UNIVERSITÉ DU QUÉBEC À MONTRÉAL

IDENTITÉ NUMÉRIQUE NATIONALE ET PROTECTION DE LA VIE PRIVÉE : UNE APPLICATION DU MODÈLE EFVP

(ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE)

MÉMOIRE

PRÉSENTÉ

COMME EXIGENCE PARTIELLE

DE LA MAÎTRISE EN INFORMATIQUE

PAR

NARIMAN FOUGHALI

MARS 2026

REMERCIEMENTS

Je tiens à dédier cette page à toutes les personnes qui ont contribué, de près ou de loin, à la réalisation de cette recherche et à mon parcours académique.

En premier lieu, je souhaite remercier ma mère et mon père, sans qui je ne serais pas arrivée là où je suis aujourd'hui. Je dédie toute ma réussite à leurs sacrifices, à leur altruisme et à leurs encouragements constants.

Je souhaite également exprimer ma profonde gratitude à mes directeurs de recherche, Sébastien Gambs et Jean Privat, dont l'expertise, la rigueur scientifique et la franchise bienveillante ont été déterminantes dans l'avancement de mes travaux. Leurs conseils avisés, leurs critiques constructives et leur disponibilité m'ont permis d'approfondir mes connaissances et de développer un regard critique et structuré sur ma recherche.

Je remercie chaleureusement mes sœurs, Yasmine et Ikram, ainsi que mon frère Idris, pour leur écoute, leur patience et leur soutien indéfectible. Mes pensées reconnaissantes vont également à mes amis Yasmine, Nihad, Julia, Rihab, Othmane, Idris, Imad, Chahinaz et Radia pour leur présence et leurs encouragements tout au long de ce parcours.

Enfin, j'adresse ma profonde reconnaissance à l'Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA), dont le soutien financier a rendu possible la réalisation de cette recherche.

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES TABLEAUX

ACRONYMES

UQAM Université du Québec à Montréal.

EFVP Évaluation des Facteurs relatifs à la Vie Privée.

RPRP Responsable de la Protection des Renseignements Personnels.

CAI Commission d'accès à l'information.

INN Identité Numérique Nationale.

OIDC OpenID Connect.

SAML Security assertion markup language.

MCN Ministère de la Cybersécurité et du Numérique.

SSO Single Sign-On.

RÉSUMÉ

Ce mémoire propose une analyse approfondie de l'identité numérique nationale (INN) à travers le cas d'usage du projet de loi 82 au Québec. L'INN désigne le système d'identité numérique mis en place par le gouvernement pour permettre aux citoyens de s'authentifier de façon sécurisée et d'accéder à différents services ou plateformes publiques.

Plus précisément, une première partie décrit les technologies d'authentification utilisées dans les systèmes d'identité numérique. Elle présente les différents facteurs d'authentification définis par la norme ISO/IEC 29115, les niveaux d'assurance (LoA) et les principaux protocoles employés, tels que SAML, OAuth 2.0 et OpenID Connect. Cette analyse permet de comprendre comment ces technologies assurent la vérification de l'identité, la gestion du consentement et la protection des échanges entre utilisateurs et services.

Par la suite, une étude comparative des trois architectures d'identité numérique : isolée, fédérée et décentralisée met en évidence les liens entre les sept piliers de l'identité numérique et les choix architecturaux, afin d'offrir un cadre d'aide à la décision, visant à déterminer quelle architecture répond le mieux aux besoins identifiés. Chaque modèle est présenté avec ses caractéristiques, ses technologies associées et les contextes dans lesquels il peut être privilégié. L'analyse effectuée s'appuie sur une adaptation des critères issus de l'article (Alaca et Oorschot, 2020) afin de comparer les protocoles dans un contexte de fédération gouvernementale. Le mémoire explore également l'architecture décentralisée, analysée à travers les définitions de (Allen, 2016) et illustrée par des exemples concrets afin d'évaluer si ces solutions répondent réellement aux critères d'une décentralisation complète.

Ensuite, une analyse qualitative des mémoires déposés lors des consultations publiques a permis de dégager les principaux enjeux soulevés par les parties prenantes, tels que l'exclusion numérique, la souveraineté, la cybersécurité et la transparence. À partir de cette analyse, une définition applicable en contexte réel de l'INN a été formulée.

Dans un troisième temps, le travail s'oriente vers la méthodologie d'Évaluation des Facteurs relatifs à la Vie Privée (EFVP). Après avoir rappelé le cadre légal québécois et les situations qui imposent une EFVP, un modèle adapté au contexte de l'identité numérique a été proposé. Chaque section de ce modèle est accompagnée d'une mise en contexte spécifique à l'identité numérique. Une typologie des risques liés à la vie privée a été dressée, avec des exemples concrets issus de l'analyse menée.

Enfin, le quatrième chapitre met en pratique ce modèle au moyen d'une étude de cas fictive, « Québec-Connect », une identité numérique nationale inspirée de l'expérience de FranceConnect. Ce cas illustre comment appliquer le modèle EFVP aux choix technologiques, organisationnels et réglementaires entourant un projet d'identité numérique. L'ensemble du mémoire vise ainsi à outiller la réflexion sur l'INN au Québec, en articulant les aspects techniques et méthodologiques afin de proposer une approche équilibrée, centrée à la fois sur les besoins de l'État et sur la protection des droits des citoyens.

Mots clés : Identité numérique nationale, vie privée, authentification, architectures d'identité, souveraineté numérique, protocole d'authentification, niveaux d'assurance (LoA), évaluation des facteurs relatifs à la vie privée (EFVP), gouvernance des données, exclusion numérique, projet de loi 82.

INTRODUCTION

Avec l'essor du numérique, notre société recourt de plus en plus aux outils technologiques dans la vie quotidienne. Les citoyens peuvent désormais consulter leur dossier médical, s'authentifier sur un portail gouvernemental ou signer des documents à distance. Dans ce contexte, l'identité numérique s'impose comme un système technologique central qui facilite l'accès à ces services. Toutefois, ce système soulève de nombreux enjeux en matière de sécurité, de gouvernance et de protection de la vie privée des utilisateurs. L'identité numérique met également en lumière deux questions essentielles liées à l'authentification : comment vérifier qu'un utilisateur en ligne est bien celui qu'il prétend être, et comment s'assurer qu'il dispose des droits nécessaires pour accéder à un service donné ? Ces interrogations revêtent une importance particulière dans le contexte des services gouvernementaux, où la certification de l'identité est indispensable. Afin de répondre à ces défis, plusieurs gouvernements envisagent la mise en place d'une identité numérique nationale (INN). Celle-ci permettrait aux citoyens d'accéder à l'ensemble des services publics à l'aide d'un identifiant unique et sécurisé. Comme l'a défini Ben Ayed (Ben Ayed, 2011), l'identité numérique représente un individu ou un système dans un environnement numérique donné, à travers un ensemble d'attributs (nom, adresse courriel, rôle, identifiant unique, etc.) permettant une identification fiable dans un contexte précis.

Au Québec, cette volonté s'est traduite par le dépôt du projet de loi n° 82, qui établit un cadre juridique pour la création, la gestion et l'utilisation de l'identité numérique nationale. Adoptée en octobre 2025, cette loi confie la gouvernance de l'INN au ministre de la Cybersécurité et du Numérique. Ce mode de gouvernance suscite toutefois plusieurs préoccupations, notamment en matière de transparence, de souveraineté numérique et d'imputabilité. Les consultations publiques sur ce projet ont donné lieu au dépôt d'une vingtaine de mémoires par des organismes, institutions et experts issus des milieux publics, syndicaux, académiques, communautaires et technologiques. Ces documents, au-delà de leurs recommandations, mettent en évidence les tensions entre les objectifs d'efficacité administrative et les impératifs de protection des renseignements personnels, de transparence et de respect des droits des citoyens. Si le regroupement de l'accès aux services au sein d'un même système offre des gains indéniables en efficacité et en confort, il comporte également des risques notables : perte de contrôle sur ses données, utilisation ou partage sans consentement, profilage, surveillance étatique, ou encore fuites de données en cas d'attaque informatique. Ces risques, régulièrement soulignés dans les mémoires, peuvent fragiliser la confiance des citoyens et remettre en question la légitimité de la solution.

Chaque étape d'un tel projet, de la conception technique à la mise en œuvre, influence directement la vie privée des utilisateurs, ce qui soulève plusieurs questions : quelles technologies privilégier pour réduire les risques ? Quels principes juridiques doivent encadrer la gestion de l'identité numérique ? Qui en porte la responsabilité ? Comment garantir la transparence, le contrôle par l'utilisateur et son consentement éclairé ? Et surtout, quelles étapes concrètes suivre pour intégrer la protection de la vie privée dès la conception ? La problématique de ce mémoire porte précisément sur ces préoccupations en se focalisant sur la question de recherche suivante : "**Quelles sont les considérations à prendre en compte et les étapes à suivre pour mettre en place une identité numérique nationale qui respecte pleinement la vie privée des citoyens ?**"

Trois approches ont orienté cette recherche. Le chapitre 1 regroupe deux analyses complémentaires : Premièrement, une analyse comparative a été effectuée pour examiner diverses architectures techniques (isolée, fédérée et décentralisée) ainsi que les protocoles d'authentification. Les critères de comparaison, s'appuyant sur la documentation scientifique et adaptés au contexte gouvernemental, reflètent les avantages notés dans l'article Comparative Analysis and Framework Evaluating Web Single Sign-On Systems (Alaca et Oorschot, 2020) pour le SSO. Ces avantages ont été transformés en critères pertinents pour évaluer les protocoles fédérés. Deuxièmement, une analyse comparative a été réalisée en confrontant l'architecture décentralisée aux principes proposés par Christopher Allen (Allen, 2016). Cette démarche a permis d'évaluer dans quelle mesure les solutions dites décentralisées respectent réellement les critères associés à la décentralisation. Dans le chapitre 2, une analyse thématique des mémoires soumis lors des consultations publiques sur le projet de loi 82 a permis d'identifier et de classer les enjeux récurrents. Cette étape a servi de point de départ pour formuler une définition opérationnelle de l'INN, basée sur les préoccupations exprimées par les parties prenantes.

Ce mémoire s'inscrit ainsi dans une démarche de réflexion sur la mise en œuvre d'une INN respectueuse de la vie privée. Pour cela, une méthode spécifique a été employée, incluant l'analyse des enjeux soulevés par le projet de loi 82, l'examen des diverses structures techniques de l'identité numérique, et l'application d'un modèle d'évaluation des facteurs liés à la vie privée dans une situation réelle. La méthodologie repose principalement sur une approche qualitative et comparative. Elle associe une analyse de documents, l'étude de textes de loi et d'institutions, et la comparaison de modèles et de protocoles techniques. Le but n'est pas de générer des données issues d'observations directes, mais plutôt de bâtir une réflexion organisée à partir de sources déjà disponibles. L'approche qualitative se justifie par la nature complexe de l'identité numérique, à la fois juridique, technique et sociale. Au lieu de quantifier des usages par des statistiques, il

semble plus pertinent d'étudier les documents, les normes et les technologies qui structurent ce domaine. La méthodologie employée repose donc sur trois axes : une analyse thématique des mémoires soumis lors des consultations publiques sur le projet de loi 82, une étude comparée des architectures d'identité numérique et de leurs protocoles, puis une adaptation et une application du modèle d'Évaluation des Facteurs relatifs à la Vie Privée (EFVP) au cas précis de l'INN.

Le corpus de cette recherche repose sur plusieurs ensembles de sources complémentaires. Tout d'abord, les mémoires déposés à l'Assemblée nationale dans le cadre de l'étude du projet de loi 82 (Assemblée Nationale du Québec, 2024) ont permis de mettre en évidence les principaux enjeux soulevés par les parties prenantes, comme l'exclusion numérique, la transparence, la gouvernance ou encore la souveraineté (Mouvement Desjardins, 2025; Leclerc, 2025; Loiseau *et al.*, 2025; Fédération des cégeps, 2025; Syndicat de la fonction publique et parapublique du Québec (SFPQ), 2025; Institut de gouvernance numérique (IGN), 2025; Commission de l'éthique en science et en technologie (CEST), 2025; Comité de parents du Centre de services scolaire de la Capitale, 2024; Regroupement des groupes populaires en alphabétisation du Québec (RGPAQ), 2025; Aide Pédagogique aux Adultes et aux Jeunes (APAJ), 2025; Steve Waterhouse, 2025; Leclerc, 2025; Micrologic, 2025; Réseau d'informations scientifiques du Québec (RISQ), 2025; Président-directeur général de la Régie de l'assurance maladie du Québec, 2025; Commission d'accès à l'information du Québec (CAI), 2025; Ligue des droits et libertés, 2025; Association québécoise des technologies (AQT), 2025). À cela s'ajoute la littérature scientifique et technique, mobilisée pour analyser les modèles d'architecture numérique (Chari *et al.*, 2021; Gariépy et al., 2023; Mole *et al.*, 2023; Mole *et al.*, 2023; Pöhn *et al.*, 2023; Dimova *et al.*, 2023; Fantenberg, 2022; Almeida *et al.*, 2024), les niveaux d'assurance (LoA) (International Organization for Standardization, 2013; Sharif *et al.*, 2022) ainsi que les protocoles d'authentification (France Connect, 2024; Auth0, 2024; Google Identity, 2024; Dodanduwa et Kaluthanthri, 2018; France Connect, 2024; Wu et Yu, 2009). Le corpus comprend également des textes légaux et réglementaires, notamment la Loi sur la protection des renseignements personnels dans le secteur privé (Gouvernement du Québec, 2024b; Gouvernement du Québec, 2021; Gouvernement du Québec, 2024a), les guides publiés par la Commission d'accès à l'information (CAI) (Commission d'accès à l'information du Québec (CAI), 2025; Commission d'Accès à l'Information du Québec , 2024), ainsi que des références internationales telles que le règlement eIDAS (Union européenne, 2014; Parlement Européen et Conseil de l'Union Européenne, 2024; eIDAS Expert Group, 2024; International Organization for Standardization, 2013; Kloza *et al.*, 2020). Enfin, certaines études comparatives existantes (Alaca et Oorschot, 2020), ont été utilisées afin d'adapter leurs critères d'évaluation au contexte spécifique d'une identité numérique fédérale.

Dans le contexte québécois, l'évaluation des facteurs relatifs à la vie privée (EFVP) constitue un outil structuré visant à identifier et à atténuer les risques associés au traitement de renseignements personnels. Encadrée notamment par la Loi 25, elle doit être réalisée dès les premières phases de conception d'un projet impliquant des données personnelles, afin d'intégrer les considérations relatives à la vie privée dès l'origine. Une étape clé de la méthodologie a consisté à adapter l'EFVP au domaine de l'identité numérique. Pour chaque section du modèle EFVP, une mise en contexte spécifique à l'identité numérique a été ajoutée. Ce travail a permis d'intégrer concrètement les enjeux techniques et organisationnels dans la démarche d'évaluation. Enfin, pour donner une dimension appliquée à la recherche, la méthodologie prévoit une mise en pratique du modèle EFVP à travers un cas fictif : QuébecConnect. Inspiré de l'expérience de FranceConnect et du cadre eIDAS, ce scénario permet de tester le modèle en conditions simulées et d'illustrer les choix technologiques et organisationnels que pourrait faire le Québec.

En somme, avant de réaliser une INN, plusieurs éléments doivent être pris en considération. Le présent mémoire vise justement à identifier ces éléments en étudiant les avis des parties prenantes, le cadre législatif qui entoure une INN, ainsi que la manière dont ces choix influencent, et sont influencés par les aspects techniques. Cette approche permet d'avoir une vision complète des enjeux, tant du point de vue juridique et organisationnel que technologique. Ainsi, ce mémoire est structuré en quatre chapitres. Le chapitre 1 présente les fondements techniques de l'identité numérique. Il décrit les principales architectures de l'identité numérique (isolée, fédérée et décentralisée) ainsi que les technologies qui les soutiennent. Une analyse comparative est également réalisée afin d'évaluer les protocoles d'authentification dans le contexte d'une infrastructure gouvernementale d'identité numérique fédérée. Le chapitre 2 analyse les mémoires déposés lors des consultations publiques sur le projet de loi n°82. Cette analyse permet d'identifier les principaux enjeux soulevés par les parties prenantes et de dégager les éléments clés qui devraient guider la mise en œuvre d'une identité numérique nationale. Le chapitre 3 présente le modèle d'Évaluation des Facteurs relatifs à la Vie Privée (EFVP) et examine son cadre juridique et méthodologique dans le contexte québécois. Une adaptation de ce modèle est proposée afin de l'appliquer plus spécifiquement aux systèmes d'identité numérique. Enfin, le chapitre 4 applique ce modèle adapté à un cas fictif, QuébecConnect, inspiré de certaines initiatives existantes telles que FranceConnect et du cadre européen eIDAS. Cette étude de cas permet d'illustrer concrètement les risques liés à la gestion des renseignements personnels et les choix technologiques et organisationnels pouvant influencer la protection de la vie privée dans un système d'identité numérique nationale.

CHAPITRE 1
AUTHENTIFICATION ET ARCHITECTURES D'IDENTITÉ NUMÉRIQUE

Comme le rappelle Ben Ayed (Ben Ayed, 2011), l'identité numérique désigne la représentation d'un individu ou d'un système dans un environnement numérique donné, constituée d'un ensemble d'attributs (nom, adresse courriel, rôle, identifiant, etc.) permettant de l'identifier de façon unique. Mais lorsqu'un gouvernement souhaite mettre en place une identité numérique pour ses citoyens, plusieurs questions fondamentales émergent : sous quelle forme cette identité existera-t-elle ? Qui en sera responsable ? Et comment s'assurer qu'elle reste fiable, sécurisée et respectueuse des droits des individus ?

Ce chapitre vise à répondre à ces questions en présentant les principales technologies d'authentification utilisées dans l'identité numérique, puis en examinant trois modèles architecturaux majeurs : l'architecture isolée, l'architecture fédérée et l'architecture décentralisée. La première section décrit les mécanismes techniques permettant de confirmer l'identité d'un utilisateur, ainsi que les niveaux d'assurance reconnus internationalement. La deuxième section s'intéresse à l'architecture isolée, dans laquelle chaque service gère localement l'identité de ses utilisateurs. La troisième section analyse l'architecture fédérée, son fonctionnement technique et l'évaluation des protocoles d'authentification qui la soutiennent. Enfin, la dernière section explore l'architecture décentralisée, les technologies qui la rendent possible et les exemples concrets de son utilisation.

1.1 Les technologies d'authentification dans l'identité numérique

Dans cette section, nous présentons les principaux mécanismes techniques utilisés pour authentifier les utilisateurs. Nous commencerons par les facteurs d'authentification définis par la norme ISO/IEC 29115 (International Organization for Standardization, 2013), qui distinguent les différents éléments sur lesquels repose la vérification d'identité. Nous aborderons ensuite les niveaux d'assurance (LoA), qui permettent d'évaluer le degré de confiance associé à chaque méthode, selon la sensibilité du service visé. Enfin, nous décrirons plusieurs protocoles d'authentification largement utilisés dans les systèmes d'identité numérique, notamment OAuth 2.0, OpenID Connect, SAML, Mobile Connect et Interac Sign-In. Ces protocoles illustrent concrètement la manière dont les mécanismes d'authentification sont mis en œuvre pour permettre des échanges sécurisés et interopérables entre différents acteurs. L'objectif de cette section est de poser les bases techniques nécessaires à la compréhension des architectures d'identité numérique présentées plus

loin. Les protocoles étudiés ici seront ensuite réutilisés pour illustrer le fonctionnement de l'authentification dans les modèles isolé, fédéré et décentralisé, afin de mieux comprendre leurs différences et leurs impacts sur la protection de la vie privée.

1.1.1 Les facteurs d'authentification (ISO/IEC 29115) et niveaux d'assurance (LoA)

Selon la norme ISO/IEC 29115 (International Organization for Standardization, 2013), les facteurs d'authentification sont classés en quatre catégories : un élément que possède l'entité (ex. : signature de l'appareil, passeport, dispositif matériel contenant un justificatif, clé privée), un élément que connaît l'entité (ex. : mot de passe, code PIN), un élément qui caractérise l'entité (ex. : caractéristique biométrique), et un comportement typique de l'entité (ex. : schéma d'interaction ou de comportement). Ainsi, l'authentification repose sur l'utilisation d'un ou plusieurs de ces facteurs.

Dans leur étude sur le règlement eIDAS, Sharif, et al. (Sharif *et al.*, 2022) ont catégorisé les différents mécanismes d'authentification selon plusieurs niveaux d'assurance (*Level of Assurance LOA*). Le niveau **LoA Low (L)** correspond à une situation où une seule méthode d'authentification est requise. Les méthodes d'authentification les plus couramment utilisées pour ce niveau d'assurance incluent l'utilisation d'un mot de passe où l'utilisateur se connecte en utilisant un identifiant unique et un mot de passe. Cette méthode repose principalement sur ce que l'utilisateur sait (mot de passe), offrant une sécurité de base pour des applications nécessitant un faible niveau d'assurance. Le niveau **LoA Substantial (S)** repose sur l'utilisation d'au moins deux facteurs d'authentification. Les méthodes employées à ce niveau reposent sur diverses combinaisons destinées à renforcer la sécurité, en associant généralement un mot de passe à un second facteur. Selon l'article (Sharif *et al.*, 2022), cela peut prendre la forme d'un mot de passe complété par un code reçu par SMS ou généré par une application (OTP), par un dispositif matériel (clé de sécurité, générateur électronique) ou encore par un document physique contenant des codes uniques. D'autres approches consistent à coupler le mot de passe avec un mécanisme visuel (QR code) ou une notification « push » validée par un code PIN ou des données biométriques. Toutes ces méthodes poursuivent le même objectif : réduire le risque de compromission en exigeant au minimum deux facteurs distincts pour l'authentification. Enfin, le niveau **LoA High (H)** exige l'utilisation d'au moins deux facteurs d'authentification, tout en garantissant une protection contre la duplication ou la manipulation par des attaquants sophistiqués. Contrairement au niveau **Substantial**, qui repose principalement sur des combinaisons de facteurs classiques (comme mot de passe et SMS), le niveau **High** requiert des mécanismes cryptographiques avancés, spécifiquement conçus pour

résister à des attaques ciblées. Ces méthodes d'authentification reposent généralement sur des dispositifs matériels sécurisés, parfois complétés par des logiciels spécialisés (Sharif *et al.*, 2022). Parmi les approches courantes, on retrouve l'utilisation de cartes à puce contenant une clé privée et un certificat, qui peuvent être intégrées à des cartes d'identité électroniques ou dédiées au stockage sécurisé. De même, certaines solutions s'appuient sur des cartes SIM cryptographiques, capables de stocker des secrets et certificats pour une authentification fondée sur l'infrastructure à clé publique. Les clés de sécurité matérielles, comme celles basées sur la norme FIDO, renforcent aussi la protection contre les attaques par hameçonnage en signant directement les défis d'authentification. Enfin, des authentificateurs logiciels peuvent être employés, générant et stockant une paire de clés sur l'appareil de l'utilisateur, protégée par un code PIN. Ces techniques combinent ce que l'utilisateur connaît (mot de passe, PIN) avec ce qu'il possède (carte à puce, SIM, clé de sécurité).

