NON CLASSIFIÉ

Gouvernement du Canada

Cadre de référence pour la Gestion de l'identité et des justificatifs d'accès du gouvernement du Canada (GIJA du GC)

VERSION 1.1

Le 28 janvier 2022

GCdocs n° 51822376

Historique des révisions

Numéro de version du document	Modifications	Date
0.1	Première ébauche aux fins de discussion préparée par le Bureau de la dirigeante principale de l'information (BDPI) du Secrétariat du Conseil du Trésor du Canada (SCT), Cybersécurité.	28 septembre 2021
1.0	Modification pour tenir compte des commentaires découlant de l'examen par les pairs et intégration d'autres améliorations.	6 janvier 2022
1.1	Inclusion des modifications supplémentaires en fonction de la rétroaction de suivi.	28 janvier 2022

Avertissement

Toute référence à des fournisseurs ou à des produits de fournisseurs, implicite ou autre, est présentée strictement à des fins d'illustration et ne doit pas être considérée comme une approbation par le gouvernement du Canada.

Table des matières

Liste des images

1. Introduction

1.1 Contexte

La Gestion de l'identité et des justificatifs en matière d'accès (GIJA) est essentielle à la vaste majorité des transactions et des interactions qui se produisent à l'appui des opérations internes et externes du gouvernement du Canada (GC). Elle constitue le fondement de la confiance entre les parties qui échangent des renseignements ou qui permettent l'accès aux ressources protégées. Il s'agit d'un outil essentiel de sécurité et de protection de la vie privée et, dans le domaine électronique, de transactions qui peuvent être beaucoup plus efficaces et efficientes que les méthodes héritées qu'elles remplacent. Les processus opérationnels du gouvernement doivent continuer d'évoluer pour tirer parti des avantages offerts par les nouvelles technologies et remplacer les méthodes obsolètes et coûteuses héritées[1].

La portée de la GIJA est vaste et touche de nombreux aspects des activités du gouvernement. Compte tenu de la nature horizontale de la GIJA, les bonnes pratiques dans son application doivent être omniprésentes et constamment appliquées pour être efficaces. Les pratiques internes existantes du GC en matière de GIJA sont fortement fragmentées en vase clos, tant aux limites ministérielles qu'aux limites des services et des applications, avec une interopérabilité limitée entre ces limites. En résumé, de nombreux fournisseurs de services au sein du GC ont assumé la responsabilité et le coût de la prestation de ces services à leur groupe de travailleurs internes du GC, ce qui fait que les utilisateurs ont beaucoup trop de justificatifs d'identité à gérer, ce qui a une incidence sur leur efficience, et les propriétaires de systèmes supportent le fardeau de l'exploitation de leurs propres systèmes de GIJA qui, lorsqu'ils sont regroupés dans le GC, entraînent une augmentation des coûts et une réduction de la sécurité.

Le GC s'est engagé à améliorer ses services en offrant une expérience de transparence et de convivialité accrues, tout en protégeant la vie privée et en améliorant la sécurité. Un système de GIJA GC fiable est un élément clé de la protection de la vie privée et de la sécurité sans heurts et sans faille des systèmes numériques, car il fournira les bases d'un contrôle et d'une responsabilisation renforcés en matière d'accès, de l'intégrité et de la confidentialité des données et des services, tout en respectant les droits des utilisateurs conformément aux lois canadiennes sur la protection des renseignements personnels. L'objectif est de réaliser des économies et des gains en efficience pour le GC, de protéger les droits des utilisateurs, d'habiliter les employés du GC et d'améliorer l'intégrité globale des services et des capacités.

Pour que le GC puisse pleinement exploiter le potentiel de l'identité numérique, il doit s'harmoniser avec un ensemble général de principes qui sont indépendants de la technologie et qui permettent d'avoir un écosystème rentable, évolutif, fiable, solide et axé sur l'utilisateur. Le GC a également la responsabilité de respecter les instruments de politique applicables, comme la Politique sur la sécurité du gouvernement [1] et la Politique sur les services et le numérique [2] et leurs directives, normes et lignes directrices connexes. Selon la *Directive sur la gestion de l'identité*, [3] le GC doit :

[1] Il est reconnu que le GC continuera d'offrir des services par d'autres moyens comme le téléphone ou en personne.

- gérer l'identité de façon à atténuer les risques pour la sécurité personnelle, organisationnelle et nationale, à protéger l'intégrité des programmes et à permettre une prestation de services bien gérés et axés sur le client;
- gérer les risques relatifs à l'identité de façon uniforme et collaborative à l'échelle du gouvernement du Canada et au sein d'autres compétences et secteurs de l'industrie lorsque la validation de l'identité des employés, des organisations, des appareils et des personnes est nécessaire;
- gérer de façon efficace les justificatifs, authentifier les utilisateurs ou accepter des identités numériques dignes de confiance pour les besoins de l'administration d'un programme ou de la prestation d'un service interne ou externe.

Pour atteindre ces objectifs, il faut disposer d'un système de GIJA GC exhaustif à l'échelle organisationnelle, basé sur le cadre décrit dans le présent document.

1.2 Objectif

Le présent document a pour but de présenter les éléments clés du cadre de GIJA du GC qui peuvent être utilisés de la manière suivante :

- un guide pour la mise en place d'un programme pangouvernemental de GIJA au sein du GC;
- un outil pour créer une feuille de route pour la mise en œuvre des services;
- une base pour l'élaboration d'architectures de solution de GIJA plus détaillées;
- un outil pour aider les organes directeurs à évaluer les initiatives en quête d'approbation;
- un outil pour décrire les initiatives existantes afin d'identifier les lacunes, les redondances et les initiatives qui se chevauchent;
- une référence pour s'harmoniser avec la vision du GC de la gestion des composantes de la GIJA.

Il convient de noter que ce cadre a été fortement influencé par le programme de la Federal Identity, Credential and Access Management (FICAM) des États-Unis [4], mais il a été élargi et contextualisé pour le GC. De plus, le manuel de la FICAM des États-Unis est décrit à l'aide d'une architecture axée sur les services, tandis que le cadre de la GIJA GC est surtout en harmonie avec une approche basée sur des composantes.

1.3 Public cible

Le public cible de ce document comprend, sans s'y limiter, le Conseil d'examen de l'architecture intégrée du GC (CEAI), les comités d'examen de l'architecture ministérielle, les architectes, les praticiens de la sécurité et d'autres qui pratiquent la GIJA au sein du GC ou qui s'y intéressent.

1.4 Portée

Le présent document est destiné à décrire les concepts, les processus et les technologies d'un point de vue de haut niveau qui peut servir de base au développement d'architectures de solutions détaillées. Le cadre s'applique aux systèmes en ligne internes et externes et aux services appuyés par le

gouvernement fédéral, soit les systèmes qui interagissent avec le public, ainsi que les systèmes qui mettent en œuvre des processus internes du gouvernement. Les services qui sont fournis par d'autres moyens (p. ex., par téléphone ou en personne) ne sont pas visés.

Bien que bon nombre des concepts présentés dans le présent document puissent s'appliquer à d'autres domaines, la portée de ce document se limite aux environnements non classifiés, protégé A et protégé B.

2. Contexte

2.1 Aperçu

La GIJA GC comprend les politiques, les procédures, le personnel et la technologie afin de veiller à ce que l'accès aux ressources protégées ne soit fourni qu'aux entités autorisées et que l'étendue de cet accès soit limitée aux fonctions nécessaires à l'exécution des responsabilités de ces entités. Comme le définit Gartner, la GIJA[2] est la discipline qui permet aux bonnes personnes d'accéder aux bonnes ressources au bon moment pour les bonnes raisons. [5] Dans le cadre de la GIJA GC, cela s'applique non seulement aux particuliers, mais aussi aux appareils, aux applications, aux entreprises et aux autres consommateurs de ressources.

Pour atteindre les résultats ci-dessus, le cadre de la GIJA GC donne une vue non préférentielle de la technologie et des fournisseurs des différentes couches et composantes de l'écosystème de l'identité numérique qui, à son tour, prend en charge les services, les programmes et les applications du GC en aval, telles que représentées à la Figure 2-1 :

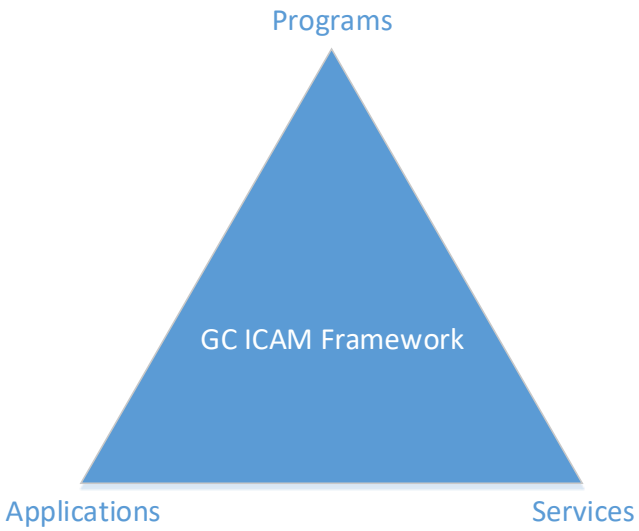


Figure 2-1 Cadre du GIJA GC relatif aux services, aux applications et aux programmes.

Veuillez prendre note que ce cadre est une sous-composante de l'architecture globale de l'Architecture de sécurité intégrée (ASI), qui en soi est un sous-ensemble de l'architecture intégrée du GC[3]. La Figure 2-2 décrit comment le cadre de la GIJA GC est situé par rapport à d'autres architectures du BDPI.

[2] Gartner parle en fait de cela comme de la gestion des identités et de l'accès (IAM).

[3] Veuillez consulter https://www.gcpedia.gc.ca/wiki/Government_of_Canada_Enterprise_Security_Architecture_(ESA)_Program pour obtenir de plus amples renseignements sur l'architecture de sécurité intégrée (ASI) et https://www.gcpedia.gc.ca/wiki/ICAM pour la GIJA GC.

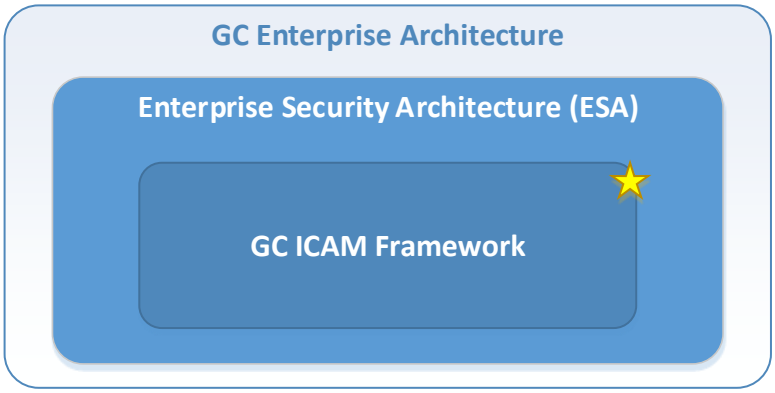


Figure 2-2 Cadre de la GIJA GC concernant l'architecture intégrée du GC

Ces éléments de base peuvent être mis en référence et utilisés comme guide pour façonner le programme et les services de GIJA d'un ministère conformément aux exigences et aux objectifs énoncés dans le présent document. Cela devrait permettre à un ministère de mettre son propre programme sur pied et de veiller à ce qu'il soit conforme à la vision d'architecture intégrée du GC. Toutefois, les services de GIJA intégrés existants doivent être exploités conformément à la Politique sur les services et le numérique [2][4] plutôt que par la création de solutions uniques et isolées qui se traduisent généralement par une pire expérience utilisateur, une position de sécurité affaiblie et une augmentation des coûts dans l'ensemble du GC. De plus, la dirigeante principale de l'information du Canada est chargée de fournir une orientation et de définir les exigences à l'échelle organisationnelle pour la gestion des identités, des justificatifs d'identité et de l'accès pour le gouvernement du Canada et les ministères[5], tandis que les administrateurs généraux sont chargés de gérer les approches ministérielles en matière d'assurance de l'identité et d'accepter des identités numériques de confiance pour appuyer l'interopérabilité en utilisant des cadres de confiance approuvés[6]. Il convient de plus de prendre note que toutes les mises en œuvre de programmes, d'applications et de services doivent être conformes aux Normes relatives au numérique du GC [6] comme indiqué à la section **Error! Reference source not found.** ci-dessous.

2.2 Interne par rapport à externe

Comme il est indiqué dans la section Portée ci-dessus, le cadre de GIJA GC traite des exigences internes et externes. Bien que les éléments de base du cadre de GIJA GC soient les mêmes, il est important de reconnaître que le contexte est différent, par exemple, la façon dont une organisation gère l'identité d'un employé peut être différente de la façon dont le GC gère l'identité des Canadiens et des résidents qui demandent des services. Il peut y avoir des cas d'utilisation, des risques, des implications et des objectifs différents. Néanmoins, à mesure que la GIJA GC et les technologies de soutien évoluent, il peut

[4] Conformément à la section 4.4.2.3 de la Politique sur les services et le numérique [2].
[5] Conformément à la section 4.4.1.10 de la Politique sur les services et le numérique [2]
[6] Conformément à la section 4.4.2.8 de la Politique sur les services et le numérique [2]

y avoir des synergies entre les domaines externes et internes qui peuvent fournir une intégration accrue menant à une expérience utilisateur plus transparente.

