Identité essentielle : Rétablir la chaîne de confiance pour l'identité

Perspectives du groupe d'intérêt particulier du CCIAN

DIACC CCIAN

Table des matières

À propos du CCIAN **2**

À propos des groupes d'intérêt particuliers du CCIAN **2**

À propos de l'auteur **2**

Glossaire **3**

Introduction **4**

Identité essentielle : Le contexte canadien **5**

Groupe d'intérêt particulier sur l'identité essentielle **6**

Observations **7**

- Silos d'identité, identités contextuelles et identités *de facto* 8
- Biométrie 9
- Fraude 9
- Prestation de services 10

Conclusions **11**

Recommandations **12**

- Initiatives proposées 14

Appel à l'action **19**

Annexe 1 – Initiatives supplémentaires **20**

- Jetons d'exclusion mutuelle pour l'inscription à des programmes 20
- Relations : L'ADN d'une identité 21

Annexe 2 – Scénario de fraude **22**

Annexe 3 – Démonstrations **26**

Le contenu de ce rapport a été soumis par le groupe d'intérêt particulier sur l'identité essentielle du CCIAN.
Pour en savoir davantage sur les conclusions ou explorer les occasions de collaboration, veuillez écrire à info@diacc.ca.
Pour vous joindre à la communauté du CCIAN, visitez www.diacc.ca.

À propos du CCIAN

Fruit des recommandations du groupe de travail du gouvernement fédéral chargé d'examiner le système de paiements, le Conseil canadien de l'identification et de l'authentification numériques (CCIAN) est une coalition sans but lucratif de leaders des secteurs public et privé déterminés à développer un cadre canadien de l'identification et de l'authentification numériques qui permettra au Canada de participer pleinement et en sécurité à l'économie numérique mondiale.

À propos des groupes d'intérêt particulier du CCIAN

Les groupes d'intérêt particulier (GIP) du CCIAN fournissent un mécanisme pour amener notre communauté de parties prenantes à discuter d'un intérêt spécifique. Ils permettent de mettre en contact des experts du monde entier et d'élargir les conversations en dehors du cercle de membres du CCIAN.

Un GIP du CCIAN ne crée pas de propriété intellectuelle; il se penche plutôt sur une question spécifique pour recommander les étapes suivantes à intégrer dans la stratégie et la feuille de route du CCIAN.

À propos de l'auteur

Bill A.V. Pezoulas est un consultant et un entrepreneur en TI qui s'intéresse tout particulièrement à l'identité. Comme consultant, il s'est concentré sur les architectures techniques et de solutions, et il a eu des contrats avec de nombreux ministères du gouvernement fédéral canadien ainsi qu'une poignée de clients du secteur privé et des ONG. Son travail d'entrepreneur et de consultant consistant à développer des applications et des cadres logiciels lui a fait prendre conscience du rôle essentiel que la gestion de l'identité joue dans les contextes opérationnels d'entreprise, B2B et B2C.

Dans la foulée des attentats terroristes de 2001 perpétrés contre le World Trade Center (WTC), Bill a pris part à un effort visant à sécuriser davantage la délivrance des passeports en élaborant un système pour valider les certificats de naissance à la source. Le prototype de ce système a évolué et fini par être déployé dans chaque province et territoire. Cela a incité Bill à explorer l'identité selon un contexte sociétal, ce qui a mené à d'autres projets impliquant des sources d'identité essentielle et ensuite, avec Narciso Zorzi, à la création de Valid8ID Solutions Inc. en vue de développer des solutions d'identité.

Membre actif du CCIAN depuis 2016, Bill a contribué au Comité de l'innovation et au Comité d'experts du cadre de confiance (IEC et TFEC). En plus de participer fréquemment à Identity North, Bill a dirigé des conférences collaboratives et y a prononcé des allocutions. Enfin, Bill a modéré le GIP du CCIAN sur l'identité essentielle et aidé l'équipe du CCIAN à produire ce

rapport. Ajoutons à cela la contribution d'organisations des secteurs public et privé ayant participé à ce GIP.

Glossaire

Ancre biométrique : Approche hypothétique utilisant une ou plusieurs données biométriques qui peuvent être testées pour s'assurer qu'une identité est toujours associée à une seule personne naturelle, « ancrant » ainsi une identité à cette personne.

Identité contextuelle : Identité créée pour un besoin opérationnel spécifique (limité) dans un contexte opérationnel étroit, contrairement à une identité qui a été créée pour un large éventail de motifs.

Identité de facto : Identité utilisée à de multiples fins bien que non conçue pour cela et qu'il est très souvent interdit d'utiliser de multiples façons (p. ex., permis de conduire, carte santé, identité d'emploi). Dans ces cas-là, l'émetteur interdit rigoureusement de s'en servir comme identité, sauf pour le besoin spécifique pour lequel elle a été conçue.

Identité essentielle : Identité qui a été établie ou changée en raison d'un événement essentiel (p. ex., naissance, changement du nom légal d'une personne, immigration, résidence légale, citoyenneté par naturalisation, décès). Elle est définie dans le Profil du secteur public du Cadre de confiance pancanadien (PSP CCP)

Jeton d'exclusion mutuelle : Mécanisme conçu pour empêcher un accès concurrent à des ressources protégées par plus d'un processus ou d'une entité. Dans le contexte de ce document, il empêche qu'une identité soit inscrite à plus d'un programme d'un type donné qui doit être mutuellement exclusif (p. ex., une personne ne peut être inscrite qu'à un seul régime d'assurance santé provincial à n'importe quel moment).

Justificatif d'identité : Type de représentation numérique qui décrit un ensemble d'attributs ou de propriétés d'une personne. Ces renseignements peuvent exister par eux-mêmes (p. ex., en tant que justificatif qui ne renferme pas de renseignements personnels, uniquement un identifiant de chaîne unique) ou être reliés à des renseignements personnels.

Justificatif vérifiable : Un justificatif vérifiable peut représenter les mêmes renseignements qu'un justificatif physique. L'ajout de technologies (p. ex., signatures numériques) rend les justificatifs vérifiables plus inviolables et plus fiables que leurs correspondants physiques. Pour obtenir une définition plus approfondie, veuillez vous référer au document Verifiable Credentials Data Model v1.1 (w3.org).

Livre de noms : Registre familier pour désigner la liste d'identités faisant autorité.

Niveau d'assurance : Niveau d'assurance auquel d'autres peuvent se fier. Dans le CCP appliqué comme mesure de la certitude qu'un sujet est celui ou ce qu'il affirme être, ou encore qu'un sujet a gardé le contrôle d'un authentifiant, et que l'authentifiant n'a pas été compromis.

Dans le contexte du CCP, les niveaux d'assurance sont ceux définis par la Directive du gouvernement du Canada sur la gestion de l'identité – Annexe A : Norme sur l'assurance de l'identité et des justificatifs. La Recommandation finale du glossaire du CCP V1.0 fournit une définition.

Titulaire : Personne, organisation ou machine qui contrôle, ou est en voie d'obtenir une représentation numérique dans l'écosystème de l'identité numérique réglementé par le Cadre de confiance pancanadien (CCP).

Introduction

La confiance est le fait de se fier avec assurance aux caractéristiques, à la capacité, à la force ou à la véracité d'une personne ou d'une chose. La confiance est le pilier indispensable d'une démocratie, d'une économie et d'une société hautement fonctionnelles. La sécurité est un facteur essentiel de confiance. À défaut de sécurité, la confiance s'érode.

