CIOSC TS 115:202X (D3)
SPÉCIFICATION TECHNIQUE NATIONALE

Spécification technique nationale pour les justificatifs d'identité et les services de confiance numériques

35.030

AVERTISSEMENT

Le présent document n'est pas une norme officielle du Conseil stratégique des DPI. Il est distribué aux fins d'examen et de commentaires. Il peut être modifié sans préavis et ne constitue pas une spécification technique nationale.

Les destinataires du présent document provisoire sont invités à soumettre tout droit de brevet pertinent dont ils ont connaissance, ainsi que leurs commentaires et des documents à l'appui.

Page laissée intentionnellement vierge

Table des matières

Avant-propos

Le Conseil stratégique des DPI (CSDPI) est un organisme sans but lucratif offrant une tribune nationale aux membres des secteurs public et privé qui s'emploient à transformer, à façonner et à orienter l'écosystème canadien de l'information et de la technologie.

Ses spécifications techniques sont élaborées conformément au document *Élaboration des normes canadiennes – Spécifications techniques nationales* (2 août 2019) du Conseil canadien des normes (CCN).

Il est à noter que certains éléments de la présente spécification technique nationale peuvent faire l'objet de droits de brevet. Le CSDPI ne saurait être tenu responsable de ne pas avoir indiqué ces droits. Ceux relevés lors de l'élaboration de la présente norme figurent dans l'introduction.

Pour en savoir plus sur le CSDPI :

Conseil stratégique des DPI
1000, promenade Innovation, bureau 500
Ottawa (Ontario)
K2K 3E7
ciostrategycouncil.com

Introduction

Voici la première version de la spécification CIOSC TS 115:20XX, Spécification technique nationale pour les justificatifs d'identité et les services de confiance numériques.

Cette spécification a été élaborée par le comité technique du CSDPI sur les justificatifs d'identité numériques, composé de plus de XXXX grands penseurs et experts en gestion de l'identité, en justificatifs d'identité et portefeuilles numériques, et de domaines connexes. Elle a été approuvée par un groupe avec droit de vote formé par le Comité technique comprenant X producteurs, X représentants du secteur public, d'un organisme de réglementation ou d'un organisme responsable des politiques, X utilisateurs et X représentants de la collectivité.

Elle a été produite conformément au document *Élaboration des normes canadiennes – Spécifications techniques nationales* (2 août 2019) du CCN.

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

La spécification sera soumise à l'examen du Comité technique au plus tard un an après sa date de publication, à la suite de quoi elle pourra être rééditée, révisée, confirmée ou abandonnée.

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

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

Nous saluons et remercions le CCN pour sa contribution à l'élaboration de la spécification.

ICS 35.030

Page laissée intentionnellement vierge

Contexte

La présente spécification technique vise à procurer un modèle de programme d'évaluation de la conformité pour les justificatifs d'identité et les services de confiance numériques, soit une méthode d'essai qui fournira des procédures répétables et reproductibles permettant d'obtenir des résultats uniformes dans l'évaluation de produits donnés.

Les justificatifs d'identité numériques sont des ensembles d'affirmations lisibles par machine et vérifiables. Ils peuvent être utilisés pour améliorer l'efficacité du partage de renseignements fiables tout en réduisant ou en éliminant les risques de fraude découlant d'un mésusage ou de modifications. Les justificatifs d'identité numériques peuvent s'appliquer à de nombreuses utilisations internes et externes, comme l'identification sécurisée pour l'accès à des services en ligne, les permis de conduire et passeports, la consultation de données sur la santé, les diplômes d'études et la responsabilité d'actifs.

Une organisation qui émet des justificatifs d'identité numériques peut agir à titre d'émetteur, de détenteur ou de vérificateur.

La présente spécification comprend un petit ensemble de critères d'évaluation de la conformité qui peuvent appuyer les politiques et les objectifs réglementaires du secteur public canadien, composé des gouvernements fédéral, provinciaux, territoriaux et autochtones.

Elle vise à combler les besoins en matière d'évaluation de la conformité dans le but de :

- fournir une structure de marché et des précisions quant aux justificatifs d'identité et aux services de confiance numériques;
- permettre l'interopérabilité, la protection de la vie privée et le renforcement mutuel des justificatifs d'identité et des produits et services de confiance numériques à l'échelle nationale et internationale;
- ouvrir une avenue pour la différenciation des produits et la concurrence entre les développeurs et les fournisseurs;
- renforcer la confiance des consommateurs à l'égard des justificatifs d'identité et des produits et services de confiance numériques;
- permettre à des tiers d'évaluer la sécurité, l'efficacité et le profil éthique des justificatifs d'identité et des produits et services de confiance numériques.
- fournir aux gouvernements du Canada un outil fondé sur des normes qui s'applique aux politiques et à la réglementation.

Elle porte sur les objets d'évaluation de la conformité suivants :

- Composant de l'émetteur
- Composant du détenteur
- Composant du vérificateur
- Composant du registre de confiance numérique

Page laissée intentionnellement vierge

Spécification technique nationale pour les justificatifs d'identité et les services de confiance numériques

1 Portée

La présente spécification technique nationale décrit une méthode d'essai et des critères à respecter pour valider la conformité d'un système relative à la délivrance, à la gestion, au stockage, à la présentation et à la vérification des justificatifs d'identité numériques lisibles par machine.

NOTE: Les exigences spécifiées dans la spécification technique nationale sont à des fins de test et de conformité et ne remplacent ni ne remplacent l'autorité compétente ayant des normes, des politiques et des directives. Ainsi, les exigences sont rédigées de manière à démontrer la conformité. Par comparaison, l'autorité compétente ayant des normes, des politiques et des lignes directrices compétentes peut imposer ou recommander la conformité pour une mise en œuvre particulière.

2 Références normatives

La spécification renvoie au document suivant de telle sorte qu'une partie ou la totalité de son contenu constitue une exigence normative. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, c'est la dernière édition des documents mentionnés qui s'applique (y compris les éventuelles modifications).

CAN/CIOSC 103-1:2020, *Confiance et identité numérique – Partie 1 : Notions fondamentales*

CSA ISO/IEC/IEEE 29119-4:2022, *Ingénierie du logiciel et des systèmes – Essais du logiciel – Partie 4 : Techniques d'essai* (ISO/IEC/IEEE 29119-4:2021, IDT)

EN 301-549, *Harmonized European Standard on Accessibility requirements for ICT products and services*

ISO/IEC 27001 *Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences*

ISO/IEC 27002 *Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information*

ISO/IEC 27017 *Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage*

ISO/IEC 29100, *Technologies de l'information – Techniques de sécurité – Architecture de référence de la protection de la vie privée*

ISO/IEC 27018, *Technologies de l'information – Techniques de sécurité – Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII*

ITSP.40.111, *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B*

W3C *Identifiants décentralisés (DID) v1.0 Recommandations 19 juillet 2022*

3 Termes et définitions

Pour les besoins de la spécification, les termes et définitions des normes CAN/CIOSC 103-1 et CSA ISO/IEC/IEEE 29119-4:2022 (ISO/IEC/IEEE 29119-4:2021, IDT) s'appliquent.

affirmation
Énoncé formulé concernant un sujet.

composant de l'émetteur
Technologie de l'information qui fournit un dossier numérique portable sur un sujet (p. ex. organisation, personne ou produit) et constitue une représentation numérique d'un certificat ou d'un renseignement traditionnellement physique.

composant du détenteur
Technologie de l'information à partir de laquelle une présentation peut être faite à un vérificateur, notamment sous forme de portefeuille numérique contrôlé ou de service de confiance numérique.

composant du stockage
Fondement du stockage sécurisé des données, dont les renseignements personnels, comprenant des modèles de données pour le stockage et le transport, la syntaxe et la protection des données au repos.

composant du vérificateur
Technologie de l'information à partir de laquelle un justificatif d'identité numérique peut être authentifié et validé.

détenteur
Une entité qui contrôle une ou plusieurs informations d'identification à partir desquelles une présentation peut être exprimée à un vérificateur. Un détenteur est généralement, mais pas toujours, le sujet d'un justificatif d'identité.