Pour les services internes, la vision est de créer et d'émettre une identité numérique unique, forte et persistante pour les employés du GC (p. ex., les employés et les entrepreneurs) qui peut être acceptée partout dans l'organisation.

Les principes directeurs qui s'appliquent aux entités et capacités internes comprennent ce qui suit :

- Amélioration de l'expérience utilisateur dans toute la mesure du possible (p. ex., réduire le nombre de justificatifs d'identité requis, appuyer une identification unique [IU] et fournir des interfaces utilisateur cohérentes et faciles à utiliser, entre autres).
- Mise à profit des sources d'autorité existantes, dans la mesure du possible.
- Le soutien de plusieurs options d'authentification en tant qu'approche à guichet unique risque de ne pas répondre à toutes les exigences du GC (p. ex., les solutions de justificatifs d'identité et d'authentification qui fonctionnent bien dans un environnement donné peuvent ne pas fonctionner correctement dans un autre). Cependant, les utilisateurs individuels ne devraient pas avoir à être accablés par de nombreux justificatifs ou authentificateurs, sauf si cela est absolument nécessaire.
- La mise à profit des appareils existants dans la mesure du possible (p. ex., les téléphones intelligents gérés par le GC qui sont déjà déployés pourraient servir de deuxième facteur d'authentification) afin de réduire le coût total de possession (CTP) et l'incidence sur l'expérience utilisateur.
- Les solutions doivent être fondées sur des normes, des protocoles et des interfaces de programmation d'applications (API) ouverts et acceptés par l'industrie pour promouvoir l'interopérabilité et éviter l'immobilisation des fournisseurs.
- Faire évoluer les capacités de Gestion de l'identité et des justificatifs en matière d'accès à l'appui du modèle de sécurité zéro confiance[7].

Il est à noter qu'une solution centralisée d'authentification intégrée est un élément essentiel de la stratégie de GIJA GC, car elle appuiera bon nombre des principes mentionnés ci-dessus, y compris la réduction du fardeau sur les utilisateurs et les applications, l'activation de l'IU et la facilitation de la prise en charge de plusieurs méthodes d'authentification, y compris l'authentification à facteurs multiples (AFM).

Pour les services externes, la vision est de permettre aux particuliers et aux entreprises d'utiliser une identité numérique de leur choix pour accéder aux services du GC avec confiance et facilité. Les principes directeurs pour les entités externes sont les suivants :

- Le contrôle et le choix pour les particuliers et les entreprises. Les utilisateurs pourront accéder à des services en ligne en utilisant un justificatif d'identité approuvé de leur choix[8].

[7] Veuillez vous référer au *Cadre de sécurité « zéro confiance » du GC* [12] pour obtenir de plus amples de renseignements.

[8] Cela suppose que les justificatifs d'identité doivent être appuyés par le GC et satisfaire au niveau minimal d'assurance requis pour accéder à la ressource protégée.

- La mise à profit des sources d'identité de confiance du secteur public. L'émission de preuves d'identité fondamentales (p. ex., certificats de naissance, cartes de résident permanent, documents constitutifs) doit continuer de relever du secteur public, car on veut veiller à ce que tous les particuliers obtiennent des justificatifs de compétences fondamentaux. Elle devrait donc être utilisée pour construire l'écosystème de l'identité numérique.
- L'utilisation et la conservation minimales des renseignements d'identité pour la prestation de services. Le GC utilisera et conservera seulement autant de renseignements d'identité que nécessaires. Le consentement, la révocation du consentement et les options d'exclusion sont mis en œuvre par conception et clairement mis à la disposition des utilisateurs.
- Un partage de renseignements transparent et sans heurts où les utilisateurs n'ont qu'à prouver leur identité une fois (c'est-à-dire « Une fois suffit »), en utilisant leur identité numérique de confiance pour accéder aux services, selon les modalités qu'ils acceptent. Le GC sera transparent sur les renseignements personnels des clients qui sont recueillis et sur l'objectif de la collecte.
- L'utilisation de la technologie numérique fondée sur des normes et des processus existants pour simplifier les services, améliorer la sécurité et accroître l'interopérabilité, tout en donnant aux administrations la souplesse nécessaire pour mettre en œuvre des solutions qui répondent le mieux aux besoins de leurs clients respectifs.
- Être capable d'évoluer et de s'adapter. Les efforts d'identité numérique aujourd'hui doivent continuer d'être viables dans l'économie numérique de demain, qui est sur le point de connaître une importante croissance.

2.3 Description des normes relatives au numérique du GC

Les principes directeurs ci-dessous s'appuient sur les normes relatives au numérique du GC [6] sous l'angle d'une identité numérique appliquée sur eux.

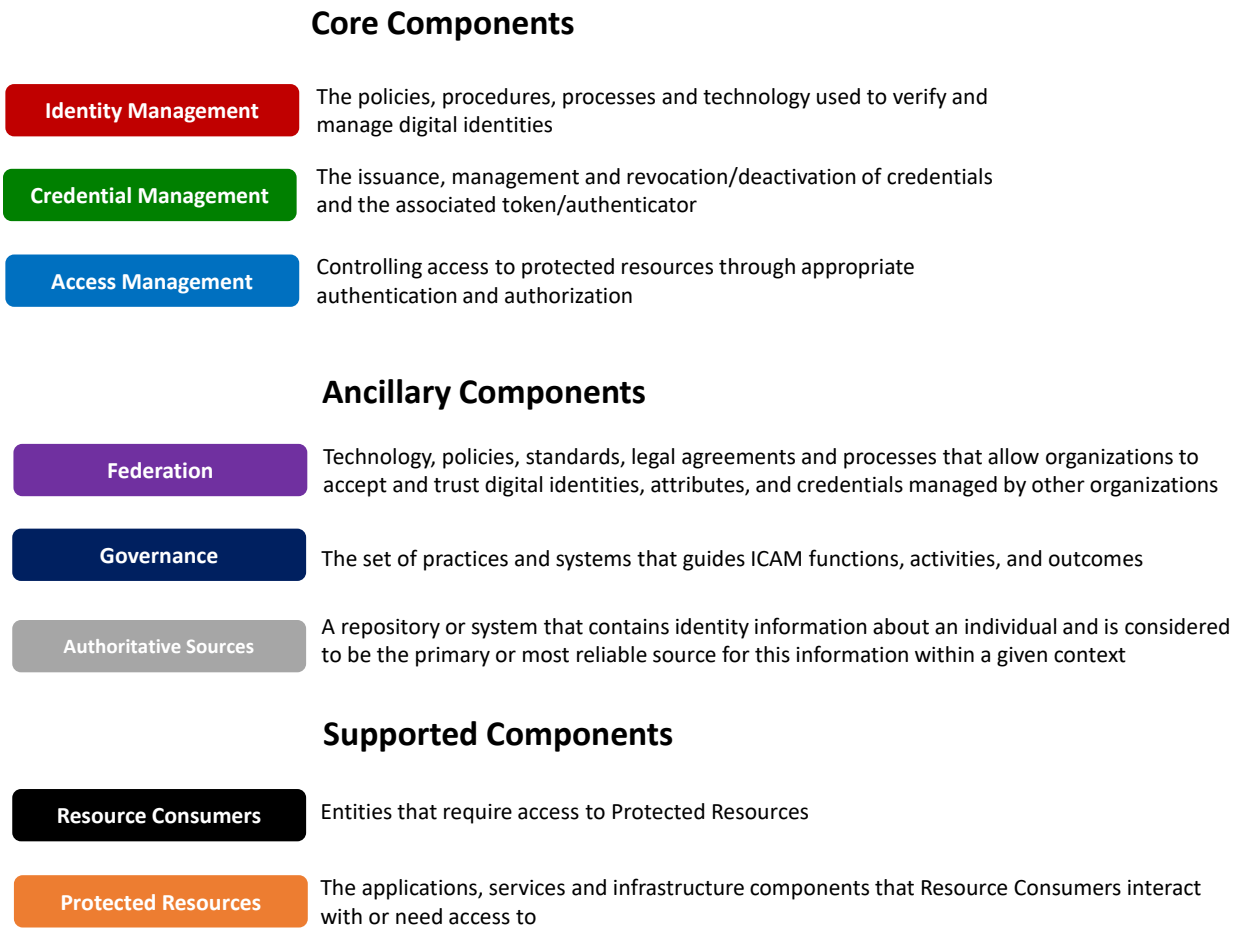
- **Concevoir avec les utilisateurs** en réalisant une mise à l'essai par les utilisateurs afin de veiller à ce que tout le monde soit à l'aise et ait l'assurance d'utiliser son identité numérique fiable afin d'accéder aux services.
- **Effectuer des itérations et des améliorations fréquemment** en ayant recours à des méthodes souples (p. ex., preuve de concepts, projets-pilotes) afin de veiller à ce que l'accès aux services avec une identité numérique de confiance soit correctement testé sur une population diversifiée avant d'être déployé dans l'ensemble du pays.
- **Travailler ouvertement par défaut** en tirant parti des cadres de confiance approuvés pour les diffuser plus largement au monde extérieur (p. ex., le secteur privé).
- **Utiliser des normes et des solutions ouvertes** pour faciliter l'interopérabilité à l'ensemble des appareils, des plateformes, des administrations et des frontières, et éviter le blocage des fournisseurs.
- **S'attaquer aux risques liés à la sécurité et à la vie privée** en utilisant la technologie et les méthodes d'échange de renseignements qui réduisent au minimum la divulgation non

nécessaire ou non autorisée de renseignements d'identité et atténuent le niveau de sécurité et de protection des renseignements personnels du début à la fin.

- **Intégrer l'accessibilité au départ** pour permettre aux utilisateurs de voir tous leurs renseignements et de contrôler la manière dont ils sont utilisés et partagés, ainsi que pour veiller à ce que l'accès à des services du gouvernement avec une identité numérique de confiance et leur prestation répondent aux différents besoins des utilisateurs et qu'ils soient pratique pour tous.
- **Permettre au personnel d'offrir de meilleurs services** en utilisant des outils, des méthodes (p. ex., souples) et des régimes de travail flexibles afin de maintenir et de retenir les talents, et offrir des initiatives d'identité numérique accélérées qui reflètent l'optimisation des ressources.
- **Être de bons intendants des données** en utilisant et en conservant seulement autant de renseignements d'identité que nécessaire. Le consentement, la révocation du consentement et les options d'exclusion devraient être mis en œuvre par conception et clairement mis à la disposition des utilisateurs. En outre, la preuve de validation d'identité est enregistrée et stockée de manière sécurisée.
- **Concevoir des services éthiques** pour veiller au traitement équitable de tous les utilisateurs et respecter leurs droits à la protection de leurs renseignements personnels, et se conformer aux lignes directrices pour un concept éthique à la conception et à l'utilisation de systèmes qui automatisent la prise de décisions, comme la reconnaissance faciale ou d'autres données biométriques.
- **Collaborer largement avec des équipes multidisciplinaires** (p. ex., la technologie de l'information [TI], les communications, les politiques, la protection des renseignements personnels et la sécurité) pour accélérer les initiatives d'identité numérique au niveau organisationnel et offrir de la valeur aux utilisateurs.

3. Composantes du cadre de la GIJA GC

Le cadre du GIJA GC comprend un ensemble de composantes de base, de composantes auxiliaires et de composantes prises en charge, comme suit :



Ces composantes et leurs sous-composantes connexes travaillent conjointement pour former le fondement du cadre de la GIJA GC, tel qu'illustré à la Figure 3-1. Veuillez prendre note que les dépendances et les interactions entre ces composantes et les sous-composantes peuvent être complexes et varient selon le scénario ou le cas d'utilisation particulier. Ce degré de granularité sera traité dans le cadre du développement d'une architecture de solution détaillée. Veuillez également prendre note que l'ovale Niveau d'assurance (NA) dans le diagramme n'est pas une composante distincte en soi. Tel qu'illustré, elle s'applique à plusieurs domaines et fait l'objet de discussions dans les sections applicables.