La confiance élimine les contraintes qui sont appliquées pour augmenter le niveau d'assurance dans une transaction. Si ces contraintes sont supprimées, il n'y a pas de limites aux occasions, à la prospérité et aux objectifs collectifs que les personnes, les entreprises et les gouvernements peuvent réaliser. La confiance permet de conclure des contrats, de prêter de l'argent, de faire des achats, d'accéder à des services, et de partager de l'information avec assurance et sécurité.

Sans confiance, on peut facilement perdre des occasions et des contrats propices à la croissance économique, et des gens peuvent être laissés en dehors ou derrière. Sans confiance, personne ne peut avoir la certitude que ses plans, achats et renseignements sont en sécurité et en sûreté.

La confiance a toujours été indispensable pour les relations économiques et sociales, à plus forte raison dans l'économie numérique où des décisions irrévocables peuvent être prises en un clin d'œil ou d'un clic de souris; alors que l'acheteur ou le prêteur n'est pas nécessairement à côté ou à un coin de rue, mais possiblement à l'autre bout du monde; que les renseignements sont partagés plus souvent en ligne qu'en personne; et que des personnes déterminées manipulent les identités et les processus de vérification faibles pour leurs propres besoins malveillants. Il est d'autant plus difficile de gagner la confiance de la population canadienne dans l'écosystème numérique en

expansion rapide que la méfiance envers les institutions gouvernementales et économiques augmente parmi un segment grandissant de la population canadienne.

La participation accrue du Canada à l'économie numérique a fait ressortir certains défis reliés à l'environnement de confiance existant, en particulier ses silos d'identité territoriaux.

C'est essentiel de développer une identité numérique robuste pour que le Canada puisse établir une confiance numérique et saisir le potentiel de l'économie numérique du 21e siècle. Les gouvernements et le secteur privé au Canada et dans le monde savent cela, et ils ont fait d'importants progrès pour concevoir de nouveaux réseaux et écosystèmes d'identité numérique modernes et basés sur des normes, qui sont robustes et sûrs, procurent commodité et choix, et permettent à l'utilisateur de contrôler l'accès à ses renseignements personnels et l'emploi qui en est fait. À défaut de s'attaquer aux défis que posent les silos d'identité territoriaux, ce travail important sera incomplet et risque de créer de sérieux problèmes.

Le CCIAN juge fondamental d'intégrer les sources d'identité essentielle dans l'écosystème en évolution de l'identité numérique afin de relever ces défis, et c'est pourquoi il a formé un GIP d'experts en identité pour faciliter les progrès et focaliser les efforts dans ce domaine.

Ce rapport présente les observations et les recommandations du GIP et les initiatives qu'il propose pour aider à préparer le système d'identité canadien à faire la transition vers un écosystème d'identité numérique mondial. Il précise les exigences d'une identité de confiance et les mérites relatifs des identités existantes par rapport à ces exigences, et présente une stratégie pour une identité nationale.

Identité essentielle : Le contexte canadien

Le Canada n'a pas de carte d'identité nationale, les raisons à cela étant enracinées dans la structure unique de notre fédération et la répartition des responsabilités entre nos gouvernements national et provinciaux. Les Canadiens s'inquiètent d'un registre gouvernemental centralisé pouvant servir à surveiller leurs activités, un argument qui a été systématiquement avancé devant les tribunaux pour limiter l'utilisation des dossiers d'assurance sociale fédéraux (numéro d'assurance sociale ou NAS) et des identifiants connexes pour les besoins de l'assurance emploi et de la fiscalité.

Historiquement, l'identité au Canada a été fragmentée en de multiples silos territoriaux, de sorte que le pays n'a pas d'identifiant unique qui sert d'identité. Les silos d'identité (identités contextuelles) ont évolué pour soutenir diverses fins, comme les permis de conduire, l'assurance emploi et la fiscalité (NAS), les services gouvernementaux (cartes pour les services

gouvernementaux, cartes santé), l'immigration (visas d'immigration, documents de résidence permanente et de citoyenneté) et les voyages (passeports). Les organisations responsables de chacun de ces silos ont fait preuve de diligence pour avoir leurs propres systèmes d'identité pour leurs besoins, mais ces systèmes n'ont pas été conçus pour servir d'instrument d'identité ommiprésent. Il s'agit de certaines formes *de facto* de documents d'identité physique dont dépend le système d'identité canadien.

Les identités essentielles sont créées à la suite d'un événement essentiel (c.-à-d., naissance ou immigration) et sont du ressort exclusif des organisations de l'état civil [OEC] des provinces et des territoires, et d'Immigration, Réfugiés et Citoyenneté Canada [IRCC], respectivement.

Une « chaîne de confiance » basée sur l'examen des pièces d'identité physiques et une concordance imparfaite des noms sert couramment à résoudre les identités entre ces silos, mais les identités essentielles ne sont pas systématiquement incorporées dans cette chaîne de confiance pour lier les identités contextuelles à leurs correspondants essentiels.

La biométrie, surtout les photographies faciales, a aussi été insérée dans ces formes d'identité pour aider à vérifier les identités. Mais les moyens de les vérifier avec leur émetteur ne sont fournis qu'à quelques-uns seulement à l'intérieur du silo émetteur. L'utilisation de ces formes de biométrie en dehors du silo émetteur s'est faite par inspection manuelle, sans grandes garanties que les éléments biométriques apparaissant sur la pièce d'identité physique soient les bons.

Des progrès considérables ont été, et continuent d'être, faits au Canada et dans le monde pour concevoir de nouveaux réseaux et écosystèmes d'identité numérique modernes basés sur des normes, qui sont robustes et sûrs, et qui fournissent une commodité, un choix et un contrôle des renseignements personnels. Au Canada malheureusement, ces nouveaux réseaux d'identité avancés sont peuplés d'identités ayant été établies à l'intérieur de cette chaîne de confiance brisée, ce qui amplifie davantage les préjudices passés.

La prémisse de base qui sous-tend ce rapport est le fait que cette chaîne de confiance est ***brisée***, en dépit de la biométrie et des autres avancées introduites au fil des ans. Cette réalité engendre des pertes économiques graves et croissantes pour l'économie canadienne en raison de la fraude reliée à l'identité et de la prestation inefficace des services, mais elle menace aussi l'intégrité des écosystèmes d'identité numérique qui ont rapidement évolué ces dernières années. Ces défis, s'ils restent non résolus, vont se répercuter d'une manière

encore plus marquée sur l'économie du Canada et continuer à freiner la participation de la population canadienne à la croissance exponentielle de l'économie numérique mondiale.

Ce rapport contient une série d'observations et de recommandations qui justifient à elles toutes et d'une manière convaincante la nécessité d'élaborer et de mettre en œuvre une stratégie pour une identité nationale, et de prendre des initiatives supplémentaires pour rétablir la chaîne de confiance de l'identité, et qui pavent la voie à l'écosystème d'identité numérique en évolution.