émetteur
Une entité qui fait valoir une ou plusieurs revendications concernant un ou plusieurs sujets, crée un credential à partir de ces revendications et attribue le credential à un détenteur.

entité
Chose ayant sa propre existence indépendante (personne, organisation, appareil) qui peut être assujettie à des lois, politiques ou règlements dans certains contextes, qui peut avoir des droits, devoirs et obligations, et qui peut remplir un ou plusieurs rôles dans l'écosystème numérique.

format du justificatif
Format utilisé pour décrire l'identifiant de l'émetteur du justificatif, le schéma du justificatif émis, les clés servant à signer les affirmations associées au justificatif et les méthodes de chiffrement appliquées. Les méthodes de révocation sont facultatives.

identifiant décentralisé
Identifiant universel, permanent et unique ne nécessitant aucune autorité d'enregistrement centralisée et qui est souvent généré ou enregistré par chiffrement.

justificatif
Affirmation de l'identité, des qualifications, des compétences, de l'autorité, des droits, des privilèges, des autorisations, de l'état, de l'admissibilité ou de la responsabilité d'actifs (ou d'une combinaison de ceux-ci). Un justificatif comprend un ensemble d'une ou de plusieurs affirmations formulées sur un ou plusieurs sujets.

justificatif d'identité numérique (ou justificatif vérifiable)
Dossier numérique portable sur un sujet (p. ex. organisation, personne ou produit) qui peut être conservé et présenté au moyen d'un portefeuille ou d'un coffre-fort numérique contrôlé par l'utilisateur. Il s'agit de la représentation numérique de certificats ou de renseignements traditionnellement physiques.

justificatif vérifiable
Ensemble de renseignements sécurisés par cryptographie qui est :

a. créé conformément aux normes ouvertes qui respectent les mécanismes de protection existants;
b. présenté au moyen d'un dispositif portable contrôlé par l'utilisateur qui peut être authentifié par les services publics disponibles.

module cryptographique
Ensemble de matériel informatique, de logiciels ou de micrologiciels appliquant des fonctions de sécurité cryptographique (y compris des algorithmes de chiffrement et la génération de clés de chiffrement) et qui est contenu dans le périmètre cryptographique.

protégé B (marqué comme PROTÉGÉ B)
Niveau de sécurité du gouvernement du Canada s'appliquant aux renseignements et aux biens qui

pourraient causer un grave préjudice à une personne, une organisation ou un gouvernement s'ils étaient compromis.

registre de confiance numérique (ou registre des données vérifiables)
Système facilitant la création et la vérification d'identifiants,de clés et de données pertinentes – p. ex. schémas de justificatifs, registres de révocation et clés publiques de l'émetteur – qui peuvent être nécessaires pour utiliser les justificatifs.

service de confiance numérique
Service d'appui aux justificatifs d'identité numériques, p. ex. registre de données vérifiables sous forme de chaînes de blocs, service de délivrance et de vérificateur, ou portefeuille ou coffre-fort numérique.

suject
Une entité à propos de laquelle des réclamations sont revendiquées par un émetteur.

vérificateur
Une entité qui accepte une présentation d'un titulaire dans le but de fournir des services ou d'administrer des programmes.

4 Objets d'évaluation de la conformité

4.1 Conformité

4.1.1 Pour être jugées conformes, les applications doivent être soumises à des techniques fondées sur les spécifications applicables et respecter les exigences de la présente spécification. Les résultats des essais, y compris le plan d'essai pour l'exécution des techniques, doivent être examinés avant la décision finale afin de déterminer si l'objet de la conformité a été démontré de façon fiable. Il faut utiliser une expression normalisée pour indiquer si les exigences d'évaluation de la conformité ont été respectées.

NOTE: Une déclaration de conformité peut comprendre des exigences non respectées.

4.1.2 Les applications doivent être couvertes par la portée et comprendre un ou plusieurs des services suivants :

a. Composant de l'émetteur
b. Composant du détenteur
c. Composant du vérificateur
d. Composant du registre de confiance numérique

4.2 Méthodes d'essai

4.2.1 Les deux techniques d'essai fondées sur les spécifications suivantes doivent être exécutées conformément à la norme ISO/IEC/IEEE 29119-4 de sorte que les scénarios d'essai permettent de générer des preuves pour vérifier le respect des exigences relatives à l'objet de l'essai :

a. Essais par scénarios
b. Essais fondés sur les exigences

NOTE: Lorsqu'il est pertinent de le faire, il est possible de recourir à d'autres techniques d'essai fondées sur les spécifications, les structures ou l'expérience conformes à la norme ISO/IEC/IEEE 29119-4 pour confirmer avec plus de certitude que les exigences de la présente spécification techniques sont respectées.

4.2.2 Les résultats d'essai doivent démontrer la conformité à la spécification ou au standard ouvert connexe décrit à l'article 4.3.1, et respecter les exigences de l'évaluation de la conformité décrites aux articles 4.3, 4.4 et 4.5 et aux articles 9 à 12 qui s'appliquent.

4.3 Modèles de données et formats de fichiers et d'échanges de données

4.3.1 Les modèles de données et les formats de fichiers et d'échanges de données doivent être publiés par un organisme reconnu et peuvent comprendre un ou plusieurs des exemples suivants :

a. Standard ouvert JSON
b. Spécification JSON-LD
c. W3C, Verifiable Credentials Data Model
d. Norme ISO 18013-5

4.4 Essais par scénarios

4.4.1 Le plan pour l'exécution des scénarios d'essai selon le modèle de données et les formats de fichiers et d'échanges de données décrits à l'article 4.3.1 doit être suffisamment détaillé et comprendre les intrants et extrants spécifiques, les conditions d'exécution, les procédures d'essai et les résultats attendus conformément à la présente spécification.

4.4.2 Le service visé doit être soumis à des scénarios d'essai qui illustrent comment le justificatif d'identité numérique se comporte en contexte. Les scénarios doivent comprendre un ou plusieurs des éléments suivants, selon la portée du service :

a. Délivrance et révocation du justificatif
b. Présentation du justificatif
c. Stockage du justificatif

d. Validation et vérification du justificatif
e. Rétablissement du justificatif

4.4.3 Les résultats du scénario de mise à l'essai doivent être consignés dans un rapport d'essai.

4.4.4 Les scénarios d'essai exécutés doivent démontrer ou préserver les caractéristiques générales du justificatif d'identité numérique, conformément à l'article 5 à 8 et aux dispositions des articles 9 à 12 qui s'appliquent.