1.1.2 OAuth 2.0

OAuth 2.0 est un protocole d'autorisation qui permet à un utilisateur de donner à une application tierce un accès limité à certaines de ses données, sans devoir lui transmettre ses identifiants personnels. L'objectif initial d'OAuth était précisément de séparer l'authentification de l'autorisation, afin de remédier à plusieurs faiblesses de sécurité observées dans les premières intégrations entre applications et services web. En effet, avant OAuth :

> « *les applications tierces devaient stocker les identifiants du propriétaire de la ressource pour un usage ultérieur, souvent un mot de passe en clair. Les serveurs étaient tenus de prendre en charge l'authentification par mot de passe, malgré les faiblesses de sécurité inhérentes à cette méthode. Les applications tierces obtenaient un accès trop large aux ressources protégées du propriétaire, sans que celui-ci ait la possibilité de restreindre la durée ou la portée de cet accès. Le propriétaire ne pouvait pas révoquer l'accès d'une seule application sans révoquer celui de toutes les autres, et devait pour cela changer son mot de passe. Enfin, le compromis d'une seule application tierce entraînait la compromission du mot de passe de l'utilisateur final et de toutes les données protégées par ce mot de passe*. » (Hardt, 2012).

Ainsi, le protocole introduit une couche d'autorisation distincte : l'utilisateur peut consentir à ce qu'une application accède à des informations précises (par exemple, une adresse de courriel ou une liste de contacts), sans lui transmettre ses identifiants. L'« autorisation » désigne donc ici le fait d'accorder un droit d'accès, tandis que l'« authentification » qui consiste à vérifier l'identité de la personne n'entre pas dans le champ

d'application de ce protocole. La spécification précise également que « cette norme est conçue pour être utilisée avec HTTP. L'utilisation d'OAuth avec tout autre protocole que HTTP est hors de portée de la présente spécification ». Publiée en octobre 2012 par l'*Internet Engineering Task Force* (IETF), cette norme repose sur l'utilisation de jetons d'accès, dont la spécification définit le concept comme suit : « Un jeton d'accès est une chaîne représentant une autorisation accordée au client. Cette chaîne est généralement opaque pour le client. Le jeton représente des portées et des durées d'accès spécifiques, accordées par l'utilisateur et appliquées par le fournisseur d'identité et le fournisseur de services ». Dans le contexte d'une identité numérique, le protocole fonctionnerait de la manière suivante, tel qu'illustré dans la figure 1.1 (Hardt, 2012).

1. **Enregistrement du fournisseur de services.** Le fournisseur de services s'enregistre auprès du fournisseur d'identité pour obtenir un identifiant client et un secret, nécessaires pour faire une demande d'autorisation.
2. **Demande d'autorisation.** Lorsque l'utilisateur tente d'accéder à une ressource via le fournisseur de services (comme une application mobile ou un site web), celle-ci redirige l'utilisateur vers le fournisseur d'identité, en spécifiant les permissions souhaitées (*scopes* en anglais) et une URL de redirection.
3. **Authentification de l'utilisateur et consentement.** Le fournisseur d'identité authentifie l'utilisateur (s'il ne l'est pas déjà) et lui demande s'il consent à accorder l'accès au fournisseur de services.
4. **Délivrance d'un jeton.** Si l'utilisateur donne son accord, le fournisseur d'identité envoie un jeton d'accès au fournisseur de services.
5. **Demande d'accès à la ressource.** Le fournisseur de services utilise le jeton d'accès pour demander l'accès aux ressources au serveur de ressources.
6. **Validation du jeton et accès.** Le serveur de ressources vérifie la validité du jeton d'accès et autorise le fournisseur de services à accéder aux ressources.

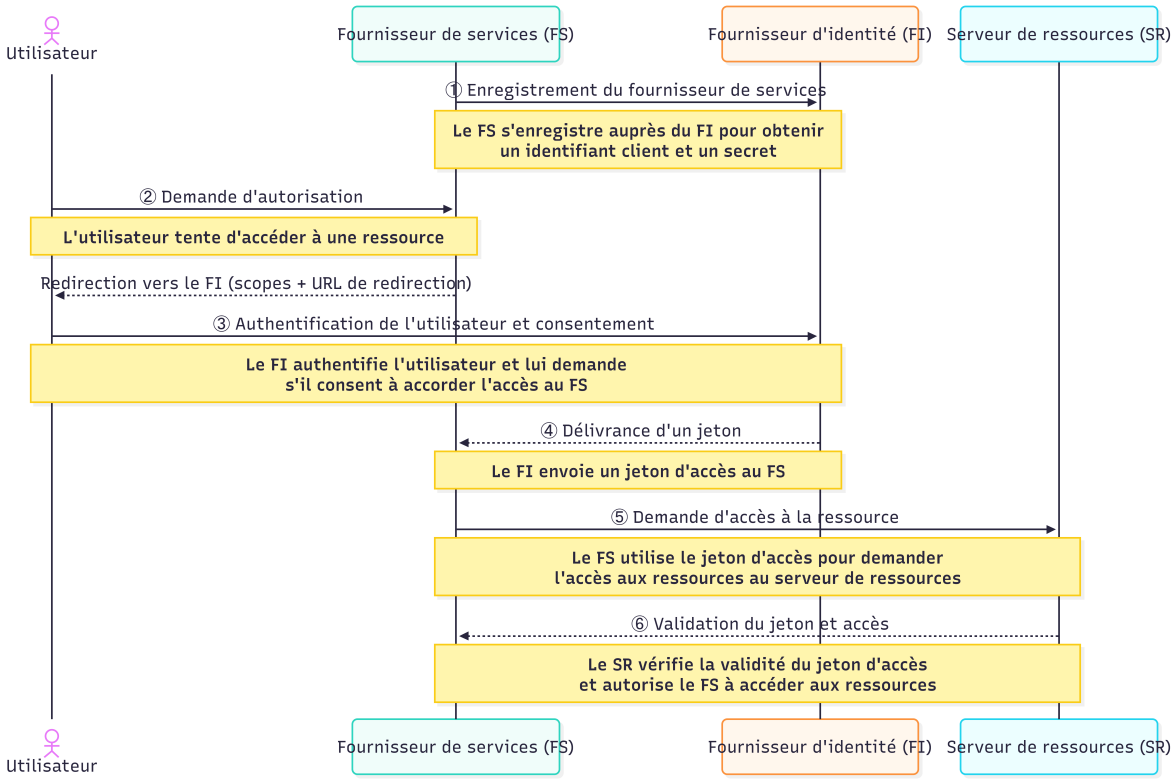

Figure 1.1 Diagramme de séquence du protocole OAuth 2.0.

Dans le cadre de cette analyse, le terme « fournisseur d'identité » est utilisé de manière générique pour désigner l'entité qui authentifie l'utilisateur et émet le jeton d'accès. Dans OAuth 2.0, ce rôle correspond techniquement au « serveur d'autorisation » défini par la RFC 6749 (Hardt, 2012).

1.1.3 OpenID Connect

Publié par l'*OpenID Foundation* en février 2014, le standard OpenID Connect Core 1.0 (OpenID Foundation, 2014b) étend le protocole OAuth 2.0 en y ajoutant une couche d'authentification permettant aux utilisateurs de vérifier leur identité et de partager de manière sécurisée certaines informations de profil avec des fournisseurs de services externes. Alors qu'OAuth 2.0 se limite à la délégation d'autorisation, OpenID Connect introduit une dimension identitaire en intégrant un ID Token au format *JWT* (*JSON Web Token*), contenant des informations telles que l'identifiant de l'utilisateur, la date de l'authentification ou l'émetteur du jeton (Dodanduwa et Kaluthanthri, 2018). Conformément à la spécification *OpenID Connect Core 1.0* (OpenID Foundation, 2014b), toutes les communications reposent sur le protocole HTTP sécurisé (HTTPS). Cette exigence s'inscrit dans la continuité du modèle défini par la RFC 6749 (Hardt, 2012), sur laquelle OpenID

Connect est fondé. Ainsi, le déroulement du protocole suit les mêmes étapes qu'OAuth 2.0 (Hardt, 2012), à la différence que (OpenID Foundation, 2014b) :

- La demande d'autorisation indique que le fournisseur de services souhaite obtenir un ID Token en plus du jeton d'accès.
- Le fournisseur d'identité délivre ces deux jetons simultanément : un jeton d'accès pour accéder aux ressources et un ID Token servant à authentifier l'utilisateur.
- Le fournisseur de services vérifie la signature du ID Token à l'aide de la clé publique du fournisseur d'identité pour confirmer l'identité de l'utilisateur et établir une session sécurisée.

Ainsi, OpenID Connect conserve la logique d'autorisation d'OAuth 2.0 tout en ajoutant un mécanisme d'authentification standardisé.

1.1.4 Le Security Assertion Markup Language (SAML)

SAML est un protocole fondé sur XML, publié par *Organization for the Advancement of Structured Information Standards (OASIS)* en 2005. SAML est conçu pour l'échange d'informations d'authentification et d'attributs d'identité entre entités. Il repose sur des assertions SAML, des jetons structurés en XML et généralement signés numériquement pour assurer la confiance entre les entités. et s'appuie géneralement sur HTTPS comme mode de transport (OASIS Security Services Technical Committee, 2005). Dans certains cas plus complexes, notamment dans des architectures inter-domaines, un acteur supplémentaire peut intervenir : le serveur d'authentification unifiée, qui gère les relations de confiance entre différents domaines d'authentification (Wu et Yu, 2009).

Le fonctionnement général de SAML 2.0 suit les mêmes étapes qu'OAuth 2.0, à la différence que dans OAuth 2.0, le fournisseur de services obtient un identifiant client et un secret pour interagir avec le serveur d'autorisation, tandis que dans SAML, cette configuration repose sur un échange de métadonnées XML signées entre le fournisseur de services et le fournisseur d'identité. Cet échange vise à établir une relation de confiance. L'assertion SAML peut ensuite transiter directement vers le fournisseur de services ou passer par le serveur d'authentification unifiée, qui vérifie la relation de confiance et, dans certains cas, enrichit l'assertion avec des attributs supplémentaires. Le fournisseur de services reçoit l'assertion SAML, la vérifie (signature, validité, etc.), et accorde ou refuse l'accès à la ressource selon les attributs contenus dans l'assertion (Wu et Yu, 2009).

1.1.5 Mobile Connect

Mobile Connect est un protocole d'authentification standardisé par la GSMA (*GSM Association*) en 2014, reposant sur les standards OpenID Connect/OAuth 2.0. Le fonctionnement général de Mobile Connect reprend la même logique qu'OAuth 2.0, mais s'en distingue par le rôle central de l'opérateur mobile en tant que fournisseur d'identité (Orange Developer, 2024). Au lieu de s'appuyer sur un compte en ligne classique, Mobile Connect utilise les informations stockées sur la carte SIM pour authentifier l'utilisateur et établir une connexion sécurisée (Alaca et Oorschot, 2020).

Lorsqu'un utilisateur choisit Mobile Connect comme méthode d'authentification, l'opérateur mobile (fournisseur d'identité) l'identifie à l'aide de ses données SIM et déclenche une vérification, souvent par notification sur le téléphone ou par saisie d'un code de confirmation. Une fois l'authentification validée, un jeton d'identité est émis et transmis au fournisseur de services, qui l'utilise pour confirmer l'identité de l'utilisateur et autoriser l'accès au service demandé. Ainsi, contrairement à OAuth 2.0, où l'identité repose sur un compte géré par un fournisseur tiers (ex. Google, Facebook), Mobile Connect utilise un opérateur mobile, offrant un niveau de confiance plus élevé grâce à la possession de la carte SIM et à la vérification du numéro de téléphone.

1.1.6 Interac Sign-In

Interac Sign-In, anciennement connu sous le nom de SecureKey Concierge, est un service d'authentification qui permet aux utilisateurs d'accéder de manière sécurisée à divers services en ligne (comme les services gouvernementaux) en utilisant les identifiants fournis par des institutions financières approuvées, telles que des banques canadiennes (Alaca et Oorschot, 2020). Implémenté en 2012, ce service agit en tant qu'intermédiaire entre le fournisseur de services et le fournisseur d'identité. Ce mécanisme est notamment utilisé pour permettre l'accès sécurisé aux services numériques de l'Agence du revenu du Canada (ARC).

Le fonctionnement général de Interac Sign-In suit une logique comparable à celle d'OAuth 2.0, mais s'en distingue par son approche fondée sur la fédération d'identité et la pseudonymisation des identifiants. Au lieu d'émettre des jetons d'accès liés à des ressources comme dans OAuth 2.0, le protocole repose sur la création d'identifiants pseudonymes (MBUN, iPAI et rpPAI) permettant de dissocier l'identité réelle de l'utilisateur des services auxquels il accède. L'utilisateur s'authentifie auprès de sa banque, qui agit comme fournisseur d'identité, tandis que Interac Sign-In joue le rôle d'intermédiaire de confiance chargé de transformer ces

identifiants afin d'empêcher toute corrélation entre différents services. Ainsi, ni la banque ni le fournisseur de services ne connaissent l'identité complète de l'utilisateur, ce qui renforce la protection de la vie privée et la minimisation des données.

Ces protocoles constituent les briques techniques de base sur lesquelles reposent les différentes architectures d'identité numérique. Les trois sections suivantes examinent comment ces mécanismes s'organisent concrètement selon trois modèles architecturaux distincts : isolé, fédéré et décentralisé.

1.2 Architecture isolée de l'identité numérique

Le modèle isolé (Gariépy et al., 2023) est le premier modèle d'architecture de l'identité numérique et se caractérise par une approche centralisée où le fournisseur de service agit également en tant que fournisseur d'identité. Cela signifie que l'utilisateur doit posséder un compte distinct auprès de chaque fournisseur de service, comme illustré dans le schéma où l'utilisateur possède une authentification pour chaque service (voir figure 1.2).

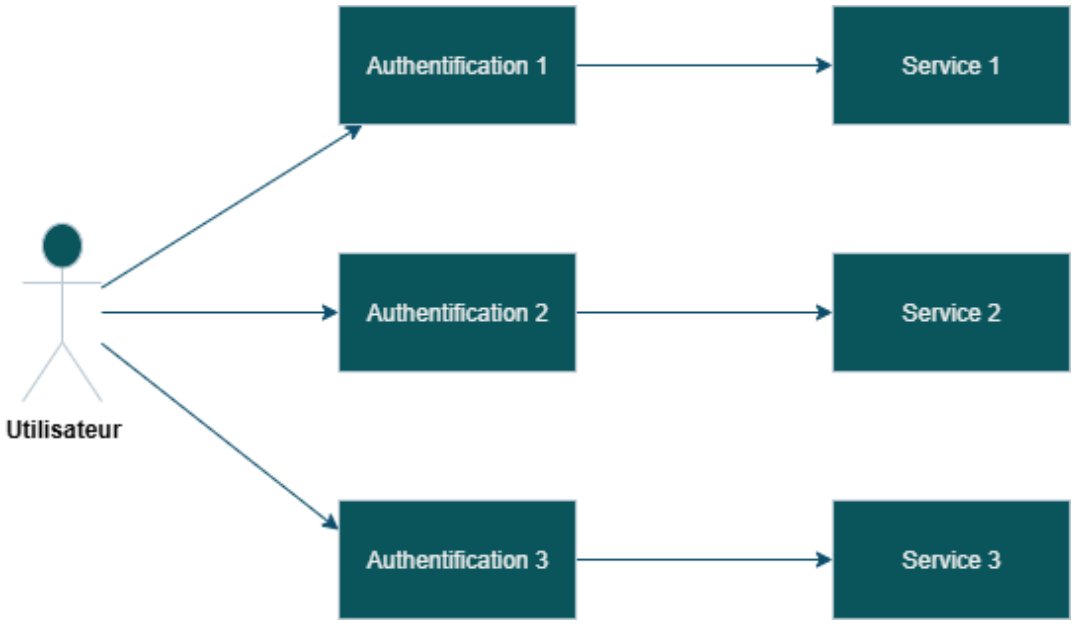

Figure 1.2 Schéma de l'architecture isolée.

Dans un modèle isolé, chaque fournisseur d'identité fonctionne de manière indépendante, mais conserve généralement l'ensemble des données personnelles de ses utilisateurs dans son propre système. Cette concentration peut engendrer divers problèmes liés à la sécurité, à la protection de la vie privée et à la gestion de l'information. L'analyse qui suit s'appuie en partie sur les travaux de Mole et collaborateurs (Mole

et al., 2023), une étude comparative des architectures d'identité numérique (centralisées, fédérées et décentralisées). Bien que leur cadre n'aborde pas explicitement le « modèle isolé », plusieurs constats qu'ils formulent à propos des systèmes centralisés, comme la concentration des données, la transparence limitée et la vulnérabilité à un point unique de défaillance, peuvent, par analogie, être transposés à une architecture isolée, où chaque fournisseur administre de manière autonome son propre système.

Dans les systèmes isolés, chaque fournisseur est responsable de la gestion complète des renseignements de ses propres utilisateurs. Cela implique souvent que les données soient regroupées en un seul système, même si elles peuvent être réparties sur plusieurs serveurs. Cette configuration crée un point unique de vulnérabilité (Mole *et al.*, 2023) : si une attaque cible ce système, elle peut compromettre un grand volume d'informations sensibles. Par ailleurs, chaque fournisseur gère ses propres données de manière indépendante, ce qui évite la création d'un point unique d'échec, mais multiplie les points d'attaque potentiels. La sécurité globale dépend donc du niveau de protection mis en place par chaque fournisseur. Si l'un d'eux est compromis, l'impact reste limité à son système, mais des failles multiples peuvent accroître les risques globaux pour les utilisateurs, incluant des fuites d'informations, des usurpations d'identité, ou le profilage abusif.

De plus, dans une architecture isolée, l'interopérabilité est limitée, car chaque fournisseur développe ses propres mécanismes indépendamment. Cette absence de coordination complique la communication entre services et freine la création d'un écosystème numérique cohérent. Comme le décrit l'article « Modeling the Threats to Self-Sovereign Identities » (Pöhn *et al.*, 2023), le fait que les utilisateurs doivent gérer plusieurs comptes et mots de passe pour chaque service les conduit souvent à adopter des pratiques risquées, telles que l'utilisation de mots de passe simples ou la réutilisation de mots de passe sur plusieurs services, ce qui augmente mécaniquement le risque de compromission des comptes.

Dans un modèle isolé, chaque fournisseur crée et maintient sa propre base de données pour ses utilisateurs. Cela entraîne une redondance des informations, puisque les mêmes données relatives à un utilisateur sont conservées à plusieurs endroits par différents fournisseurs. Cette redondance entraîne une surcharge : les utilisateurs doivent répéter les mêmes démarches auprès de chaque service, et les fournisseurs doivent chacun assurer séparément la gestion et la sécurisation de données similaires. Il est vrai que cette duplication peut être perçue comme une forme de robustesse, car si un système tombe en panne, les autres restent fonctionnels, mais elle se fait au prix d'une perte d'efficacité globale, d'une augmentation des coûts et d'un risque d'incohérences entre les versions des données. Enfin, dans une architecture isolée, chaque

fournisseur détient un contrôle complet sur sa base de données. La concentration du pouvoir sur les données sans mécanismes de transparence peut entraîner des abus, nuire à l'intégrité des informations et réduire la confiance des utilisateurs.

Bien que l'INN ne repose pas généralement sur une architecture isolée, plusieurs entreprises choisissent de conserver ce modèle pour des raisons stratégiques, économiques et techniques. Il leur permet de garder un contrôle complet sur les identifiants des utilisateurs et sur les données générées par leur activité (comportements, historiques, préférences). Par exemple, des plateformes comme Netflix, Amazon ou Zara exigent que les utilisateurs créent un compte propre à leur service, sans passer par un fournisseur d'identité tiers comme Google ou Facebook. En conservant ces données en interne, ces entreprises peuvent personnaliser leur offre, segmenter leurs utilisateurs pour le marketing et optimiser leurs stratégies commerciales, tout en protégeant leur relation directe avec leurs clients.

Sur le plan technique, le modèle isolé se distingue par sa simplicité d'implémentation et de maintenance. Chaque fournisseur déploie son propre système d'authentification, reposant le plus souvent sur des identifiants locaux (formulaire *username/password*), éventuellement renforcés par un second facteur (OTP, application d'authentification, clé matérielle ou biométrie), conformément aux facteurs définis par l'ISO/IEC 29115 (International Organization for Standardization, 2013) et aux niveaux d'assurance de Sharif *et al.* (Sharif *et al.*, 2022). À la différence des modèles fédérés, l'usage de protocoles d'interopérabilité (OAuth 2.0, OpenID Connect, SAML, etc voir section 1.1) est minimal ou absent, sauf dans le cas d'intégrations internes. Cette autonomie technologique crée une grande diversité entre les services : certains se limitent à un niveau d'assurance *Low* (mot de passe seul), tandis que d'autres atteignent les niveaux *Substantial* ou *High* grâce à des facteurs matériels et des mécanismes cryptographiques avancés, au prix d'un effort de mise en œuvre et de maintenance entièrement assumé par chaque organisation.