Groupe d'intérêt particulier sur l'identité essentielle

En 2021 et au début de 2022, le CCIAN a collaboré avec un GIP pour examiner la façon dont l'intégration des identités essentielles dans l'écosystème d'identité numérique pourrait améliorer la résolution de l'identité entre les silos, introduire de nouvelles efficacités dans la prestation des services et réduire la fraude. Il y avait, parmi les membres du GIP, des représentants des bureaux de l'état civil et des initiatives en matière d'identité numérique au niveau provincial, d'Immigration, Réfugiés et Citoyenneté Canada (IRCC), et des secteurs de la finance et de l'assurance au Canada, ainsi que d'autres participants des secteurs privé et public. Les membres du GIP ont pris part à 14 séances de travail pour examiner des volets dans divers sujets, notamment les dossiers de naissance, les répercussions sur la prestation des services et la fraude, et l'établissement de feuilles de route. En outre, le modérateur du GIP et certains membres ont préparé une série de cinq démonstrations technologiques (voir la liste et les liens à l'annexe 3) pour illustrer les principes opérationnels de certaines des initiatives proposées (comme on le verra dans les sections qui suivent).

Cette section du rapport présente des observations, des conclusions et des recommandations, notamment une liste de 12 initiatives proposées pour aborder et résoudre certains des enjeux ardus auxquels notre communauté est confrontée aujourd'hui.

Observations

Les dossiers de naissance et d'immigration documentent les événements qui attestent et créent une identité juridique. Ces dossiers sont essentiels à l'identité d'une personne au Canada et contiennent des identifiants uniques. Les bureaux de l'état civil, au niveau provincial, et IRCC, au niveau fédéral, sont des sources qui font autorité pour ces identifiants essentiels.

Les dossiers de naissance ont été institués à des fins statistiques et pour d'autres besoins reliés à la santé publique. Les dossiers d'immigration ont été institués pour gérer et contrôler l'immigration. La législation (provinciale

pour les premiers et fédérale pour les seconds) est axée sur les motifs initiaux de ces registres, mais ces deux types de dossiers sont utilisés comme forme d'identité dans certains contextes uniques. La *Loi sur les services de l'état civil*, *Loi sur les statistiques de l'état civil* ou *Vital Statistics Act* au niveau provincial ou territorial, et la *Loi sur l'immigration et la protection des réfugiés* ne reconnaissent ou ne soutiennent pas l'utilisation omniprésente des documents délivrés et des ensembles de données sous-jacents comme formes d'identité valides dans le cas généralisé.

Les identifiants uniques, associés aux noms légalement reconnus dans les registres, pourraient être utilisés pour résoudre efficacement une identité entre des silos.

Silos d'identité, identités contextuelles et identités *de facto*

De nombreux silos dans les secteurs public et privé au Canada saisissent et maintiennent des données d'identité contextuelle. Chaque silo a traditionnellement délivré et maintenu des identités contextuelles pour son propre programme ou service et administration ou pour des raisons commerciales (p. ex., cartes santé, permis de conduire, passeports, cartes d'identité d'étudiants, cartes d'identité délivrées par les employeurs, etc.). Les silos ne prévoient ou ne planifient généralement pas que leurs identités soient utilisées dans d'autres silos et ne valident pas ces identités pour d'autres parties dépendantes. Cette structure en silos entraîne les conséquences suivantes :

- Processus et coûts redondants pour créer et maintenir des identités
- Éléments et caractéristiques variables d'une identité, en particulier en ce qui concerne la sécurité et la protection de la vie privée
- Conditions d'admissibilité variables pour une identité
- Processus d'établissement de l'identité variables, preuve d'identité exigée, exceptions et solutions de rechange
- Identité contenant des identifiants uniques qui ne peuvent être résolus que dans un contexte ou silo

La plupart des identités contextuelles ne sont pas ancrées à un identifiant externe unique au monde. Même quand une identité essentielle a été utilisée comme preuve d'identité dans le processus de délivrance, son identifiant unique n'est pas incorporé dans l'identité contextuelle ID.

Certaines identités contextuelles ont fini par être acceptées comme formes d'identité *de facto* dans d'autres silos (permis de conduire, passeports, cartes santé, cartes de résidence permanente, etc.) même si :

- Il n'y a pas d'infrastructure universelle pour valider ces identités ou pour recevoir des avis de changement de statut (c.-à-d., expiration, révocation, perte ou vol de documents) ou en cas de changement de nom ou de décès
- L'organisation émettrice a émis des avis de non-responsabilité concernant l'utilisation de l'identité à des fins autres que celle pour laquelle elle a été initialement délivrée

- Il est facile d'obtenir ou de créer des identités physiques falsifiées

De nombreux programmes de prestations et de réglementation gouvernementaux trouvent difficile d'augmenter le niveau d'assurance (au-dessus de LOA2) de leurs identités, étant donné le manque de preuves d'identité vérifiables et incorruptibles.

Biométrie

La biométrie est parfois utilisée dans des silos précis pour vérifier l'identité d'une personne, mais pas systématiquement en dehors du silo pour lequel l'identité a été saisie.

Il n'existe pas de données biométriques « du berceau à la tombe » saisies à la naissance qui peuvent être utilisées efficacement pour vérifier l'identité d'une personne tout au long de sa vie, ni d'éléments biométriques qui soient activement saisis à la naissance. Sans cette ancre biométrique, les identités sont vulnérables à la fraude, car chaque processus d'inscription offre une occasion supplémentaire que les données biométriques d'une autre personne soient associées à une identité.

Les photographies faciales sont largement utilisées sur les pièces d'identité imprimées, mais il n'y a pas d'infrastructure omniprésente pour vérifier systématiquement l'identité d'une personne d'après la source qui fait autorité au moyen de ces données biométriques. Bien souvent, ces pièces d'identité imprimées avec photo sont soumises à une inspection humaine pour vérifier les identités, mais cette méthode n'est pas fiable et la plupart des tentatives pour automatiser cette reconnaissance faciale à partir de pièces d'identité imprimées (donc s'en servir comme éléments biométriques) comparent uniquement l'image réelle du titulaire avec l'image imprimée, ce qui permet à de fausses identités de passer le test.

Fraude

Les crimes reliés à la fraude à l'identité sont nombreux et en hausse. Le crime organisé et les criminels déterminés utilisent des identités frauduleuses aux fins suivantes :

- Vol
- Soustraction aux conséquences criminelles
- Contournement des processus d'immigration et des conditions d'entrée
- Fraude aux prestations sociales
- Enlèvement parental
- Blanchiment d'argent
- Financement et camouflage des produits du crime
- Brouillage des bénéficiaires effectifs des sociétés pour la fraude aux valeurs mobilières et à l'impôt
- Terrorisme (intérieur et international)

Les crimes reliés à la fraude à l'identité sont faciles à commettre et lucratifs pour ceux qui les perpètrent, car :

- Les renseignements sur l'identité d'une personne peuvent être obtenus assez facilement en recueillant de l'information sur les réseaux sociaux ou en accédant à des données déjà disponibles (sur le Web noir) qui sont exposées par les brèches continuelles dans les bases de données des entreprises et des gouvernements
- Une identité synthétique peut être créée d'une manière relativement facile
- Un élément biométrique peut être facilement associé à une identité volée ou synthétique
- La résolution des identités entre les silos est problématique en raison de :
    - La dépendance à des méthodes de concordance des noms qui sont imparfaites
    - L'absence d'identifiants uniques pouvant être utilisés à une échelle nationale
    - Le manque d'infrastructures pour valider toutes les formes d'identité
    - La facilité avec laquelle on peut créer de faux documents d'identité
    - La facilité avec laquelle on peut inscrire une identité fausse ou volée à un programme légitime et créer ainsi une identité contextuelle valide

On n'a pas facilement accès à des renseignements exhaustifs et détaillés sur les répercussions de la fraude au Canada. L'information qui suit n'est pas partagée ouvertement dans tous les secteurs :

- Fréquence des crimes reliés à la fraude à l'identité
- Vecteurs d'attaque les plus répandus
- Montants des pertes par secteur
- Autres impacts (p. ex., perte de réputation et de confiance au niveau local, national et international)

Prestation de services

Chaque programme ou service, administration ou entreprise commerciale dépense des sommes importantes pour obtenir, valider et maintenir les renseignements d'identité de leurs clients et parties prenantes. Ces processus visant à prouver l'identité dépendent d'identités contextuelles provenant d'autres silos et la plupart sont tributaires de méthodes de concordance des noms pour résoudre les identités.