4.5 Essais fondés sur les exigences

4.5.1 Les critères énoncés à l'article 5 à 8 et dans les articles 9 à 12 qui s'appliquent doivent comprendre le modèle d'essai et un cas connexe couvrant chaque exigence élémentaire, et doivent être exécutés conformément à la norme ISO/IEC/IEEE 29119-4.

5 Justificatifs d'identité numériques

5.1 Exigences

5.1.1 Un justificatif d'identité numérique doit comprendre trois éléments :

a. Métadonnées : Ensemble d'un ou de plusieurs attributs décrivant les propriétés ou les caractéristiques du justificatif;
b. Données utiles : Ensemble d'une ou de plusieurs affirmations formulées sur un ou des sujets;
c. Preuves : Un ou plusieurs mécanismes ou méthodes utilisés pour confirmer que l'émetteur a créé le justificatif et que ce dernier n'a pas été altéré.

5.1.2 Les justificatifs d'identité numériques doivent :

a. comprendre des affirmations sur un ou plusieurs sujets;
b. référer à un événement ou à une activité d'importance;
c. identifier l'émetteur;
d. définir une période de validité;
e. être inviolables et uniques dans une population donnée;
f. être lisibles par machine;
g. g. être révocable

5.1.3 L'auteur d'un justificatif d'identité numérique doit être vérifiable par cryptographie.

5.1.4 Il faut pouvoir prouver que les justificatifs d'identité numériques peuvent être stockés dans au moins deux applications distinctes, et aussi présentés à partir de celles-ci.

5.1.5 Il faut pouvoir prouver que les justificatifs d'identité numériques peuvent être vérifiés par cryptographie dans au moins deux applications distinctes.

5.1.6 Au moins un authentifiant doit être arrimé au justificatif d'identité numérique.

6 Stockage

6.1 Exigences

6.1.1 Toutes les données doivent être protégées pendant les données en transit et les données au repos conformément à la section 7.

NOTER: Une organisation peut envisager d'utiliser la norme CAN/CIOSC 100-1, Gouvernance des données – Partie 1 : Sécurité centrée sur les données, dans le but de protéger les données d'identification numériques et/ou les données au repos des composants de l'émetteur, du détenteur et du vérificateur. , en transit et en cours d'utilisation.

6.1.2 Les données stockées dans un appareil ou sur le nuage doivent être chiffrées conformément à l'article 7 de la présente spécification.

6.1.3 Le système de stockage infonuagique doit être déployé conformément à la norme ISO/IEC 27018 pour protéger les PII, et à la norme ISO/IEC 29100 pour protéger les renseignements personnels.

7 Module cryptographique

7.1 Exigences

7.1.1 Les données doivent être chiffrées à l'aide d'un module cryptographique certifié aux termes du Programme de validation des modules cryptographiques.

7.1.2 Les données doivent être protégées à l'aide de CAN/CIOSC 100-1, Gouvernance des données – Partie 1 : Sécurité centrée sur les données.

7.1.3 Les algorithmes cryptographiques doivent être conformes aux recommandations relatives aux informations protégées B de la publication du CST intitulée Algorithmes cryptographiques pour les informations non classifiées, protégées A et protégées B (ITSP.40.111).

7.1.4 Le module cryptographique doit assurer la prise en charge de la cryptographie à sécurité quantique à l'aide d'algorithmes cryptographiques, de tailles de paramètres cryptographiques, de longueurs de clé et de périodes de chiffrement qui sont configurables et qui peuvent être mis à jour dans les protocoles, les applications et les services pour être cohérents avec les directives de transition à temps pour respecter les dates de transition spécifiées.

8 Identifiant décentralisé

8.1 Exigences

8.1.1 Les identifiants décentralisés doivent être déployés conformément à la recommandation *Decentralized Identifiers (DIDs) v1.0* du W3C.

9 Composant de l'émetteur

9.1 Exigences

9.1.1 Le composant de l'émetteur doit arrimer un justificatif à un enregistrement d'une activité ou d'un événement pertinent.

9.1.2 Le composant de l'émetteur doit arrimer un justificatif à un identifiant décentralisé conformément à l'article 8 de la présente spécification.

9.1.3 Le composant de l'émetteur doit consigner les renseignements sur la délivrance du justificatif, y compris le détenteur.

9.1.4 Le composant de l'émetteur doit identifier l'émetteur dans le justificatif d'identité numérique.

9.1.5 Le composant de l'émetteur doit exiger du détenteur qu'il complète les processus d'arrimage entre justificatif et authentifiant lancés par un administrateur.

NOTE : Par exemple, le détenteur doit fournir un nouveau mot de passe après que l'administrateur ait réinitialisé l'ancien.

9.1.6 Le composant de l'émetteur peut permettre au détenteur de modifier les authentifiants arrimés à un justificatif qui lui est attribué. Dans ce cas, il faut commencer par le scénario d'essai de validation et de vérification du justificatif.

9.1.7 Le composant de l'émetteur doit permettre au personnel autorisé de modifier les affirmations utilisées pour créer un justificatif, et possiblement aussi les authentifiants arrimés à un justificatif.

9.1.8 Le composant de l'émetteur doit consigner la partie qui modifie l'attribut d'un justificatif et la date de modification.

9.1.9 Le composant de l'émetteur doit définir une période de validité pour les justificatifs d'identité numériques.

NOTE : La période de validité définie peut être ouverte, p. ex. dans le cas d'une période sans date d'expiration précise.

9.1.10 Le composant de l'émetteur doit fournir et conserver les justificatifs d'identité numérique conformément aux caractéristiques générales décrites à l'article 5.1 de la présente spécification.

9.1.11 Le composant de l'émetteur doit consigner et conserver tous les événements liés aux justificatifs pour une période prédéfinie.

9.1.12 Le composant de l'émetteur doit fournir les justificatifs d'identité numériques à un détenteur légitime.

9.1.13 Le composant de l'émetteur doit fournir un justificatif d'identité numérique unique au sein d'une population donnée.

9.1.14 Le composant de l'émetteur doit aviser le détenteur de toute modification des renseignements liés au justificatif.

9.1.15 Le composant de l'émetteur doit pouvoir suspendre, révoquer et redélivrer un justificatif délivré à un détenteur.

NOTE : Par exemple, en cas de dépassement de la date d'expiration ou de détection d'activités suspectes.

9.1.16 Le composant de l'émetteur doit être conçu pour produire un justificatif que les systèmes récepteurs peuvent analyser ou vérifier.

NOTE : Il est fortement recommandé que les composants d'émetteur déployés dans un environnement de production soient remis à l'essai conformément à l'article 5 et que leur conformité soit vérifiée aux termes de la présente spécification.

9.1.17 Le composant de l'émetteur doit aviser l'émetteur, réévaluer le justificatif et potentiellement le suspendre lorsque des preuves de modification potentielle des attributs d'identité ou du justificatif sont portées à son attention par une source d'information.

9.1.18 Le composant de l'émetteur doit consigner les renseignements suivants à la suspension du justificatif :

a. la date d'entrée en vigueur de la suspension;
b. le motif de la suspension;
c. la partie à l'origine de la suspension.