1.3 Architecture fédérée de l'identité numérique

Comme expliqué dans (Gariépy et al., 2023), ce modèle d'architecture a été introduit après le modèle isolé afin de faciliter l'interopérabilité entre différents systèmes et fournisseurs. Dans ce modèle, chaque fournisseur de service délègue le processus d'authentification aux fournisseurs d'identité rattachés à la fédération SSO, qui centralisent la vérification des identités (voir figure 1.3).

Bien qu'il permette de résoudre certains problèmes du modèle isolé, notamment la multiplication des mots

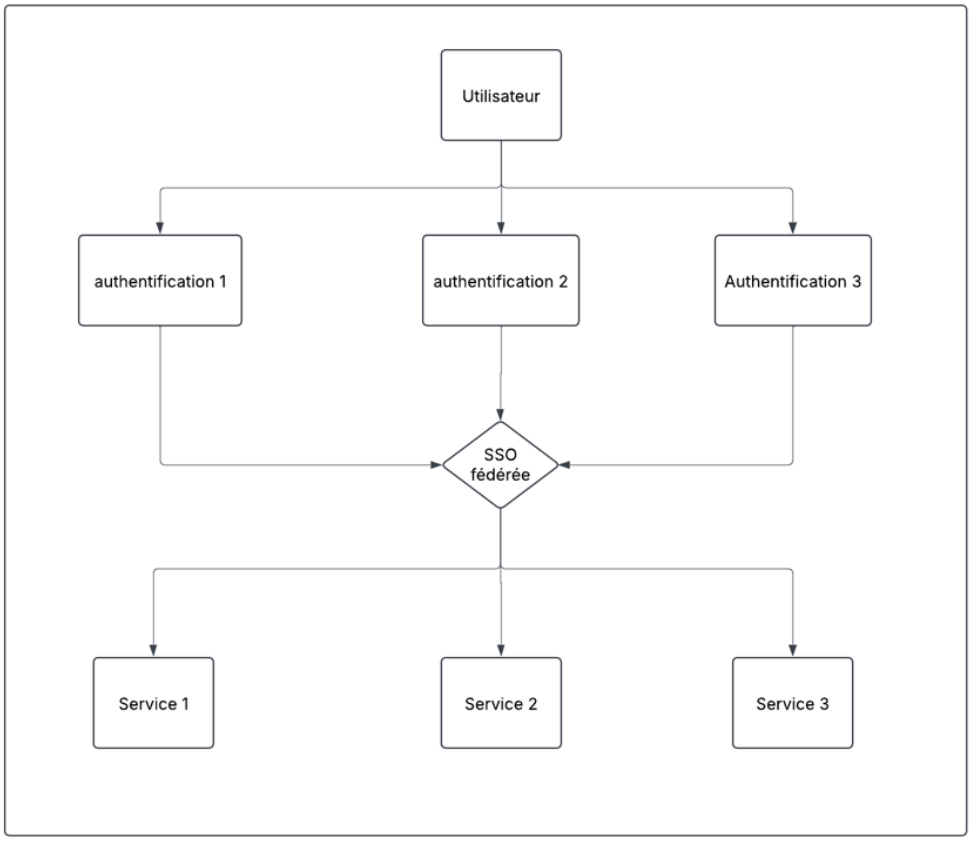

Figure 1.3 Schéma de l'architecture fédérée.

de passe et le manque d'interopérabilité, le modèle fédéré peut lui aussi rencontrer des limites. Lorsque des institutions appartiennent à des fédérations différentes reposant sur des systèmes d'authentification incompatibles, l'interopérabilité devient un défi. Deux options, toutes deux coûteuses ou contraignantes, se présentent alors : soit les utilisateurs doivent gérer manuellement plusieurs identifiants, soit les fédérations doivent procéder à une migration vers un système commun, ce qui implique des efforts techniques et organisationnels importants. Ainsi, le modèle fédéré ne permet pas d'éliminer complètement les enjeux liés à l'interopérabilité (Catuogno et Galdi, 2014).

1.3.1 Fonctionnement technique du modèle fédéré

L'authentification fédérée, souvent appelée Federated SSO, permet à un utilisateur d'accéder à plusieurs services numériques fournis par des organisations distinctes en utilisant les identifiants d'un seul fournisseur d'identité. Ce modèle repose sur une relation de confiance entre les fournisseurs d'identité et les fournisseurs de services, rendue possible grâce à des protocoles d'authentification standardisés tels que SAML, OAuth 2.0

ou OpenID Connect, etc. (voir section 1.1). Il s'appuie sur un mécanisme de Single Sign-On étendu à plusieurs organisations, comme expliqué par Ping Identity (Fantenberg, 2022). Nous nous appuyons ici sur les travaux de (Almeida *et al.*, 2024), (Dimova *et al.*, 2023) ainsi que (Chari *et al.*, 2021), pour illustrer le fonctionnement de ce modèle.

Dans le modèle fédéré, trois rôles principaux se distinguent. *L'utilisateur* est la personne qui possède une identité numérique et souhaite accéder à plusieurs services numériques sans devoir créer un compte distinct pour chacun. *Le fournisseur d'identité* est l'entité qui gère et vérifie l'identité de l'utilisateur, et qui émet des jetons (tokens) ou des assertions (via SAML, OAuth 2.0, OpenID Connect, etc.) pour permettre son authentification auprès de différents fournisseurs de services. Enfin, *le fournisseur de service* correspond à l'application ou au site web qui fait confiance à un ou plusieurs fournisseurs d'identité au sein d'une fédération, afin d'authentifier l'utilisateur et de lui donner accès aux ressources ou services.

Le processus d'authentification dans un modèle fédéré suit généralement les étapes suivantes :

1. **Inscription du fournisseur de service auprès de la fédération.** Le fournisseur de service doit s'inscrire au sein d'une fédération d'identité, ce qui permet d'établir une relation de confiance avec les fournisseurs d'identité. Une fois inscrit, il peut accepter les identités issues de cette fédération pour authentifier ses utilisateurs. *Exemple – eduGAIN (SAML) :* Une université européenne souhaitant offrir des services à des étudiants d'autres établissements doit rejoindre la fédération eduGAIN. Les étudiants peuvent ensuite se connecter avec les identifiants de leur propre université.
2. **Demande d'autorisation.** Lorsqu'un utilisateur souhaite se connecter à un service, le fournisseur de service le redirige vers un fournisseur d'identité reconnu dans la fédération (déterminé automatiquement ou choisi manuellement). Selon le protocole, l'utilisateur visualise les détails du service ainsi que les autorisations demandées. *Exemple – FranceConnect (OAuth 2.0 / OIDC).* Un utilisateur voulant accéder à un service public est redirigé vers FranceConnect, où il choisit son fournisseur d'identité (Impots.gouv, Ameli, La Poste) et accepte le partage d'informations (France Connect, 2024).
3. **Authentification et autorisation.** L'utilisateur saisit ses identifiants sur l'interface du fournisseur d'identité. Une fois authentifié et la demande acceptée, un code d'autorisation est généré pour le fournisseur de service. *Exemple – eduGAIN (SAML).* Un étudiant de l'UQAM souhaitant consulter une ressource académique européenne est redirigé vers l'interface UQAM, sans interaction avec l'université partenaire.
4. **Obtention du jeton d'accès.** Le fournisseur de service échange le code contre un jeton d'accès auprès

du fournisseur d'identité. Ce jeton permet d'accéder aux données ou ressources autorisées sans redemander les identifiants. *Exemple – FranceConnect :* Le service retraite reçoit un jeton d'accès depuis FranceConnect et peut obtenir les informations nécessaires via le fournisseur d'identité sélectionné.

5. **Accès aux ressources.** Avec ce jeton, le fournisseur de service authentifie l'utilisateur localement et lui donne accès aux fonctionnalités prévues. Tant que la session ou le jeton est valide, aucune nouvelle authentification n'est requise. *Exemple – eduGAIN :* Une fois connecté via son université, un étudiant peut naviguer librement entre différents services académiques européens.

L'authentification avec le fournisseur d'identité se fait généralement avec les mêmes technologies que celles utilisées dans le modèle isolé (voir section 1.2). La différence réside dans l'interopérabilité entre les différents systèmes. Pour comprendre ce fonctionnement, nous allons prendre des exemples réels de l'utilisation de quelques protocoles vus dans la section 1.1.

— *OpenID Connect*. FranceConnect peut servir d'exemple pour démontrer l'application du modèle fédéré à l'aide d'OpenID Connect. FranceConnect offre aux citoyens français la possibilité de se connecter à divers services publics en recourant à un compte déjà existant chez un fournisseur d'identité reconnu (tels qu'Impots.gouv, Ameli ou La Poste), évitant ainsi la nécessité de concevoir un nouvel identifiant pour chaque service. Dans ce modèle, les fournisseurs d'identité et les fournisseurs de services sont connectés via une fédération d'identité, avec FranceConnect agissant en tant qu'intermédiaire fiable. Quand un utilisateur désire se connecter à un service web (par exemple : vérification de ses droits à la retraite), il est orienté vers FranceConnect, qui lui offre la possibilité de sélectionner son fournisseur d'identité. Après avoir été authentifié auprès de celui-ci, un jeton d'identité OpenID Connect est créé et envoyé au service sollicité, assurant une authentification sécurisée et interopérable (France Connect, 2024).

— *SAML*. Un bon exemple de modèle fédéré basé sur SAML est celui du réseau eduGAIN, qui permet à des étudiants ou chercheurs d'accéder à des ressources académiques à l'étranger en utilisant les identifiants de leur université. Par exemple, un étudiant de l'UQAM souhaitant accéder à une bibliothèque numérique européenne est redirigé vers une liste de fournisseurs d'identité affiliés. Il sélectionne son université, s'authentifie via la page de connexion de l'UQAM, puis une assertion SAML est générée avec ses informations (identité, rôle, autorisations). Cette assertion est ensuite transmise à la bibliothèque, qui vérifie qu'elle provient d'un fournisseur de confiance selon les règles de la fédération. Si elle est valide, l'accès est accordé sans que l'étudiant ait à créer un compte propre à la bibliothèque (eduGAIN, 2024).

Maintenant que le fonctionnement du modèle fédéré est établi, il est possible d'évaluer dans quelle mesure chacun des protocoles présentés répond aux exigences spécifiques d'une INN.

1.3.2 Évaluation des protocoles d'authentification

Cette étude s'appuie sur les bénéfices identifiés dans l'article « Comparative Analysis and Framework Evaluating Web Single Sign-On Systems » (Alaca et Oorschot, 2020), utilisés ici comme critères pour évaluer les protocoles spécifiques à l'identité numérique. Tous les critères et leur description proviennent de cet article ; seuls deux critères ont été modifiés afin d'ajuster leur formulation et de transposer les résultats dans un contexte d'architecture fédérée, plus pertinent pour l'INN. L'article analyse les systèmes SSO en identifiant 14 critères organisés en quatre catégories principales : facilité d'utilisation, déployabilité, sécurité et confidentialité.

Critères liés à la facilité d'utilisation :

- **C1 – Identité portable à travers les fournisseurs d'identité.** Les utilisateurs peuvent changer de fournisseur d'identité sans devoir recréer ou mettre à jour leurs comptes auprès des fournisseurs de services. Par exemple, si un utilisateur utilise son compte Google pour accéder à plusieurs services, il pourrait décider de passer à un fournisseur d'identité comme Apple ou un service gouvernemental sans perdre l'accès à ces services à condition que le système d'identité supporte cette portabilité. Cela leur donne plus de flexibilité, notamment s'ils changent de préférences en matière de sécurité ou de vie privée.
- **C2 – Pas de configuration d'appareil.** Aucune configuration logicielle ou matérielle n'est nécessaire pour l'utilisateur lors de l'authentification depuis un nouvel appareil, ce qui facilite l'accès aux services, même pour des personnes peu à l'aise avec la technologie.
- **C3 – Aucun jeton matériel requis.** Les utilisateurs n'ont pas besoin de transporter un jeton d'authentification matériel , ce qui réduit les coûts, les risques de perte, et facilite l'accès sur n'importe quel appareil, en particulier pour les environnements à distance ou en mobilité.
- **C4 – Résilience aux pannes temporaires.** Les utilisateurs peuvent continuer à s'authentifier même si le serveur SSO subit une panne temporaire, minimisant ainsi le risque de perte de trafic pour les fournisseurs de services. Par exemple, dans une fédération SSO comme FranceConnect (voir section 1.3.1) si l'un des fournisseurs d'identité partenaires (par ex. L'Identité Numérique La Poste ou Ameli) subit une panne temporaire, les utilisateurs peuvent tout de même accéder à certains services grâce

à une session déjà active ou à un jeton d'authentification encore valide. Cela évite une interruption complète.

Critères liés à la déployabilité :

- **C5 – Absence de validation préalable des fournisseurs d'identité.** Les fournisseurs d'identité n'ont pas besoin de s'enregistrer auprès d'une fédération, ce qui simplifie le déploiement. Cependant, ce critère n'est pas pertinent pour les systèmes d'identité numérique fédérée où la validation des fournisseurs d'identité est essentielle pour garantir sécurité et confiance.
- **C6 – Absence d'enregistrement des fournisseurs de services.** Les fournisseurs de services n'ont pas besoin de s'enregistrer auprès de chaque fournisseur d'identité qu'ils souhaitent utiliser, simplifiant ainsi la gestion des services.
- **C7 – Aucune donnée confidentielle utilisateur stockée par le fournisseur de services.** Le fournisseur de services n'a pas à stocker de mot de passe ou autre secret utilisateur, réduisant ainsi les risques en cas de compromission.

Dans l'analyse comparative proposée (Alaca et Oorschot, 2020), les critères C5 (absence de validation préalable des fournisseurs d'identité) et C6 (absence d'enregistrement des fournisseurs de services) sont présentés comme des avantages dans certains systèmes d'authentification, en raison de la souplesse qu'ils permettent dans le déploiement. Cependant, dans le cadre du modèle fédéré étudié dans ce rapport, ces deux critères ne sont pas appropriés. La validation des fournisseurs d'identité (C5) et l'enregistrement des fournisseurs de services (C6) sont au contraire essentiels pour garantir la sécurité, la traçabilité et la cohérence des relations de confiance au sein de la fédération. Ces critères seront donc reformulés dans notre grille d'évaluation respectivement en *validation préalable des fournisseurs d'identité* pour C5, et *enregistrement des fournisseurs de services* pour C6, afin de mieux refléter les exigences spécifiques du modèle fédéré.

Critères liés à la sécurité :

- **C8a – Résistance aux fuites côté client.** Un attaquant ne peut pas contourner l'authentification en récupérant, à partir du dispositif de l'utilisateur, des éléments sensibles comme des jetons, des mots de passe ou d'autres données d'accès éventuellement exposées en mémoire, sur le disque ou via les frappes clavier.
- **C8b – Résistance aux fuites côté fournisseur de services.** Un attaquant ne peut pas contourner l'authentification en exploitant des données d'authentification sensibles stockées sur les serveurs des fournisseurs de services, telles que des mots de passe, des clés cryptographiques ou des jetons de session.
- **C8c – Résistance aux fuites liées à des tiers.** Les attaquants ne peuvent pas contourner l'authentifica-

tion en accédant aux données d'authentification d'un tiers, un fournisseur d'identité par exemple.

- **C9 – Transmission du niveau d'assurance aux fournisseurs de services.** Les fournisseurs d'identité peuvent transmettre aux fournisseurs de services le niveau d'assurance (LoA) associé à l'authentification de l'utilisateur, afin que ces derniers adaptent le niveau d'accès ou de sécurité en fonction de la robustesse du mécanisme d'authentification utilisé.
- **C10 – Filtrage des fournisseurs d'identité par les fournisseurs de services.** Les fournisseurs de services peuvent choisir les fournisseurs d'identités qu'ils autorisent, selon des critères de sécurité définis.
- **C11 – Protection contre l'usurpation d'identité par des serveurs tiers.** Le système SSO doit empêcher qu'un serveur tiers, y compris un fournisseur d'identité, puisse se faire passer pour un utilisateur sans son consentement. Par exemple, dans une fédération comme FranceConnect, un fournisseur de service compromis ne peut pas exploiter les jetons d'accès émis par FranceConnect pour accéder à d'autres services au nom de l'utilisateur, puisque chaque authentification repose sur un consentement explicite et des jetons d'accès distincts pour chaque session.

Critères liés à la protection de la vie privée

- **C12 – Navigation privée.** Le fournisseur d'identité ne connaît pas les fournisseur de services auxquels ses utilisateurs s'authentifient.
- **C13 Non-traçabilité entre les fournisseurs de services.** Le système empêche les fournisseurs de services de corréler l'activité d'un même utilisateur entre plusieurs plateformes, en évitant la transmission d'un identifiant unique commun. Ainsi, aucun lien ne peut être établi entre les comptes de cet utilisateur sur différents services, ce qui préserve la confidentialité de ses interactions.
- **C14 – Pas de partage des données utilisateur.** Les systèmes qui autorisent les fournisseurs de services à accéder aux données utilisateur ne fournissent pas cet avantage, comme c'est souvent le cas avec OAuth 2.0 et OpenID Connect.

Comparaison des protocoles SSO en fonction des critères. Le tableau qui suit reprend la grille comparative proposée l'article (Alaca et Oorschot, 2020), laquelle évalue plusieurs protocoles d'authentification selon quatorze critères regroupés en quatre catégories : facilité d'utilisation, déployabilité, sécurité et protection de la vie privée. Afin de l'adapter au contexte de l'INN, certains critères ont été reformulés, notamment ceux portant sur la validation préalable des fournisseurs d'identité (C5) et l'enregistrement des fournisseurs de services (C6), qui sont considérés ici comme des exigences incontournables d'une fédération. La logique d'évaluation reste cependant identique à celle de l'étude d'origine.

Afin d'illustrer concrètement comment un protocole fédéré peut répondre aux besoins spécifiques de l'INN,

Protocole	Facilité d'utilisation				Déployabilité			Sécurité				Vie privée		
	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14
OAuth 2.0		•	•			•	•	C8b		•				
OpenID Connect		•	•			•	•	C8b		•				
Mobile Connect		•			•		•	•	•	•			•	
Interac Sign-In	○	•	•		•	•	•	C8b	•	•	†	•	•	•

Table 1.1 Évaluation des protocoles SSO selon les critères de facilité d'utilisation, de déployabilité, de sécurité et de confidentialité pour une architecture fédérée. Case vide - critère non offert, • - critères offert, ○ - critère partiellement offert, C8b - Résistance aux fuites côté fournisseur de services. † - Vulnérable à une usurpation d'identité par l'un des deux acteurs tiers impliqués dans la fédération.

tout en mettant en évidence ses limites, nous allons discuter plus en détail du cas de Interac Sign-In, en nous appuyant sur les informations présentées dans l'article (Alaca et Oorschot, 2020). Ce protocole remplit un grand nombre de critères en matière de facilité d'utilisation, de déployabilité, de sécurité et de protection de la vie privée, ce qui en fait une option solide pour un système fédéré.

- **C1 – Identité portable à travers les fournisseurs de services.** Interac Sign-In attribue à chaque utilisateur un identifiant pseudonyme unique, associé à son fournisseur d'identité de choix. Bien que l'utilisateur puisse changer de fournisseur d'identité au sein de la fédération, un nouvel identifiant pseudonyme est alors généré, ce qui empêche par défaut les fournisseurs de services de reconnaître l'utilisateur comme étant le même. Ainsi, la portabilité est partielle.
- **C2 – Pas de configuration d'appareil.** L'utilisateur n'a besoin d'aucune configuration spécifique de logiciel ou matériel, l'authentification par mot de passe étant suffisante.
- **C3 – Aucun jeton matériel requis.** L'authentification par mot de passe suffit, évitant ainsi le besoin de jeton matériel.
- **C4 – Non-résilience aux pannes temporaires.** Le système n'offre pas de mécanisme de résilience si le fournisseur d'identité est temporairement indisponible. L'utilisateur ne peut pas s'authentifier auprès d'un fournisseur de services sans passer par son fournisseur d'identité, ce qui rend l'accès impossible en cas de panne de ce dernier.
- **C5 – La validation de fournisseur d'identité est requise.** Interac Sign-In requiert que les fournisseurs de services soient approuvés.
- **C6 – Enregistrement des fournisseurs de services requis.** Interac Sign-In prend en charge l'enregistrement des fournisseurs de services à travers une plateforme commune. Cela évite à chaque fournisseur de service de devoir se configurer manuellement avec chaque fournisseur d'identité.

— **C7 – Aucun secret utilisateur stocké par le fournisseur de services.** Les fournisseurs de services ne stockent que les identifiants pseudonymes fournis par Interac Sign-In, minimisant les risques en cas de fuite de données.

— **C8a – Résistance aux fuites côté client.** Ce critère n'est pas pleinement offert pour l'authentification par mot de passe, car les données d'authentification peuvent être extraites d'un appareil compromis.

— **C8b – Résistance aux fuites côté fournisseur de service.** Les fournisseur de services ne stockent aucun secret d'authentification, protégeant ainsi contre les fuites.

— **C9 – Niveau d'assurance transmis aux fournisseurs de services.** Interac Sign-In permet au fournisseur d'identité d'indiquer au fournisseur de services le niveau d'assurance (LoA) de l'authentification de l'utilisateur. Cela permet au fournisseur de services d'ajuster le niveau d'accès accordé selon la fiabilité de l'identité vérifiée.

— **C10 – Les fournisseurs de services peuvent filtrer les fournisseurs d'identité.** Interac Sign-In permet aux fournisseurs de services de sélectionner les fournisseurs d'identité qu'ils souhaitent autoriser pour l'authentification des utilisateurs. Ce filtrage s'effectue parmi les fournisseurs d'identité inscrits dans la fédération Interac Sign-In, ce qui offre aux services un contrôle sur leurs politiques de sécurité et de confiance.