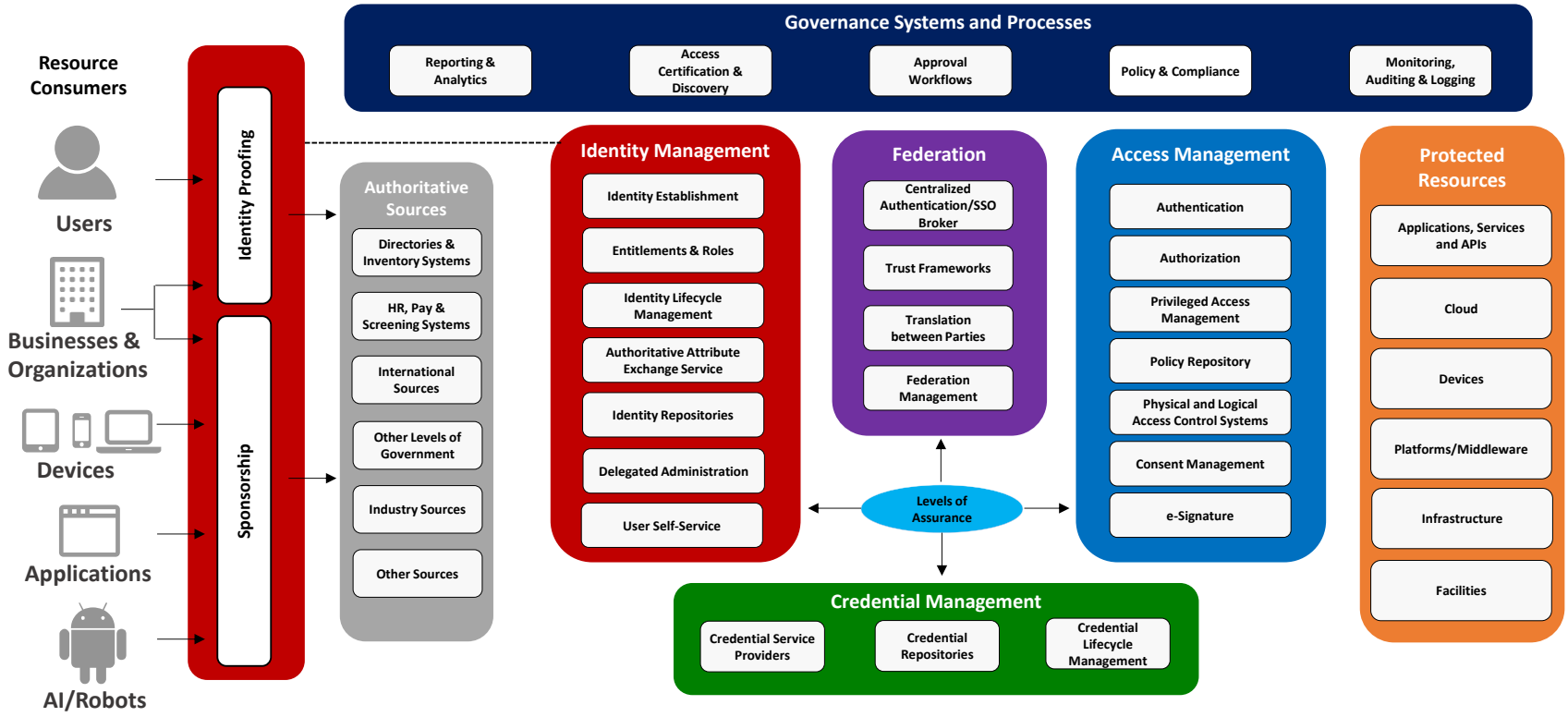


Figure 3-1 Composantes du cadre de la GIJA GC

Les sous-sections ci-dessous fournissent des détails supplémentaires sur ces composantes et sous-composantes.

3.1 Composantes de base (Gestion de l'identité et des justificatifs en matière d'accès)

3.1.1 Gestion de l'identité

La gestion de l'identité est composée des politiques, des procédures, des processus et de la technologie utilisés pour vérifier et gérer les identités numériques À son niveau le plus fondamental, une identité numérique est composée d'une collection d'attributs d'identité qui sont gérés dans toute l'organisation afin d'appuyer le contrôle d'accès et la prestation de services sur mesure. Les divers sous-éléments qui composent la gestion de l'identité sont abordés dans les sous-sections qui suivent.

3.1.1.1 Vérification de l'identité

L'identité est une référence ou une désignation utilisée pour différencier une personne, une organisation, une application ou un appareil unique ou particulier, ou toute autre ressource applicable[9]. La vérification de l'identité est « la fonction de collecte de preuves [attributs identitaires] qui appuie une déclaration d'identité [pour une entité particulière] ainsi que la validation et la vérification de cette preuve afin de déterminer la véracité (ou autrement) de la revendication » [7].

La rigueur du processus de vérification de l'identité dépend du niveau d'assurance (NA) requis tel que décrit dans la *Ligne directrice sur l'assurance de l'identité*. [8]. Dans certains cas, des exigences précises en matière de vérification de l'identité sont établies en fonction du programme ou du service offert (p. ex., la preuve d'identité pour un passeport ou une carte de santé est publiée en ligne)[10].

La vérification de l'identité peut être effectuée de façon centralisée pour le compte de plusieurs programmes et services du GC (p. ex., filtrage de sécurité du personnel et fonctions des ressources humaines [RH]) ou directement par le programme ou le service auquel on a accès (p. ex., Mon dossier Service Canada lie un justificatif d'identité anonyme, tel que CléGC, à une personne en utilisant un code envoyé directement à cette personne par un mode de livraison fiable, comme le courrier physique à une adresse postale pré-enregistrée).

3.1.1.2 Parrainage

Le parrainage est nécessaire pour établir officiellement qu'une organisation ou une entité qui n'est pas une personne doit avoir accès aux ressources du GC. Le parrain autorisé devient responsable de la gestion du cycle de vie de ces relations au fil du temps.

[9] Définition élargie de l'« identité » de la *Ligne directrice sur l'assurance de l'identité* [8].
[10] Consultez https://www.canada.ca/fr/immigration-refugies-citoyennete/services/passeports-canadiens/nouveau-passeport-adulte/documents-identite.html et https://www.ontario.ca/fr/page/documents-pour-obtenir-une-carte-sante.

3.1.1.3 Établissement de l'identité

Un attribut d'identité est une propriété ou une caractéristique associée à une entité identifiable (p. ex., une personne, un appareil ou une entreprise)[11]. Une collection ou un ensemble d'attributs d'identité suffisants pour distinguer une entité d'une autre dans un contexte donné est appelé un enregistrement d'identité (ou des renseignements d'identité)[12]. L'établissement de l'identité fait référence à la création d'un dossier d'identité faisant autorité et sur lequel se basent des tiers dans le cadre d'activités, de programmes et de services gouvernementaux subséquents [8]. Cet ensemble d'attributs est parfois appelé « attributs d'identité de base ». Les autres catégories d'attributs d'identité comprennent les attributs de coordonnées (p. ex., adresse, numéro de téléphone, adresse électronique), les attributs d'autorisation (p. ex., privilèges ou droits – voir la section **Error! Reference source not found.**) et les attributs auxiliaires (p. ex., préférence de langue – voir la section **Error! Reference source not found.**).

Veuillez prendre note que les attributs d'identité peuvent être récupérés à partir d'une ou plusieurs sources faisant autorité (voir les sections **Error! Reference source not found.**et 3.2.3).

3.1.1.4 Droits et rôles

Une fois qu'une identité de base a été établie, l'ensemble des privilèges ou droits associés à cette entité doit être établi afin d'appuyer des décisions éclairées en matière de contrôle de l'accès. Les privilèges peuvent être spécifiés comme attributs d'autorisation individuels ou être associés à un rôle spécifique (p. ex., un administrateur système est autorisé à exécuter des fonctions spécifiques associées à ce rôle). Ces attributs d'autorisation peuvent être ajoutés à un enregistrement d'identité ou être stockés et récupérés séparément d'une ou de plusieurs sources faisant autorité.

3.1.1.5 Gestion du cycle de vie de l'identité

Une fois que les différents attributs associés à une identité numérique ont été établis, ils doivent être gérés au fil du temps. La gestion du cycle de vie des identités numériques est composée des éléments suivants :

- Approvisionnement : Création d'attributs d'identité associés à l'identité numérique
- Maintenance : Conserver des attributs précis et à jour dans un enregistrement d'identité[13] tout au long de son cycle de vie.
- Retrait : Désactiver ou supprimer les attributs d'identité ou les enregistrements d'identité au besoin.

3.1.1.6 Service d'échange d'attributs autorisés

Le Service d'échange d'attributs autorisés (SEAA) sert de courtier entre plusieurs sources disparates faisant autorité et les consommateurs de renseignements sur l'identité, servant ainsi de référentiel d'identité regroupé. Comme l'illustre la Figure 3-2, le SEAA est composé d'un gestionnaire d'attributs

[11] Définition élargie de l'« attribut d'identité » de la *Ligne directrice sur l'assurance de l'identité* [8].
[12] Dérivé de FICAM [4] et la *Ligne directrice sur l'assurance de l'identité* [8].
[13] Cela comprend tous les attributs associés à l'entité, qu'ils fassent partie ou non de l'enregistrement d'identité.

faisant autorité qui récupère et regroupe les attributs d'identité de plusieurs sources faisant autorité, et en fait la correspondance, et d'un distributeur d'attributs autorisés qui fournit un point d'accès unique aux consommateurs pour récupérer les attributs d'identité. Le SEAA peut être mis en place comme référentiel virtuel ou méta-référentiel avec stockage d'attributs d'identité locale, comme illustré à la Figure 3-2. Les attributs d'identité peuvent être utilisés directement par les applications ou les services, et le SEAA peut aider à remplir d'autres référentiels d'identité en aval au besoin. Afin d'assurer une certaine souplesse, les consommateurs d'attributs d'identité peuvent obtenir leurs attributs d'identité auprès du SEAA (consommateur 1), d'un autre référentiel d'identité (consommateur 2) ou des deux (consommateur 3).

En association avec les flux opérationnels appropriés, le SEAA peut également prendre en charge d'autres fonctions telles que la gestion des données de référence[14] et l'approvisionnement et le retrait automatisé des comptes.

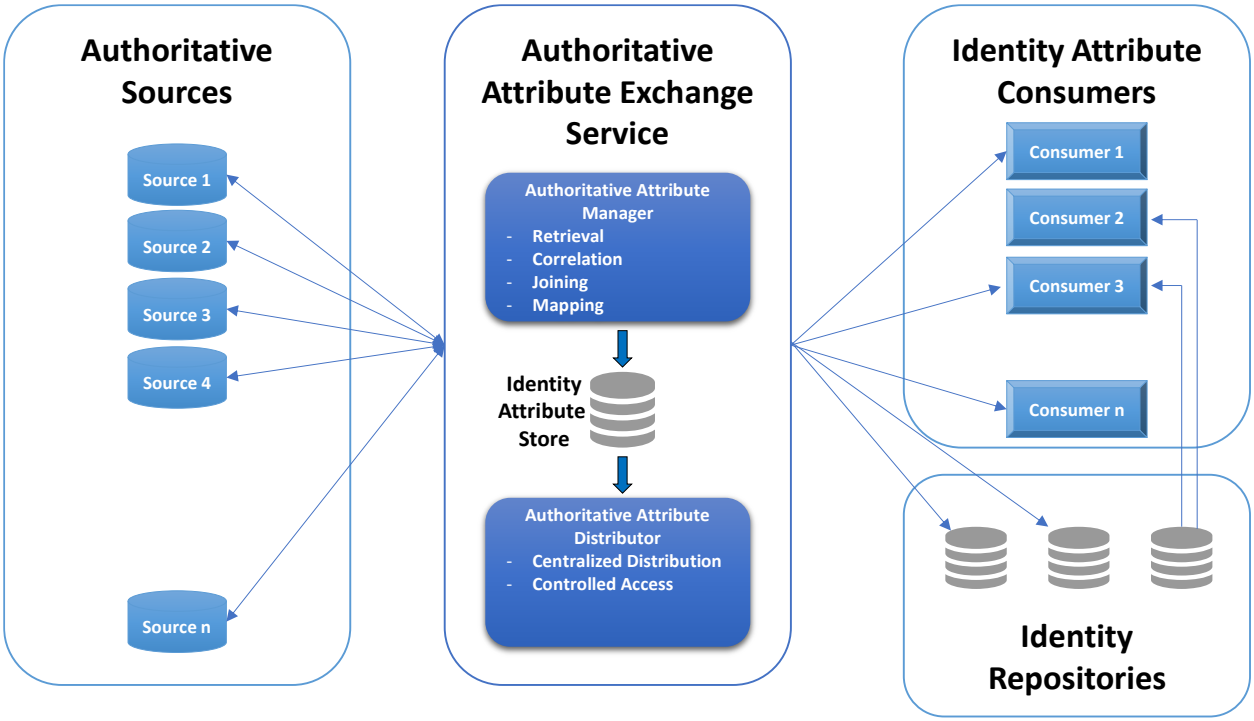


Figure 3-2 – Diagramme conceptuel pour le Service d'échange d'attributs autorisés

3.1.1.7 Référentiels d'identité

En termes simples, un référentiel d'identité est un référentiel de données qui stocke des renseignements d'identité. Il peut s'agir d'une base de données des RH, d'une unité de stockage d'attributs d'identité centralisée qui recueille des renseignements d'identité à partir de plusieurs

[14] Consultez https://www.gartner.com/en/information-technology/glossary/master-data-management-mdm pour la définition de Gartner.

sources faisant autorité (comme indiqué à la section **Error! Reference source not found.**ci-dessus) ou d'un référentiel de composantes dédié et distinct tel qu'Active Directory.