9.1.19 Le composant de l'émetteur doit informer le détenteur du changement d'état du justificatif.

9.1.20 Le composant de l'émetteur doit être disponible en français et en anglais, et devrait l'être en d'autres langues (p. ex. langues autochtones).

9.1.21 Le composant de l'émetteur doit être conforme à la norme EN 301-549, *Harmonized European Standard on Accessibility requirements for ICT products and services.*

9.1.22 Le composant de l'émetteur doit veiller à ce que le détenteur et tout vérificateur aient accès aux renseignements sur la suspension.

9.1.23 Le composant de l'émetteur doit aviser l'émetteur qu'il doit réévaluer le justificatif suspendu, selon les politiques et procédures officielles du système, pour déterminer s'il doit être rétabli ou révoqué.

9.1.24 Le composant de l'émetteur doit lancer un processus pour invalider le justificatif, en vue d'une éventuelle révocation, s'il détecte un quelconque signe de corruption des renseignements, du traitement automatisé ou de l'authentifiant.

9.1.25 Le composant de l'émetteur doit pouvoir rétablir le justificatif suspendu.

9.1.26 Le composant de l'émetteur doit permettre au détenteur de demander le rétablissement du justificatif suspendu.

9.1.27 Le composant de l'émetteur doit vérifier l'identité du détenteur avant de procéder au rétablissement.

9.1.28 Le composant de l'émetteur doit consigner les renseignements suivants sur le rétablissement :

a. la date d'entrée en vigueur du rétablissement;

b. la partie à l'origine du rétablissement.

9.1.29 Le composant de l'émetteur doit veiller à ce que le détenteur et tout vérificateur aient accès aux renseignements sur le rétablissement du justificatif.

9.1.30 Le composant de l'émetteur doit pouvoir révoquer le justificatif.

NOTE : Par exemple, en cas de dépassement de la date d'expiration ou de détection d'activités suspectes.

9.1.31 Le composant de l'émetteur doit donner au détenteur la possibilité de révoquer un justificatif qui lui a été délivré.

9.1.32 Le composant de l'émetteur doit consigner les renseignements suivants à la révocation du justificatif :

a. la date d'entrée en vigueur de la révocation;
b. le motif de la révocation;
c. la partie à l'origine de la révocation.

9.1.33 Le composant de l'émetteur doit informer le détenteur du changement d'état du justificatif.

9.1.34 Le composant de l'émetteur doit veiller à ce que le détenteur et tout vérificateur aient accès aux renseignements sur la révocation du justificatif.

9.1.35 Le composant de l'émetteur doit être conçu pour créer ou modifier des affirmations sur un ou des sujets découlant de ses processus de rapprochement d'identificateurs, de vérification de l'identité, de détermination de preuve d'identité et de confirmation de la continuité de l'identité, conformément à la norme CAN/CIOSC 103-1.

9.1.36 Le composant de l'émetteur doit faire en sorte que les renseignements sur l'émission des justificatifs, y compris les renseignements sur le détenteur, sont stockés conformément à l'article 6 de la présente spécification.

9.1.37 Le composant de l'émetteur doit chiffrer les données liées aux justificatifs ainsi que toutes autres données sensibles, y compris les informations personnelles identifiables (PII) et les renseignements personnels, lorsqu'elles sont communiquées au composant du détenteur, conformément à l'article 7 de la présente spécification.

9.1.38 Si le composant de l'émetteur a recours à un registre de confiance numérique pour émettre et vérifier les justificatifs, ce dernier doit être déployé conformément à l'article 12 de la présente spécification.

10 Composant du détenteur

10.1 Exigences

10.1.1 Le composant du détenteur doit détecter les signes de mésusage ou de compromission des renseignements sur l'identité.

NOTE : Par exemple, en cas de dépassement de la date d'expiration ou de détection d'activités suspectes.

10.1.2 Le composant du détenteur doit utiliser des mots de passe ou des systèmes d'authentification biométriques pour prévenir les accès non autorisés.

a. Le composant du détenteur devrait encourager l'utilisation de mots de passe conformes aux Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032).
b. Le composant du détenteur doit limiter le nombre de tentatives d'authentification infructueuses sans conséquence (p. ex. suspension de l'accès au composant du détenteur ou suppression de son contenu).
c. Le composant du détenteur doit exiger une nouvelle authentification après une période d'inactivité déterminée par le détenteur.
d. Le composant du détenteur peut permettre d'autoriser, de suspendre ou de rétablir l'accès au composant à distance.

10.1.3 Le composant du détenteur doit pouvoir demander un justificatif à un émetteur.

a. La demande de justificatif doit permettre de lier le détenteur et le sujet, permettant ainsi au composant du détenteur de générer des identifiants constituant une preuve de contrôle de l'identifiant.

NOTE : Par exemple, des paires d'identifiants décentralisés ou d'autres types d'identifiants décentralisés, et d'autres méthodes permettant de générer un identifiant URI qui peut servir de sujet pour un justificatif vérifiable ou de détenteur pour une présentation vérifiable.

10.1.4 Le composant du détenteur peut générer des preuves de contrôle des identifiants.

10.1.5 Le composant du détenteur doit pouvoir demander un justificatif à un émetteur en réponse à une action du détenteur.

10.1.6 Le composant du détenteur peut demander un justificatif au moyen d'un modèle d'adhésion dans le cadre duquel les justificatifs d'identité numérique associés à un ou plusieurs émetteurs sont demandés, reçus et conservés, de sorte que le composant du détenteur ait à sa disposition une liste à jour des justificatifs de ces émetteurs.

10.1.7 Le composant du détenteur doit pouvoir recevoir les justificatifs d'un émetteur.

10.1.8 Le composant du détenteur doit pouvoir refuser les justificatifs d'un émetteur.

10.1.9 Le composant du détenteur doit pouvoir conserver les justificatifs dans leur format de chiffrement natif afin de pouvoir générer l'enregistrement original et intact en entier.

10.1.10 Le composant du détenteur doit stocker les justificatifs avec suffisamment de métadonnées pour exécuter les fonctions minimales décrites à l'article 6.1 de la présente spécification.

10.1.11 Le composant du détenteur peut être en mesure d'extraire les données utiles, mais n'est pas tenu de le faire.

10.1.12 Le composant du détenteur doit pouvoir retirer un justificatif et cesser de le conserver à la demande du détenteur.

10.1.13 Le composant du détenteur doit assigner le contrôle d'un justificatif délivré au détenteur de sorte qu'il puisse être vérifié ultérieurement.

10.1.14 Le composant du détenteur doit disposer d'un mécanisme de création et de soumission d'une présentation vérifiable pour une partie utilisatrice en réponse à :

a. une action du détenteur;
b. une demande de présentation vérifiable du vérificateur, si elle est approuvée par le détenteur.

10.1.15 Le composant du détenteur peut disposer d'un mécanisme de réception et de traitement des demandes de présentation.

10.1.16 Le composant du détenteur doit pouvoir gérer les connexions (émetteurs, parties requérantes et autres parties) conformément aux exigences de la section 7.

10.1.17 Le composant du détenteur être conforme à la norme EN 301-549, *Harmonized European Standard on Accessibility requirements for ICT products and services*.