— **C11 – Protection contre l'usurpation d'identité par des serveurs tiers.** Le critère d'absence d'usurpation par un tiers n'est pas satisfait, puisque tant Interac Sign-In que les fournisseurs d'identité peuvent se faire passer pour l'utilisateur.

— **C12 – Navigation privée.** Interac Sign-In masque les informations des utilisateurs pour garantir qu'aucun fournisseur d'identité ne connaît les fournisseurs de services auxquels l'utilisateur se connecte.

— **C13 – Non-traçabilité entre les fournisseurs de services.** Aucun identifiant utilisateur permettant de lier plusieurs fournisseurs de services n'est transmis, évitant toute corrélation entre services.

— **C14 – Pas de partage des données utilisateur.** Interac Sign-In ne communique aucune donnée personnelle à travers le processus d'authentification. Le système se contente de confirmer que l'utilisateur a bien été vérifié par un fournisseur d'identité de confiance, sans dévoiler son identité réelle, ce qui assure la confidentialité des données.

1.4 Architecture décentralisée de l'identité numérique

À l'opposé des approches centralisées, un modèle d'identité décentralisée, souvent appelé identité auto souveraine *Self-Sovereign Identity* ou SSI (Schardong et Custódio, 2022), a émergé dans les dernières années. Contrairement aux modèles isolé et fédéré, qui reposent tous deux sur une autorité centrale chargée de valider ou de gérer l'identité des utilisateurs, le modèle décentralisé a pour objectif principal de donner à l'utilisateur le contrôle total sur ses données personnelles, sans dépendre d'une autorité centrale.

1.4.1 Fonctionnement

Afin d'illustrer concrètement le fonctionnement d'une architecture décentralisée, nous nous basons sur le modèle du SSI présenté par Pohn et al. (Pöhn *et al.*, 2023). Ce modèle propose que chaque utilisateur possède un portefeuille numérique personnel contenant ses justificatifs vérifiables (*verifiable credentials*), comme un diplôme ou une attestation de résidence. Ces justificatifs peuvent ensuite être utilisés pour s'authentifier ou prouver certaines informations, sans avoir à passer par une autorité centrale (voir schéma 1.4).

Dans le cadre du SSI, trois rôles principaux sont définis. Tout d'abord *le détenteur* est l'utilisateur qui possède et contrôle son identité numérique alors que *l'émetteur* correspond à l'entité qui émet les justificatifs numériques, qu'il s'agisse d'une institution ou d'une organisation de confiance. Enfin, *le vérificateur* est l'entité qui examine les justificatifs numériques présentés par le détenteur afin de s'assurer que les informations d'identité sont authentiques et valides. Par exemple, certains systèmes utilisent une liste de vérificateurs de confiance. Avant de partager un justificatif, le portefeuille du détenteur consulte cette liste pour s'assurer que le vérificateur est autorisé à demander ce type d'information (Jeyakumar *et al.*, 2025). **Remarque :** dans le schéma 1.4, les termes « fournisseur d'identité » et « service » sont conservés afin de maintenir une cohérence terminologique avec les architectures isolée et fédérée. Cependant, dans le cadre du SSI, ces rôles correspondent respectivement à l'« émetteur » et au « vérificateur » , tandis que l'utilisateur agit en tant que « détenteur » des justificatifs numériques.

Outre ces rôles, plusieurs composantes sont essentielles au fonctionnement du SSI (Pöhn *et al.*, 2023) :

— **DID (Decentralized Identifiers).** Un DID est un identifiant unique qui permet d'identifier une entité (comme un détenteur, un émetteur ou un vérificateur) sans passer par une autorité centrale. Il peut être enregistré directement dans le registre distribué ou pointer vers une URL servant de point d'accès

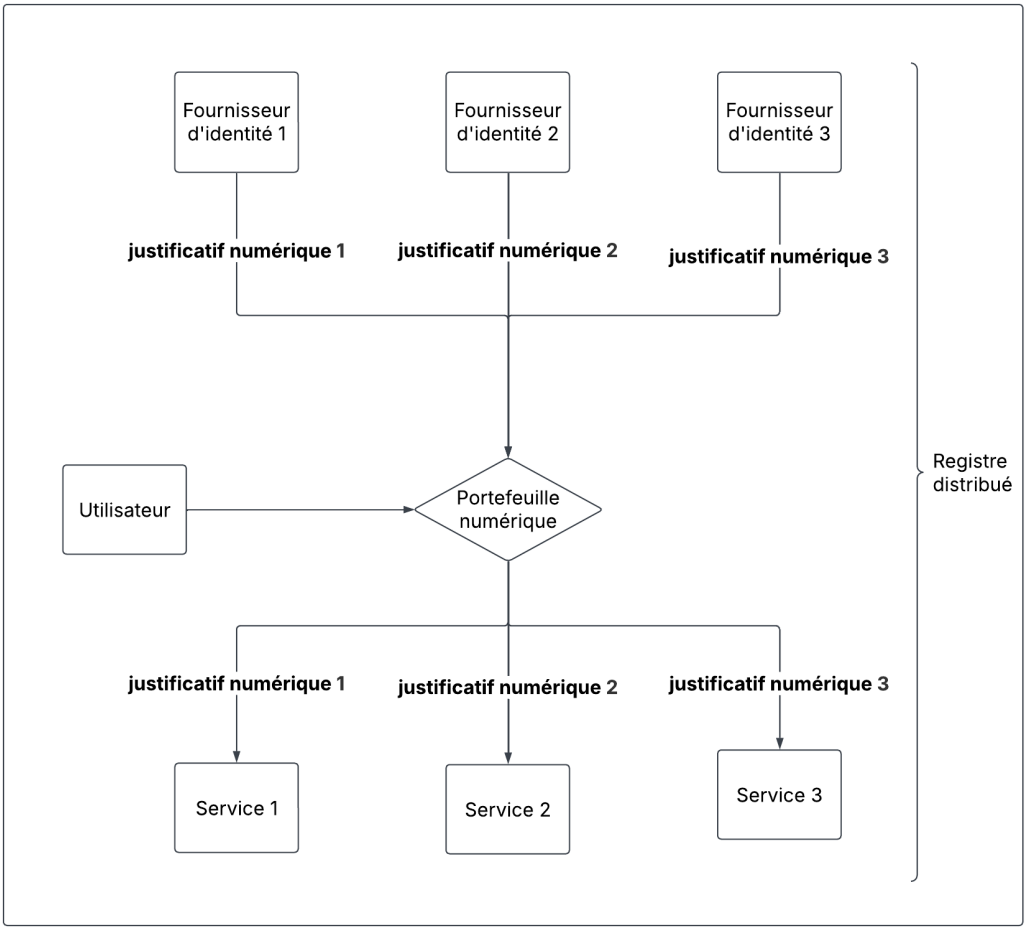

Figure 1.4 Schéma de l'architecture décentralisée.

aux services ou métadonnées associés .

- **Registre distribué.** La technologie décentralisée qui enregistre les transactions. Elle est utilisée pour stocker les identifiants décentralisés (DIDs) et autres métadonnées (par exemple la chaîne de blocs).
- **Certificats.** Preuves numériques de l'identité émises par les émetteurs. Ils sont Utilisés par les détenteurs pour prouver leur identité de manière sécurisée et fiable.
- **Portefeuille.** L'application utilisée par les détenteurs pour gérer leurs identités numériques. Elle permet de stocker, gérer et présenter les justificatifs numériques.

Déroulement du fonctionnement du SSI :

1. **Création de l'identité.** Le détenteur utilise son portefeuille pour générer un identifiant (DID) et publier les métadonnées associées (comme les clés publiques) dans un registre distribué. Ce lien vers le registre permet à d'autres acteurs de retrouver et vérifier les informations nécessaires à l'échange

d'identifiants, tout en assurant traçabilité et intégrité grâce à l'immutabilité du registre.

2. **Émission des certificats.** L'émetteur crée des justificatifs numériques pour le détenteur, contenant des informations vérifiables sur son identité (par exemple, nom, âge, qualifications). Ces certificats sont signés numériquement par l'émetteur. Dans un système décentralisé, le détenteur initie généralement la demande ou accepte une offre d'émission via son portefeuille.
3. **Stockage des certificats.** Le détenteur reçoit les certificats dans son portefeuille. Les certificats sont stockés de manière sécurisée dans l'application de portefeuille, souvent avec des mesures de chiffrement et d'authentification supplémentaires.
4. **Présentation des certificats.** Lorsque le détenteur souhaite prouver son identité ou une information précise, il utilise son portefeuille pour générer une présentation vérifiable (Verifiable Presentation) destinée au vérificateur. Il sélectionne les éléments spécifiques à partager, garantissant ainsi la minimisation des données. Un des avantages clés de ce modèle est que l'utilisateur peut prouver une information sans révéler l'intégralité du justificatif numérique d'origine. Par exemple, il peut prouver qu'il est majeur sans dévoiler sa date de naissance, ni son nom. Cette fonctionnalité permet de renforcer la confidentialité et le contrôle sur les données personnelles (Schardong et Custódio, 2022).
5. **Vérification des certificats.** Le vérificateur reçoit les certificats présentés par le détenteur. Il utilise le DID pour récupérer, via le registre distribué, les métadonnées nécessaires à la vérification (par exemple : clés publiques). Ces éléments lui permettent de s'assurer que les certificats sont authentiques, qu'ils n'ont pas été modifiés, et qu'ils ont bien été émis par une source de confiance.
6. **Validation et autorisation.** Une fois les certificats vérifiés, le vérificateur accorde l'accès ou les privilèges demandés au détenteur en fonction des informations vérifiées.

Cette vérification repose sur plusieurs mécanismes techniques qui permettent d'assurer l'authenticité et la fiabilité des certificats présentés. Les fournisseurs de services peuvent notamment vérifier que le justificatif numérique est signé par une entité de confiance, qu'il n'a pas été falsifié ou modifié et qu'il n'a pas été révoqué (grâce à un registre public). Les technologies comme la chaîne de blocs ou les registres distribués assurent un moyen sécurisé et transparent de publication et de vérification des clés publiques. Grâce à ce mécanisme, l'authentification peut se faire sans interroger directement l'émetteur du justificatif numérique, les clés étant déjà disponibles sur un registre distribué, ce qui garantit un fonctionnement à la fois décentralisé et respectueux de la confidentialité des données (Schardong et Custódio, 2022; Avellaneda *et al.*, 2019). Un utilisateur peut aussi émettre lui-même un justificatif numérique, mais celui-ci sera crédible uniquement si le destinataire a confiance en l'émetteur. Ainsi, même si tout le monde peut créer une identité, la valeur

d'un justificatif numérique dépend toujours de la réputation de l'émetteur (Schardong et Custódio, 2022).

Dans leur article « Decentralized Identity : Where Did It Come From and Where Is It Going ? » (Avellaneda *et al.*, 2019) soulignent que, malgré l'intérêt croissant pour cette approche, plusieurs défis restent à relever pour en faire une réalité à grande échelle. Le principal enjeu demeure la standardisation. Des efforts importants sont en cours, notamment au sein du W3C et de fondations comme la Decentralized Identity Foundation, afin de définir des normes communes garantissant l'interopérabilité et la portabilité des identités. D'autres défis concernent la sécurité, la gestion du cycle de vie des identifiants (perte de clés, portefeuilles, etc.), ainsi que la conformité aux lois sur la vie privée. Par exemple, l'irréversibilité des données inscrites sur blockchain peut entrer en conflit avec le droit à l'oubli. Des solutions doivent donc être pensées à la fois sur les plans technique, juridique et organisationnel. Enfin, l'article souligne que la technologie seule ne suffit pas. Il faut aussi penser à l'expérience utilisateur, à la gouvernance de la confiance entre parties, et à l'adoption de modèles comme les preuves à divulgation nulle de connaissance pour renforcer la confidentialité. L'identité décentralisée repose donc sur un équilibre entre contrôle utilisateur, fiabilité technique et cadres normatifs solides. Suivant cette logique, (Allen, 2016) propose une série de principes fondamentaux pour encadrer une identité vraiment auto-souveraine qui incluent :

- **Existence.** L'identité numérique doit être liée à une personne réelle qui existe indépendamment du système de l'INN. Le système ne crée pas l'individu, il en représente seulement l'existence dans l'espace numérique.
- **Contrôle.** L'utilisateur doit pouvoir gérer son identité, la modifier, la masquer ou la retirer.
- **Accès.** Les utilisateurs doivent toujours pouvoir accéder librement à l'ensemble des données associées à leur identité numérique, sans intermédiaire ni restriction, même s'ils ne peuvent pas forcément les modifier (un utilisateur ne peut pas modifier son diplôme, par exemple), ni accéder à celles des autres.
- **Transparence.** Les systèmes et algorithmes utilisés pour gérer les identités doivent être ouverts et transparents, leur fonctionnement, gestion et mise à jour doivent être accessibles, et les algorithmes doivent être libres, ouverts, largement connus et accessibles à tous, tout en restant indépendants de toute architecture particulière.
- **Persistance.** Les identités numériques doivent pouvoir exister aussi longtemps que nécessaire, mais pouvoir être effacées à la demande.
- **Portabilité.** Les identités numériques doivent être transportables et ne pas dépendre d'une seule entité, même de confiance, car ces entités peuvent disparaître ou changer ; la portabilité garantit que

l'utilisateur garde toujours le contrôle de son identité, peu importe les circonstances, ce qui renforce sa durabilité dans le temps.

— **Interopérabilité.** Les identités numériques doivent être utilisables le plus largement possible, même au-delà des frontières internationales, afin d'avoir une valeur réelle, tout en préservant le contrôle par l'utilisateur et assurant leur disponibilité continue grâce à la persistance et l'autonomie.
— **Consentement.** Le partage des données d'identité doit toujours nécessiter le consentement explicite et éclairé de l'utilisateur, même si ce consentement n'est pas toujours interactif (par exemple, lorsqu'un employeur souhaite vérifier les qualifications professionnelles via un tiers, cela peut être fait de manière transparente, mais uniquement si l'utilisateur a donné son consentement préalable) ; aucun partage ou validation de données ne peut se faire sans cet accord délibéré.
— **Minimisation.** Seules les données strictement nécessaires à une tâche doivent être partagées : par exemple, si seule une preuve d'âge minimum est requise, l'âge exact ne devrait pas être divulgué, et si un simple âge est demandé, la date de naissance complète ne doit pas être partagée.
— **Respect des droits fondamentaux.** « Les droits des utilisateurs doivent être protégés. En cas de conflit entre les besoins du réseau d'identité et les droits des individus, la priorité doit toujours être donnée aux libertés et aux droits des utilisateurs » (Allen, 2016). En pratique, cela veut dire que l'usager doit toujours garder le contrôle sur ses données et sur leur utilisation. Il doit pouvoir prouver qui il est ou retirer son accord sans dépendre d'une entité centrale qui pourrait restreindre, surveiller ou empêcher ses actions liées à la gestion de son identité numérique.

1.4.2 Briques technologiques pour l'architecture décentralisée

Il existe plusieurs approches pour implémenter une identité numérique décentralisée. Dans cette section, on abordera les plus courantes. Chacune repose sur une architecture et des mécanismes cryptographiques différents, avec des implications différentes en matière de vie privée, de traçabilité et de gouvernance de la révocation.

SD-JWT. Le SD-JWT (*Selective Disclosure for JWTs*) est une extension des JWT d'OpenID Connect, fondée sur le mécanisme des JSON Web Signatures (JWS), qui garantit l'intégrité des données échangées. Comme dans OpenID Connect, la minimisation des données s'effectue au moment de l'émission : le serveur détermine quelles informations inclure dans le jeton selon ce qui est nécessaire pour le tiers destinataire (Fett *et al.*, 2025). Le SD-JWT introduit un mécanisme de divulgation sélective des données grâce à l'utilisation de

hachages salés. Pour chaque information que l'utilisateur pourrait vouloir révéler plus tard, l'émetteur (comme une université) n'inclut pas la donnée en clair dans le jeton, mais uniquement son hachage combiné avec un sel aléatoire. Par exemple, au lieu d'écrire '123 Rue Exemple', le SD-JWT contiendra le hachage de cette adresse mélangée à un sel, comme « xy23z ». Plus tard, si l'utilisateur souhaite prouver son adresse, il envoie cette adresse en clair (« 123 Rue Exemple ») ainsi que le sel (« xy23z ») au destinataire. Ce dernier recalcule le hachage avec les deux éléments reçus, et vérifie qu'il correspond bien à celui présent dans le SD-JWT signé (Fett *et al.*, 2025). Pour éviter qu'un SD-JWT soit utilisé sans le consentement du détenteur, le standard introduit aussi un mécanisme de liaison à une clé (*Key Binding*). Ce mécanisme impose que le détenteur prouve qu'il contrôle une clé privée associée au SD-JWT. Cela permet de s'assurer que seul le véritable détenteur peut l'utiliser. Lorsque cette preuve est incluse dans la présentation, on parle alors de SD-JWT+KB (Fett *et al.*, 2025).

BBS+. Le schéma BBS+, dont le nom provient du schéma *BBS* conçu par Boneh, Boyen et Shacham en 2004 (Boneh *et al.*, 2004), a été introduit en 2006 par Au, Susilo et Mu (Au *et al.*, 2006). Il permet de signer simultanément plusieurs informations, telles que le nom, l'âge ou la nationalité d'une personne, à l'aide d'une seule signature de taille fixe, indépendamment du nombre d'attributs signés (Doerner *et al.*, 2023). Ce système est idéal pour les justificatifs numériques anonymes, car il permet de ne révéler qu'une partie des informations si on le souhaite, tout en prouvant qu'elles ont bien été signées grâce à des preuves à divulgation nulle de connaissance (*zero-knowledge proofs*) (Doerner *et al.*, 2023). Pour renforcer la sécurité, les chercheurs proposent aussi une version distribuée de BBS+, appelée threshold BBS+ : la clé de signature est partagée entre plusieurs serveurs, ce qui évite qu'un seul point de défaillance mette le système en danger (Doerner *et al.*, 2023).

SD-BLS. Avec le modèle SD-BLS (*Selective Disclosure using Boneh-Lynn-Shacham* signatures), les chercheurs ont cherché à répondre simultanément à plusieurs limites observées dans BBS+ et SD-JWT : l'absence de mécanismes de révocation respectueux de la vie privée et la centralisation des pouvoirs. Leur objectif était de proposer un cadre cryptographique permettant à un individu de prouver certaines informations (comme sa majorité ou son statut de résident) sans divulguer l'ensemble de ses données personnelles, *tout en intégrant une gouvernance distribuée et un système de révocation anonyme*, afin de renforcer la souveraineté de l'utilisateur dans un contexte réellement décentralisé (Roio *et al.*, 2024). En particulier, cet article explique que SD-BLS repose sur des signatures BLS pour générer des preuves de possession de justificatifs. Lors de l'émission, chaque attribut est signé avec sa clé privée et sa clé de révocation, ce qui permet au détenteur de

prouver un élément spécifique sans révéler les autres. La présentation peut se faire sous forme de preuve simple ou de preuve unique (*One Time Proof*), ajoutant une signature de session pour éviter les attaques de rejeu. La révocation, quant à elle, est opérée par un ensemble d'acteurs à travers un mécanisme de seuil (*threshold revocation*) : une clé de révocation est divisée et distribuée à plusieurs entités et sa reconstitution nécessite l'accord d'un quorum (Roio *et al.*, 2024).

1.4.3 Exemples de mise en œuvre de l'identité numérique décentralisée

L'objectif de cette section est d'examiner quelques exemples de mise en œuvre de l'identité numérique souveraine, en les comparant aux principes de Christopher Allen (Allen, 2016) évoqués précédemment.

EUDI Wallet. Le portefeuille d'identité numérique de l'Union européenne (*EU Digital Identity Wallet*) est un système combinant une architecture décentralisée avec l'architecture fédérée (une gouvernance encadrée par les états membres), applicable aussi bien aux services gouvernementaux que privés. Présenté sous forme d'application, ce système repose sur les principes de l'identité auto-souveraine : chaque utilisateur dispose de ses propres justificatifs numériques vérifiables et détermine librement quand et avec qui ces informations seront partagées (Esther Saurí, 2023). D'après Gataca (Esther Saurí, 2023), le règlement européen sur l'identité numérique laisse à chaque État membre la liberté de déterminer son approche : développer son propre portefeuille, désigner un fournisseur unique ou adopter un modèle de marché ouvert en certifiant plusieurs prestataires privés.

L'EUDI Wallet permet aux citoyens d'accéder à divers services et d'effectuer des transactions dans l'ensemble de l'Union européenne, en ligne comme en personne. Parmi ces utilisations figurent la demande de services publics, l'ouverture de comptes bancaires, les candidatures universitaires, la vérification d'identité, la gestion des prescriptions médicales, ainsi que la sécurisation des transactions, sans avoir à transporter ni documents physiques ni copies numérisées (Esther Saurí, 2023). Le cadre EUDI-ARF (le cadre technique et réglementaire qui définit comment doit être conçu et opéré l'EUDI Wallet) impose l'usage de technologies comme SD-JWT (*Selective Disclosure JSON Web Token*) et mDOC. Or, le SD-JWT repose sur des HMAC (*Hash-Based Message Authentication Codes*) pour générer les preuves, ce qui signifie que chaque présentation d'un même justificatif produit la même preuve, ce qui permet potentiellement de relier plusieurs transactions d'un même utilisateur et compromet l'anonymat (Roio *et al.*, 2024).

Un point clé dans toute architecture d'identité décentralisée est la gestion des révocations (par exemple, la

désactivation d'une carte d'identité volée). Dans le système EUDI, la révocation d'un justificatif est actuellement effectuée par un seul acteur, généralement l'émetteur du justificatif (Roio, 2025). Cette concentration du pouvoir de révocation soulève des préoccupations majeures : un acteur unique peut abuser de ce pouvoir, par exemple en révoquant arbitrairement l'identité de minorités persécutées, journalistes ou opposants politiques (Roio *et al.*, 2024). Ce danger est appelé corruption de l'émetteur (*issuer corruption*) : ainsi si l'autorité qui émet les justificatifs est corrompue, elle peut les révoquer sans contre-pouvoir. Or, dans une architecture réellement auto-souveraine, la gouvernance des révocations devrait être décentralisée, avec plusieurs parties impliquées et un mécanisme de consensus comme vu dans la section 1.4.2. Cependant, même si le rôle principal de l'EUDI était de transformer l'identité numérique en un système auto-souverain, où l'utilisateur aurait un contrôle total sur ses données, ce sont en réalité les États et certains grands fournisseurs technologiques qui conservent une influence significative sur l'infrastructure et la gouvernance de l'écosystème (Roio, 2025).