La Figure 3-2 ci-dessus illustre les interrelations entre ces diverses sous-composantes. Veuillez prendre note que les référentiels d'identité situés sur le côté droit du diagramme peuvent obtenir ou non des attributs de la composante du SEAA.

3.1.1.8 Administration déléguée

Dans le contexte informatique, l'administration déléguée permet la décentralisation de certaines fonctions administratives. Essentiellement, une personne jouant un rôle d'administrateur (p. ex., un administrateur système) peut attribuer un sous-ensemble de fonctions administratives moins essentielles à une autre personne qui est généralement mieux adaptée à l'exécution de la ou des tâches. Par exemple, un administrateur pourrait confier la gestion des profils d'un groupe d'employés à son superviseur. L'administration déléguée peut également servir à faciliter la délégation de pouvoirs (c'est-à-dire qu'un gestionnaire ayant un certain ensemble de pouvoirs peut attribuer un sous-ensemble de ces pouvoirs à d'autres, ou l'ensemble de ces pouvoirs). Cela permet d'accroître l'efficacité, de réduire la charge de travail des administrateurs système, d'appuyer la continuité de l'activité et d'assurer l'évolutivité d'une grande organisation comme le GC.

3.1.1.9 Libre-service des utilisateurs

Dans un système de GIJA de grande organisation, le libre-service est une capacité importante pour aider à la gestion de l'échelle. Dans le cas d'attributs d'identité qui ne font pas autorité, comme les préférences des utilisateurs (p. ex., les préférences linguistiques), un modèle libre-service peut satisfaire aux exigences sans le besoin de vérifier l'exactitude des attributs. Pour les attributs d'identité faisant autorité (p. ex., nom, numéro d'identification de l'employé, ministère) qui peuvent être utilisés pour les décisions de contrôle d'accès, un mécanisme permettant de confirmer l'exactitude de l'attribut d'identité modifié par le libre-service est nécessaire. Le libre-service permet également aux utilisateurs de demander de nouveaux droits ou de nouveaux rôles qui sont soumis à l'approbation d'un agent autorisé (qui peuvent être appuyés par des flux opérationnels d'approbation, comme il est indiqué à la section **Error! Reference source not found.**).

3.1.2 Gestion des justificatifs d'identité

Dans le monde physique, les justificatifs d'identité peuvent prendre plusieurs formes, dont un certificat de naissance, un permis de conduire, un passeport, un diplôme universitaire ou un certificat de constitution en société, entre autres[15]. Dans le contexte du monde numérique, un justificatif d'identité est un objet ou une structure de données qui lie de façon autoritaire une entité (p. ex., une personne, un appareil, une organisation) à un jeton ou un authentifiant[16]. Les renseignements de justificatif d'identité et l'authentifiant associé sont utilisés afin d'appuyer le processus d'authentification (voir la section **Error! Reference source not found.**). La gestion des justificatifs d'identité traite de la délivrance, de la gestion continue et de la révocation ou désactivation des justificatifs d'identité et des authentificateurs connexes, comme il est question à la section **Error! Reference source not found.**.

Comme pour les identités, les justificatifs d'identité sont associés à un niveau d'assurance, et les ressources cibles doivent généralement avoir une exigence de sécurité selon laquelle un niveau spécifique d'assurance des justificatifs d'identité doit être utilisé pour interagir avec ces ressources (p. ex., connexion). Les quatre niveaux d'assurance associés aux justificatifs d'identité sont définis dans la *Norme sur l'assurance de l'identité et des justificatifs* [9] et les exigences précises à chaque niveau d'assurance sont fournies dans le *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031v3)* [10].

Comme il a été discuté dans les *Considérations et stratégie d'authentification multifactorielle des services organisationnels de la TI du GC* [11], le GC doit prendre en charge plusieurs types de justificatifs d'identité et d'authentificateurs et développer ce soutien au fil du temps à mesure que de nouvelles exigences et technologies sont introduites. Cela pourrait inclure l'authentification sans mot de passe basée sur les normes FIDO2, l'utilisation de la biométrie pour s'authentifier localement sur un appareil, ainsi que d'autres nouvelles technologies tels que les justificatifs d'identification vérifiables.

3.1.2.1 Fournisseurs de services de justificatifs d'identité

Un fournisseur de services de justificatifs (FSJ) est une « une entité de confiance qui [établit] ou enregistre des authentificateurs d'abonnés et émet des justificatifs d'identité électronique aux abonnés ». Un FSJ peut être un tiers indépendant, ou peut émettre des justificatifs d'identité pour son propre usage »[17]. Veuillez prendre note que les justificatifs d'identité émis par le FSJ lient l'identité de l'abonné à l'authentificateur associé. Les FSJ sont responsables de la gestion du cycle de vie de ces

[15] Le terme « jeton » est utilisé dans les versions précédentes de NIST SP 800-63 ainsi que dans la version la plus récente d'ITSP.30.031 (Version 3). Cependant, NIST a changé ce terme en « authentificateur » avec l'introduction de NIST SP 800-63-3. Aux fins du présent cadre de GIJA GC, le terme « authentificateur » est utilisé conformément aux tendances récentes de l'industrie.

[16] La définition de justificatif d'identité est tirée du *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031v3)* [10]. Il est reconnu que la distinction entre un justificatif d'identité et un authentificateur est souvent floue, mais il y a une différence entre les deux. Veuillez consulter ITSP.30.031v3 ou NIST SP 800-63-3 pour obtenir de plus amples renseignements.

[17] Définition tirée du NIST SP 800-63-3, également compatible avec ITSP.30.031v3.

justificatifs d'identité ou authentificateurs au fil du temps (voir la section **Error! Reference source not found.**).

Pour ce qui est des exigences externes, le GC accepte actuellement plusieurs sources différentes de justificatifs d'identité, dont un certain nombre d'institutions financières, des titres de compétence provinciaux (actuellement l'Alberta et la Colombie-Britannique seulement) et un justificatif d'identité du GC appelé CléGC. Ces justificatifs sont appuyés par les services externes de fédération du GC et les utilisateurs peuvent choisir leurs justificatifs d'identité préférés pour accéder aux services en ligne gouvernementaux. Bien que certains ministères continuent de conserver leurs propres justificatifs d'identité, ils sont encouragés à passer aux services de fédération externe du GC dans la mesure du possible et tous les nouveaux déploiements devraient inclure cette exigence obligatoire.

Pour ce qui est des besoins internes, il existe un certain nombre de sources qui fournissent des références, notamment l'infrastructure à clé publique (ICP) de la gestion des justificatifs internes (GJI), les ICP ministérielles, les référentiels ministériels actifs et regroupés de Services partagés Canada (SPC) et des ministères, et diverses autres sources, y compris celles qui sont gérées par des applications ou des services individuels.

Il est à noter que l'ICP est un élément fondamental d'une architecture moderne des justificatifs d'identité. L'ICP peut être utilisée pour établir et gérer le cycle de vie des justificatifs des utilisateurs et des entités qui ne sont pas des personnes, tels que les périphériques et les applications. En outre, l'ICP peut être utilisée pour prendre en charge plusieurs services de sécurité, tels que la liaison d'une identité à un justificatif d'identité, le chiffrement, les signatures numériques ainsi que l'authentification.

De plus, le GC a récemment lancé un service de fédération interne appelé GCpass, qui est un courtier d'authentification centralisée ou d'identification unique (IU) qui sera également en mesure d'émettre des justificatifs d'identité aux utilisateurs internes à l'avenir, comme il est indiqué à la section **Error! Reference source not found.**. Toute application ou service organisationnel existant ou nouveau doit utiliser le service de fédération interne GCpass.

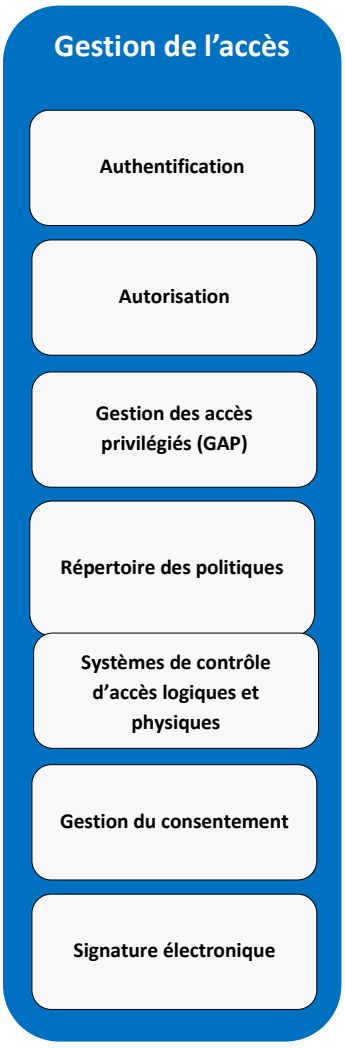
3.1.2.2 Référentiels de justificatifs d'identité

Les référentiels de justificatifs d'identité sont un élément fondamental de l'identité numérique. Dans le cadre de la gestion des justificatifs d'identité, ils sont souvent les titulaires des justificatifs principaux comme le numéro d'identification de l'utilisateur ou le mot de passe et sont parfois également titulaires d'autres facteurs d'authentification (secondaires). Souvent, les référentiels de justificatifs d'identité comme Active Directory effectuent également l'authentification des utilisateurs par rapport aux justificatifs d'identité qui y sont stockés. Veuillez prendre note que les référentiels peuvent stocker des justificatifs, ainsi que d'autres attributs qui jouent un rôle important dans le pilier des systèmes de gestion des identités.

3.1.2.3 Gestion du cycle de vie des justificatifs d'identité

La gestion du cycle de vie des justificatifs d'identité (pour les personnes et les entités qui ne sont pas des personnes) est composée de ce qui suit :

- Création, émission – création et activation d'un ou de plusieurs justificatifs d'identité qui lient l'identité de l'entité à l'authentificateur(s) associé(s) et attribution de ces justificatifs ou authentificateur(s) à une entité spécifique.
- Récupération, réinitialisation – pour gérer la perte ou le compromis d'un justificatif d'identité (p. ex., un utilisateur oublie son mot de passe).
- Suspension, blocage, déblocage – désactivation temporaire d'un justificatif résultant d'une absence prolongée (p. ex., pour un congé personnel de longue durée) ou risque de compromettre un justificatif.
- Renouvellement, nouvelle émission, mise à jour – pour maintenir la validité et l'exactitude des justificatifs dans le temps.



- Révocation, retrait, expiration et destruction – désactivation permanente d'un justificatif en raison de l'expiration préétablie, d'une compromission ou d'une cessation d'emploi, entre autres. Selon le type de justificatif d'identité, il peut être réinitialisé et réaffecté à un autre utilisateur.

3.1.3 Gestion de l'accès

La gestion de l'accès est la façon dont une organisation authentifie les identités et autorise l'accès approprié aux ressources protégées [4]. Les différentes composantes qui composent le pilier Gestion de l'accès sont décrites ci-dessous.

3.1.3.1 Authentification

L'authentification vérifie l'identité d'un utilisateur, d'un processus ou d'un dispositif, souvent comme condition préalable à l'accès aux ressources d'un système d'information [14] ou, dit autrement, l'authentification est la façon dont l'identité d'un sujet qui tente d'accéder à une ressource est vérifiée [4]. Dans le domaine numérique, cela se fait en validant que le sujet qui tente d'accéder à une ressource est en possession d'un authentificateur associé aux justificatifs d'identité du sujet et que les renseignements sont valides[18]. À l'avenir, d'autres éléments peuvent jouer un rôle dans le processus d'authentification (p. ex., les modèles de comportement des utilisateurs).

Comme pour les identités et les justificatifs, il y a quatre niveaux d'assurance associés au processus d'authentification tel que défini dans la

[18] Par exemple, dans un contexte d'ICP, un sujet activerait son authentificateur d'ICP pour produire des données de sortie signées numériquement avec sa clé privée, et la clé publique du sujet (extraite de son certificat de clé publique X.509) est utilisée pour valider les données de sortie de l'authentificateur. En outre, la validité des justificatifs d'identité du sujet, qui est le certificat de clé publique X.509 dans cet exemple, doit être évaluée, ce qui comprend de veiller à ce que le certificat de clé publique X.509 se trouve dans la période de validité spécifiée et qu'il n'ait pas été révoqué.

Ligne directrice sur la définition des exigences en matière d'authentification. [15]. Des renseignements supplémentaires sont également fournis dans le *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031v3)* [10].

Veuillez prendre note que l'authentification est l'un des éléments utilisés pour prendre en charge les décisions de contrôle d'accès. Au fur et à mesure que le GC se dirige vers la mise en œuvre d'un modèle de sécurité zéro confiance, les décisions relatives au contrôle de l'accès devraient être fondées sur de nombreuses considérations telles que l'authentification, les droits et rôles, l'état de l'appareil, les considérations environnementales, les modèles comportementaux, l'évaluation des menaces en temps réel, les contraintes politiques ou les ressources cibles, entre autres.