10.1.18 Le composant du détenteur doit pouvoir permettre au détenteur de gérer les paramètres de confidentialité et de partage.

10.1.19 Le composant du détenteur doit pouvoir permettre à l'utilisateur de contrôler le partage des données liées aux justificatifs en tout, en partie ou par dérivation.

10.1.20 Le composant du détenteur doit veiller à obtenir le consentement du détenteur avant de partager les données liées aux justificatifs ou d'accepter, de refuser ou de retirer des justificatifs.

10.1.21 Le composant du détenteur doit signaler au détenteur toute modification des justificatifs.

10.1.22 Le composant du détenteur doit conserver les justificatifs d'identité numériques conformément aux caractéristiques générales décrites à l'article 5.1 de la présente spécification.

10.1.23 Le composant du détenteur doit être disponible en français et en anglais, et devrait l'être en d'autres langues (p. ex. langues autochtones).

10.1.24 Le composant du détenteur doit stocker les justificatifs conformément à l'article 6 de la présente spécification.

10.1.25 Le composant du détenteur doit crypter toutes les données lorsqu'elles sont partagées avec le Composant Emetteur ou le Composant Vérificateur, conformément à la Section 7 de la présente Spécification.

11 Composant du vérificateur

11.1 Exigences

11.1.1 Le composant du vérificateur doit s'assurer, à l'aide de méthodes acceptables, que le justificatif n'a pas été altéré, corrompu ni modifié.

NOTE : Par exemple, les méthodes cryptographiques ou l'examen par un examinateur qualifié sont des méthodes acceptables.

11.1.2 Le composant du vérificateur peut résoudre les justificatifs avec un identifiant décentralisé, conformément à l'article 8 de la présente spécification.

11.1.3 Le composant du vérificateur ne doit pas utiliser un justificatif suspendu ou révoqué pour accorder l'accès à un bien ou à un service.

11.1.4 Le composant du vérificateur doit s'assurer que le détenteur a le contrôle sur le justificatif au moyen d'un ou de plusieurs authentifiants.

11.1.5 Le composant du vérificateur doit aviser le détenteur lorsque ce dernier démontre qu'il a le contrôle du justificatif au moyen d'un ou de plusieurs authentifiants.

11.1.6 Le composant du vérificateur doit aviser le détenteur des échecs d'authentification : justificatif suspendu ou révoqué, ou détection de mésusage ou de compromission du justificatif.

11.1.7 Le composant du vérificateur doit être disponible en français et en anglais, et devrait l'être en d'autres langues (p. ex. langues autochtones).

11.1.8 Le composant du vérificateur doit être conforme à la norme EN 301-549, Harmonized European Standard on Accessibility requirements for ICT products and services.

11.1.9 Le composant du vérificateur doit conserver les justificatifs d'identité numériques conformément aux caractéristiques décrites à l'article 5.1 de la présente spécification.

11.1.10 Le composant du vérificateur doit chiffrer les données liées aux justificatifs ainsi que toutes autres données sensibles, y compris les PII et les renseignements personnels, lorsqu'elles sont communiquées au composant du détenteur, conformément à l'article 7 de la présente spécification.

11.1.11 Si le composant du vérificateur a recours à un registre de confiance numérique pour vérifier les justificatifs, ce dernier doit être déployé conformément à l'article 12 de la présente spécification.

11.1.12 Le composant vérificateur peut informer l'émetteur lorsqu'il résout un identifiant numérique qui est suspendu, révoqué ou lorsqu'une mauvaise utilisation ou compromission d'un identifiant numérique est détectée.

12 Registre de confiance numérique

12.1 Exigences

12.1.1 Le registre de confiance numérique doit stocker des clés et d'autres données pertinentes requises pour l'émission et la vérification des justificatifs.

12.1.2 Le registre de confiance numérique doit disposer de contrôles d'authentification et d'accès pour prévenir les accès non autorisés et la compromission ou la destruction des données.

12.1.3 Le registre de confiance numérique doit fournir des assurances cryptographiques pour confirmer que les clés et les autres données pertinentes qu'il contient sont complètes et n'ont pas été modifiées.

Annexe A : Survol des justificatifs

(annexe informative)

Qu'est-ce qu'un justificatif?

La confiance est au cœur de toute transaction : elle permet de confirmer que toute affirmation d'une entité engagée dans une transaction peut être considérée comme véridique. Par exemple, une entité pourrait devoir confirmer l'identité d'une autre entité avec laquelle elle transige pour s'assurer que cette dernière peut réaliser certaines activités ou qu'elle possède un actif donné.

Au fil du temps, de nombreux types de justificatifs ont été créés et délivrés pour combler les lacunes relatives à la confiance entre les entités. Ces justificatifs donnent réponse à certaines questions, p. ex. « Cette personne peut-elle conduire une voiture en Ontario? »; « Cette personne est-elle admissible aux prestations d'assurance-emploi? »; « Cette entreprise est-elle autorisée à couper du bois en Colombie-Britannique? »; ou « Cette entreprise est-elle admissible à un prêt pour petites entreprises? »

Dans son sens le plus général, un justificatif est une affirmation de l'identité, des qualifications, des compétences, de l'autorité, des droits, des privilèges, des autorisations, de l'état, de l'admissibilité ou de la responsabilité d'actifs (ou d'une combinaison de ceux-ci). Plus précisément, un justificatif comprend un ensemble d'une ou de plusieurs affirmations formulées sur un ou plusieurs sujets. Le justificatif est délivré par une entité, l'« émetteur », pour une autre entité, le « détenteur ». L'émetteur possède l'autorité de droit pour délivrer les justificatifs ou, par voie d'ententes et de consensus, se voit accorder l'autorité de fait pour les délivrer.

Les justificatifs comprennent deux types d'information de base : le premier correspond à l'information sur le justificatif lui-même exprimée par un ensemble d'attributs :

- Type de justificatif;
- Identité de l'émetteur du justificatif;
- Date d'émission du justificatif;
- Toute restriction relative au justificatif (p. ex. date d'expiration ou conditions d'utilisation);
- État du justificatif (actif, suspendu ou révoqué).

Le deuxième type correspond à un ensemble d'attributs décrivant les propriétés ou les caractéristiques des entités qui sont les sujets du justificatif : il s'agit d'une sélection d'attributs d'identité ainsi que d'autres attributs des sujets, p. ex. langue de préférence, adresse de résidence et actifs totaux. Si un justificatif indique qu'il existe une relation entre les sujets, il comprendra aussi des attributs de relation. Tous ces attributs servent à formuler une ou plusieurs affirmations concernant un ou plusieurs sujets.