L'absence d'identifiants uniques et de documents d'identité vérifiables et infalsifiables augmente les risques pour ces organisations, ce qui les oblige à atténuer les efforts et les coûts grandissants pour remplir leur mandat.

Les programmes qui ont une obligation d'exclusion mutuelle (p. ex., une personne ne peut s'inscrire qu'à un régime d'assurance santé provincial) ne peuvent pas déceler efficacement des inscriptions multiples.

La prestation de services bénéficierait de justificatifs d'identité numérique de confiance.

Conclusions

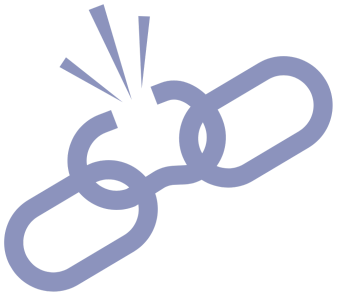
Il manque au système d'identité en silos qui a évolué au Canada au cours des dernières décennies certaines intégrations unificatrices qui ont laissé de nombreuses failles, incohérences et vulnérabilités parmi et entre les silos, ce que nous avons appelé une *chaîne de confiance brisée* dans l'identité. Cela a entraîné, et continue d'entraîner, des inefficacités dans la prestation des services et une fraude reliée à l'identité.

Il manque dans les identités établies à partir de cette chaîne de confiance brisée une ou plusieurs des caractéristiques suivantes d'une « identité de confiance » :

- Aboutit à une seule personne **au niveau national**
- L'authenticité est facile à prouver
- Est infalsifiable et il n'y a pas moyen d'apporter des changements aux renseignements d'identité
- Contient des protections pour empêcher une appropriation malveillante
- Permet de modifier les renseignements qu'elle contient (noms, décès) et statut (révoqué, perdu ou volé, expiré) pour transmission rapide aux parties dépendantes
- Permet au titulaire d'être vérifié d'une manière fiable comme étant le sujet de l'identité conformément aux lois, politiques et règlements dans un contexte spécifique
- Permet au titulaire de garder le contrôle de l'identité, ce qui augmente la confidentialité et la sécurité
- Le livre de noms ne doit pas contenir de dossiers frauduleux ou erronés non découverts

Le système d'identité en silos du Canada manque aussi de ce qui suit :

- Une stratégie pour résoudre l'identité entre des silos existants
- Des normes communes pour les éléments fondamentaux (c.-à-d. justificatifs, authentification, partage et interopérabilité)
- Une feuille de route sur la façon de créer des identités de confiance physiques et numériques telles que décrites ci-dessus, qui seraient :
    - Convenablement soutenues par les lois
    - Appuyées par une infrastructure à l'échelle nationale
    - Acceptées universellement



- Un partage de connaissances entre toutes les parties intéressées et investies sur la fraude à l'identité et le crime relié pour déterminer :
    - L'ampleur du problème
    - Ses causes profondes
    - Les stratégies d'atténuation
- Une méthode pour tester et améliorer continuellement notre système d'identité

En dépit des progrès constants pour bâtir un robuste écosystème d'identité numérique, nous le peuplons avec des identités qui ont été établies à partir de cette chaîne de confiance brisée et, ce faisant, nous enchâssons et amplifions les préjudices passés et créons de nouveaux risques.

Recommandations

Comme l'écosystème de l'identité numérique continue de croître et d'évoluer à un rythme de plus en plus rapide, nous devons travailler simultanément à restaurer la chaîne de confiance en établissant une identité de confiance à une échelle pancanadienne. Une identité de confiance, qui est créée, maintenue et consommée indépendamment de n'importe quel silo, peut être obtenue en :

1. Développant une stratégie nationale de l'identité pour les identités de confiance.
2. Officialisant le principe de l'identité essentielle pour qu'elle puisse être incorporée dans les cadres politiques, règlements ou lois applicables.
3. Transformant les certificats de naissance et les documents d'immigration en identités essentielles véritables de sorte qu'ils :
    - Reconnaissent les droits qu'ont les titulaires de les utiliser comme identités, ce qui obligera à apporter des changements aux politiques et aux lois connexes
    - Améliorent la sécurité et la protection de la vie privée en étant délivrés dans un format numérique
    - Adoptent des pratiques exemplaires pour délivrer des identités sous une forme physique
    - Repèrent et colmatent les failles dans les processus pour délivrer et maintenir ces artéfacts comme identités essentielles (au lieu des certificats de naissance ou documents d'immigration).
    - Donnent au titulaire la capacité de contrôler qui voit et utilise les renseignements d'identité
4. Tirant parti des identifiants uniques de l'identité essentielle pour mieux résoudre les identités contextuelles
5. Mettant en place une détection ou une application mutuelle de l'exclusivité pour les programmes qui ont ce mandat (permis de conduire, assurance santé, etc.). L'annexe 1 traite davantage de cette recommandation.

Le système d'identité et l'économie dans son ensemble vont bénéficier d'une identité de confiance en :

- Réduisant la duplication et les coûts
- Uniformisant le niveau de confiance accordé à n'importe quelle identité grâce aux niveaux d'assurance standards
- Ayant une seule source de notifications reliées à l'identité, comme les changements de nom, décès, vols d'identité, changements de statut (p. ex., expiration, révocation, perte ou vol, activité frauduleuse décelée) des instruments d'identité
- Permettant aux administrateurs de programmes de se concentrer davantage sur l'admissibilité d'un demandeur et moins sur la preuve d'identité

Les titulaires d'une identité de confiance bénéficieront en :

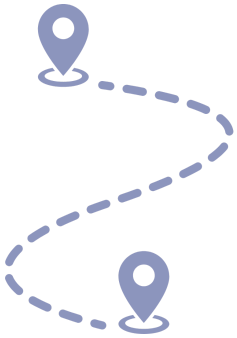
- Rendant plus difficile la falsification des documents d'identité essentiels
- Réduisant la valeur des documents d'identité essentiels falsifiés
- Faisant en sorte qu'il soit plus difficile de s'approprier d'une façon malveillante des documents d'identité essentiels
- Fournissant un mécanisme permettant à toutes les parties dépendantes de valider des documents d'identité essentiels
- Décelant et empêchant les utilisations multiples (frauduleuses) d'une identité légitime
- Recevant des notifications sur les moments et les endroits où leur identité est utilisée (s'apparente beaucoup à certains comptes en ligne comme Google)
- En la rendant plus sécuritaire et en renforçant la protection de la vie privée

L'identité de confiance va améliorer la capacité qu'a une partie dépendante d'attribuer une identité à une seule personne en :

- Tirant parti des identifiants uniques provenant de sources essentielles pour toutes les formes d'identité
- Consolidant et améliorant les processus de changement de nom légaux, notamment en cas de mariage
- Mettant à profit la biométrie et en définissant le cycle de vie d'une identité avec des éléments biométriques associés pour obtenir une ancre biométrique du berceau à la tombe

La section qui suit énumère des initiatives proposées qui mettraient en place les recommandations ci-dessus.

