : obtenir un consentement éclairé avant la collecte de renseignements et garder un dossier avec la date. Il remplace le critère de consentement pour les justificatifs numériques uniquement (102.1.6.70.1, supprimé). La teneur du consentement reste régie par les lois sur la protection de la vie privée.

- **Réécriture de la section 2.3.** Les directives sur les concessionnaires ont été réécrites une fois pour répondre globalement à un ensemble de commentaires : avant-propos en langage clair sur la façon d'utiliser le document, limite de responsabilité entre un fournisseur certifié et un concessionnaire, correction de l'entité déclarante (les concessionnaires qui vendent ou louent des véhicules sont à présent des entités déclarantes en vertu des articles 105, 106 et 107 de la LRPCFAT, des directives sur la détermination des mécanismes des articles 105, 106 et 107, et des points mis à jour sur la confidentialité, l'escalade et l'accessibilité.
- **Certification de la sécurité des fournisseurs.** L'équipe de conception s'est prononcée contre un critère OBLIGATOIRE exigeant la norme SOC 2 Type II, SOC 3 ou ISO/IEC 27001. La section 2.3 conseille plutôt aux concessionnaires de vérifier si un fournisseur de SVI proposé détient une telle certification et de pondérer le risque résiduel qu'ils acceptent en passant un marché avec un qui ne le fait pas.
- **Nouveaux critères horizontaux.** La revérification en cas de doute (102.1.0.20, conformément au paragraphe 155(1) de la LRPCFAT) et la divulgation de la résidence des données et du sous-traitant (102.1.0.30, divulgation seulement) ont été ajoutées sous une nouvelle section intitulée Exigences générales (102.1.0).

La vérification basée sur les risques est reportée. La demande structurelle qui a le plus de conséquences dans l'examen invitait le profil à cartographier la rigueur de la vérification d'après le risque de la transaction (valeur, type de client, alertes de fraude, transaction commerciale plutôt qu'au détail). L'équipe de la conception a été incapable de s'entendre sur cette approche dans les discussions initiales, même si elle a fait remarquer que la norme NIST SP 800-63-4, les directives du Groupe d'action financière (GAFI) et la *Digital ID Act* de l'Australie l'ont adoptée. La conception de tiers, de seuils et de déclencheurs progressifs vérifiables est un travail de conception qui ne peut pas être fait d'une manière responsable à la révision finale, de sorte qu'une vérification par niveau de risque est reportée à la prochaine version du profil. Entre-temps, la politique d'évaluation des risques documentée de l'autorité responsable (102.1.1.80) demeure le mécanisme pour évaluer les indicateurs de risque élevé et la section 2.3 demande à chaque partie dépendante de faire sa propre détermination basée sur les risques comme quoi une vérification certifiée convient au cas d'utilisation. Voici des reports connexes sur la même base : méthode agent-mandataire (art. 106), notation structurée de l'assurance des résultats de la vérification et le tableau de correspondance eIDAS-ETSI.

Total des commentaires : 76 acceptés, 35 rejetés, 12 reportés. Les résultats complets, incluant chaque disposition et les résumés des décisions, se trouvent dans le registre de Disposition des commentaires pour ce profil.