Types de justificatifs

Voici une liste non exhaustive comprenant de nombreux types de justificatifs existants ainsi que des exemples de documents connexes :

- Citoyenneté et résidence légale (p. ex. certificat de naissance, de citoyenneté ou de résidence permanente, passeport)
- Adhésion aux services (p. ex. carte d'assurance-maladie provinciale ou territoriale, carte d'assurance-maladie privée, carte d'assurance soins dentaires privés, carte d'assurance voyage privée, carte de programme de fidélisation et de récompenses, carte de membre de groupe ou de club)
- Permis d'exploitant (p. ex. permis de conduire automobile, permis de conducteur d'équipement lourd)
- Entreprise (p. ex. licence, permis, certificat d'inspection)
- Services financiers (carte de débit ou de crédit)
- Responsabilité d'actifs (p. ex. immatriculation de véhicule automobile, acte de propriété, preuve d'assurance automobile)
- Santé (p. ex. « passeport vaccinal », certificat de vaccination)
- Éducation (p. ex. diplôme, grade, certificat, certification, relevé de notes)
- Emploi (p. ex. lettre d'emploi)
- Adhésion à une association commerciale ou professionnelle (p. ex. carte de membre d'un syndicat d'électriciens)
- Diplomatie (p. ex. lettre de présentation d'ambassade)
- Journalisme (p. ex. carte de presse)
- Habilitation de sécurité (p. ex. carte d'accès à un bâtiment ou à une zone sécurisée)
- Accès à un système (p. ex. combinaison d'un nom d'utilisateur et d'un mot de passe)

Modèle de justificatif

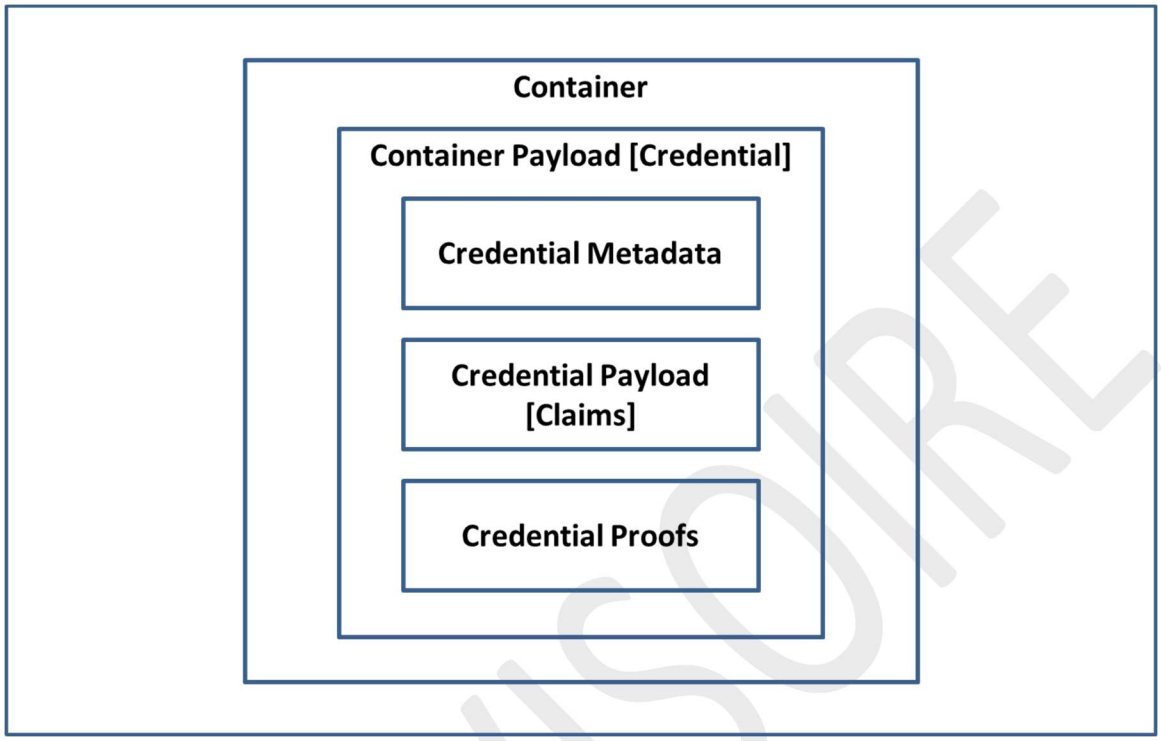

Figure 1 : Modèle de justificatif

Dans ce modèle, le justificatif comporte trois éléments

- **Métadonnées :** Ensemble d'un ou de plusieurs attributs décrivant les propriétés ou les caractéristiques du justificatif;
- **Données utiles :** Ensemble d'une ou de plusieurs affirmations formulées sur un ou des sujets;
- **Preuves :** Un ou plusieurs mécanismes ou méthodes utilisés pour confirmer que l'émetteur a créé le justificatif, que ce dernier n'a pas été altéré, et qu'il est lié à un détenteur.

Il est à noter que si un vérificateur peut vérifier l'auteur d'un justificatif et détecter les signes d'altération, il ne peut pas vérifier la véracité des données utiles (autrement dit, il est impossible de vérifier l'exactitude d'une affirmation, p. ex. « le ciel est vert »). En acceptant un justificatif, il déclare essentiellement juger que l'émetteur du justificatif a adéquatement vérifié la véracité des affirmations avant de créer les données utiles.

Le détenteur reçoit généralement des documents prouvant qu'il possède le justificatif concerné. Ces preuves ont longtemps pris la forme de documents papier ou de cartes de plastique. Graduellement, les mécanismes d'authentification (dont les mécanismes d'authentification électronique) ont été intégrés aux cartes de plastique. De plus en plus, les justificatifs sont délivrés sous forme électronique. On peut voir les documents de preuve de justificatif comme des *contenants* ou des supports pour le transport des justificatifs : ces derniers sont placés dans le contenant et deviennent donc des *données utiles*.

Modèles de déclaration d'affirmation

Modèle de déclaration d'affirmation sur un sujet

L'affirmation sur un sujet consiste en une déclaration concernant un sujet donné. Elle s'exprime par un ou plusieurs attributs d'entité. La figure 2 illustre le modèle de déclaration d'affirmation sur un sujet.