Évaluation selon les principes de Christopher Allen (voir section 1.4.1). L'approche décrite dans le cadre de référence technique (EUDI-ARF) pour le portefeuille d'identité numérique européenne repose sur les recommandations formulées par le groupe d'experts eIDAS, tel que précisé dans le document de référence (eIDAS Expert Group, 2024). Bien que ce document ne soit pas juridiquement contraignant et qu'il ne préjuge pas des décisions finales des co-législateurs, il constitue néanmoins la base technique actuelle pour le développement des implémentations et des spécifications du portefeuille EUDI. Le cadre ARF est donc utilisé comme référence principale pour orienter le développement de l'infrastructure, tout en restant susceptible d'être révisé ou ajusté à la suite des consultations et des évolutions législatives.

- **Existence : *globalement respectée*.** L'identité numérique repose sur des identités légales déjà établies. Le portefeuille EUDI ne remplace pas l'existence légale, il la prolonge numériquement.
- **Contrôle : *partiellement respecté*.** L'utilisateur contrôle l'usage de ses justificatifs (quand et avec qui il les partage), mais ne contrôle pas leur création ni leur révocation. Ces opérations sont centralisées entre les mains de l'émetteur, souvent un organisme public ou accrédité (eIDAS Expert Group, 2024).
- **Accès : *globalement respecté*.** Les utilisateurs ont accès à leurs justificatifs dans le portefeuille. Ils peuvent les consulter, les stocker et les présenter de manière autonome.
- **Transparence : *partiellement respectée*.** Bien que l'UE promeuve l'interopérabilité et des normes ouvertes, la gouvernance réelle du système (algorithmes de révocation, règles d'interopérabilité, etc) n'est pas encore entièrement transparente ni standardisée au niveau de l'implémentation par

chaque État membre.

- **Persistance : *partiellement respectée*.** Les identités peuvent persister tant que l'État membre les considère valides. Cependant, un émetteur unique peut révoquer un justificatif à tout moment, sans qu'un mécanisme distribué ne protège l'utilisateur contre les abus (Roio, 2025).
- **Portabilité : *globalement respectée*.** L'EUDI Wallet est conçu pour être utilisé à travers tous les États membres de l'UE et pour accéder à divers services publics et privés. Il vise une portabilité européenne harmonisée.
- **Interopérabilité : *globalement respectée*.** L'EUDI s'appuie sur des standards internationaux tels que SD-JWT pour garantir une compatibilité technique à travers les États membres. Cependant, certaines limitations cryptographiques inhérentes à ces technologies compromettent une interopérabilité parfaitement harmonisée. En particulier, SD-JWT utilise des HMAC pour générer des preuves, mais ces HMAC sont statiques pour un même justificatif, rendant possible le traçage des transactions basées sur le même justificatif (Roio *et al.*, 2024). Cette approche peut créer des divergences dans l'implémentation de SD-JWT, certains États pouvant tenter d'atténuer ce problème de traçabilité en modifiant la structure des HMAC, nuisant ainsi à l'interopérabilité globale .
- **Consentement : *globalement respecté*.** Le consentement est globalement respecté, permettant à l'utilisateur de choisir à la fois quand et quelles données partager. Le règlement souligne que « les portefeuilles européens d'identité numérique doivent exiger une confirmation sécurisée, explicite et active de l'utilisateur pour chaque opération réalisée via ces portefeuilles » (Parlement Européen et Conseil de l'Union Européenne, 2024).
- **Minimisation : *partiellement respectée*.** L'usage du SD-JWT avec HMAC signifie que plusieurs présentations du même justificatif génèrent la même preuve, ce qui permet de relier les usages et limite la minimisation réelle en pratique (Roio *et al.*, 2024).
- **Respect des droits fondamentaux : *partiellement respectée*.** Le RGPD encadre fortement l'usage des données. Néanmoins, la concentration des pouvoirs (ex : révocation par un seul émetteur) et l'absence de mécanisme de gouvernance distribuée exposent l'utilisateur à des risques de révocation arbitraire ou de mauvaise gestion de son identité numérique (Roio, 2025).

RealDID. Dans cette section, nous nous appuyons sur les informations fournies dans le site officiel de *RealDID* (BSN Development Association, 2024). RealDID est la solution d'identité numérique développée par la Chine, fondée sur l'utilisation de clés publiques et privées. Un utilisateur peut générer et utiliser plusieurs clés publiques au sein du système RealDID, chaque clé étant associée à sa véritable identité validée par CTID (la

plateforme nationale chinoise qui valide l'identité réelle des utilisateurs), tout en restant techniquement distincte des autres. Le système a plusieurs cas d'usage : confirmer les droits d'accès aux données personnelles par signature cryptographique, transférer de façon sécurisée des données chiffrées entre entreprises, ou établir une connexion pseudonyme à des services en ligne. Dans ce dernier cas, l'utilisateur peut prouver certains attributs (par exemple être majeur) sans révéler directement son nom réel au fournisseur de service, même si cette identité reste connue de la plateforme CTID en arrière-plan. D'autres cas d'usage incluent l'émission de certificats d'identité vérifiés par CTID (nom, photo, carte officielle) et la divulgation sélective d'informations selon le contexte, bien que cette minimisation dépende de l'implémentation des services connectés.

Évaluation selon les principes de Christopher Allen (voir section 1.4.1). Le système RealDID peut être évalué à l'aide des dix principes vus précédemment, qui définissent les fondements d'une identité auto-souveraine. Voici l'analyse de chaque principe, appliquée à l'architecture actuelle du RealDID :

- **Existence : *globalement respecté*.** RealDID s'appuie sur l'identité légale existante de l'utilisateur, sans créer une identité fictive détachée de la personne réelle.
- **Contrôle : *partiellement respecté*.** L'utilisateur peut utiliser son DID pour signer ou s'authentifier, mais il ne contrôle pas directement la création, la révocation ou la gestion des DIDs, qui restent entre les mains des autorités centrales.
- **Accès : *partiellement respecté*.** L'utilisateur n'a pas accès, de manière directe et autonome, à l'ensemble des données personnelles validées par la plateforme CTID, qui reste sous le contrôle des autorités. L'accès à ces données ne se fait que via des portails ou services officiels, ce qui limite la transparence attendue (BSN Development Association, 2024).
- **Transparence : *non-respecté*.** Les mécanismes de vérification, la gouvernance et les algorithmes utilisés par RealDID ne sont pas publics ni open-source, rendant impossible tout audit externe indépendant.
- **Persistance : *présumée mais non garantie*.** Aucune documentation officielle ne précise si l'autorité centrale peut désactiver un identifiant RealDID, ni si l'utilisateur peut en demander la suppression complète.
- **Portabilité : *non-respectée*.** L'identité RealDID est liée à l'écosystème BSN/CTID. Elle ne peut pas être transférée vers d'autres systèmes indépendants et reste dépendante de l'infrastructure chinoise centralisée.
- **Interopérabilité : *partiellement respectée*.** Le système peut être utilisé par plusieurs entreprises ou

plateformes chinoises, mais il est conçu pour rester dans l'écosystème national. Il n'existe pas de compatibilité native avec d'autres standards internationaux.

- **Consentement : *partiellement respecté*.** Le partage de données repose sur des signatures ou autorisations de l'utilisateur, mais comme l'identité est vérifiée à la source (CTID), le contrôle réel du consentement reste limité, notamment en cas de demande gouvernementale.
- **Minimisation : *partiellement respecté*.** Le système prévoit la divulgation sélective d'attributs, mais son efficacité dépend de la mise en œuvre par les services connectés et reste limitée par l'architecture centralisée.
- **Protection : *non-respecté*.** Les droits de l'utilisateur ne sont pas priorisés en cas de conflit avec l'État ou les opérateurs. La gouvernance centralisée, les obligations de coopération avec les autorités, et l'absence de recours indépendants affaiblissent la protection réelle de l'utilisateur.

Ce chapitre a permis de présenter les principaux fondements techniques de l'identité numérique. L'analyse des différentes architectures isolée, fédérée et décentralisée a mis en évidence leurs caractéristiques, leurs avantages ainsi que les enjeux qu'elles soulèvent en matière de gestion des identités et de protection de la vie privée. L'étude des protocoles d'authentification et des niveaux d'assurance a également permis de mieux comprendre les mécanismes techniques qui soutiennent ces architectures et qui permettent de sécuriser l'accès aux services numériques.

Toutefois, la mise en œuvre d'une INN ne repose pas uniquement sur des considérations techniques. Elle soulève également une question plus fondamentale : comment définir ce qu'est réellement une INN et quels éléments doivent être pris en compte dans sa conception et son déploiement. Le chapitre suivant s'intéresse précisément à cette question en examinant les réflexions et préoccupations exprimées par différents acteurs dans le cadre des consultations publiques entourant le projet de loi n°82.

CHAPITRE 2
ANALYSE DES ENJEUX SOULEVÉS PAR LES MÉMOIRES DÉPOSÉS DANS LE CADRE DU PROJET DE LOI 82

Dans le cadre des consultations publiques organisées par l'assemblée nationale, plusieurs mémoires ont été soumis en fin janvier 2025, apportant un éclairage sur les défis, les attentes et les inquiétudes soulevés par la mise en œuvre de l'INN. Ces mémoires ne se contentent pas de critiquer ou d'appuyer la démarche gouvernementale : ils révèlent les tensions entre, d'un côté, la volonté de moderniser les services publics à travers une solution numérique unifiée et, de l'autre, la nécessité de préserver la vie privée, l'autonomie des institutions, la souveraineté des données et l'équité d'accès aux services. Ils permettent ainsi de mieux comprendre les conditions essentielles à réunir pour garantir un déploiement responsable, inclusif et sécuritaire de l'INN. Cette section présente les principaux enjeux soulevés dans ces documents afin de situer clairement le contexte dans lequel s'inscrit la problématique de ce mémoire.

2.1 Clarté juridique et responsabilité

Sur le plan juridique, certaines dispositions du projet de loi soulèvent des interrogations. L'article 10.6, par exemple, confie au ministère de la cybersécurité et du numérique le rôle de source officielle des données numériques gouvernementales. Il l'autorise également à « recueillir, utiliser ou communiquer » ces données, y compris des renseignements personnels, « auprès de toute personne » (Assemblée Nationale du Québec, 2024). Pour le mouvement Desjardins (Mouvement Desjardins, 2025), cette formulation manque de clarté et il serait préférable de préciser dès le premier alinéa que cela s'applique autant aux personnes physiques qu'aux personnes morales. Il souligne également l'absence de mécanismes de responsabilité clairement établis : à ce jour, le projet de loi ne prévoit aucune disposition en cas d'utilisation frauduleuse des attestations numériques ou d'erreurs dans le traitement des renseignements personnels, ce qui pourrait nuire à la confiance du public.

À ce sujet, La CAI (Commission d'accès à l'information du Québec (CAI), 2025) recommande d'ajouter des recours clairs pour les citoyens qui souhaiteraient contester une utilisation inappropriée de leurs données ou corriger une erreur liée à l'INN. La CAI déplore également l'absence de sanctions prévues en cas de non-respect des règles, ce qui affaiblit l'application concrète des règles prévues par la loi. Elle propose donc d'introduire des obligations précises pour les acteurs concernés ainsi que des sanctions applicables en cas d'infraction, afin de renforcer la protection des droits des citoyens. L'article 11 oblige les organismes

touchés par un incident de sécurité à en informer le ministre de la cybersecurité. Toutefois, aucun mécanisme clair n'est prévu pour vérifier que cette obligation est respectée, ni pour imposer des sanctions en cas de manquement (Leclerc, 2025).

Au-delà des enjeux juridiques et de protection des droits individuels, l'Obvia souligne que le projet de loi 82 met principalement l'accent sur la centralisation de la gouvernance des infrastructures et des services de télécommunications, sans toutefois encadrer de manière claire la gestion des ressources informationnelles, financières et humaines, pourtant essentielles à une mise en œuvre efficace de l'identité numérique nationale (Loiseau *et al.*, 2025).

2.2 Gestion centralisée de la gouvernance numérique

Cette gouvernance unifiée se manifeste aussi dans les pouvoirs conférés au ministre responsable. L'article 10.7 du projet de loi lui permet d'ajouter « toute autre fonctionnalité déterminée par règlement » au registre de l'identité numérique nationale (Assemblée Nationale du Québec, 2024). Cette grande marge de manœuvre soulève de fortes préoccupations, notamment parce qu'elle permet de modifier la portée du système sans débat parlementaire. Comme le souligne la Ligue des droits et libertés (LDL), cela revient à accorder « une carte blanche sur un élément fondamental du système » (Ligue des droits et libertés, 2025), avec un risque d'extension non encadrée de la collecte ou de l'utilisation des données personnelles.

De plus, le Comité de parents du Centre de services scolaire de la Capitale souligne que le MCN pourrait imposer ses directives aux établissements scolaires, remettant en question l'autonomie des conseils d'administration et des enseignants, ainsi que la capacité des écoles à choisir les outils numériques les plus adaptés aux besoins de leurs élèves. Une telle gouvernance pourrait également influencer la gestion des infrastructures technologiques des centres de services scolaires. L'identité numérique risquerait d'être imposée dans des démarches comme l'inscription scolaire, l'accès aux résultats ou l'utilisation de services éducatifs en ligne. Or, la création d'une identité numérique dès la naissance soulève des enjeux majeurs de protection des données et de surveillance (Comité de parents du Centre de services scolaire de la Capitale, 2024).

La Fédération des cégeps insiste par ailleurs sur le manque de consultation dans l'élaboration du projet de loi (Fédération des cégeps, 2025). Elle recommande qu'un véritable dialogue soit instauré avec les parties concernées, afin d'assurer une gouvernance numérique adaptée aux réalités de terrain. Cette centralisation

menace aussi des infrastructures existantes comme le Réseau d'informations scientifiques du Québec (RISQ), essentiel pour les cégeps et les universités (Fédération des cégeps, 2025). L'obligation d'utiliser exclusivement les infrastructures du MCN pourrait fragiliser ce réseau, qui joue un rôle clé dans la qualité et la sécurité des communications dans l'enseignement supérieur et la recherche scientifique.

2.3 Centralisation des données et cybersécurité

Plusieurs mémoires alertent également sur les risques liés à la centralisation de l'identité numérique sous l'autorité du MCN (Ligue des droits et libertés, 2025; Institut de gouvernance numérique (IGN), 2025). Regrouper autant de renseignements personnels dans un seul registre augmente les risques de fuites de données, de surveillance ou de mauvaise utilisation. Le projet de loi ne précise pas si les données seront hébergées au Québec ou à l'étranger, ce qui soulève des inquiétudes concernant leur protection (Ligue des droits et libertés, 2025). Pour limiter ces dangers, certains recommandent de réduire les données collectées au strict minimum (Syndicat de la fonction publique et parapublique du Québec (SFPQ), 2025), d'envisager une architecture décentralisée comme en Estonie ou avec FranceConnect (Institut de gouvernance numérique (IGN), 2025), et de mieux encadrer l'usage de données techniques comme l'adresse IP (Commission de l'éthique en science et en technologie (CEST), 2025). D'autres demandent plus de transparence sur les choix techniques pour permettre une évaluation dès la conception (Loiseau *et al.*, 2025).

Les articles 10.9 et 10.10 permettent au gouvernement de fixer par règlement les normes de sécurité et d'usage des données biométriques, mais sans contrôle indépendant. Cela soulève des inquiétudes sur la fiabilité du système. À ce sujet, plusieurs mémoires recommandent que la CAI valide tout changement futur (Mouvement Desjardins, 2025; Syndicat de la fonction publique et parapublique du Québec (SFPQ), 2025). De plus, la CAI insiste pour que des normes minimales soient définies avant le déploiement de l'INN dans les organismes publics, comme un registre des preuves pour toute attestation numérique (Commission d'accès à l'information du Québec (CAI), 2025). Sans cadre clair dès le départ, la gouvernance risque de devenir incohérente.

Pour garantir une gestion responsable, le Comité de parents (Comité de parents du Centre de services scolaire de la Capitale, 2024) recommande de prévoir des sanctions en cas de mauvaise gestion des données, incluant les ministres, fonctionnaires et sous-traitants. L'Association québécoise des technologies (AQT) (Association québécoise des technologies (AQT), 2025) propose d'outiller les citoyens en mettant à leur disposition un journal des accès, des notifications en cas de consultation de leurs données, ainsi qu'une

obligation d'authentification forte. Enfin, l'Institut multidisciplinaire en cybersécurité et cyberrésilience (IMC2) (Institut multidisciplinaire en cybersécurité et cyberrésilience (IMC²), 2025) recommande d'encadrer plus strictement les mécanismes d'authentification, notamment en imposant l'usage de l'authentification à plusieurs facteurs et en interdisant les questions secrètes, jugées peu sécuritaires.

2.4 Profilage

La question du profilage suscite également de fortes inquiétudes. L'article 10.7 du projet de loi n° 82 définit le profilage comme : « Le profilage s'entend de la collecte et de l'utilisation de renseignements personnels afin d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou du comportement de cette personne. » (Assemblée Nationale du Québec, 2024) Bien qu'une interdiction spécifique s'applique au ministre concernant l'usage des données de l'INN à des fins de profilage (Assemblée Nationale du Québec, 2024), cette mesure ne couvre pas les autres entités publiques ou privées. La CAI recommande donc d'interdire explicitement tout usage des données à des fins non prévues par la loi (Commission d'accès à l'information du Québec (CAI), 2025).

D'autre part, la Commission de l'éthique en science et en technologie (Commission de l'éthique en science et en technologie (CEST), 2025) appelle à élargir la définition du profilage, notamment au profilage social, qui peut entraîner des traitements discriminatoires. De son côté, la LDL (Ligue des droits et libertés, 2025) alerte sur le risque d'usages détournés, comme les enquêtes policières, et insiste pour que l'INN reste strictement limitée à l'identification et à l'authentification. En lien avec cela, l'article 10.9 permet l'usage de données biométriques comme la reconnaissance faciale sans encadrement clair (Assemblée Nationale du Québec, 2024), alors que la CAI rappelle les risques de biais, de fuites et de discriminations liés à ce type de technologie (Commission d'accès à l'information du Québec (CAI), 2025).

2.5 Exclusion numérique

Plusieurs mémoires soulignent aussi les risques d'exclusion sociale liés à l'implantation de l'INN, en plus des enjeux de sécurité et de gouvernance. En particulier, les personnes moins à l'aise avec les outils numériques pourraient avoir de la difficulté à accéder aux services publics. Bien que l'article 10.3 affirme que l'INN ne sera pas obligatoire (Assemblée Nationale du Québec, 2024), environ 25% des Québécois n'utilisent pas les services en ligne, notamment en raison de leur âge, de leur niveau d'éducation, de leur revenu ou de leur

statut d'immigration (Hébert *et al.*, 2024). Or, le projet de loi ne précise pas quelles alternatives concrètes seront proposées aux personnes qui refusent ou ne peuvent pas utiliser l'INN, comme les démarches en personne ou l'usage d'identifiants papier (Mouvement Desjardins, 2025). Fixer des cibles d'utilisation suggère que l'INN pourrait être favorisée, au détriment des solutions traditionnelles (Regroupement des groupes populaires en alphabétisation du Québec (RGPAQ), 2025), alors même que les services en personne sont déjà en recul (Ligue des droits et libertés, 2025).

L'Aide Pédagogique aux Adultes et aux Jeunes (APAJ) insiste sur l'impact direct pour les personnes en situation de vulnérabilité, notamment celles ayant peu de littératie numérique ou vivant dans la précarité. Elle rappelle qu'une personne sur quatre au Québec a déjà de la difficulté à naviguer sur Internet, et que l'absence de solutions accessibles, comme le téléphone ou des services physiques, pourrait accentuer leur marginalisation (Aide Pédagogique aux Adultes et aux Jeunes (APAJ), 2025). Elle s'inquiète aussi de l'ampleur de la collecte de données personnelles, notamment biométriques, et de l'insuffisance des garanties encadrant leur utilisation. Pour éviter cette dérive, le Syndicat de la fonction publique et parapublique du Québec (Syndicat de la fonction publique et parapublique du Québec (SFPQ), 2025) recommande de supprimer l'objectif d'un accès « entièrement numérique » dans la Loi sur la gouvernance et la gestion des ressources informationnelles. La CAI propose également de confier à un organisme indépendant la surveillance de l'application de la loi, afin d'éviter que l'INN ne devienne une obligation de fait (Commission d'accès à l'information du Québec (CAI), 2025). Enfin, la LDL demande que les services publics restent accessibles en format traditionnel, dans des conditions équivalentes aux services numériques, pour assurer une égalité réelle d'accès (Ligue des droits et libertés, 2025). En complément, le mémoire de Steve Waterhouse (Steve Waterhouse, 2025) met l'accent sur la nécessité d'accompagner la mise en œuvre de l'INN par des formations accessibles et des interfaces simples, afin de garantir son adoption inclusive. Il insiste aussi sur le rôle fondamental de la confiance du public, qui repose sur des actions concrètes de sensibilisation et d'éducation au numérique.