3.1.3.2 Autorisation

L'autorisation est le processus permettant de déterminer si une entité authentifiée est autorisée à accéder à une ressource particulière. L'autorisation est généralement basée sur les autorisations statiques attribuées au sujet ou des règles dynamiques régissant le système global.

L'autorisation est généralement basée sur un (ou plusieurs) des quatre modèles [4] :

- Listes de contrôle d'accès (LCA)
- Contrôle d'accès basé sur les rôles (CABR)
- Contrôle d'accès basé sur les politiques (CABP)
- Contrôle d'accès basé sur les attributs (CABA)

Veuillez prendre note que ces modèles ne s'excluent pas nécessairement mutuellement. Par exemple, Gartner recommande une combinaison de CABR et de CABA pour répondre aux exigences complexes généralement associées à la mise en œuvre de solutions d'autorisation [16].

La spécification eXtensible Access Control Markup Language (XACML) [17] décrit un modèle de CABA complet qui comprend un certain nombre de composantes, dont les Policy Enforcement Points (PEP) qui contrôlent l'accès aux ressources (serveurs, applications, données), et un ou plusieurs points de décision de politique (PDP) qui rendent des « décisions d'autorisation »[19] fondées sur des demandes émanant des PEP. Dans le contexte actuel de la prestation de services numériques, les décisions d'autorisation sont généralement prises localement (c'est-à-dire que chaque application est responsable de prendre des décisions d'autorisation pour ses propres ressources), de sorte qu'en pratique les PEP et les PDP ont tendance à être regroupés. Toutefois, le modèle XACML permet également de centraliser les décisions d'autorisation[20] de la même manière que l'authentification est centralisée par l'intermédiaire de la fédération (voir la section 3.2.1), ce qui permet une souplesse accrue à l'avenir. En outre, un profil JSON [18] a été défini qui fournit une méthode RESTful simplifiée pour la mise en œuvre des requêtes et des réponses XACML entre les PEP et les PDP. Par ailleurs, le National Institute of Standards and Technology (NIST) des États-Unis a récemment achevé sa publication *Zero Trust Architecture* (NIST SP 800-207) [19]

[19] Le terme « décision d'autorisation » est défini et utilisé dans la *spécification XACML* de base.
[20] On parle parfois d'« autorisation externalisée ».

qui adopte le modèle XACML. Le GC étudie cette démarche dans le cadre de son initiative de sécurité zéro confiance.

3.1.3.3 Gestion d'accès privilégié

La Gestion d'accès privilégié (GAP) est un domaine spécialisé de la GIJA qui traite spécifiquement de la protection des comptes privilégiés. Les acteurs mal intentionnés ont tendance à cibler les comptes d'utilisateurs privilégiés, car cela leur donne accès à des privilèges supérieurs que des utilisateurs non privilégiés n'ont pas. Par conséquent, des mesures de sécurité supplémentaires pour protéger les comptes d'utilisateurs privilégiés sont essentiels afin d'aider à atténuer les risques associés à l'accès non autorisé à ces comptes.

Selon Gartner[21], la GAP est composée des capacités de base suivantes :

- Découverte de comptes privilégiés sur plusieurs systèmes, infrastructures et applications.
- Gestion des justificatifs d'identité pour les comptes privilégiés.
- Délégation de l'accès aux comptes privilégiés.
- Établissement, gestion, suivi et enregistrement des séances pour un accès privilégié interactif.
- Renforcement contrôlé des commandes.

Parmi les autres considérations figurent le principe du moindre privilège, la séparation des fonctions, le contrôle par deux personnes et l'accès juste à temps.

3.1.3.4 Répertoire des politiques

Afin d'assurer un contrôle et un accès sûrs et rapides à toutes les ressources, il faut disposer de renseignements exacts, fiables et à jour sur les ressources, les utilisateurs et les appareils. La mise en correspondance de ces renseignements entraîne la création de règles et de politiques qui définissent les attributs qu'un demandeur doit avoir pour accéder à une ressource particulière. Le référentiel des politiques stocke ces règles et politiques, qui pourraient simplement être, dans les cas les plus simples, des listes de contrôle d'accès (LCA) ou des affectations de rôle pour le CABR, mais qui sont, dans les systèmes complexes comme ceux basés sur le CABA, constitués de règles traitées de manière dynamique pour le contrôle d'accès.

3.1.3.5 Systèmes de contrôle d'accès logiques et physiques

Un système de GIJA complet doit traiter à la fois le contrôle d'accès logique et physique.

Un système de contrôle d'accès physique (SCAP) vise à contrôler l'accès aux installations comme un immeuble à bureaux et à restreindre l'accès aux zones de nature délicate d'une installation comme une salle qui abrite des actifs informatiques. Le contrôle de l'accès physique peut être mis en œuvre de diverses façons, y compris par des cartes d'accès à l'immeuble, des clés physiques, des données biométrie, la reconnaissance vocale ou des verrouillages clavier électroniques.

[21] Magic Quadrant for Privilege Access Management, le 19 juillet 2021.

Un système de contrôle d'accès logique (SCAL) est « un système automatisé qui contrôle la capacité d'une personne d'accéder à une ou plusieurs ressources d'un système informatique, comme un poste de travail, un réseau, une application ou une base de données. Un système de contrôle d'accès logique exige la validation de l'identité d'une personne par l'entremise d'un mécanisme tel qu'un numéro d'identification personnel (NIP), une carte, des données biométriques ou un autre authentificateur. Il a la capacité d'attribuer différents privilèges d'accès à différentes personnes, selon leurs rôles et responsabilités au sein d'une organisation »[22].

Idéalement, le SCAP et le SCAL seraient entièrement intégrés aux attributs partagés afin d'appuyer les opérations de sécurité qui combinent un accès physique et logique. Cela pourrait inclure la prise en charge de la géolocalisation ou la possibilité de désactiver simultanément l'accès physique et logique.

3.1.3.6 Gestion du consentement

La gestion du consentement permet aux utilisateurs de contrôler la façon dont leurs renseignements personnels sont recueillis, utilisés, conservés et divulgués. Cela comprend l'avis, le consentement, la révocation du consentement et les options d'exclusion, qui devraient être mis en œuvre par conception et clairement mis à la disposition des utilisateurs. Cette gestion est orientée par le respect des lois sur la protection des renseignements personnels, comme la *Loi sur la protection des renseignements personnels* [20] et la partie I de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) [21][23, 24].

À l'avenir, OAuth 2.0 pourrait être utilisé par le GC pour appuyer la gestion du consentement au moyen d'autorisations déléguées.

3.1.3.7 Signature électronique

À l'appui de la conduite des opérations par voie électronique, les signatures électroniques permettent aux utilisateurs de satisfaire aux exigences relatives à la signature sous forme numérique. Cela peut se faire pour différentes fins connexes, telles que l'expression du consentement, l'approbation, l'accord, l'acceptation ou l'autorisation des activités commerciales quotidiennes.

Veuillez prendre note que les signatures électroniques peuvent être mises en œuvre de plusieurs façons et à différents niveaux d'assurance. Veuillez consulter l'*Orientation du gouvernement du Canada sur l'utilisation des signatures électroniques* [22] pour obtenir des renseignements supplémentaires.

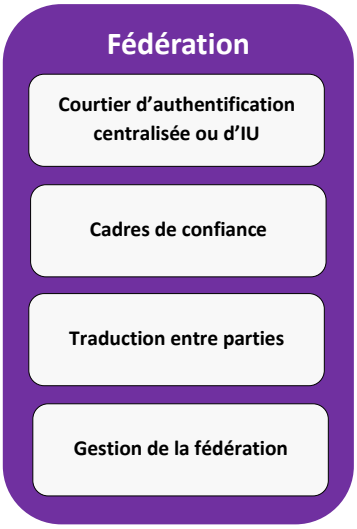
[22] Définition fournie par le glossaire du NIST des États-Unis (consultez https://csrc.nist.gov/glossary/term/logical_access_control_system)

[23] Il est à noter qu'au moment de la rédaction du présent document, une nouvelle loi appelée *Loi sur la protection de la vie privée des consommateurs* (partie de la *Loi sur la mise en œuvre de la Charte du numérique* ou du projet de loi C-11) a été proposée pour remplacer la partie I de la *Loi sur la protection des renseignements personnels et les documents électroniques*.

[24] La question de savoir si le consentement explicite est requis est régie par la législation, et il existe des exemples dans le secteur public où le consentement explicite de l'utilisateur n'est pas requis.

3.2 Composantes auxiliaires (fédération, gouvernance, sources autorisées.)

3.2.1 Fédération



La fédération est composée de la technologie, des politiques, des normes, des ententes et des processus juridiques qui permettent à une organisation d'accepter les identités, attributs et justificatifs numériques gérés par d'autres organisations et d'y faire confiance[25].

3.2.1.1 Courtier d'authentification centralisée ou d'IU

Un élément de courtier d'authentification centralisée ou d'IU permet aux organisations de connecter plusieurs fournisseurs de services avec différents fournisseurs d'identité (FI), tout en fournissant une capacité d'identification unique (IU)[26] aux utilisateurs finaux. Cela facilite la relation de confiance avec les fournisseurs d'identité et simplifie la façon dont les fournisseurs de services peuvent utiliser les identités numériques de confiance existantes, plutôt que de créer leur propre identité (le problème de silo de l'identité). Cela fournit également une interface utilisateur commune qui améliore et unifie l'expérience utilisateur.

Le GC prend en charge les courtiers externes et internes d'authentification centralisée ou d'AU selon les protocoles du langage de balisage des assertions de sécurité (SAML) et d'OpenID Connect pour permettre la fédération avec des entités externes et internes. Ces protocoles appuient la possibilité pour les parties de confiance de spécifier les NA requis pour le processus d'authentification utilisateur associé. Les profils de déploiement du GC pour la fédération externe sont disponibles sur Github (voir https://github.com/canada-ca/CATS-STAE) et les profils de déploiement du GC pour la fédération interne sont disponibles sur GCpédia (voir les profils de déploiement du GCpass). Des exemples de haut niveau de la façon dont ces protocoles fonctionnent sont présentés à l'annexe A.

Veuillez prendre note que, même si la fédération permet la reconnaissance des références émises par un fournisseur de justificatifs d'identité d'un domaine dans d'autres domaines, il est important de reconnaître que la fédération n'est pas toujours possible. Cela pourrait être dû à un certain nombre de raisons, y compris le choix de l'utilisateur (p. ex., l'utilisateur ne veut pas utiliser ses justificatifs existants, comme les justificatifs bancaires, pour accéder à d'autres services). Entre autres, le cadre de confiance dans un domaine peut être incompatible avec un autre domaine ou le nombre de domaines peut devenir ingérable. Par conséquent, il est essentiel de pouvoir fournir un justificatif d'identité universel de libre-service afin de veiller à ce que tous les utilisateurs aient accès aux applications ou aux services dont ils ont besoin, et les applications ou les services n'aient pas besoin de gérer leurs propres

[25] La définition est dérivée de FICAM (consultez https://playbooks.idmanagement.gov/arch/federation/).

[26] L'IU permet d'accéder à plusieurs ressources protégées à l'aide d'un seul événement d'authentification. Cela ne doit pas être confondu avec les gestionnaires de mots de passe qui stockent plusieurs mots de passe auxquels on accède par un mot de passe maître. Pour obtenir de plus amples renseignements sur les gestionnaires de mot de passe, veuillez consulter le site https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/orientation-sur-mots-passe.html#toc11.

solutions distinctes de justificatifs d'identité (ce qui empêche également les utilisateurs de se réinscrire sur plusieurs applications). Afin de répondre aux besoins internes, GCpass appuiera les justificatifs d'identité universels en libre-service. CléGC est le justificatif d'identité universel de libre-service pour les utilisateurs externes.

3.2.1.2 Cadres de confiance

Un cadre de confiance est un ensemble convenu de principes, de définitions, de normes, de spécifications et de critères de conformité et d'une approche d'évaluation [23].

Pour le GC, le *Profil du secteur public du Cadre de confiance pancanadien (CCP)* [23] et le pont de l'ICP fédérale canadienne (PIFC) sont deux cadres de fiducie fondamentaux qui permettent l'interopérabilité entre le GC et les organisations partenaires (comme les provinces et les territoires) partout au Canada. Le SCT cerne les politiques comme la *Directive sur la gestion de l'identité* [3] et la *Ligne directrice sur l'assurance de l'identité* [8], ainsi que la *GC X.509 Public Key Infrastructure Certificate Policy for Person Entity* [24] et le Consumer Financial Protection Bureau, qui sont essentiels pour la confiance au sein du GC (c'est-à-dire entre les ministères).