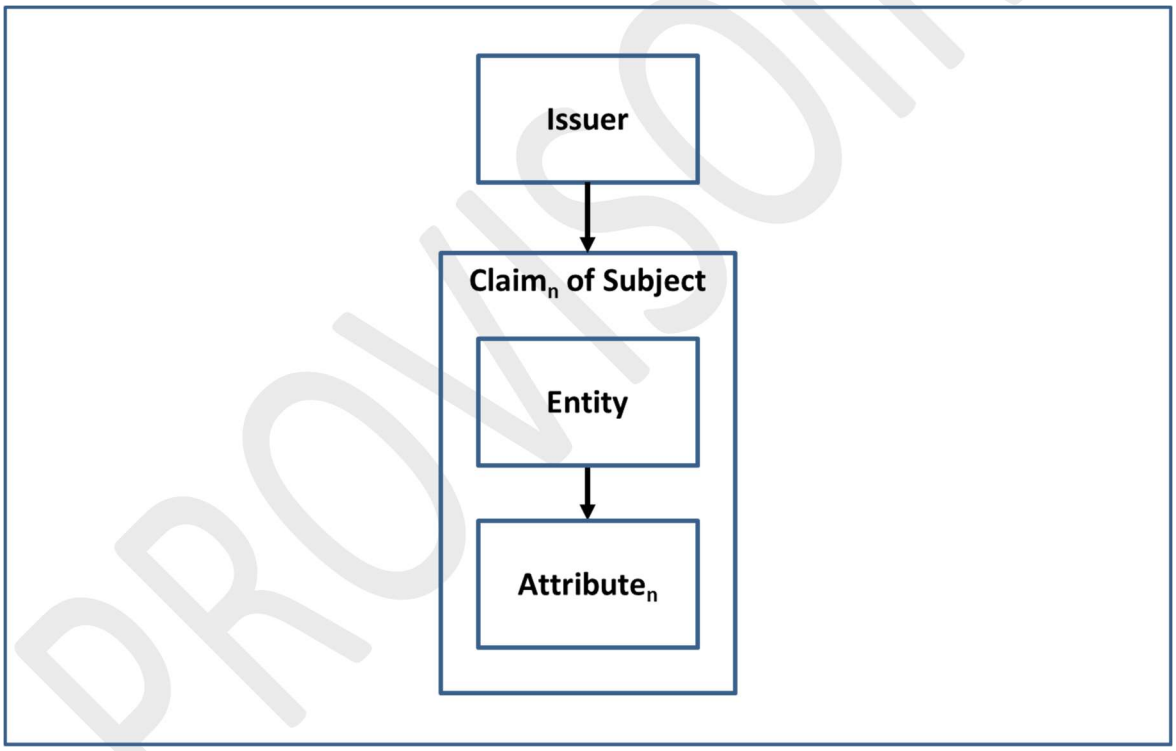

Figure 2 : Modèle de déclaration d'affirmation sur un sujet

Modèle de déclaration d'affirmation de relation

L'affirmation de relation consiste en une déclaration concernant l'association entre au moins deux sujets. Elle s'exprime par un ou plusieurs attributs de relation. La figure 3 illustre le modèle de déclaration d'affirmation de relation.

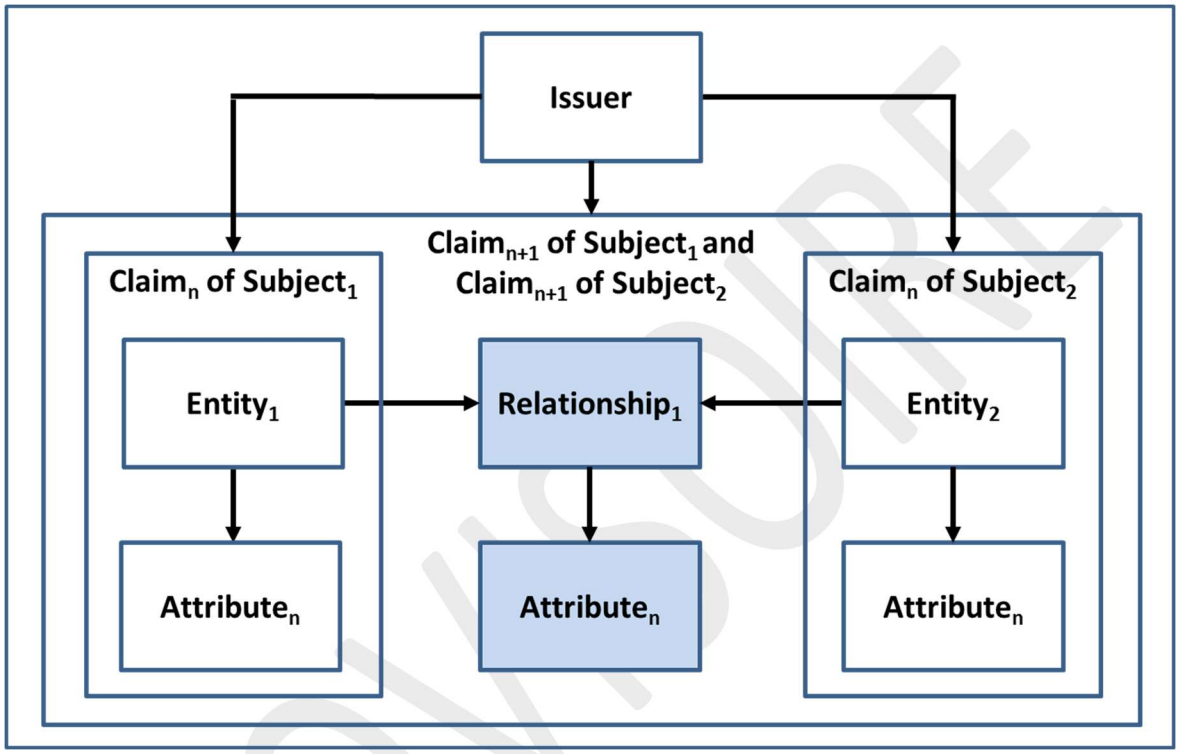

Figure 3 : Modèle de déclaration d'affirmation de relation

Modèle de délivrance de justificatif

Un émetteur fait une ou plusieurs affirmations concernant un ou plusieurs sujets, établit un justificatif à partir de ces affirmations, et attribue le justificatif à un détenteur. La figure 4 illustre le modèle de délivrance de justificatif.

NOTE : Certains déploiements de processus de délivrance d'un justificatif peuvent comprendre d'autres étapes et résultats. La définition ci-dessus indique les conditions minimales nécessaires pour assurer la conformité à la spécification, mais pas nécessairement suffisantes pour atteindre les objectifs d'un système de gestion des justificatifs d'identité numériques donné.

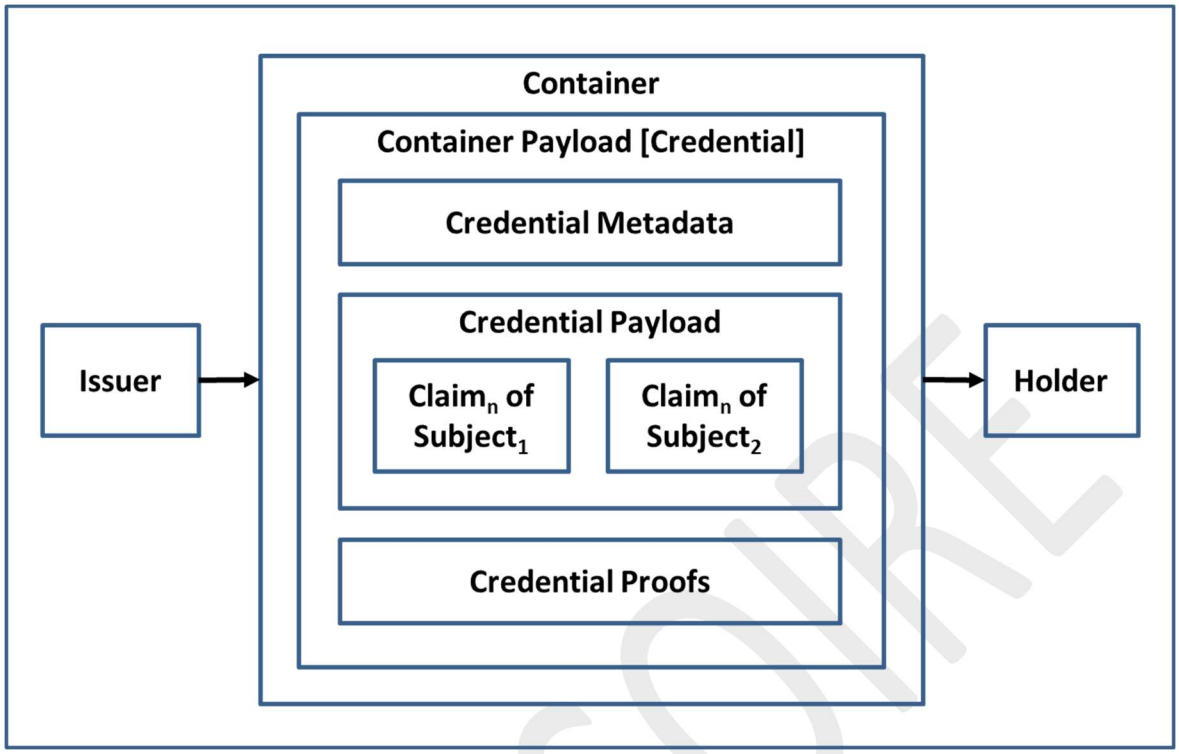

Figure 4 : Modèle de délivrance de justificatif

Annexe B : Renseignements détaillés sur la vérification des justificatifs

(annexe informative)