Un autre enjeu important concerne le manque de dialogue avec les parties prenantes dans le développement de l'INN. Le mémoire de Guylaine Leclerc souligne qu'un manque de consultation peut mener à un décalage entre les besoins réels des utilisateurs et les services offerts. Le mémoire recommande au ministère de la Cybersécurité et du Numérique d'engager un dialogue avec les citoyens, les organismes publics et les professionnels concernés afin d'assurer la pertinence du système et l'adhésion de la population. À défaut, il existe un risque d'accentuer les inégalités d'accès, en particulier pour les personnes les plus vulnérables (Leclerc, 2025). Ce besoin d'implication touche aussi les milieux professionnels, comme celui des juristes. La Chambre

des notaires souligne que l'INN aura un impact majeur sur leur pratique, les notaires étant légalement tenus de vérifier l'identité des parties lors de nombreuses démarches (contrats de mariage, testaments, ventes immobilières, etc.) (Chambre des notaires du Québec, 2025). Elle recommande que l'INN intègre une photo d'identité et que la profession soit consultée dès la conception du système, afin d'assurer la conformité aux obligations légales et la sécurité des transactions.

2.6 Hébergement et gouvernance

L'Obvia insiste sur la nécessité de renforcer la transparence du projet de loi en définissant clairement le cadre des partenariats public-privé et la localisation des données gouvernementales et des attestations numériques. Il est essentiel de garantir que ces données restent sous juridiction québécoise afin de préserver la souveraineté numérique et de limiter les risques liés à leur externalisation (Loiseau *et al.*, 2025).

L'hébergement des données de l'INN suscite de vives inquiétudes, notamment en raison de la dépendance potentielle à des fournisseurs étrangers comme Microsoft ou Amazon (AWS). Un tel choix, qui externalise la gestion des données hors du Québec, accroît les risques en matière de cybersécurité, de protection de la vie privée des utilisateurs et de résilience des systèmes, particulièrement en contexte de tensions géopolitiques. Le mémoire de Micrologic (Micrologic, 2025) avertit également du danger d'un verrouillage technologique : le recours systématique aux GAFAM enferme les institutions dans des écosystèmes difficiles à quitter. Cette dépendance, renforcée par le rôle du courtier infonuagique permettant d'attribuer des contrats sans appel d'offres, nuit à la souveraineté technologique du Québec et désavantage les entreprises locales.

Face à ces enjeux, plusieurs mémoires recommandent de favoriser les infrastructures locales pour limiter les risques juridiques et stratégiques liés à l'externalisation. Le Réseau d'informations scientifiques du Québec (Réseau d'informations scientifiques du Québec (RISQ), 2025) propose d'utiliser ses infrastructures existantes pour soutenir l'INN, afin d'éviter les redondances, d'optimiser les ressources publiques et de mieux protéger les données sensibles.

2.7 Interopérabilité

L'article 10.8 permet au gouvernement d'établir des ententes pour rendre l'INN interopérable avec d'autres infrastructures, mais il reste à clarifier si cela concernera uniquement des collaborations entre gouvernements ou si les entreprises privées, comme les institutions financières, pourront également utiliser ces attestations

numériques à des fins d'identification et d'authentification (Mouvement Desjardins, 2025). D'autre part, l'interopérabilité de l'INN devrait être garantie non seulement au sein des services gouvernementaux, mais également avec les gouvernements provinciaux et fédéraux, ainsi qu'avec les institutions financières et les commerçants, afin de ne pas pénaliser les citoyens québécois dans leurs transactions quotidiennes (Steve Waterhouse, 2025).

De plus, la LDL (Ligue des droits et libertés, 2025) indique que l'absence de réglementation claire encadrant l'interopérabilité de l'INN avec d'autres systèmes soulève des préoccupations quant à la protection des renseignements personnels :

> *« Une interopérabilité avec toute personne ou entité tant locale qu'internationale, sans critères ni restrictions prédéfinies, paraît excessivement large et hasardeuse. Au minimum, l'interopérabilité doit préalablement et obligatoirement exclure toute personne ou entité, étatique ou privée, qui ne respecte pas les droits humains et les droits à la vie privée, ou qui aurait commis ou facilité de graves violations à cet égard. »*

Dans ce contexte, le Comité de parents (Comité de parents du Centre de services scolaire de la Capitale, 2024) demande l'exclusion des projets en ressources informationnelles menés par les établissements scolaires, les centres de services scolaires et les commissions scolaires du cadre d'application du PL 82. Cette recommandation vise à préserver l'autonomie des écoles et à garantir que les outils numériques utilisés à des fins pédagogiques ne soient pas soumis aux mêmes contraintes administratives que les infrastructures gouvernementales. De plus, le comité insiste sur la nécessité de soumettre à une vérification des antécédents judiciaires toute personne désignée par le MCN qui pourrait avoir accès aux établissements scolaires, afin d'assurer la sécurité des élèves.

Enfin, la question de l'identification physique reste aussi centrale dans les débats. La RAMQ considère que l'introduction de l'INN met en lumière l'absence d'une carte d'identité nationale au Québec. Actuellement, la carte d'assurance maladie est souvent utilisée à des fins d'identification, ce qui dépasse sa fonction initiale liée à l'accès aux soins de santé. La RAMQ propose donc que la création de l'INN soit accompagnée du développement d'une carte d'identité nationale distincte, accessible à l'ensemble des résidents du Québec, indépendamment de leur admissibilité à l'assurance maladie. Une telle initiative permettrait non seulement de clarifier le rôle de la carte d'assurance maladie, mais aussi d'uniformiser l'identification des citoyens pour divers services, qu'ils soient numériques ou physiques. De plus, cette approche pourrait faciliter la transition vers une identité numérique en offrant une alternative tangible pour les populations qui éprouvent des

difficultés à accéder aux services en ligne (Président-directeur général de la Régie de l'assurance maladie du Québec, 2025).

2.8 L'adoption de la loi 82

La loi nº 82 a été sanctionnée en octobre 2025, à la suite des consultations publiques tenues au début de l'année. Malgré les multiples inquiétudes soulevées dans les mémoires, la structure globale du projet de loi a largement conservé sa forme initiale. Les articles présentés dans les sections précédentes ont été conservés tel quel dans la version définitive, sans changements majeurs.

Trois aspects principaux ont été modifiés dans le cadre de la révision de la loi. Premièrement, le MCN est désormais tenu de consulter le public avant de mettre en place la première réglementation concernant l'usage des données biométriques. Cette initiative répond aux appels à la transparence formulés dans les mémoires, puisqu'ils imposent au ministère de clarifier et d'expliquer ses décisions. Cependant, cette consultation n'impose pas une restriction véritable sur l'utilisation des données biométriques : elle crée un moment d'interaction sans toutefois instaurer un contrôle plus clair. Ensuite, la loi introduit une nouvelle disposition visant à renforcer la « souveraineté numérique » du Québec. L'article 19.2 prévoit en effet que « Le ministre peut développer des moyens visant à renforcer la souveraineté numérique en matière de gouvernance et de gestion des ressources informationnelles, notamment en ce qui a trait aux données numériques gouvernementales qui comprennent des renseignements personnels sensibles » (Assemblée Nationale du Québec, 2024). Cette addition peut être interprétée comme une réponse aux préoccupations exprimées dans les mémoires concernant la dépendance du gouvernement envers des fournisseurs étrangers. Toutefois, la portée de cette disposition demeure limitée : elle confère un pouvoir discrétionnaire (« peut développer des moyens ») sans imposer d'obligations concrètes, par exemple l'hébergement obligatoire des données au Québec. L'absence de mesures contraignantes réduit donc la capacité de cette modification à répondre pleinement aux enjeux soulevés. Enfin, un chapitre a été ajouté pour autoriser des projets pilotes de services judiciaires numériques. Même si cette évolution élargit le numérique au domaine judiciaire, elle reste indépendante à l'INN et ne répond pas aux défis soulevés dans les mémoires.

Globalement, ces ajustements démontrent que certaines inquiétudes ont été prises en compte, néanmoins ils demeurent restreints et ne remettent pas en cause les bases du modèle examiné. Les défis mis en lumière dans les mémoires, y compris la centralisation de la gouvernance, les risques liés à l'usage des données biométriques, les mécanismes de responsabilité et les risques d'exclusion numérique, demeurent donc

pertinents pour l'analyse.

2.9 Conclusion

En conclusion, l'analyse des mémoires déposés montre que le projet de loi sur l'INN soulève plusieurs enjeux importants. Même si la volonté de moderniser les services publics est globalement bien accueillie, les mémoires présentés précédemment rappellent que cette transformation doit se faire avec prudence et transparence. Les préoccupations portent surtout sur le manque de clarté juridique, la centralisation de la gouvernance, les risques liés à la sécurité des données, le profilage, l'exclusion numérique et la dépendance envers des fournisseurs étrangers.

Dans l'ensemble, les mémoires insistent sur la nécessité d'un cadre clair pour définir les responsabilités, d'une meilleure protection des renseignements personnels et d'une participation plus ouverte des citoyens et des professionnels concernés. Ils soulignent aussi l'importance d'offrir des solutions accessibles à tous, afin que personne ne soit laissé de côté dans la transition vers le numérique. Enfin, ces enjeux mettent en évidence un aspect essentiel souvent sous-estimé : la transparence. Une dimension importante de cette transparence concerne la transparence technique. Pour que les citoyens puissent faire confiance à l'INN, il est nécessaire que les choix technologiques soient expliqués, documentés et évalués de manière ouverte. Cette transparence technique est un moyen important pour que le gouvernement pourra renforcer la confiance du public et garantir un déploiement de l'identité numérique à la fois sécuritaire, éthique et crédible sur le plan technologique.

Afin de structurer ces préoccupations et d'en dégager une lecture synthétique, ces enjeux ont été regroupés en dimensions plus générales. À partir de cette synthèse, sept piliers fondamentaux peuvent être identifiés. Ces piliers ne constituent pas de nouveaux enjeux, mais plutôt une structuration des préoccupations analysées dans ce chapitre, permettant de guider la mise en œuvre d'une INN à la fois éthique, sécuritaire et inclusive.

1. **Protection de la vie privée.** Ce pilier découle principalement des enjeux liés au *profilage*, à la *centralisation des données et à la cybersécurité*, ainsi qu'aux préoccupations concernant la *clarté juridique et la responsabilité*. Ces enjeux mettent en évidence la nécessité d'assurer une protection forte des renseignements personnels dans toute infrastructure d'identité numérique. Une INN doit intégrer la protection de la vie privée dès sa conception. Ce pilier repose sur des principes fondamentaux :

minimisation des données, consentement éclairé, contrôle individuel sur l'usage des données et finalités limitées. Dans une approche éthique, l'État ne doit pas seulement se conformer aux lois sur les renseignements personnels : il doit aller au-delà, en garantissant une transparence totale sur les usages et en excluant par défaut les pratiques de surveillance ou de profilage. Le respect de la vie privée n'est donc pas un simple enjeu technique, mais un fondement de la confiance numérique.

2. **Sécurité et fiabilité.** Ce pilier prend appui sur les enjeux liés à la *centralisation des données et à la cybersécurité*, ainsi qu'aux préoccupations concernant l'*hébergement et la gouvernance* des infrastructures numériques. Une identité numérique ne peut fonctionner correctement que si elle inspire confiance. Cela suppose que les données personnelles soient protégées contre les accès non autorisés, les erreurs et les cyberattaques. Il faut aussi garantir que les informations utilisées soient exactes, à jour, et traitées selon des règles strictes. Pour cela, il est essentiel d'intégrer des mécanismes de sécurité dès la conception. La sécurité doit être une priorité technique, mais aussi organisationnelle, pour assurer la stabilité et la fiabilité du système dans le temps.
3. **Gouvernance.** Ce pilier s'appuie sur les enjeux liés à la *clarté juridique et à la responsabilité*, ainsi qu'à la *gestion centralisée de la gouvernance numérique* identifiés dans les sections précédentes. Pour que l'identité numérique soit déployée de manière responsable, il est essentiel de s'appuyer sur un cadre juridique clair, qui définit les rôles, les responsabilités et les limites d'usage. Ce cadre doit aussi prévoir des mécanismes permettant aux citoyens de faire valoir leurs droits et de contester les décisions en cas d'erreur ou d'abus. Une supervision indépendante est également nécessaire pour s'assurer que les pratiques numériques respectent les principes éthiques et les droits fondamentaux.
4. **Interopérabilité.** Une INN doit pouvoir fonctionner avec différents systèmes, qu'ils soient publics ou privés, sans compromettre la sécurité ni les droits des citoyens. Cela suppose une interopérabilité encadrée par des règles claires : seules les entités respectant des normes établies de protection des données devraient pouvoir interagir avec l'INN.
5. **Inclusivité et équité.** Ce pilier s'appuie sur les enjeux liés à l'*exclusion numérique* identifiés dans les sections précédentes, qui soulignent les risques que certaines populations soient désavantagées par la transition vers des services publics entièrement numériques. L'INN doit être accessible à l'ensemble de la population, sans distinction. Ce pilier repose sur l'idée que chacun, peu importe ses capacités numériques, son âge ou sa situation socio-économique, doit pouvoir accéder aux services publics. Cela implique de prévoir des parcours alternatifs, comme des services en personne ou par téléphone, et de concevoir des outils simples et compréhensibles.
6. **Transparence.** Ce pilier s'appuie sur l'ensemble des enjeux identifiés dans les sections précédentes.

En effet, plusieurs mémoires soulignent que la transparence constitue un fondement essentiel pour instaurer la confiance dans un système d'identité numérique. Les citoyens doivent savoir quelles données sont utilisées, à quelles fins, et par qui. Il est donc nécessaire de garantir un accès clair à l'historique des consultations, d'envoyer des notifications en cas d'utilisation, et de fournir une information accessible sur leurs droits. Cette exigence s'étend aussi aux choix technologiques faits par l'État : les outils, partenaires et méthodes employés doivent être compréhensibles et justifiables aux yeux du public.

7. **Souveraineté numérique.** Ce pilier s'appuie sur les enjeux liés à l'*hébergement et à la gouvernance des données*, ainsi qu'aux préoccupations concernant la dépendance envers des infrastructures technologiques et des fournisseurs étrangers. Une INN doit garantir que les données des citoyens restent sous le contrôle du Québec. Cela implique que leur hébergement et leur gestion soient effectués localement, en conformité avec les lois québécoises. L'objectif est de limiter la dépendance aux fournisseurs étrangers, souvent soumis à des juridictions extérieures.

Pour mettre en œuvre ces sept piliers, le choix de l'architecture technique est essentiel. L'architecture de l'identité numérique détermine comment les différents éléments du système interagissent entre eux. Toutefois, au-delà de cette structuration technique, il est nécessaire de disposer d'un cadre d'analyse permettant d'évaluer concrètement les impacts de ces choix sur la vie privée, ce qui justifie le recours à l'EFVP, abordée dans le chapitre suivant.

CHAPITRE 3
ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE POUR UNE IDENTITÉ NUMÉRIQUE

Après avoir défini ce qu'est une identité numérique et présenté les principales technologies qui la sous-tendent, il est essentiel d'en cadrer l'analyse sous l'angle de la protection de la vie privée. Le chapitre précédent a mis en lumière sept piliers essentiels pour un déploiement responsable de l'identité numérique nationale : protection de la vie privée, sécurité, gouvernance, interopérabilité, inclusivité, transparence et souveraineté numérique. Ces piliers résument les attentes récurrentes exprimées dans les mémoires étudiés et constituent, ensemble, les conditions minimales pour assurer la confiance du public. Or, pour que ces piliers ne demeurent pas théoriques, il faut les traduire dans une démarche d'analyse capable d'identifier les risques concrets et de documenter les décisions prises tout au long du projet. La meilleure manière d'y parvenir, et en particulier de répondre au pilier de la transparence, qui exige une justification claire des choix technologiques, organisationnels et juridiques est de réaliser une EFVP.

Dans ce chapitre, nous aborderons donc l'évaluation des facteurs relatifs à la vie privée, d'abord de manière générale afin d'en comprendre les fondements et les objectifs, puis dans le contexte particulier de l'identité numérique. Ce cadre conceptuel permettra, dans le chapitre suivant, d'appliquer concrètement la méthodologie de l'EFVP à un projet d'identité numérique fictif. L'EFVP est un outil méthodologique visant à structurer l'évaluation des impacts d'un projet sur la vie privée, en encadrant l'identification des risques, la justification des choix techniques et organisationnels, ainsi que la mise en place de mesures d'atténuation appropriées. Elle est généralement élaborée par l'équipe responsable du projet, en collaboration avec le responsable de la protection des renseignements personnels désigné par l'organisation. Conformément à la Loi 25, c'est ce dernier qui porte la responsabilité légale de s'assurer qu'une EFVP est réalisée lorsque requise, qu'elle est complète, et qu'elle respecte les obligations prévues par le cadre législatif applicable. La rédaction du document peut toutefois mobiliser d'autres intervenants, comme des analystes spécialisés, des experts techniques ou juridiques, ainsi que des partenaires externes, selon la nature et la complexité du projet.

L'EFVP doit être réalisée dès les premières phases de conception d'un système, d'un service ou d'une solution impliquant des données personnelles, afin d'intégrer les considérations relatives à la vie privée dès le départ. L'EFVP est principalement un outil interne, validé par la direction de l'organisation et appuyé de documents techniques. Elle peut être consultée par des auditeurs, la CAI ou d'autres autorités en cas de besoin. Dans

certains cas précis, comme lors du dépôt d'une entente de communication entre deux organismes publics, son envoi à la CAI est requis pour démontrer la conformité à la Loi 25 (Commission d'Accès à l'Information du Québec , 2024). Certaines organisations choisissent également d'en publier un résumé à des fins de transparence.

L'EFVP comprend plusieurs éléments importants : la justification du projet, la nature des renseignements personnels concernés, les parties prenantes impliquées, les technologies utilisées, ainsi que l'évaluation des risques liés à la collecte, l'utilisation, la conservation et la destruction des données. De manière générale, une EFVP est accompagnée de documents techniques annexes permettant d'appuyer l'analyse : schémas d'architecture du système, modèles de consentement, rapports d'analyse de sécurité, et documentation sur les mécanismes d'authentification ou de chiffrement mis en place. Ces documents facilitent la compréhension des enjeux techniques et permettent aux parties prenantes, incluant les autorités externes, d'évaluer la conformité globale du projet.

Enfin, l'EFVP ne constitue pas un document figé. Elle doit faire l'objet d'un suivi tout au long du cycle de vie du projet, être mise à jour en cas de modifications importantes (changement de fournisseur, nouvelles fonctionnalités, nouvelle finalité, etc.), et faire l'objet d'audits réguliers afin de s'assurer que les mesures prévues sont bien appliquées.

3.1 Détermination du besoin de faire une EFVP

Au Québec, la Loi sur la protection des renseignements personnels dans le secteur privé (P-39.1) (Gouvernement du Québec, 2024b) et la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (A-2.1) (Gouvernement du Québec, 2024a) exigent la réalisation d'une EFVP dans cinq situations précises, toutes susceptibles de s'appliquer à un projet d'identité numérique.

La **communication de renseignements personnels à l'extérieur du Québec** requiert une EFVP tenant compte de la sensibilité des données, de la finalité de leur utilisation, des mesures de protection contractuelles en place, et du régime juridique applicable dans l'État destinataire. Tout **projet d'acquisition, de développement ou de refonte d'un système d'information** impliquant des renseignements personnels est également visé. Un projet d'INN y correspond pleinement, puisqu'il implique la collecte de données sensibles (biométrie, identifiants uniques), leur utilisation pour l'authentification et la gestion des accès, leur communication éventuelle à des tiers, et leur conservation et destruction sécurisée selon les obligations légales. La **communication à**

des fins d'étude, de recherche ou de production de statistiques sans consentement est permise uniquement si l'EFVP confirme que l'identification est nécessaire, que l'intérêt public prime sur l'atteinte à la vie privée, et que la confidentialité des renseignements est assurée. La **collecte pour le compte d'un autre organisme public** s'applique notamment lorsqu'une plateforme d'identité numérique commune est développée pour donner accès à plusieurs services gouvernementaux. Elle doit être encadrée par une entente écrite précisant l'identification des organismes, les fins et la nature des renseignements collectés, les moyens et mesures de protection, la périodicité et la durée. Cette entente est transmise à la Commission et entre en vigueur 30 jours après sa réception. Enfin, la **communication sans consentement dans le cadre d'une entente** est permise si l'EFVP conclut que l'objectif ne peut être atteint qu'avec une identification nominale, qu'il est déraisonnable d'exiger le consentement, que l'intérêt public l'emporte sur l'atteinte à la vie privée, et que la confidentialité est garantie. L'entente suit les mêmes exigences formelles que celles décrites précédemment.

3.2 Description du projet

Après avoir déterminé que le projet nécessite une EFVP et dans quel cadre cela s'applique, il faut procéder à une analyse du projet de l'identité numérique. Cette première section de l'EFVP vise à décrire le projet en détaillant ses objectifs, son contexte, les personnes responsables, les renseignements personnels concernés et le cycle de vie des données. Ceci permettra de mieux comprendre les enjeux et les impacts potentiels sur la vie privée.

3.2.1 Définir le projet et ses objectifs

Comme défini par la CAI (Commission d'Accès à l'Information du Québec , 2024), le projet et son contexte doivent être présentés en expliquant en quoi consiste le projet, son contexte d'apparition, la situation initiale, l'échéancier de mise en œuvre, ainsi que son utilité pour l'organisation. L'évaluateur doit ensuite préciser les objectifs du projet et expliquer pourquoi l'utilisation de renseignements personnels est nécessaire à leur atteinte. Pour définir clairement le projet, les éléments suivants doivent être abordés :

- En quoi consiste le projet ?
- Contexte ayant mené à sa création.
- Situation initiale.
- Échéancier (date de début, durée prévue, etc.).
- Utilité pour l'organisation.

Les objectifs du projet doivent aussi justifier les renseignements personnels requis. Dans le cas d'un projet

d'identité numérique, ils peuvent également éclairer le choix de l'architecture adoptée.

3.2.2 Définir les rôles et les responsabilités

Dans une EFVP, il faut identifier clairement les responsables du projet : l'entreprise porteuse, la personne chargée du projet, les partenaires impliqués, ainsi que le responsable de la protection des renseignements personnels (RPRP). Selon la CAI (Commission d'Accès à l'Information du Québec , 2024), l'EFVP doit être réalisée par l'organisation qui détient les renseignements personnels. Les sous-traitants ou partenaires peuvent être consultés pour des aspects techniques (authentification, hébergement, etc.), mais la responsabilité globale doit rester interne.