Il est à noter que, dans certaines situations d'assurance inférieure, les identités numériques qui ne sont pas conformes à un cadre de confiance approuvé par le GC peuvent être acceptées afin, par exemple, d'améliorer l'expérience utilisateur. Apportez votre propre identité (AVPI) et la connexion aux médias sociaux en sont des exemples et pourraient être utilisés dans des situations telles que la gestion de conditions d'assurance inférieures comme la réservation d'un terrain de camping.

3.2.1.3 Traduction entre parties

Dans une fédération impliquant de nombreuses organisations différentes qui partagent l'identité numérique, il est nécessaire d'effectuer certaines fonctions de traduction pour permettre aux parties de partager l'information de manière appropriée et efficace.

Les caractéristiques de la traduction comprennent, entre autres :

- la traduction de protocole – traduire entre différents protocoles (p. ex., lorsqu'une organisation utilise SAML et que l'autre utilise OIDC);
- masquer, pseudonymiser ou anonymiser – pour protéger la vie privée des personnes;
- la traduction d'attributs – pour concilier les différences dans les représentations d'attributs (p. ex., lorsqu'une organisation ajuste le format des noms sous la forme nomdefamille, prénom et l'autre sous la forme prénom, nomdefamille).

3.2.1.4 Gestion de la fédération (confiance)

Il s'agit de la gestion du cycle de vie de la confiance entre les partenaires de fédération. Cela comprendrait tout, de l'intégration de nouveaux partenaires à la mise à jour des politiques et au maintien des relations avec les partenaires existants, en passant par l'élimination des partenaires expirés ou non conformes.

3.2.2 Systèmes de gouvernance et processus

La gouvernance est l'ensemble de pratiques et de systèmes qui guident (p. ex., par la prise de décisions, la mesure, la certification et l'élaboration de politiques) les fonctions, les activités et les résultats de la GIJA[27].

3.2.2.1 Établissement de rapports et analyses

L'établissement de rapports est « le processus d'organisation des données en résumés d'information afin de surveiller la façon dont les différentes composantes de la GIJA fonctionnent et se conforment à la politique ». L'analyse est « le processus d'exploration des données et des rapports afin d'obtenir des renseignements utiles qui peuvent être utilisés pour mieux comprendre le système global et améliorer l'efficacité [25] ».

L'établissement de rapports et les analyses couvrent de nombreux systèmes de GIJA (sinon tous), y compris (mais sans s'y limiter) : couche de l'application, couche de données, couche de présentation, ainsi que les systèmes physiques qui interagissent avec les composantes de la GIJA.

Des exemples de l'établissement de rapports et d'analyses sont les suivants :

- Certification d'application ou plateforme (Attestation)
- Certification d'accès aux données ou fichiers (Attestation)
- Signalement des exceptions
- Rapports axés sur les activités
- Certification de rôle (attestation)

3.2.2.2 Certification et découverte d'accès

La certification et la découverte d'accès sont le processus de validation des droits d'accès au sein des systèmes. Ce processus est nécessaire à la gestion des risques de sécurité et à une gouvernance efficace. Avec la certification d'accès, les organisations et les réglementations visent à valider formellement les utilisateurs au sein des systèmes et à veiller à ce que leurs droits d'accès soient appropriés [26].

3.2.2.3 Flux opérationnels d'approbation

Les flux opérationnels d'approbation sont utilisés pour gérer le cycle de vie d'une identité numérique, y compris l'approvisionnement, la maintenance continue et le retrait des attributs d'identité (p. ex., nom, privilèges, rôles). Il existe ou peut exister généralement plus d'une autorité d'approbation selon le contexte. En outre, un seul flux opérationnel d'approbation peut nécessiter plusieurs vérifications de la part de divers intervenants[28].

Les flux opérationnels d'approbation pourraient :

[27] La définition est dérivée de FICAM (consultez https://playbooks.idmanagement.gov/arch/governance/).
[28]La définition est partiellement dérivée de https://kissflow.com/workflow/create-approval-workflow-in-less-than-15-min/ [30].

- être déclenchés automatiquement, par exemple à l'intégration d'un nouvel employé;
- suivre la demande d'accès en libre-service d'un utilisateur à une ressource nécessitant une approbation distincte;
- être configurés directement par une autorité autorisée (p. ex., le gestionnaire ajoute des membres d'équipe à un groupe).

3.2.2.4 Politique et conformité

La politique et la conformité assurent le respect des politiques de l'organisation et des lois applicables. Cette application de la loi peut se faire par une combinaison de processus automatisés et manuels. La conformité peut être améliorée ou renforcée grâce à des mécanismes très formels, comme des audits, ou informels, comme les examens par les pairs, qui peuvent être produits périodiquement. Certains systèmes peuvent avoir des exigences spécifiques en matière d'audit afin de maintenir la reconnaissance ou la certification.

Les types de politiques pourraient comprendre :

- la protection des renseignements personnels;
- la sécurité;
- les ressources humaines.

La politique et la conformité comprennent la résolution de toute violation de politique.

3.2.2.5 Surveillance, audit et consignation

Un journal d'audit est un registre chronologique des activités du système, y compris des registres des accès au système et des opérations effectuées au cours d'une période donnée [27]. Les journaux d'audit fournissent un enregistrement des événements importants qu'un système donné (ou une collection de systèmes) a effectués. Cet enregistrement peut être utilisé pour construire une piste d'audit afin d'examiner l'ordre des activités entourant une opération, une procédure ou un événement spécifique dans une transaction liée à la sécurité, ou y menant [27] pour faciliter les audits officiels. Consultez l'Orientation sur la journalisation des événements du GC [28] pour obtenir de plus amples renseignements.

La surveillance est un terme général qui peut inclure de nombreuses facettes de l'évaluation du système. Il s'agit d'un processus de collecte, d'agrégation et d'analyse des mesures pour mieux évaluer l'utilisation du système.

Ces composantes collaborent afin de veiller à ce que le système soit sain, qu'il fonctionne efficacement et qu'il soit essentiel pour la détection et la prévention des anomalies et des menaces.

3.2.3 Sources autorisées

Aux fins du présent cadre, une source faisant autorité est un référentiel ou un système qui contient des renseignements d'identité sur une entité et qui est considéré comme la source principale ou la plus fiable de ces renseignements dans un contexte donné[29]. En général, les sources faisant autorité sont déterminées par une décision de principe de l'autorité responsable. Idéalement, une source émettrice[30] serait également une source faisant autorité, mais ce n'est pas toujours possible. Il est à noter que les sources faisant autorité devront refléter les changements apportés à l'information sur l'identité au fil du temps afin de veiller à ce qu'elle demeure exacte.

Essentiellement, ces sources autorisées servent de référentiels pour les attributs d'identité faisant autorité qui peuvent être récupérés et utilisés afin d'appuyer les fonctions de Gestion de l'identité et des justificatifs en matière d'accès, y compris l'établissement d'un lien entre un justificatif et une identité, la gestion des privilèges et une prestation de services sur mesure. (Les renseignements connexes concernant l'échange d'attributs sont fournis à la section **Error! Reference source not found.**

Il convient de noter que tous les renseignements conservés par ces systèmes ne sont pas nécessairement autorisés (p. ex., certains renseignements peuvent ne pas être mis à jour dans le délai requis pour satisfaire aux exigences de gestion de l'identité). De plus, certaines de ces sources peuvent ne pas vouloir participer ou être en mesure de participer pour diverses raisons, dont des préoccupations en matière de protection de la vie privée ou le manque de technologie pour appuyer les fonctionnalités nécessaires. La disponibilité peut également poser un problème, car certaines sources faisant autorité ne sont pas toujours en ligne.

3.2.3.1 Répertoires et systèmes d'inventaire

Les répertoires sont un mécanisme commun de stockage des renseignements sur les utilisateurs et les entités qui ne sont pas des personnes. Les répertoires ont l'avantage d'être largement accessibles. Ils peuvent être utilisés pour publier des attributs autorisés d'autres sources et être également la source autorisée pour certains attributs tels que les références et pour certains attributs d'identité.

Les systèmes d'inventaire permettent de déterminer quelles composantes sont valides à certaines fins. Par exemple, l'inventaire de tous les appareils d'une organisation doit faire partie d'une architecture zéro confiance, de sorte qu'il est possible de limiter l'accès aux appareils qui ont été approuvés de façon appropriée et qui sont connus de l'organisation.

[29] Il est à noter qu'il n'existe pas de définition universellement reconnue de source faisant autorité. Cette définition est tirée de la définition de « source de données faisant autorité » de l'ordonnance DOE O 206.2 du département de l'Énergie des États-Unis [32].

[30] La source émettrice est l'auteur définitif des attributs d'identité. Par exemple, les certificats de naissance sont des sources fondamentales de preuves délivrées par une province à des citoyens nés au Canada.

3.2.3.2 Systèmes de RH, de paye et de filtrage.

Il s'agit de sources fondamentales d'attributs utilisateur du GC qui peuvent être utilisées pour prendre des décisions en matière de contrôle de l'accès et peut-être aussi en matière de vérification de l'identité. Des exemples d'attributs autorisés comprennent le nom d'un employé à partir d'un système de RH, le nom d'un entrepreneur d'un système de finances ou le niveau d'habilitation de sécurité d'une personne à partir d'une base de données des mesures de sécurité du personnel.

3.2.3.3 Sources internationales

L'information sur l'identité des non-citoyens devra provenir de sources non canadiennes de confiance. Les organisations gouvernementales ont des relations avec des entités étrangères et ont besoin de sources fiables pour obtenir de l'information sur l'identité avant de permettre l'accès aux ressources du GC. Des exemples de sources internationales de confiance pourraient être les passeports de pays partenaires de confiance et les attestations d'organisations étrangères de confiance (p. ex., dans le domaine de la défense ou de l'application de la loi).

3.2.3.4 Autres ordres de gouvernement

Le gouvernement du Canada interagit avec divers ordres de gouvernement, des provinces et des territoires aux municipalités, y compris, par exemple, les organismes d'application de la loi, les soins de santé et la justice. Les provinces et les territoires jouent un rôle essentiel dans l'identité fondamentale en exploitant les organismes responsables des données de l'état civil qui enregistrent tous les événements de la vie (p. ex., naissances, décès, mariage, changement de nom) ainsi que l'information commerciale (p. ex., statuts constitutifs, permis et licences) dans leur territoire. De plus, un certain nombre de ministères du GC (p. ex., la Gendarmerie royale du Canada et Santé Canada) doivent partager l'accès aux données gouvernementales avec d'autres ordres de gouvernement, ce qui exige l'authentification des utilisateurs et des décisions de contrôle d'accès de confiance qui s'appuient sur des sources autorisées d'autres ordres de gouvernement.

L'expérience et la sécurité des utilisateurs peuvent être améliorées en exploitant des identités numériques de confiance déjà établies d'autres ordres de gouvernement.

3.2.3.5 Sources industrielles

Le GC interagit avec de nombreux partenaires de l'industrie pour échanger de l'information ou donner accès à ses ressources. Les entreprises sont la source d'information faisant autorité sur leurs opérations, comme le nom de l'entreprise, le secteur d'activité et l'information sur les employés.

L'industrie recueille également des renseignements sur l'identité de ses clients (p. ex., institutions financières, compagnies d'assurance, fournisseurs de services de télécommunication), qui peuvent être utilisés (avec le consentement de l'utilisateur) dans le cadre de l'identification ou de la validation des utilisateurs qui accèdent aux systèmes du GC. Toutefois, il convient de noter que les sources d'identité de l'industrie peuvent ne pas toujours être aussi solides que les sources gouvernementales

fondamentales, mais qu'elles pourraient néanmoins servir de sources d'appui pour accroître les cas où les sources gouvernementales ne sont pas suffisantes.

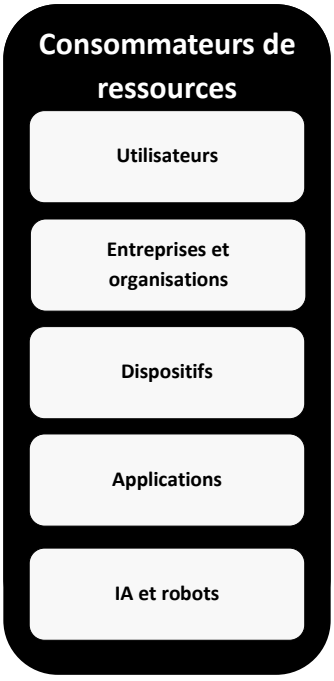
3.2.3.6 Autres sources

Il existe de nombreuses autres sources d'identité qui peuvent jouer un rôle dans la fourniture d'attributs d'identité. En voici des exemples :

- Les systèmes de gestion de l'apprentissage, qui sont la source de preuve de l'obtention d'un diplôme d'études pouvant être un préalable à l'accès à une certaine ressource ou à l'exercice d'un certain emploi.
- Les systèmes comportementaux, peut-être basés sur l'intelligence artificielle (IA), qui permettent de suivre les habitudes d'utilisation et de comportement typiques d'un utilisateur afin d'identifier les modèles d'accès anormaux qui peuvent être associés à un imposteur.
- Les référentiels de gestion des privilèges d'accès (GPA).
- Les médias sociaux ou l'identité collaborative (probablement faible niveau d'assurance).
- Les référentiels pour les droits et référentiels et les règles de politique.
- Les journaux d'activité.
- Les référentiels de règles fondés sur les risques.
- Les attributs stockés dans les certificats d'ICP (niveau d'assurance probablement élevé).
- Les référentiels spécifiques à une plateforme (p. ex., OS/400).