Initiatives proposées



Les initiatives proposées sont réparties sur un certain nombre d'années à partir de 2023 (année 1). La description des initiatives contient des liens vers des vidéos de démonstration de l'application qui illustrent une initiative proposée. De plus amples détails sur les initiatives sont fournis dans la feuille de route élargie. Deux initiatives supplémentaires qui n'ont été que brièvement explorées dans les séances de travail du GIP sont incluses dans l'annexe 1.

Les auteurs reconnaissent que le fait de proposer des initiatives interterritoriales allant aussi loin pose un défi de taille, de sorte que les dates suggérées sont hypothétiques et représentent des années ciblées et une séquence d'initiatives pour avoir un impact maximal.

1. **Élaborer une stratégie nationale en matière d'identité** : Élaborer, ou améliorer, une stratégie nationale en matière d'identité pour toutes les principales identités essentielles et contextuelles, notamment reconnaître leur statut ou utilisation en tant qu'identités omniprésentes ainsi que les droits et les attentes des titulaires, les services d'identité, la résolution appropriée de l'identité entre les silos, etc. Un accent particulier devrait être mis pour renforcer les processus de vérification et de preuve de l'identité.

   - Objectifs
     - Reconnaître la nature fondamentale de l'identité essentielle et enchâsser l'utilisation *de facto* de certaines identités contextuelles en dehors de leurs silos d'origine
     - Soutenir les droits et les attentes des titulaires par rapport à l'utilisation qu'ils font de ces identités
     - Fournir un système d'identité plus cohérent et intégré
     - Soutenir la transition vers un écosystème d'identité numérique

   - Parties prenantes
     - Conseil stratégique de DPI
     - Initiatives provinciales reliées à l'identité
     - Émetteurs de cartes de services gouvernementaux
     - Secrétariat du Conseil du Trésor du Canada
     - Émetteurs d'identités contextuelles des secteurs public et privé
     - Parties dépendantes des secteurs public et privé

   - Exécution : Immédiate et continue

2. **Améliorer la sécurité de notre système d'identité :** Établir un dialogue ouvert sur la fraude et la sécurité de l'identité parmi les parties prenantes, et élaborer et mettre en place un régime pancanadien pour améliorer la sécurité.

   - Objectifs
     - Accroître la sécurité du système d'identité
     - Réduire les occasions de fraude

   - Parties prenantes
     - Groupe national de coordination contre la cybercriminalité (GNC3) de la Gendarmerie royale du Canada
     - Forces policières provinciales
     - Centre antifraude du Canada
     - Groupe d'action financière (GAFI)
     - Institutions financières
     - Agence des services frontaliers du Canada (ASFC)
     - Immigration, Réfugiés et Citoyenneté Canada (IRCC)
     - Émetteurs d'identité du secteur public, incluant les émetteurs provinciaux, les bureaux de l'état civil, etc.

   - Exécution : Immédiate et continue

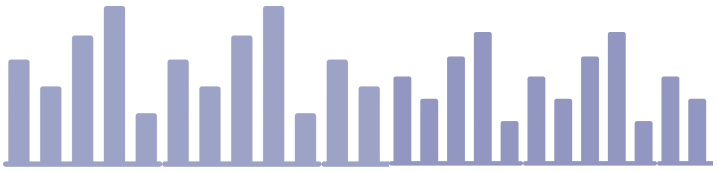
---

3. **Validation centrale de l'état civil :** Déployer un service de validation centrale pour les certificats de naissance, qui donne à une partie dépendante autorisée la capacité de valider un certificat de naissance délivré par une province ou un territoire au Canada (démonstration nº 1).

   - Objectifs
     - Tirer parti des identifiants uniques reliés à un nom légal
     - Réduire la dépendance à la concordance des noms pour résoudre l'identité

   - Parties prenantes
     - Tous les bureaux de l'état civil

   - Exécution : Dès que possible (en parallèle aux efforts de modernisation de l'état civil), déploiement initial la première année, intégration des parties dépendantes les deuxième et troisième années.



4. **Notification de décès et de changements de noms légaux de l'état civil :** Déployer un service de notification de décès et de changement de noms légaux de l'état civil à toutes les parties dépendantes (extension de la démonstration nº 1).

   - Objectifs
     - Réduire la possibilité de fraude reliée à l'identité
   - Parties prenantes
     - Tous les bureaux de l'état civil
   - Exécution : Immédiatement après la validation centrale de l'état civil (en parallèle aux efforts de modernisation de l'état civil), déploiement initial la deuxième année, intégration des parties dépendantes les troisième et quatrième années.

---

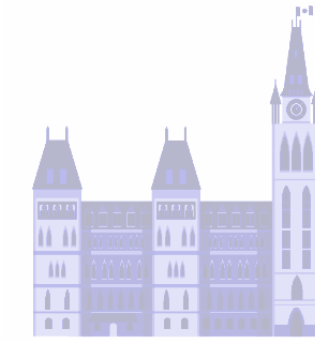
5. **Validation de l'immigration :** Déployer un service de validation pour les documents d'immigration (résident permanent, résident temporaire, citoyenneté). (extension de la démonstration nº 1).

   - Objectifs
     - Tirer parti de l'identifiant unique relié au nom légal
     - Diminuer la dépendance à la concordance des noms pour la résolution de l'identité
   - Parties prenantes
     - Immigration, Réfugiés et Citoyenneté Canada (IRCC)
   - Exécution : Dès que possible, déploiement initial la deuxième année, intégration des parties dépendantes les troisième et quatrième années.

---

6. **Validation centrale de l'identité contextuelle :** Déployer un service centralisé de validation pour d'autres identités contextuelles essentielles, avant tout les permis de conduire, et possiblement les cartes santé et de services gouvernementaux. (extension de la démonstration nº 1).

   - Objectifs
     - Réduire la possibilité de fraude reliée à l'identité
   - Parties prenantes
     - Conseil canadien des administrateurs en transport motorisé (CCATM) et ministères des Transports individuels
     - Services de santé et gouvernementaux



- Exécution : Dès que possible, déploiement initial les première et deuxième années, intégration des parties dépendantes de la troisième à la cinquième année.

---

7. **Identités contextuelles ancrées :** Intégrer les identifiants uniques de l'identité essentielle dans les principales identités contextuelles, avant tout les permis de conduire, et les cartes santé et des services gouvernementaux.

   - Objectifs
     - Réduire la possibilité de fraude reliée à l'identité
   - Parties prenantes
     - Ministères des Transports individuels
     - Services de santé et du gouvernement
   - Exécution : Immédiatement après la validation centrale de l'état civil et de l'immigration, déploiement vers les identités contextuelles initiales les deuxième et troisième années, intégration des identités restantes de la troisième à la cinquième année.