La vérification des justificatifs est le processus visant à vérifier si un détenteur a le contrôle d'un justificatif délivré. Le contrôle exercé sur un justificatif délivré est vérifié au moyen d'un ou de plusieurs authentifiants. Le degré de contrôle exercé sur le justificatif peut alors servir de base pour établir le niveau d'assurance.

Le processus de vérification des justificatifs dépend du processus d'arrimage entre justificatif et authentifiant (qui consiste à arrimer un justificatif délivré à un détenteur avec un ou plusieurs authentifiants). Le processus d'arrimage entre justificatif et authentifiant comprend aussi les activités liées au cycle de vie des authentifiants : suspension (en raison de l'oubli du mot de passe ou du verrouillage du compte pour cause d'inactivité, d'activité suspecte ou d'échecs successifs de vérification des justificatifs); retrait; arrimage (de nouveaux authentifiants); et mise à jour (changement du mot de passe, modification des questions de sécurité, changement de la photo du visage, etc.).

Authentifiants

Un authentifiant est un élément contrôlé par le détenteur et servant à prouver que ce dernier a encore le contrôle d'un justificatif délivré. Il existe trois types d'authentifiants :

- Élément que le détenteur possède (p. ex. clé de chiffrement, mot de passe à usage unique);
- Élément que le détenteur connaît (p. ex. mot de passe, réponse à une question d'authentification);
- Caractéristique ou action du détenteur (p. ex. visage, empreintes digitales, rétines, rythme de frappe au clavier, démarche).

Les authentifiants arrimés à un justificatif sont ensuite utilisés afin de prouver, pour un niveau d'assurance donné, que le justificatif renvoie au détenteur qui lui a été initialement arrimé.

Il faut noter qu'étant donné l'irrévocabilité des caractéristiques biologiques (p. ex. visage, empreintes digitales, rétines), les normes de l'industrie sont habituellement prudentes en ce qui a trait à l'utilisation de ces caractéristiques comme unique justificatif. Une caractéristique biologique n'est pas une information secrète qui peut être changée facilement ou périodiquement. De plus, les caractéristiques biologiques d'un détenteur peuvent être répliquées. Par exemple, une entité malveillante pourrait obtenir une copie des empreintes digitales du détenteur, les reproduire et réussir la vérification du justificatif (si le processus de vérification ne comprend pas de solides techniques de détection du caractère vivant pour contrer de telles attaques).

Cependant, une caractéristique biologique peut être utilisée pour accéder à un authentifiant stocké dans un dispositif local pour faciliter la vérification à distance du justificatif avec un service, p. ex. en utilisant un logiciel de reconnaissance faciale pour accéder à un mot de passe à usage unique sur un appareil mobile ou à d'autres authentifiants générés ou stockés sur place.

Bibliographie

[1] Trusted Digital Identity Framework, Australie.

[2] BSI PAS 499:2019, Code of practice for digital identification and strong customer authentication.

[3] CASCO, La boîte à outils de l'évaluation de la conformité.

[4] CAN/CIOSC 103-1:2020, Confiance et identité numérique – Partie 1 : Notions fondamentales.

[5] Digital Credentials Consortium.

[6] Union européenne, Règlement n° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

[7] Gouvernement du Canada, Justificatifs numériques.

[8] GPG 43, Requirements for Secure Delivery of Online Public Services.

[9] GPG 44, Authentication Credentials in Support of HMG Online Services.

[10] GPG 45, Identity Proofing and Verification of an Individual.

[11] GPG 53, Transaction Monitoring for HMG Online Service Providers.

[12] OACI, MRTD, série de documents Doc 9303, Documents de voyage lisibles à la machine.

[13] ISO 18013-5, Identification de personnes – Permis de conduire conforme à l'ISO – Partie 5 : Application permis de conduire sur téléphone mobile.

[14] ISO/IEC 24760-1:2019, Sécurité IT et confidentialité – Cadre pour la gestion de l'identité – Partie 1 : Terminologie et concepts.

[15] ISO/IEC 24760-2:2015, Technologies de l'information – Techniques de sécurité – Cadre pour la gestion de l'identité – Partie 2 : Architecture de référence et exigences.

[16] ISO/IEC 24760-3:2016, Technologies de l'information – Techniques de sécurité – Cadre pour la gestion de l'identité – Partie 3 : Mise en œuvre.

[17] ISO/IEC 27018, Technologies de l'information – Techniques de sécurité – Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII.

[18] ISO/IEC 29100, Technologies de l'information – Techniques de sécurité – Architecture de référence de la protection de la vie privée.

[19] ISO/IEC 29115:2013, Technologies de l'information – Techniques de sécurité – Cadre d'assurance de l'authentification d'entité.

[20] ITSP.30.031, Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information.

[21] ITSAP.30.032, Pratiques exemplaires de création de phrases de passe et de mots de passe

[22] Gouvernement de la Nouvelle-Zélande, Digital Identity New Zealand

i. Evidence of Identity Standard
ii. Authentication Standards
iii. Identification Management.

[23] NIST, Digital Identity Guidelines, Special Publication 800-63.

[24] Gouvernement de l'Ontario, L'identité numérique : technologie et normes.

[25] OpenID Connect, Spécifications.

[26] OpenWallet Foundation.

[27] Le profil du secteur public du Cadre de confiance pancanadien, version 1.4, cahier d'évaluation, Ébauche aux fins de consultation 0.1, 2021-12.

[28] Le profil du secteur public du Cadre de confiance pancanadien, version 1.4, aperçu consolidé, Ébauche aux fins de consultation 0.1, 2021-12.

[29] Secrétariat du Conseil du Trésor du Canada, Directive sur la gestion de l'identité, 2019.

[30] Secrétariat du Conseil du Trésor du Canada, Ligne directrice sur la définition des exigences en matière d'authentification, 2012.

[31] Secrétariat du Conseil du Trésor du Canada, Ligne directrice sur l'assurance de l'identité, 2016.

[32] Verifiable Credentials Explained.

[33] W3C, Verifiable Credentials Data Model 1.0.

[34] W3C, Verifiable Credentials Implementation Guidelines 1.0.

[35] W3C, Verifiable Credentials Use Cases.

[36] World Bank, Singapore's National Digital Identity and Governance Data Sharing.