Un exemple pertinent est celui de SecureKey (Milberry et Parsons, 2013), qui a collaboré avec des banques et des compagnies télécoms pour offrir une solution d'identité numérique, tout en laissant la responsabilité globale au gouvernement. La coordination de l'EFVP peut être assurée par le RPRP ou une autre personne compétente, et plusieurs parties prenantes doivent être impliquées (services juridiques, TI, partenaires externes, etc.). Pour chaque personne impliquée, il faut identifier (1) les responsables du projet, soit l'entreprise en charge du projet, la personne responsable du projet, les organismes publics ou privés impliqués ainsi que le responsable de la protection des renseignements personnels et (2) les responsables de l'évaluation. Dans le contexte de l'identité numérique, nous suivrons le modèle de la CAI, qui nous indique de renseigner les informations suivantes sur les responsables de l'EFVP : le nom, le titre, la direction/service, l'organisation, le rôle dans la démarche et enfin la raison de l'implication.

3.2.3 Identifier les renseignements personnels concernés

Cette section vise à démontrer que les renseignements personnels recueillis, utilisés ou communiqués sont indispensables à la réalisation du projet. L'EFVP doit ainsi déterminer la sensibilité, la quantité et la finalité de ces renseignements. Ainsi, selon la CAI (Commission d'Accès à l'Information du Québec , 2024), il est recommandé de répondre aux questions suivantes pour accomplir cette tâche : La question du **quoi** porte sur la nature, la sensibilité et la provenance des renseignements : quels types de renseignements personnels seront collectés, communiqués, utilisés ou conservés, sont-ils sensibles en raison de leur nature ou du contexte de leur utilisation, et d'où proviennent-ils ? Dans le contexte de l'identité numérique, il est primordial de saisir les diverses catégories de données personnelles qui peuvent être recueillies, transmises, exploitées ou stockées, car leur nature et leur sensibilité sont très différentes, ce qui a un impact direct sur les

mesures de protection et de gestion requises pour garantir leur sécurité et la protection de la vie privée. Les différents types de renseignements personnels sont classés dans le tableau 3.1, avec des exemples concrets pour chaque catégorie. Ce tableau s'inspire e la catégorisation faite par le guide d'encadrement sécuritaire de l'identité numérique de l'université de Sherbrooke (Université de sherbrooke, 2022) et présente une classification détaillée des données personnelles couramment traitées dans divers contextes.

Types de renseignements personnels	**Exemples**
Identité et informations personnelles de base	Nom complet, date de naissance, adresse courriel, numéro de téléphone, numéro d'identification gouvernemental, adresse postale
Informations physiques et biométriques	Empreintes digitales, reconnaissance faciale, enregistrement vocal, scan de l'iris, attributs physiques : couleur des yeux et cheveux
Informations de connexion	Noms d'utilisateur, questions de sécurité, jetons d'authentification
Codes d'identification	Numéro de client, numéro d'assurance sociale, numéro de passeport, numéro du permis de conduire
Historique des transactions et activités	Enregistrements des connexions et déconnexions, historique des transactions en ligne, données de navigation, achats et ventes
Informations financières	Détails bancaires, marges de crédit, informations de carte de crédit ou de débit, historique des paiements
Données de localisation	Adresses IP, données GPS, historique des déplacements
Informations de santé	Dossiers médicaux, historique des traitements, informations sur les assurances santé
Données contextuelles	Appareils utilisés, navigateurs, systèmes d'exploitation, paramètres de sécurité (ex. : niveaux de chiffrement)
Croyances et informations sociodémographiques	Croyances, âge, état matrimonial, identification sexuelle, langues parlées, informations sur les enfants (ex. : nombre, âge), informations sur les parents (nom de jeune fille de la mère)

Suite à la page suivante

Table 3.1 – suite

Types de renseignements personnels	Exemples
Informations d'emploi	Historique des emplois, rôles et responsabilités, informations salariales, adresse professionnelle, courriel professionnel, cuméro de téléphone professionnel

Table 3.1: Types de renseignements personnels collectés, communiqués, utilisés ou conservés dans le cadre d'un exemple d'un projet d'identité numérique

La question du **pourquoi** vise à établir la finalité de chaque traitement de renseignements personnels : pourquoi ces données sont-elles recueillies, utilisées, communiquées ou conservées, et en quoi les personnes qui y auront accès en ont-elles besoin dans l'exercice de leurs fonctions ? Cette justification est essentielle pour démontrer que chaque traitement est proportionnel à l'objectif poursuivi. La question du **combien** porte sur l'ampleur du traitement : la quantité de renseignements impliqués, le nombre de personnes concernées (en valeur absolue ou en proportion de la population), le volume ou l'étendue des données, ainsi que la durée et la portée géographique envisagées pour le projet. Il faut également inclure dans cette analyse tous les renseignements impliqués, qu'ils soient créés ou déduits à partir d'autres données, recueillis automatiquement par des appareils ou systèmes informatiques, regroupés sous forme statistique même lorsqu'ils ne permettent plus d'identifier un individu, ou encore dépersonnalisés et anonymisés.

3.2.4 Décrire le cycle de vie des données

Après avoir identifié les renseignements personnels concernés, l'évaluateur doit ensuite décrire le cycle de vie complet de ces données. Conformément aux recommandations de la CAI (Commission d'Accès à l'Information du Québec , 2024), cette description vise à préciser, pour chaque type de renseignement, la méthode de collecte, les personnes ou partenaires impliqués, ainsi que la finalité associée à leur utilisation. Le cycle de vie des renseignements personnels dans le contexte de l'identité numérique suit les mêmes étapes que dans tout autre type de projet. Le tableau 3.2 présente des exemples adaptés au contexte de l'identité numérique, illustrant comment recenser les méthodes de collecte, identifier les personnes et entités responsables de l'accès, de la collecte et de la gestion des renseignements personnels, et préciser la

finalité de chaque traitement.

Type de données	Méthodes de collecte	Personnes / partenaires impliqués	Finalité de la collecte
Identité et informations personnelles de base	Formulaires en ligne, inscription en personne, bases de données gouvernementales	Utilisateurs	Identification, accès aux services publics et privés
Informations physiques et biométriques	Capteurs biométriques (scanners d'empreintes digitales, reconnaissance faciale), examens médicaux	Utilisateurs, professionnels de santé	Sécurité renforcée, vérification d'identité, accès à des zones sécurisées
Informations de Connexion	Interfaces de connexion, outils de gestion des mots de passe	Utilisateurs, fournisseurs de services	Sécurisation de l'accès aux comptes, authentification des utilisateurs
Codes d'Identification	Formulaires d'inscription, documents officiels	Administrations publiques	Identification unique, vérification d'identité, accès à des services spécifiques
Historique des transactions et des activités	Suivi des transactions en ligne, journaux de connexion	Utilisateurs, banques, prestataires de services en ligne	Analyse de comportement, historique d'achats
Informations financières	Transactions bancaires, formulaires de demande de crédit	Banques, institutions financières, utilisateurs	Gestion financière, validation de transactions, évaluation du crédit

Type de Données	**Méthodes de collecte**	**Personnes / partenaires impliqués**	**Finalité de la collecte**
Données de localisation	GPS, adresses IP, applications de navigation	Utilisateurs, fournisseurs de services de localisation, applications mobiles	Sécurité, fourniture de services géolocalisés
Informations de santé	Dossiers médicaux électroniques, consultations médicales	Professionnels de santé, assurances, patients (utilisateur)	Suivi des traitements et soins, réclamations d'assurance
Données contextuelles	Paramètres de sécurité, journalisation des appareils	Utilisateurs, fournisseurs de services	Amélioration de la sécurité, personnalisation des services
Croyances et informations sociodémographiques	Enquêtes, déclarations personnelles, recensements	Utilisateurs, administrations publiques	Analyse sociodémographique, études de marché
Informations d'emploi	Dossiers RH, entretiens d'embauche	Employeurs, employés, agences de recrutement	Gestion des ressources humaines, planification de carrière, administration salariale

Table 3.2: Modèle de structuration des méthodes de collecte des données, des personnes impliquées et des finalités dans un système d'identité numérique décentralisé

Les catégories de personnes ayant accès aux renseignements personnels peuvent inclure des individus au sein de l'organisation ainsi que des entités externes, telles que des sous-traitants. Pour chaque catégorie, selon la CAI il est nécessaire de détailler le rôle des personnes ayant accès aux renseignements, le nombre de personnes exerçant ce rôle, le type d'accès dont elles disposent (par exemple, lecture seule, modification), les renseignements auxquels ces personnes auront accès ainsi que les raisons pour lesquelles ces personnes ont besoin d'accéder à ces renseignements. Pour structurer les informations relatives à l'utilisation, l'évaluateur

doit également prendre en compte plusieurs dimensions : les *responsables*, les personnes qui assument la responsabilité de l'utilisation des renseignements, le *moment*,le moment précis de cette utilisation ; le *lieu*, l'endroit où l'utilisation se déroulera, les *moyens*, soit les éléments employés pour cette utilisation ; et enfin les *finalités*, c'est-à-dire les objectifs poursuivis par cette utilisation.

Selon la CAI, il est aussi essentiel de préciser les éléments suivants lors de l'évaluation de la communication des renseignements personnels : Les **destinataires** doivent être identifiés, c'est-à-dire les tiers ou groupes de tiers auxquels les renseignements seront communiqués, y compris les filiales de l'entreprise responsable du projet, qui sont également considérées comme des tiers. La **juridiction** doit aussi être précisée, puisque la loi exige le respect de certaines normes si les renseignements sont communiqués en dehors du Québec. Pour structurer ces interactions, l'évaluateur doit déterminer quelles catégories de personnes auront accès aux renseignements personnels à l'intérieur ou à l'extérieur de l'organisation, par quels moyens ces renseignements seront communiqués, où et quand cette communication aura lieu. Les points d'interaction peuvent inclure des individus, des groupes, des partenaires ou des tiers qui accèdent aux renseignements, les recueillent ou approuvent leur destruction, ainsi que les moyens utilisés pour les communiquer, tels que les prestations électroniques de services, les échanges par courriel, le service à la clientèle, les sites web ou les liens électroniques sécurisés.

Lors de l'évaluation de la conservation, destruction et anonymisation des renseignements personnels, il est essentiel de prendre en compte les éléments suivants (Commission d'Accès à l'Information du Québec , 2024). En ce qui concerne la **conservation**, il faut identifier qui en est responsable, par quels moyens les renseignements sont conservés (systèmes informatiques, bases de données, services infonuagiques, copies de sauvegarde, outils de télécommunication, salles et classeurs d'entreposage), quelle est la durée de conservation, où les renseignements sont conservés en précisant la province ou l'État ainsi que le tiers hébergeur le cas échéant, et à quelle date ils seront détruits ou anonymisés. Pour la **destruction et l'anonymisation**, il faut préciser qui en est responsable, à quel moment elles sont effectuées, le délai pouvant référer à un événement spécifique comme la suppression du compte de l'utilisateur plutôt qu'à un nombre de jours ou de mois, où et par quels moyens elles sont réalisées, ainsi que quel événement en constitue le déclencheur.

Les points d'interaction avec les renseignements personnels peuvent inclure des individus ou groupes de personnes, ainsi que des partenaires et des tiers, qui accèdent aux renseignements personnels, les recueillent,

approuvent leur destruction, etc. (par exemple, employés, clients, sous-traitants, firmes de consultation, chercheurs externes, équipes d'entretien des bâtiments ou des systèmes informatiques, fournisseurs de télécommunication, etc.). D'autres informations doivent aussi être spécifiées comme les moyens utilisés pour traiter et conserver les renseignements personnels (systèmes informatiques, bases de données, services infonuagiques, copies de sauvegarde, outils de télécommunication, salles et classeurs d'entreposage des dossiers papier) ainsi que les moyens utilisés pour détruire ou anonymiser les renseignements personnels.

3.2.5 Évaluation des critères de proportionnalité

Cette analyse est essentielle pour déterminer la portée appropriée de l'EFVP à réaliser pour le projet. Selon la CAI (Commission d'Accès à l'Information du Québec , 2024), elle doit notamment prendre en compte la sensibilité des renseignements personnels, la finalité de leur utilisation ou de leur communication, la quantité de données concernées, ainsi que leur répartition et leurs modes de stockage. L'évaluation de ces éléments permet d'estimer les risques potentiels pour la vie privée et d'adapter les mesures de protection avant la mise en œuvre du projet.

Selon le site rgpd.com (source non officielle dédiée à la vulgarisation du Règlement général sur la protection des données) (RGPD, 2024), les données à caractère personnel sont classées en différents types en fonction de leur sensibilité et de leur traitement (voir tableau 3.3). Les données personnelles non sensibles regroupent par exemple le nom, l'adresse ou l'e-mail. Elles restent importantes mais présentent moins de risques en cas de compromission. Les données personnelles sensibles incluent, quant à elles, les données biométriques, les informations relatives à la santé, l'origine ethnique ou encore les opinions politiques, et font l'objet de règles strictes afin d'éviter les abus et les discriminations. Une catégorie particulière concerne les données des enfants, qui requièrent un traitement spécifique en raison de leur vulnérabilité. Les données liées aux infractions pénales ou aux condamnations doivent également être traitées avec une attention renforcée en raison des risques potentiels de discrimination ou d'autres dommages. Enfin, les données personnelles dites confidentielles englobent des éléments tels que le patrimoine, le salaire ou le numéro d'identification national, qui ne doivent généralement pas être révélés au grand public.

Type de données	Catégorisation selon la ressource	Évaluation de la sensibilité	Justification
Identité et informations personnelles de Base	Données personnelles non sensibles	Moyenne	Ces données sont largement utilisées et leur fuite peut entraîner des usurpations d'identité.
Informations physiques et biométriques	Données personnelles sensibles	Élevée	Les données biométriques sont uniques et sensibles, nécessitant une protection stricte contre les abus.
Informations de Connexion	Données sensibles	Élevée	Cruciales pour la sécurité des comptes, leur compromission peut mener à des accès non autorisés et des violations graves de la sécurité.
Codes d'Identification	Données personnelles confidentielles	Élevée	Identifiants uniques essentiels pour l'accès aux services, leur perte peut entraîner des risques majeurs.
Historique des transactions et des activités	Données personnelles non sensibles	Moyenne	Les habitudes et comportements peuvent être déduits, nécessitant une protection pour éviter les abus.
Informations financières	Données personnelles confidentielles	Élevée	Cruciales pour la sécurité financière, ces données doivent être protégées pour éviter les fraudes.
Données de localisation	Données personnelles non sensibles	Moyenne à élevée	Les déplacements peuvent révéler des informations privées importantes, nécessitant une gestion prudente.

Type de données	Catégorisation selon la ressource	Évaluation de la sensibilité	Justification
Informations de santé	Données personnelles sensibles	Très élevée	Le RGPD les considère comme extrêmement sensibles, avec des risques élevés en cas de compromission.
Données contextuelles	Données personnelles non sensibles	Moyenne	Ces données sont utilisées pour personnaliser les services mais peuvent devenir sensibles selon le contexte.
Croyances et informations sociodémographiques	Données personnelles sensibles	Élevée	Ces informations peuvent être utilisées pour discriminer, nécessitant une protection rigoureuse.
Informations d'emploi	Données personnelles non sensibles	Moyenne	Essentielles pour la gestion des ressources humaines, leur fuite peut entraîner des abus.

Table 3.3: Évaluation de la sensibilité des types de données personnelles dans un système d'identité numérique

La finalité de l'utilisation ou de la communication des renseignements personnels dans le contexte de l'identité numérique a été élaborée pour les différents types de données dans le tableau 3.2. Ces finalités assurent que les données sont collectées et utilisées de manière conforme et adaptée aux besoins spécifiques des utilisateurs et des services impliqués. Dans le cadre d'un projet d'identité numérique, il est aussi important de déterminer combien de renseignements personnels seront impliqués et si leur quantité influence l'ampleur des risques prévisibles (Commission d'Accès à l'Information du Québec , 2024). Le nombre de personnes concernées, qu'il soit exprimé en valeur absolue ou en proportion de la population, est un premier facteur déterminant : plus le nombre d'utilisateurs est élevé, plus les risques potentiels en cas de fuite ou de compromission sont importants. Le volume et l'étendue des renseignements collectés constituent un second facteur, englobant les informations recueillies (nom, adresse), observées (habitudes de connexion), inférées (préférences utilisateur) et créées (identifiants numériques), une collecte excessive augmentant la complexité

de leur gestion et les risques associés. La durée du projet doit également être précisée : un projet d'identité numérique est souvent permanent, ce qui implique une planification à long terme pour la protection, le stockage sécurisé et la suppression des données lorsqu'elles ne sont plus nécessaires. Enfin, la portée géographique du projet influence directement le niveau de conformité requis : une extension sur plusieurs régions ou pays oblige à respecter différentes réglementations sur la protection des données, ce qui accroît la complexité de la gestion et les risques associés.

Selon la CAI, il est recommandé d'évaluer la répartition des renseignements personnels selon trois dimensions. La **dimension spatiale** porte sur la localisation des renseignements, qu'ils soient au sein ou à l'extérieur de l'organisation, stockés de manière centralisée (serveurs internes, infonuagique) ou décentralisée (chaîne de blocs). Dans le contexte de l'identité numérique, cela implique de préciser le modèle d'architecture retenu (isolé, fédéré ou décentralisé), la localisation des nœuds le cas échéant, et les lois de protection des données applicables selon les juridictions concernées. La **dimension humaine ou administrative** concerne la communication des renseignements aux parties prenantes. Il s'agit de déterminer qui aura accès aux données (intervenants internes, prestataires externes, partenaires, nœuds de la chaîne de blocs), comment sont gérées les interactions avec des tiers notamment via des justificatifs numériques dans un modèle SSI, et dans quelle mesure les utilisateurs peuvent contrôler quelles informations sont partagées et avec qui. Dans un modèle fédéré ou décentralisé, il convient également de préciser comment l'accès à l'identité numérique est géré par les différents fournisseurs de services et vérificateurs. La **dimension quantitative** porte sur le nombre de personnes ayant accès aux données et le nombre de supports les hébergeant. Dans le contexte de l'identité numérique, cela inclut le niveau d'accès des différents intervenants (administrateurs, utilisateurs, partenaires), le nombre de supports sur lesquels les données sont stockées (serveurs, bases de données, nœuds de chaîne de blocs, portefeuilles numériques), les mécanismes de contrôle d'accès mis en place, ainsi que les moyens offerts aux utilisateurs pour gérer leurs propres données, notamment via un portefeuille numérique dans un modèle SSI.

Il est aussi primordial d'identifier les différents supports utilisés pour consulter, consigner ou stocker, de façon temporaire ou permanente, les informations personnelles liées au projet d'identité numérique (Commission d'Accès à l'Information du Québec , 2024). Trois caractéristiques principales doivent être prises en compte. La nature du support, **matérielle ou numérique**, détermine d'abord comment les données sont hébergées : sur des serveurs physiques ou sur des infrastructures infonuagiques, voire de manière décentralisée sur les nœuds d'une chaîne de blocs dans un modèle d'identité numérique basé sur l'architecture décentralisée. Le

caractère **sécurisé ou non** du support constitue un enjeu essentiel, impliquant de garantir la conservation et l'accès aux données à travers des dispositifs protégés intégrant notamment le chiffrement. Enfin, la **connectivité** du support avec d'autres systèmes détermine le niveau d'interopérabilité entre services, par exemple : un système d'identité numérique pourrait être intégré à un réseau de services gouvernementaux ou de santé, auquel cas les connexions entre systèmes doivent être sécurisées pour prévenir toute fuite de données. Dans un modèle décentralisé, les supports peuvent être partiellement isolés, ce qui réduit les risques liés à une interconnexion non sécurisée.

3.2.6 Conformité et liste des obligations de protection des renseignements personnels

Ensuite, la CAI (Commission d'Accès à l'Information du Québec , 2024) recommande d'énumérer les obligations et pratiques de protection des renseignements personnels pour le projet, en respectant les obligations provinciales, fédérales et internationales, ainsi que les pratiques organisationnelles et les normes. Dans le cadre de la réalisation d'un projet d'identité numérique, ces obligations peuvent être issues de diverses sources. Ainsi au Québec, les principales obligations en matière de protection des renseignements personnels sont régies par la Loi sur l'accès et la Loi sur le privé. Ces lois couvrent le cycle de vie des renseignements personnels, de leur collecte à leur destruction (voir la section 3.1 pour obtenir davantage d'informations).

En cas d'activités au-delà du Québec ou du Canada, le projet d'identité numérique doit également respecter les lois fédérales et internationales. Au Canada, la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) s'applique dans l'ensemble des provinces et fixe un cadre national de protection des données. Si le projet concerne des utilisateurs en Europe, il doit respecter le Règlement général sur la protection des données (RGPD), qui impose des règles strictes en matière de consentement et de transfert transfrontalier de données. Enfin, d'autres juridictions possèdent leurs propres législations, comme le California Consumer Privacy Act (CCPA) aux États-Unis, qui établit des obligations spécifiques pour les entreprises manipulant les données de résidents californiens.

Au-delà des obligations légales, il est important de respecter les politiques internes de l'organisation concernant la gestion des renseignements personnels. Tel que : les politiques, des processus, des procédures, des méthodes de travail, un plan et un calendrier de conservation, etc. (Commission d'Accès à l'Information du Québec , 2024). Enfin, pour garantir que le projet d'identité numérique respecte les meilleures pratiques en matière de protection des données, il est pertinent de se référer à des normes internationales reconnues. Par exemple, la norme ISO/IEC 27001 (International Organization for Standardization and International Elec-

trotechnical Commission, 2022) définit les exigences relatives aux systèmes de management de la sécurité de l'information, tandis que la ISO/IEC 29100 (International Organization for Standardization and International Electrotechnical Commission, 2024) propose un cadre de protection de la vie privée applicable aux systèmes d'information. Le document du NIST SP 800-63 (National Institute of Standards and Technology) (National Institute of Standards and Technology, 2017) établit, quant à lui, des lignes directrices pour l'authentification numérique et les niveaux d'assurance (LoA). À l'échelle nationale et internationale, on peut également se référer au Cadre de confiance pancanadien (CFC) (DIACC's Trust Framework Expert Committee TFEC, 2025) et aux lignes directrices de l'OCDE en matière de gouvernance et de protection des données.