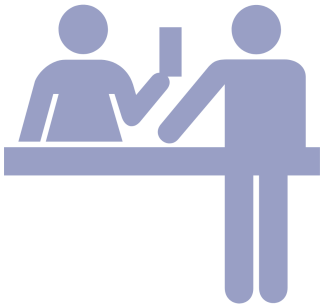
---

8. **Délivrance centralisée de justificatifs vérifiables de certificats de naissance :** Déployer un service central qui utilise les services de validation du Système national d'acheminement (SNA) dans l'ensemble des provinces et territoires pour délivrer automatiquement des justificatifs vérifiables de certificats de naissance en validant des secrets partagés existants (amélioration de la démonstration nº 2).

   - Objectifs
     - Accélérer l'intégration de la population dans une infrastructure de portefeuille numérique
     - Renforcer la relation entre les bureaux de l'état civil en tant qu'émetteurs et personnes (possibilités de transactions futures)
     - Fournir au titulaire la capacité d'agir, offrir plus de commodité pour prouver son identité
     - Augmenter le niveau d'assurance en combinaison avec d'autres justificatifs vérifiables
     - Réduire la possibilité de fraude reliée à l'identité

   - Parties prenantes
     - Tous les bureaux de l'état civil
   - Exécution : Immédiatement après la validation centrale de l'état civil et de l'immigration, déploiement vers les identités contextuelles initiales les deuxième et troisième années, intégration des identités restantes de la troisième à la sixième année.

9. **Notification de la validation au titulaire :** Déployer un service de notification pour aviser le titulaire d'un justificatif vérifiable lorsqu'un certificat de naissance ou un document d'immigration traditionnel est validé (extension de la démonstration nº 2).



- Objectifs
  - Permettre au titulaire de déceler plus tôt une fraude, réduire l'impact de la fraude
- Parties prenantes
  - Tous les bureaux de l'état civil
  - Immigration, Réfugiés et Citoyenneté Canada (IRCC)
- Exécution : Quatrième année après que les justificatifs vérifiables sont délivrés et que les identités contextuelles sont ancrées dans les identités essentielles.

---

10. **Délivrance de justificatifs vérifiables provenant de sources d'identité essentielle faisant autorité :** Les bureaux de l'état civil et de l'immigration vont instaurer la délivrance de justificatifs d'identité essentielle, notamment des certificats de naissance, et des justificatifs de résidents permanents et temporaires et de citoyenneté (extension de la démonstration nº 4).

- Objectifs
  - Renforcer la relation entre les bureaux de l'état civil en tant qu'émetteurs et citoyens (possibilités de transactions futures)
  - Fournir au titulaire la capacité d'agir, offrir plus de commodité pour prouver son identité
  - Augmenter le niveau d'assurance en combinaison avec d'autres justificatifs vérifiables
  - Réduire la possibilité de fraude reliée à l'identité
- Parties prenantes
  - Bureaux de l'état civil
  - Immigration, Réfugiés et Citoyenneté Canada (IRCC)
- Exécution : Résultat de la modernisation de l'état civil et de l'immigration pour ce qui est de l'identité de la quatrième à la sixième année. Intégration de la population de la sixième à la dixième année.

---

11. **Signalement par le CIOC des pièces d'identité perdues ou volées :** Mettre à profit le Centre d'information de la police canadienne (CIPC) pour délivrer des identités contextuelles Centre/les émetteurs d'identité essentielle pour signaler les pièces d'identité

perdues ou volées.

- Objectifs
  - Renforcer la sécurité de l'écosystème de l'identité
- Parties prenantes
  - Gendarmerie royale du Canada
  - Tous les bureaux de l'état civil
  - Immigration, Réfugiés et Citoyenneté Canada (IRCC)
  - Tous les émetteurs d'identité contextuelle
- Exécution : Deuxième année

---

12. **Surveillance de l'utilisation frauduleuse d'une identité :** Utiliser (d'une manière qui protège la vie privée) la corrélation entre une identité essentielle et son utilisation pour déceler et prévenir la fraude. Par exemple, si une identité réside dans une province, mais apparaît soudainement dans des cas d'utilisation très spécifiques ailleurs, elle pourrait être signalée comme étant frauduleuse.

- Objectifs
  - Faire en sorte qu'il soit plus difficile pour quelqu'un de revendiquer et d'utiliser l'identité de quelqu'un d'autre
- Parties prenantes
  - Bureaux de l'état civil
  - Immigration, Réfugiés et Citoyenneté Canada (IRCC)
  - Agence des services frontaliers du Canada (ASFC) en tant que titulaire d'identifiants uniques
  - Principaux émetteurs d'identité contextuelle
- Exécution : Quatrième et cinquième années – Peut être mis en place une fois que les identités contextuelles sont ancrées dans les identités essentielles

Appel à l'action

Étant donné la portée, la cadence et la complexité de l'économie numérique mondiale, la confiance et la protection contre la fraude et le piratage sont plus importantes que jamais.

Avec de la confiance, il n'y a pas de limite à ce que la population canadienne, les gouvernements et le secteur privé peuvent accomplir pour promouvoir la croissance économique, attirer des investissements, créer des emplois, renforcer la prestation des services et améliorer la mobilisation citoyenne.

En l'absence de confiance, les conséquences pourraient être profondes et durables, et reléguer le Canada au statut d'arrière-pensée numérique mondiale.

Compte tenu de ces enjeux élevés, le CCIAN estime que le Canada doit prêter davantage attention à l'infrastructure nécessaire pour accroître cette confiance.

Ce rapport démontre en conclusion que le système d'identité en silos qui a évolué au Canada au cours des dernières décennies est fracturé et contient de nombreuses failles, incohérences et vulnérabilités, ce qui s'est traduit et continue de se traduire par de grandes inefficacités au niveau de la prestation des services et une importante fraude reliée à l'identité. De plus, ces failles et vulnérabilités sont largement répandues et profondément enracinées, et leurs effets se répercutent sur l'écosystème de l'identité numérique.

Le CCIAN exhorte les gouvernements et le secteur privé à collaborer pour développer une stratégie exhaustive de l'identité nationale qui intègre pleinement les sources d'identité essentielle, et à agir d'une façon mesurée au cours des prochaines années pour restaurer la chaîne de confiance pour l'identité et assurer l'avenir numérique du Canada. Nous sommes prêts à fournir une assistance pour aider le Canada à atteindre cet objectif fondamental.

Annexe 1 – Initiatives supplémentaires

Les initiatives qui suivent ont été discutées brièvement par le GIP, mais n'ont pas été étudiées adéquatement et ne font donc pas partie des recommandations du CCIAN. Elles sont incluses ici par souci d'exhaustivité, mais auraient besoin d'être étudiées davantage.