3.3 Composantes prises en charge (consommateurs de ressources, ressources protégées)

3.3.1 Consommateurs de ressources



Les consommateurs de ressources sont des entités qui ont besoin d'un accès aux ressources protégées. Les consommateurs de ressources représentés dans ce cadre sont à la fois internes et externes au gouvernement. Les principaux consommateurs de ressources impliqués dans l'écosystème de GIJA GC sont décrits dans les sous-sections ci-dessous.

3.3.1.1 Utilisateurs

Cela comprend :

- les utilisateurs internes tels que :
    - les fonctionnaires, entrepreneurs, agents de la GRC ou membres des Forces canadiennes, le personnel engagé sur place (p. ex., le personnel de l'ambassade) et les invités de confiance (p. ex., échanges d'autres gouvernements);
- les utilisateurs externes tels que :
    - le public, les visiteurs, les membres d'autres ordres de gouvernement, d'entreprises et d'autres organisations.

Les utilisateurs peuvent agir en leur propre nom ou comme mandataires pour d'autres personnes. Un utilisateur peut aussi avoir de nombreux rôles ou personnalités dans ses interactions avec le GC.

3.3.1.2 Entreprises et organisations

Cela comprend les entreprises commerciales, les organismes sans but lucratif, les gouvernements autochtones autonomes et tous les ordres de gouvernement qui devraient interagir avec le gouvernement fédéral à une fin quelconque.

3.3.1.3 Dispositifs

On entend tout périphérique qui doit être authentifié pour accéder à une ressource, comme :

- les périphériques mobiles (y compris les tablettes);
- les ordinateurs portatifs et les ordinateurs de bureau;
- l'Internet des objets (IdO) et les appareils intelligents;
- les appareils réseau;
- les serveurs;
- les assistants vocaux.

Les dispositifs utilisés pour accéder aux ressources internes du GC seront généralement détenus et gérés par le GC et seront authentifiés (p. ex., au moyen de certificats de dispositifs) et évalués avant que l'accès aux ressources internes du GC ne soit autorisé. Toutefois, il peut y avoir des exceptions à cette règle pour tenir compte de certaines situations qui impliquent par exemple des consultants (p. ex., permettre l'utilisation d'un téléphone non géré comme deuxième facteur d'authentification) ou l'autorisation accordée à des employés d'utiliser leurs appareils personnels pour accéder à des applications ou services moins critiques (assurance moindre), comme la formation en ligne. D'autre part, le GC n'a aucun contrôle sur les appareils utilisés par le public pour accéder aux services externes du GC.

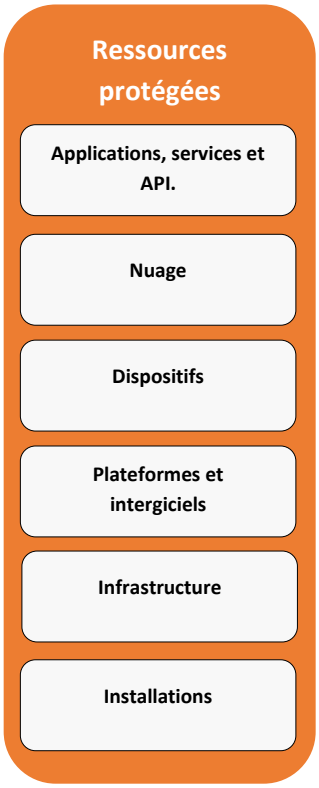
3.3.1.4 Applications

Cela comprend toute application qui doit être authentifiée pour interagir avec une autre application ou un autre service.

3.3.1.5 IA et robots

L'intelligence artificielle (IA) et les robots sont des technologies nouvelles qui influencent déjà la prestation de services numériques et qui devraient jouer un rôle important à l'avenir. Ils peuvent être mis en place sous différentes formes, y compris en tant qu'entités autonomes qui agissent pour le compte d'un utilisateur (et semblent donc être cet utilisateur), ou qui sont intégrés à un appareil ou une application.

3.3.2 Ressources protégées



Les ressources protégées sont les applications, les services et les éléments d'infrastructure avec lesquels les consommateurs de ressources interagissent ou auxquels ils doivent avoir accès. Les ressources protégées sont la principale raison pour laquelle la GIJA est nécessaire (c'est-à-dire pour prendre les décisions appropriées en matière de contrôle d'accès).

Veuillez prendre note que certaines ressources protégées (p. ex., les dispositifs et les applications) apparaissent également comme consommateurs de ressources dans ce cadre. Il s'agit de reconnaître le fait que les entités qui ne sont pas des personnes interagissent également avec d'autres entités de la même nature et doivent donc s'authentifier les unes les autres.

Les ressources protégées peuvent tirer parti d'une entreprise ou d'une infrastructure d'identité numérique partagée ou les mettre en œuvre elles-mêmes, avec des conséquences négatives importantes pour l'expérience utilisateur, la sécurité et la confidentialité dans l'ensemble de l'organisation. Un objectif important à atteindre est d'exploiter l'IU dans le plus grand nombre de ressources protégées possible pour améliorer l'expérience utilisateur et la sécurité.

Bien qu'elles ne soient pas conçues pour être exhaustives, bon nombre des ressources protégées généralement rencontrées dans la pratique sont abordées dans les sous-sections qui suivent.

3.3.2.1 Applications, services et API.

Les applications et les services prennent de nombreuses formes, comme des portails, des applications commerciales intégrées, des applications mobiles, des applications de collaboration, des services en ligne ou des charges de travail, entre autres. Les applications facilitent généralement l'accès à un service ou sont le service en soi.

Les applications et les services sont basés sur un large éventail de technologies et de plateformes modernes et anciennes, ce qui peut poser un défi à une infrastructure de GIJA pour une prise en charge efficace.

Dans les systèmes modernes, les interfaces de programmation d'applications (API) sont la norme pour transmettre des renseignements entre les systèmes. Le GC disposera de son propre magasin d'API auquel pourront accéder d'autres ministères et le public, et il aura également accès à de l'information externe provenant d'API publiques fournies par d'autres organisations. Afin d'accéder aux API du GC, les utilisateurs et les applications devront souvent s'authentifier et être autorisés à consulter ou à modifier les données disponibles sur l'API à l'aide de mécanismes sécurisés.

Les fournisseurs d'informatique en nuage utilisent également les API de GIJA pour contrôler en toute sécurité l'accès aux services. Grâce à ces outils, vous pouvez gérer de manière centralisée les utilisateurs et les justificatifs de sécurité telles que les clés d'accès et les autorisations qui contrôlent les ressources auxquelles les utilisateurs et les applications peuvent accéder [29].

3.3.2.2 Nuage

Bien que le nuage ne soit en fait qu'une façon différente de fournir des ressources et des services à un ministère, il introduit également de nouveaux mécanismes de contrôle administratif (accès privilégié) et une nouvelle composante de GIJA exhaustif pour l'authentification et l'autorisation des utilisateurs (appelé IDaaS [identité en tant que service]). Plus particulièrement, l'informatique en nuage introduit ses propres répertoires (parfois exclusifs) qui peuvent nécessiter une interaction avec les répertoires locaux et ceux d'autres fournisseurs de services d'informatique en nuage.

Les nombreuses variantes de nuage, telles que SaaS (logiciel en tant que solution), PaaS (logiciel en tant que solution) et IaaS (infrastructure en tant que solution), ainsi que les différences entre le nuage public, le nuage hybride et le nuage privé ont une incidence sur les options de GIJA disponibles.

3.3.2.3 Dispositifs

Comme pour les applications, les dispositifs prennent de nombreuses formes, comme l'ordinateur de bureau, l'ordinateur portatif, la tablette, le téléphone cellulaire, l'assistant vocal et l'IdO (p. ex., des lecteurs optiques, des caméras de surveillance ou des capteurs électroniques). Il s'agit de dispositifs gérés où le GC contrôle l'authentification et l'autorisation de leur utilisation. Les mécanismes d'authentification varient et peuvent comprendre les mots de passe, les NIP, les données biométriques (p. ex., le visage ou l'empreinte digitale) ainsi que l'authentification multifactorielle. Dans le meilleur des cas, un TPM (modules de plateforme sécurisée) est disponible sur le périphérique pour lui permettre de relayer l'authentification utilisateur effectuée sur le périphérique vers d'autres points de terminaison.

Les dispositifs sont offerts sous de nombreux différents systèmes d'exploitation, capacités et versions, ce qui peut rendre difficile d'obtenir un niveau de sécurité de GIJA cohérent sur de nombreux périphériques hétérogènes.

3.3.2.4 Plateformes et intergiciels

Une plateforme (ou plateforme informatique) est la combinaison du système d'exploitation et de l'ordinateur (en particulier l'unité centrale) sur lequel il fonctionne. L'intergiciel est un logiciel qui sert de pont entre un système d'exploitation ou une base de données et des applications, en particulier sur un réseau.[31] Comme Gartner le définit, l'intergiciel est le logiciel qui sert de « colle » en aidant les programmes et les bases de données (qui peuvent être sur différents ordinateurs) à travailler ensemble. Sa fonction la plus basique est de permettre la communication entre différents logiciels[32].

Exemples : orchestration des contenants, environnement sans serveur, virtualisation, bus de services d'entreprise, passerelle API, orchestration des opérations de développement, entre autres.

[31] Définition tirée du dictionnaire anglais de Google fourni par Oxford Languages.

[32] Définition tirée du glossaire de Gartner (consultez https://www.gartner.com/en/information-technology/glossary/middleware).

3.3.2.5 Infrastructure

L'infrastructure est une vaste catégorie qui comprend un large éventail de composantes technologiques, notamment :

- les serveurs (p. ex., bases de données, serveurs proxy, sauvegarde et récupération, contrôleurs de domaine, serveurs intermédiaires);
- les appareils (p. ex., boîtes noires, appareils virtuels, stockage, informatique, calcul de haut rendement);
- les composantes de réseau (p. ex., routeurs, commutateurs, pare-feu, points d'accès);
- les centres de données (p. ex., systèmes de chauffage, de ventilation et de conditionnement d'air, gestion de l'énergie, systèmes de sécurité physique).

Les composantes de l'infrastructure doivent être identifiées et cataloguées, et il faut émettre des justificatifs d'identité, selon les besoins, afin d'appuyer l'authentification entre (et avec) ces composantes.

3.3.2.6 Installations

Les installations ou les systèmes de contrôle d'accès physique (SCAP) ont également besoin de l'ensemble complet des fonctions de GIJA pour prendre des décisions en matière de contrôle d'accès. D'autre part, les composantes physiques qui constituent un SCAP sont complètement différentes de celles qui constituent un système de contrôle d'accès logique (SCAL), de sorte que l'interopérabilité entre le SCAP et le SCAL est un facteur important dans la réalisation d'une solution de GIJA unique et cohérente pour le GC. Plus particulièrement, les sources autorisées, les systèmes de gestion de l'identité et les systèmes de gestion des justificatifs d'identité doivent être interopérables dans les SCAL et les SCAP.

4. Conclusion

Le présent document décrit les principaux éléments constitutifs du cadre de GIJA GC. Il établit un lexique commun qui peut être utilisé pour décrire les composantes individuelles faisant partie du cadre. Le cadre décrit dans le présent document servira à établir une approche à l'échelle organisationnelle de la GIJA au sein du GC. Il peut également servir de guide pour aider les ministères à définir leur propre architecture de GIJA ou à déterminer où les déploiements de GIJA existants peuvent être améliorés en comblant les lacunes ou les écarts par rapport au cadre.

En résumé, les objectifs du présent document sont les suivants :

- un guide pour le déploiement d'un programme pangouvernemental de GIJA au sein du GC;
- un outil qui peut être utilisé pour créer une feuille de route pour la mise en œuvre des services;
- une base pour des architectures de solution de GIJA plus détaillées ou granulaires;
- un outil pour aider les organes directeurs à évaluer les initiatives en quête d'approbation;
- un outil pour cartographier les initiatives existantes afin d'identifier les lacunes, les redondances et les initiatives qui se chevauchent;
- une référence pour s'harmoniser avec la vision du GC de la gestion des composantes de la GIJA.

5. Références

[1] Secrétariat du Conseil du Trésor du Canada, « Politique sur la sécurité du gouvernement », 2019. [Accessible en ligne]. Disponible : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578.

[2] Secrétariat du Conseil du Trésor du Canada, « Politique sur les services et le numérique », 2020. [Accessible en ligne]. Disponible : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32603.

[3] Secrétariat du Conseil du Trésor du Canada, « Directive sur la gestion de l'identité ». [Accessible en ligne]. Disponible : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16577.