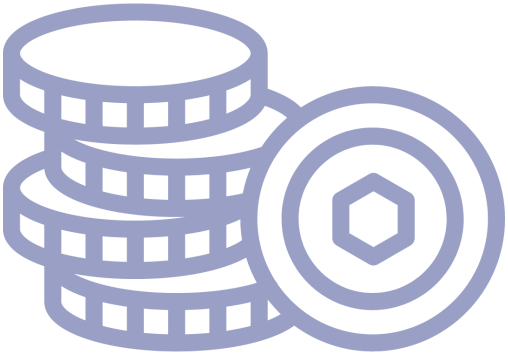
Jetons d'exclusion mutuelle pour l'inscription à des programmes

Certains programmes et permis ont des exigences fixées par la loi qui limitent l'inscription à une administration. En voici des exemples :

- Le permis de conduire est limité à une province ou un territoire
- L'assurance santé provinciale est limitée à une province ou un territoire
- L'Agence du revenu du Canada ne permet à quelqu'un de déclarer uniquement une province ou un territoire de résidence

Les membres du GIP aimeraient explorer la création d'un « jeton d'exclusion mutuelle » ou mécanisme similaire dans un registre de données vérifiables qui ferait en sorte qu'une identité unique (identité essentielle) ne pourrait être inscrite qu'à un programme d'un type donné (p. ex., régime provincial d'assurance santé) au Canada.

Cela protégerait le programme contre la fraude et la personne contre l'usurpation d'identité, car l'utilisation d'une identité unique (identité essentielle) serait relevée dans de multiples administrations. La tâche consisterait à repérer un ou plusieurs mécanismes pour mettre en place le jeton d'exclusion mutuelle dans des technologies actuellement utilisées et à s'attaquer aux problèmes qui pourraient surgir. Un principe de conception essentiel pour un tel mécanisme consisterait à appliquer ces exigences sans recourir à un registre traditionnel qui pourrait être utilisé d'une façon malveillante comme une forme quelconque de surveillance ou être une cible pour une violation de données ou une autre attaque qui compromettrait la vie privée d'une personne.



Relations : L'ADN d'une identité

À l'heure des violations de données et des réseaux sociaux, il y a peu d'éléments d'information permettant d'identifier des personnes qui sont impossibles à découvrir. Les preuves d'identité basées sur les connaissances (comme le « nom de jeune fille de la mère » ou le « nom d'un animal familier ») sont des moyens de vérifier l'identité qui tendent à être moins fiables étant donné la quantité de données qui a été violée ou publiée volontairement sur les réseaux sociaux. Le piratage psychologique de ces « secrets » devient plus facile.

Les personnes développent au cours de leur vie des associations et des relations avec d'autres personnes, endroits et choses. Certaines de ces associations essentielles commencent par l'association avec la mère et le père (qui est saisie dans le dossier de naissance essentiel d'une

personne), les lieux de résidence, les écoles fréquentées, les emplois occupés, les conjoints, les enfants et même les amitiés de longue date. Cet ensemble de relations est comme l'ADN de l'identité d'une personne et pourrait fort bien être testée pour vérifier cette identité.

Les membres du GIP aimeraient explorer l'application des « relations vérifiables » pour maintenir et utiliser cet ADN de l'identité dans le contexte d'une identité (essentielle) unique afin d'établir un haut niveau d'assurance de l'identité.

Annexe 2 – Scénarios de fraude

Cette annexe inclut des scénarios qui mettent en évidence la facilité avec laquelle des identités synthétiques peuvent être produites en utilisant des processus pour prouver l'identité et des documents d'identité établis au Canada. Les mauvais acteurs tirent parti de ces vulnérabilités pour commettre des usurpations d'identité et des fraudes qui peuvent entraîner de sérieuses pertes économiques pour les particuliers, les entreprises et les gouvernements qui acceptent l'identité synthétique, ce qui occasionne un stress et des difficultés considérables pour ceux qui sont touchés.

Nous allons commencer par introduire le principal personnage qui interviendra dans les différents scénarios :

Wally est la cible d'un vol d'identité. Il :

- A 26 ans
- Vit à Vancouver, en Colombie-Britannique, où il est né et a grandi
- A étudié le marketing à l'Université de la Colombie-Britannique et obtenu un baccalauréat en commerce
- Travaille à temps partiel comme garçon de table dans un bar
- A une cote de crédit décente de 620

Le scénario légitime montre les étapes habituelles pour obtenir des documents d'identité. Dans les scénarios illégitimes, nous montrons certaines façons dont les failles entre les silos de l'identité peuvent être exploitées pour voler une identité et créer une identité synthétique, et ensuite perpétrer des crimes financiers.

Scénario 1 : Légitime - Wally change de province

Dans ce scénario, Wally déménage à Toronto, en Ontario, où l'attend un emploi très bien payé avec une entreprise technologique en démarrage. Comme il vit maintenant en Ontario, Wally doit se procurer un permis de conduire ontarien (obligatoire après avoir vécu 60 jours en Ontario) et s'inscrire auprès de l'Assurance-santé de l'Ontario (obligatoire pour obtenir des services de santé gratuits en Ontario). Wally veut aussi ouvrir un nouveau compte dans la succursale locale d'une banque à charte. Il ne fait pas affaire avec cette banque et a été attiré par la promotion de 500 $ offerte aux nouveaux clients qui ouvrent un compte dans l'établissement.

Pour échanger son permis de conduire de la Colombie-Britannique contre un permis de conduire de l'Ontario, Wally va devoir :

- Faire une demande en personne dans un centre d'examen de conduite Test au Volant ou un point de ServiceOntario
- Passer un examen de la vue
- Apporter une pièce d'identité originale acceptée sur laquelle figurent son nom légal, sa date de naissance et sa signature
- Présenter l'original de son permis de conduire délivré par une autre province ou un autre pays
- Apporter les originaux des documents justificatifs attestant son expérience de conduite
- Payer les frais applicables
- Remplir un formulaire de demande dans lequel il indiquera depuis combien d'années il conduit

  Source : Permis de conduire | Échange d'un permis de conduire non délivré par la province de l'Ontario

Scénario 2 : Illégitime – Un fraudeur obtient certains renseignements sur Wally et s'en sert pour obtenir un prêt frauduleux

Fred, un des travailleurs occasionnels embauchés par la compagnie chargée de déménager les possessions de Wally en Ontario, fréquente occasionnellement le bar où Wally travaille à temps partiel et il entame une conversation avec lui pendant sa pause. Ils se mettent à parler du père de Wally qui vient de décéder et Wally lui montre l'avis nécrologique qu'il a récemment publié sur les réseaux sociaux.

De retour chez lui, Fred cherche la page Facebook de Wally, trouve l'avis nécrologique et prend note des renseignements suivants au sujet des parents de Wally :

- Ville et province de naissance
- Nom (de jeune fille de sa mère)
- Prénoms

Fred utilise ces renseignements ainsi que la date de naissance de Wally qu'il a trouvée dans des documents qu'il a manipulés lorsqu'il se trouvait chez Wally pour préparer le déménagement, et il commande deux exemplaires du certificat de naissance de Wally à partir de la page de commande en ligne de BC Vital Statistics. Il commande aussi deux différents permis de conduire de la Colombie-Britannique à partir du Web noir en utilisant des photos de personnes vulnérables en raison de leurs accoutumances et mêlées à des activités criminelles. Fred envoie un des faux permis de conduire et une copie du certificat de naissance à Jay, son complice, qui œuvre à partir de Winnipeg.

Fred utilise sa fausse identité pour ouvrir rapidement un compte bancaire au nom de Wally et demander un prêt de 25 000 $ à Penticton. Il donne à la personne vulnérable 500 $ sur cette

somme et ils se séparent. Fred prend les 24 500 $ qui restent et fait un voyage à Las Vegas où il mène grand train pendant un week-end.

Scénario 3 : Illégitime – Un larcin légèrement plus raffiné

Jay est quant à lui un peu plus raffiné. Il prend le certificat de naissance et le faux permis de conduire et demande un permis de conduire du Manitoba. Jay échange ensuite le faux permis de conduire de la Colombie-Britannique contre un permis de conduire du Manitoba en s'y prenant de la façon suivante :

- Il se rend chez un agent Autopac ou dans un centre de la Société d'assurance publique du Manitoba
- Il apporte les originaux de ses documents d'identité acceptés sur lesquels sont indiqués un nom légal, une date de naissance et une signature. Jay présente :
    - le faux permis de conduire et la fausse carte de services de la Colombie-Britannique
    - le certificat de naissance de la Colombie-Britannique volé
- Il apporte l'original de son permis de conduire délivré à l'extérieur de la province ou dans un autre pays
- Il apporte les originaux de preuves de résidence et présente :
    - un faux contrat de location résidentielle
    - une fausse lettre d'emploi
- Il paie les frais de 65 $

Source : Société d'assurance publique du Manitoba | Permis de conduire | Bienvenue au Manitoba

Jay reçoit son permis de conduire du Manitoba au bout de 45 jours. Avant d'utiliser son identité, il fait un changement de nom légal pour réduire les chances que quelqu'un relie l'identité à son titulaire légitime. Ensuite :

Jay remplit le formulaire de Demande de changement de nom légal et l'envoie par courrier recommandé au bureau de l'état civil, en incluant :

- L'original du certificat de naissance de la Colombie-Britannique qui a été volé
- Une copie du nouveau permis de conduire du Manitoba
- Les frais de 120 $

L'État civil enverra une feuille d'information du Manitoba sur le changement de nom légal et la prise d'empreintes digitales, avec des renseignements supplémentaires et des instructions sur la façon d'effectuer une prise d'empreintes digitales civile pour un changement de nom légal.

Jay signe une dérogation et apporte la feuille d'information du Manitoba sur le changement de nom légal et la prise d'empreintes digitales à une agence autorisée à

prendre des empreintes digitales, qui les soumet à la GRC pour voir si ses empreintes correspondent à d'autres figurant dans le répertoire national des casiers judiciaires.

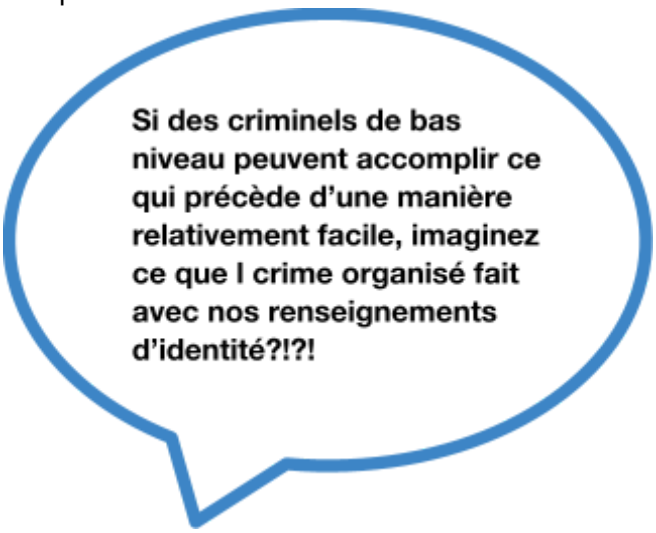
Si une concordance est trouvée dans les casiers judiciaires, le nouveau nom est ajouté à ce casier comme nom supplémentaire pour la personne. Indépendamment de ce résultat, l'État civil du Manitoba traite la demande de changement de nom légal et envoie le certificat de changement de nom par la poste au demandeur dans les 10 jours ouvrables qui suivent la réception de la confirmation de l'agence qui a pris les empreintes digitales.

Source : Changement légal de nom | Bureau de l'état civil du Manitoba | Province du Manitoba

Jay prend le certificat de changement de nom et met à jour son permis de conduire du Manitoba. Il se procure un téléphone cellulaire et ouvre un compte bancaire sous le nouveau nom. Au cours des trois années qui suivent, armé du certificat de naissance, du certificat de changement de nom et d'un permis de conduire mis à jour, Jay ouvre d'autres comptes bancaires et obtient des cartes de crédit supplémentaires, il achète et vend des voitures (il commence avec un vieux bazou, mais passe ensuite à des véhicules de plus en plus coûteux), et vit d'une façon générale sous son nom d'emprunt, tout en payant régulièrement ses comptes de crédit. Il remplit ses comptes bancaires avec les produits de son trafic de drogue, en faisant comme s'il s'agissait d'un revenu d'emploi légitime.

La quatrième année, il utilise son historique de crédit de trois ans et sa cote de crédit de 800 pour :

- Monter le solde de ses cartes de crédit à 125 000 $
- Vendre l'identité synthétique pour 5 000 $ à un immigrant illégal qui a besoin de soins médicaux
- Disparaître pour refaire la même chose dans une autre province et avec une autre identité synthétique



Annexe 3 - Démonstrations

Vidéo	Description	Contributeurs
Démonstration nº 1 : Validation de la partie dépendante	La démonstration n° 1 est un cas pratique traditionnel de validation de document où un sujet demandant un service présenterait un document d'identité à un fournisseur de services du secteur privé ou public pour prouver son identité et recevoir une prestation.	• Valid8ID Solutions • Axiell
Démonstration nº 2 : Émetteur mandataire du certificat de naissance électronique	La démonstration n° 2 est un cas pratique de délivrance de justificatifs vérifiés pour un certificat de naissance où un sujet obtiendrait une version électronique de son certificat de naissance canadien auprès d'un service mandataire central. Le service mandataire valide les renseignements figurant sur le certificat de naissance d'après la base de données appropriée de l'État civil et délivre le justificatif vérifiable correspondant au portefeuille d'identité numérique du sujet.	• Valid8ID Solutions • Interac • Axiell
Démonstration nº 3 : Vérificateur du certificat de naissance-émetteur de la carte santé	Dans la démonstration n° 3, le ministère de la Santé de l'Ontario vérifie un certificat de naissance électronique délivré à l'extérieur de la province sans le lier à son émetteur et délivre un justificatif vérifiable de carte santé au portefeuille du demandeur. Il s'agit d'un exemple d'identité contextuelle basée sur la preuve d'une identité essentielle.	• Valid8ID Solutions • Interac
Démonstration nº 4 : Démonstration de l'émetteur faisant autorité	La démonstration n° 4 montre la délivrance d'un justificatif vérifiable par l'État civil du Manitoba. Elle tire parti des processus de demande en ligne existants pour commander un certificat de naissance électronique comme justificatif vérifiable au portefeuille d'une identité autosouveraine (SSI) vérifiable appartenant à un citoyen né au Manitoba.	• Axiell • Northern Block
Démonstration nº 5 : Vérification de l'âge et de la date de naissance	La démonstration n° 5 porte sur une demande de preuve venant de Law Firm Ottawa, une organisation extérieure (vérificateur) utilisée pour vérifier l'authenticité du justificatif vérifiable présenté.	• Northern Block