[4] Gouvernement des États-Unis, « Federal ICAM Architecture », [Accessible en ligne]. Disponible : https://playbooks.idmanagement.gov/arch/.

[5] Gartner, « Glossaire Gartner », [Accessible en ligne]. Disponible : https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam.

[6] Secrétariat du Conseil du Trésor du Canada, « Normes relatives au numérique du gouvernement du Canada : Directives », [Accessible en ligne]. Disponible : https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/normes-numeriques-gouvernement-canada.html.

[7] Kantara, "IAF-1050 Glossaire et aperçu", [Accessible en ligne]. Disponible : https://kantarainitiative.org/download/iaf-1050-glossary-and-overview/.

[8] Secrétariat du Conseil du Trésor du Canada, « Ligne directrice sur l'assurance de l'identité », [Accessible en ligne]. Disponible : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=30678.

[9] Secrétariat du Conseil du Trésor du Canada, « Directive sur la gestion de l'identité ». [En ligne]. Disponible : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32612.

[10] Centre canadien pour la cybersécurité, « Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031v3) ». [En ligne]. Disponible : https://cyber.gc.ca/fr.

[11] Secrétariat du Conseil du Trésor du Canada, *« Considérations et stratégie d'authentification multifactorielle des services organisationnels de la TI du GC ».* [En ligne]. Disponible : https://www.gcpedia.gc.ca/gcwiki/images/9/9e/GC_MFA_Strategy.pdf.

[12] Secrétariat du Conseil du Trésor, « Cadre de sécurité "zéro confiance" du GC », 2021. [Accessible en ligne]. Disponible : https://www.gcpedia.gc.ca/gcwiki/images/f/fa/GC_Zero_Trust_Security_Framework.pdf.

[13] W3C, « Verifiable Credential Data Model v1.1 ». [En ligne]. Disponible : https://www.w3.org/TR/vc-data-model/#dfn-credential.

[14] National Institute of Standards and Technology, "Annex A of FIPS 200". [En ligne]. Disponible : https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf.

[15] Secrétariat du Conseil du Trésor du Canada, « Ligne directrice sur la définition des exigences en matière d'authentification ». [Accessible en ligne]. Disponible : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26262.

[16] Gartner, « A Systematic and Practical Approach to Optimizing Authorization Architecture », 2015.

[17] OASIS, « eXtensible Access Control Markup Language (XACML) Version 3.0 ». [Accessible en ligne]. Disponible : http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html.

[18] OASIS, « JSON Profile of XACML 3.0 Version 1.0 », le 12 octobre 2017. [Accessible en ligne]. Disponible : http://docs.oasis-open.org/xacml/xacml-json-http/v1.0/xacml-json-http-v1.0.html.

[19] National Institute of Standards and Technology des États-Unis, « Zero Trust Architecture (NIST SP 800-207) ». [Accessible en ligne]. Disponible : https://csrc.nist.gov/publications/detail/sp/800-207/final.

[20] Gouvernement du Canada, « *Loi sur la protection des renseignements personnels* ». [Accessible en ligne]. Disponible : https://laws-lois.justice.gc.ca/fra/lois/p-21/index.html.

[21] Gouvernement du Canada, « *Loi sur la protection des renseignements personnels et les documents électroniques* ». [Accessible en ligne]. Disponible : https://laws-lois.justice.gc.ca/fra/lois/p-8.6/index.html.

[22] Secrétariat du Conseil du Trésor du Canada, « Orientation du gouvernement du Canada sur l'utilisation des signatures électroniques ». [Accessible en ligne]. Disponible : https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/orientation-gouvernement-canada-utilisation-signatures-electroniques.html.

[23] Secrétariat du Conseil du Trésor du Canada, « Public Sector Profile of the Pan-Canadian Trust Framework ». Version 1.3. [Accessible en ligne]. Disponible : https://canada-ca.github.io/PCTF-CCP/Version1_3/PSP-PCTF-V-1-3-Consolidated-Overview-EN-2021-04-21.pdf.

[24] Gouvernement du Canada, « GC X.509 Public Key Infrastructure Certificate Policy for Persson Entity ». [Accessible en ligne]. Disponible : https://www.gcpedia.gc.ca/gcwiki/images/0/07/GC_PKI_Certificate_Policy_for_Person_Entity.pdf.

[25] Adobe, « Reporting vs. Analysis: What's the Difference? ». [Accessible en ligne]. Disponible : https://blog.adobe.com/en/publish/2010/10/19/reporting-vs-analysis-whats-the-difference.html#gs.ay14qj.

[26] Identity Management Institute, « Access Certification ». [Accessible en ligne]. Disponible : https://identitymanagementinstitute.org/access-certification/.

[27] National Institute of Standards and Technology, « SP 800-53, Révision 5, Sécurité et contrôle de la vie privée ». [Accessible en ligne]. Disponible : https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[28] Secrétariat du Conseil du Trésor du Canada, « Guide sur la consignation d'événements », 2020. [Accessible en ligne]. Disponible : https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/guide-sur-la-consignation-evenements.html.

[29] Amazon Web Services, « IAM API Reference ». [Accessible en ligne]. Disponible : https://docs.aws.amazon.com/IAM/latest/APIReference/welcome.html.

[30] Kissflow, « How to Create an Approval Workflow in Less 15 Min ». [Accessible en ligne]. Disponible : https://kissflow.com/workflow/create-approval-workflow-in-less-than-15-min/.

[31] National Institute of Standards and Technology, « SP 800-63-3 Digital Identity Guidelines ». [Accessible en ligne]. Disponible : https://doi.org/10.6028/NIST.SP.800-63-3.

[32] Département de l'énergie des États-Unis, 2013. [Accessible en ligne]. Disponible : https://www.directives.doe.gov/directives-documents/200-series/0206.2-BOrder/@@images/file.

6. Annexe A – Exemples de protocoles de fédération de haut niveau

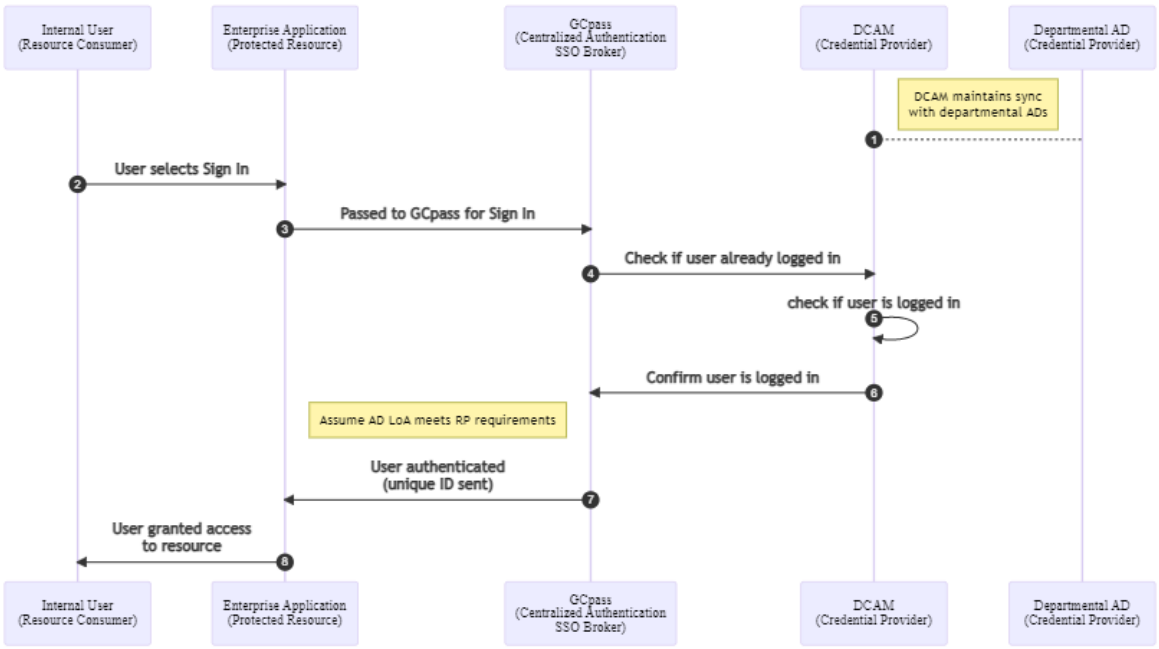


Figure A-1 : Cas d'utilisation interne

La figure A-1 représente un cas d'utilisation où un utilisateur interne (consommateur de ressources) demande l'accès à une application ou à un service intégré(e) du GC (ressource protégée) après s'être connecté par l'intermédiaire de son service Active Directory (AD). Dans ce cas d'utilisation, GCpass est le courtier d'authentification centralisée ou d'IU et l'AD ministériel de l'utilisateur est le fournisseur de justificatifs d'identité (coordonné par la Gestion des répertoires, des justificatifs d'identité et de l'accès de SPC). Ce cas d'utilisation illustre la capacité de SPC appuyée par GCpass.

Veuillez prendre note que les échanges de messages entre composantes supposent un type précis de liaison ou de flux de protocole (dans ce cas une liaison de redirection SAML 2.0) – d'autres liaisons ou flux tels que le flux de code d'autorisation OpenID Connect 1.0 sont également pris en charge. En outre, d'autres fournisseurs de justificatifs d'identité peuvent être appuyés comme il est indiqué à la section **Error! Reference source not found.**.

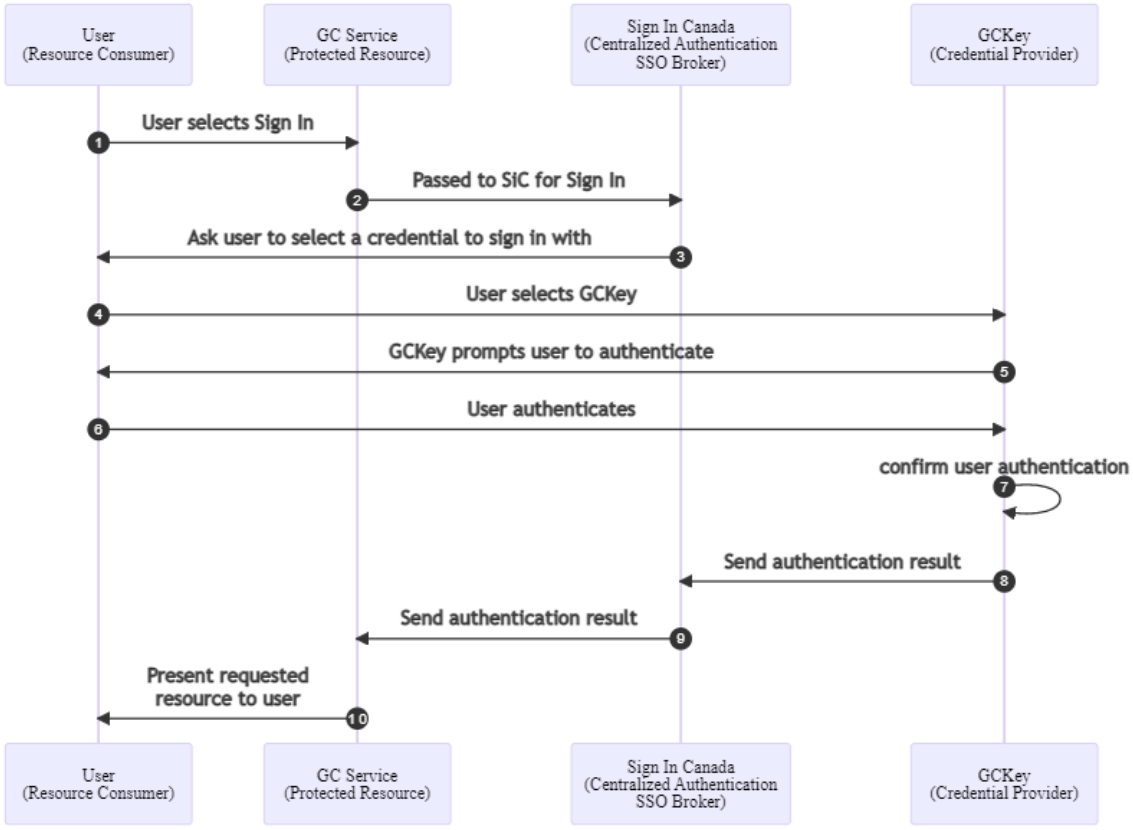


Figure A-2 : Cas d'utilisation externe

La figure A-2 représente un cas d'utilisation où un utilisateur externe (le consommateur de ressources) demande l'accès en ligne à une application ou à un service intégré du GC (la ressource protégée) lorsqu'il n'est pas connecté. Dans ce cas d'utilisation, Authenti-Canada est le courtier d'authentification centralisée ou d'IU et CléGC est le fournisseur de justificatif d'identité.

Comme dans l'exemple précédent, les échanges de messages entre composantes supposent un type spécifique de liaison ou de flux de protocole, et des échanges autres que ceux représentés sont possibles. En outre, des fournisseurs de justificatifs d'identité autres que CléGC peuvent également être appuyés, comme il est indiqué à la section **Error! Reference source not found.**.