Il est par ailleurs recommandé de solliciter l'avis d'un juriste afin de garantir l'identification et le respect de toutes les obligations légales et réglementaires applicables dans le cadre du projet.

3.3 Identification des risques d'atteinte à la vie privée et évaluation de leurs conséquences

D'après la définition donnée par la CAI, le terme « risque d'atteinte à la vie privée » désigne toute situation ou tout événement qui pourrait porter préjudice à une personne, notamment en compromettant la confidentialité ou la sécurité de ses renseignements personnels. Ce type de risque est souvent lié à une mauvaise gestion des données, une faille de sécurité, ou encore un usage non autorisé de l'information. Dans le cadre d'une EFVP, il est important d'identifier ces risques dès les premières étapes du projet. L'analyse s'effectue en examinant chaque moment du cycle de vie des renseignements personnels : depuis leur collecte, jusqu'à leur utilisation, leur communication à des tiers, leur conservation, leur destruction ou leur anonymisation. À chaque étape, certaines actions peuvent exposer les données à des atteintes potentielles à la vie privée. Les risques sont généralement regroupés par catégories correspondant à ces étapes. Pour chacune, il faut décrire les risques potentiels, identifier les causes possibles, évaluer les conséquences sur les personnes concernées et proposer des mesures concrètes pour réduire ou éliminer ces risques En plus de cette description qualitative, il est recommandé que chaque risque soit évalué à l'aide d'un système simple qui permet d'en estimer l'ampleur : nous estimons à la fois la probabilité qu'il se produise et la gravité de ses conséquences. Une fois les mesures de protection mises en place, le risque est réévalué pour vérifier leur efficacité. Ce travail permet de prioriser les interventions, d'améliorer les protections, et de démontrer que l'organisation a pris les moyens nécessaires pour assurer la sécurité et la conformité de son projet.

Par ailleurs, dans le contexte de l'identité numérique, il existe deux méthodes pertinentes pour identifier les risques. La première est le modèle PANOPTIC (pour *Pattern and Action Nomenclature Of Privacy Threats In*

Context) (MITRE Corporation, 2024), qui propose une analyse systématique des menaces en tenant compte de l'environnement, des données manipulées, des mécanismes de collecte et des vulnérabilités des systèmes. Ce modèle se présente sous la forme d'un grand tableau hiérarchique qui répertorie différents types de situations et d'actions pouvant mener à une atteinte à la vie privée. Chaque ligne du tableau est associée à un code unique (par exemple PC03.01 ou PA07.03) qui permet d'identifier une catégorie précise. Les codes commençant par PC renvoient aux domaines contextuels (*Privacy Contextual Domains*), c'est-à-dire le cadre dans lequel une action sur les données se produit, comme l'environnement numérique, le type de données ou la population concernée. Ceux commençant par PA désignent les activités de confidentialité (*Privacy Activities*), qui correspondent aux actions ou inactions pouvant causer un risque pour la vie privée, telles que la collecte, l'utilisation, le partage ou la conservation des renseignements personnels. Cette nomenclature facilite l'identification et la classification des risques dans un projet d'identité numérique, de manière claire et uniforme. La seconde est le modèle de la CAI, qui classe les risques en fonction des étapes du cycle de vie des renseignements personnels.

Dans cette section, nous avons choisi de détailler la méthode de la CAI, car elle offre une structure claire. Toutefois, comme on le verra dans le chapitre 4, l'analyse peut être enrichie en combinant les deux approches, afin de mieux couvrir à la fois la logique du cycle de vie et la taxonomie plus détaillée proposée par PANOPTIC (MITRE Corporation, 2024).

3.3.1 Risques à la collecte

La collecte d'informations personnelles constitue une étape critique dans les systèmes d'identité numérique, car une mauvaise gestion peut entraîner des atteintes à la vie privée et compromettre la sécurité des utilisateurs. Comme le souligne Dimova et al. (Dimova *et al.*, 2023), plusieurs risques émergent particulièrement lors de l'utilisation de protocoles comme OAuth, mais ils sont transposables à d'autres modèles d'authentification et d'identité numérique. Une **collecte excessive ou non minimisée** des données, causée par l'absence de principe de minimisation dès la conception, expose le système à des risques de violation de données. Pour l'atténuer, il convient d'appliquer la minimisation dès la conception, de former les équipes à une collecte responsable et de mettre en place un processus de validation des nouvelles données collectées. Une **collecte non autorisée ou sans consentement**, résultant d'une gestion déficiente du consentement et d'un manque de transparence, peut entraîner des violations de la vie privée, des sanctions légales et une perte de confiance des utilisateurs. L'atténuation passe par l'implémentation de mécanismes de consen-

tement clairs et une information transparente des utilisateurs sur les finalités de la collecte. La **collecte via des canaux non sécurisés**, due à l'utilisation de formulaires ou d'applications non sécurisés, expose les données à l'interception, au piratage et au vol d'informations. Il est recommandé de mettre en place un chiffrement de bout en bout dès la collecte et de configurer des alertes en cas de transmission non chiffrée. La **collecte de données sensibles sans précaution adéquate**, causée par l'absence de mesures de protection renforcées, crée des risques élevés de vol d'identité. Les stratégies d'atténuation incluent l'application d'un chiffrement fort, la restriction des accès via une gestion des rôles, et des audits réguliers pour détecter les abus. Enfin, les **erreurs dans la saisie des données**, résultant d'erreurs humaines ou de l'absence de double vérification, peuvent causer des inexactitudes, des usurpations d'identité et des accès incorrects aux services. La mise en place de processus de validation et la formation du personnel constituent les principales mesures d'atténuation.

3.3.2 Risques à l'utilisation

Lors de l'utilisation des données, plusieurs risques doivent être pris en considération. Les risques suivants ont été élaborés en tenant compte des principes et recommandations vus dans les sections précédentes. L'**accès non autorisé aux données collectées**, causé par un manque de mesures de sécurité appropriées telles que l'absence de chiffrement ou une authentification faible, peut entraîner la divulgation de renseignements personnels sensibles et des usurpations d'identité. Les stratégies d'atténuation incluent l'implémentation du chiffrement des données, la réalisation d'audits réguliers et le renforcement des mécanismes d'autorisation et de limitation des accès. Le **non-respect ou la manipulation des préférences de confidentialité des utilisateurs**, résultant d'une mauvaise configuration des systèmes, de pratiques trompeuses (*dark patterns*) ou d'une non-conformité aux choix exprimés, peut entraîner une utilisation des données à l'insu des utilisateurs, une perte de confiance et des sanctions réglementaires. Il convient d'y remédier en configurant les systèmes pour respecter strictement les préférences exprimées, en interdisant les pratiques trompeuses, en effectuant des audits réguliers de conformité et en garantissant une transparence totale sur l'utilisation des données. Une **faible sécurité lors de l'utilisation des données**, causée par l'absence de politiques internes claires sur la gestion des accès ou la méconnaissance des pratiques sécurisées par les employés, expose le système à des accès non autorisés, des fuites de données sensibles et une exploitation abusive des informations personnelles. Les mesures d'atténuation comprennent une séparation stricte des rôles et des permissions, l'intégration de mécanismes de journalisation en temps réel et le blocage des accès en cas d'anomalies comportementales détectées.

Enfin, la **vente des données à des fins commerciales** sans le consentement explicite des utilisateurs entraîne une exploitation commerciale des données personnelles, une perte de confiance, des violations de la vie privée et des sanctions légales. Des audits réguliers des pratiques de traitement des données constituent la principale stratégie d'atténuation.

3.3.3 Risques à la communication

Lors de la communication des données, divers risques peuvent apparaître, qu'il s'agisse de failles de sécurité ou d'une transmission inadéquate. Les **vulnérabilités lors de la transmission des données**, causées par l'utilisation de protocoles non sécurisés ou non chiffrés, peuvent permettre l'interception des données personnelles par des acteurs malveillants. Il convient d'y remédier en utilisant des protocoles sécurisés et chiffrés, en choisissant une architecture adaptée qui limite les risques de fuite, et en encadrant les transmissions via des ententes contractuelles claires avec les tiers. Le **partage non autorisé des données avec des tiers**, résultant d'une absence de contrôle strict sur les accès et les permissions ou d'une communication sans consentement préalable, peut entraîner la divulgation de données sensibles à des parties non autorisées et des violations réglementaires. La mise en place de contrats de confidentialité stricts et le renforcement du contrôle des accès constituent les principales mesures d'atténuation.

La **perte de données lors de la communication**, causée par des défauts techniques ou des erreurs humaines, peut provoquer la perte de données critiques et une interruption des services. Des systèmes de sauvegarde robustes et la formation du personnel sur la gestion des données permettent de réduire ce risque. La **ré-identification des données anonymisées**, rendue possible par des techniques avancées appliquées à des ensembles partiellement anonymisés, constitue une violation de la vie privée pouvant entraîner des risques légaux. L'emploi de techniques d'anonymisation avancées et la restriction de l'accès aux ensembles de données sensibles sont recommandés. Le **non-respect des exigences légales de communication transfrontalière**, dû à la méconnaissance ou au non-respect des réglementations locales et internationales, peut entraîner des sanctions légales et une perte de confiance des utilisateurs. Des audits de conformité réguliers et le respect des lois applicables constituent les mesures d'atténuation appropriées. Enfin, la **communication des données à des fins non prévues**, résultant du partage de données à des fins différentes de celles initialement prévues sans en informer les utilisateurs, porte atteinte à la vie privée et peut mener à une exploitation commerciale non autorisée. Il convient de limiter l'utilisation des données aux finalités prévues, d'obtenir le consentement explicite pour toute nouvelle utilisation et de réaliser des audits réguliers afin de vérifier la

conformité des pratiques de communication.

3.3.4 Risques à la conservation, à la destruction et/ou à l'anonymisation

En termes de sécurité des informations ou de gestion inadéquate des processus de suppression et d'anonymisation, il est possible de rencontrer différents risques lors de la conservation, de la destruction ou de l'anonymisation des données. La **conservation prolongée des données au-delà de la période nécessaire**, causée par l'absence de politique de rétention ou une mauvaise gestion des durées de conservation, augmente le risque de violation de données et expose l'organisation à des non-conformités légales. Il convient d'y remédier en définissant et appliquant une politique de rétention alignée sur les obligations légales, en automatisant la suppression des données arrivées à échéance et en vérifiant régulièrement la conformité par des audits. La **destruction incomplète ou non sécurisée des données**, résultant de procédures inadéquates ou d'un manque de contrôle, peut permettre la récupération de données par des acteurs non autorisés. L'établissement d'un protocole normalisé de destruction, l'intégration de mécanismes de traçabilité et des contrôles périodiques permettent de garantir que toutes les suppressions sont définitives et conformes aux normes. Une **anonymisation insuffisante des données**, due à l'utilisation de techniques faibles ou obsolètes, peut mener à la réidentification des individus et à des violations de la vie privée. Il est recommandé de mettre en œuvre des techniques modernes telles que le k-anonymat, la confidentialité différentielle ou l'agrégation contextuelle, et de réaliser régulièrement des tests de réidentification pour s'assurer que l'anonymisation résiste aux méthodes d'attaque récentes. Le **stockage dans des environnements non sécurisés**, causé par l'absence de chiffrement ou l'utilisation de systèmes inadéquats, expose les données à des accès non autorisés et des fuites d'informations sensibles. L'utilisation de systèmes de stockage sécurisés et l'application systématique du chiffrement constituent les mesures d'atténuation appropriées. L'**accès non contrôlé aux copies de sauvegarde**, résultant d'un manque de sécurité sur ces copies, peut entraîner la divulgation non autorisée des données sauvegardées. Une gestion structurée et traçable des accès, le chiffrement systématique des sauvegardes et des audits périodiques permettent de détecter toute anomalie ou tentative d'accès non autorisé. Enfin, le **non-respect des exigences légales de conservation et de destruction des données**, dû à la méconnaissance ou au non-respect des lois en vigueur, peut entraîner des sanctions légales et nuire à la réputation de l'organisation. Des audits de conformité réguliers et le respect des lois locales et internationales applicables constituent les principales mesures d'atténuation.

3.4 L’EFVP et les sept piliers d’une INN

Les sept piliers présentés dans le chapitre 2 définissent les principes fondamentaux qui doivent guider la conception d’un système d’identité numérique nationale. Toutefois, ces principes demeurent théoriques s’ils ne sont pas intégrés dans des mécanismes concrets d’évaluation et de gouvernance. L’EFVP constitue précisément un outil permettant de traduire ces principes en critères d’analyse appliqués à un système réel. En pratique, l’EFVP permet d’examiner les impacts d’un système d’identité numérique sur la protection des renseignements personnels, mais aussi sur des dimensions plus larges comme la gouvernance des données, la transparence des traitements ou la sécurité des infrastructures. Elle agit ainsi comme un cadre d’analyse permettant de vérifier si les choix techniques et organisationnels respectent les piliers définis pour une identité numérique responsable.

Tout d’abord, l’EFVP contribue directement au pilier de la **protection de la vie privée** en analysant les risques liés à la collecte, à l’utilisation, à la communication et à la conservation des renseignements personnels. Elle permet d’identifier les situations où des données pourraient être utilisées de manière excessive ou sans consentement adéquat, et de proposer des mesures visant à limiter ces risques. Elle joue également un rôle important dans l’évaluation des mécanismes de **sécurité** mis en place pour protéger les données. L’analyse des contrôles d’accès, du chiffrement ou encore des systèmes de journalisation permet de vérifier si les mesures techniques sont suffisantes pour prévenir les accès non autorisés, les fuites de données ou les attaques informatiques.

L’EFVP contribue aussi au principe de **transparence** en vérifiant si les utilisateurs sont clairement informés des données collectées, de leurs finalités et des acteurs impliqués dans leur traitement. Cette démarche encourage la mise en place de politiques de confidentialité compréhensibles et de mécanismes permettant aux citoyens de mieux comprendre le fonctionnement du système. L’EFVP permet également d’examiner les enjeux liés à l’**inclusivité et à l’équité**. Un système d’identité numérique peut en effet créer des situations d’exclusion pour certaines catégories de la population, notamment les personnes ayant un accès limité aux technologies numériques, les personnes âgées, les personnes en situation de handicap ou encore les individus ne disposant pas de documents d’identité reconnus. Dans ce contexte, l’EFVP permet d’identifier ces risques d’exclusion et d’évaluer si les mécanismes d’authentification et d’accès aux services prennent en compte la diversité des situations des utilisateurs. Elle encourage ainsi la mise en place de solutions alternatives, de mesures d’accompagnement ou de mécanismes d’accès adaptés afin de garantir que le système d’identité numérique demeure accessible et équitable pour l’ensemble de la population.

Dans un environnement où plusieurs organisations interagissent, l'EFVP permet aussi d'analyser les enjeux liés à l'**interopérabilité** des systèmes. Les échanges de données entre différents services ou juridictions peuvent en effet générer de nouveaux risques pour la vie privée, ce qui nécessite de vérifier que ces communications respectent les principes de minimisation des données et de sécurité. Par ailleurs, l'EFVP contribue à renforcer la **responsabilité et la gouvernance** des acteurs impliqués dans le système. En clarifiant les rôles et les obligations des différentes organisations, comme les organismes publics, les fournisseurs d'identité ou les fournisseurs de services, elle favorise une meilleure reddition de comptes et un encadrement plus clair du traitement des données. Enfin, cette démarche peut également soutenir l'objectif de **souveraineté numérique** en examinant les choix liés à l'hébergement des données, à leur localisation et au cadre juridique applicable. L'analyse permet ainsi de vérifier si les infrastructures utilisées et les flux de données respectent les exigences liées au contrôle et à la juridiction des renseignements personnels. Ainsi, l'EFVP constitue un mécanisme permettant d'opérationnaliser les piliers d'une identité numérique nationale en les traduisant en critères d'analyse concrets. Elle permet d'identifier les écarts entre les principes souhaités et les pratiques réelles, et de proposer des mesures correctives adaptées.

En résumé, ce chapitre a permis de présenter le modèle d'EFVP et d'exposer les principales obligations légales et méthodologiques qui encadrent son application dans le domaine de l'identité numérique. Ces bases théoriques servent de fondement à l'analyse qui suit. Dans le chapitre suivant, nous appliquerons ce modèle à un exemple fictif, QuébecConnect, inspiré d'eIDAS et de FranceConnect, afin d'illustrer concrètement comment une EFVP peut être réalisée dans le contexte canadien et québécois.

CHAPITRE 4
APPLICATION DU MODÈLE D'EFVP À UN EXEMPLE FICTIF : QUÉBECCONNECT

Le chapitre précédent a établi le cadre méthodologique de l'EFVP : ses fondements, ses obligations légales au Québec, et les catégories de risques à examiner à chaque étape du cycle de vie des données. Ce cadre reste toutefois général, indépendant de tout contexte technologique ou institutionnel particulier. Ce chapitre franchit une étape supplémentaire en appliquant cette EFVP à un projet fictif mais réaliste, afin de montrer comment les choix architecturaux et institutionnels d'un système d'identité numérique font émerger des risques concrets que le modèle général ne peut anticiper seul.

4.1 Mise en scène : eIDAS en tant que cadre fédéral canadien

Dans cette application fictive, *eIDAS* est considéré comme le cadre fédéral canadien pour l'identité numérique. Pour rappel, *eIDAS* (*Electronic Identification*, *Authentication and Trust Services*) est un cadre législatif européen adopté en 2014 par l'Union européenne (Union européenne, 2014). Il vise à faciliter les interactions numériques transfrontalières entre les états membres, en garantissant que les solutions d'identification électronique et les services de confiance soient reconnus de manière uniforme dans toute l'Union. Chaque pays peut mettre en place sa propre solution d'identité numérique, à condition qu'elle respecte les exigences définies par eIDAS. Dans notre exemple, chaque province canadienne adopte un schéma d'identité spécifique, adapté à ses besoins locaux, tout en respectant des normes fédérales fictives inspirées d'eIDAS.

Pour le Québec, nous avons choisi un modèle inspiré de *FranceConnect* (FranceConnect, 2025), en raison des similarités législatives, linguistiques et culturelles entre le Québec et la France. FranceConnect est une plateforme centralisée d'authentification, lancée en 2016 par le gouvernement français, reposant sur le protocole *OpenID Connect* (OpenID Foundation, 2014a). Son fonctionnement est simple : l'usager peut se connecter à de nombreux services publics avec un seul identifiant, sans avoir à créer de compte pour chaque plateforme. Il suffit de posséder un compte auprès d'un des fournisseurs d'identité partenaires,tels que Impots.gouv.fr (portail fiscal), Ameli.fr (portail de l'Assurance Maladie), MSA (sécurité sociale agricole), L'Identité Numérique La Poste (solution d'authentification certifiée par l'État), France Identité (projet d'identité numérique souveraine), YRIS et TrustMe (fournisseurs privés d'identité numérique et de signature électronique).

4.2 Fonctionnement technique de QuébecConnect

QuébecConnect est une solution fictive de fédération d'identité, jouant le rôle d'intermédiaire entre des services en ligne québécois (fournisseurs de services) et plusieurs fournisseurs d'identité reconnus (comme des organismes gouvernementaux ou des institutions partenaires). Elle est directement inspirée du modèle technique de *FranceConnect* (DINUM, 2025), ce qui justifie l'utilisation de sa documentation officielle comme base de référence pour la description qui suit. Lorsque certaines informations spécifiques ne sont pas explicitement détaillées dans cette documentation, elles ont été complétées en s'appuyant sur des exemples issus de solutions comparables, ainsi que sur les meilleures pratiques observées en matière d'identité numérique, de sécurité des échanges et de protection des renseignements personnels.

Lorsqu'un utilisateur souhaite accéder à un service partenaire, il peut choisir de s'authentifier via QuébecConnect. Il est alors redirigé vers la plateforme, qui lui présente une liste de fournisseurs d'identité partenaires. L'utilisateur sélectionne celui avec lequel il possède déjà un compte, puis procède à l'authentification auprès de ce fournisseur. Techniquement, QuébecConnect repose sur le protocole *OpenID Connect*, qui est une extension du protocole OAuth 2.0 (DINUM, 2025). Ce protocole permet à un fournisseur de service d'initier une demande d'authentification via un point d'accès sécurisé (/authorize). L'utilisateur est ensuite redirigé vers un fournisseur d'identité partenaire choisi pour s'authentifier.

Une fois l'utilisateur authentifié, un *ID Token* est transmis au fournisseur de service, accompagné éventuellement d'un *access token*. Ce jeton contient des informations sur l'authentification, ainsi que des attributs sur l'utilisateur, appelés *claims* (DINUM, 2025). Il est également possible pour le fournisseur de service de récupérer des informations supplémentaires via l'endpoint /userinfo (France Connect, 2024). Les données accessibles dépendent des *scopes* (autorisations) demandés par le service, comme *given_name*, *family_name* ou *birthdate* (DINUM, 2025). Seules les informations correspondant à ces scopes sont transmises, dans le respect du protocole, et uniquement après consentement explicite de l'utilisateur.

- *given_name* : prénoms de l'utilisateur (séparés par des espaces)
- *family_name* : nom de famille de naissance
- *birthdate* : date de naissance (format YYYY-MM-DD)
- *gender* : sexe (valeurs possibles : male, female)
- *birthplace* : code INSEE du lieu de naissance (ou vide si né à l'étranger)
- *birthcountry* : code INSEE du pays de naissance
- *sub* : identifiant technique unique (non corrélable entre services)

— *email* : adresse électronique de contact de l'utilisateur

— *preferred_username* : nom d'usage (facultatif).

Toutes ces données ne sont transmises que si elles ont été explicitement demandées via les *scopes OpenID Connect*, et uniquement après validation par l'utilisateur.

4.3 Description du projet QuébecConnect

Le but de cette section est de présenter en détail le projet *QuébecConnect* : sa définition et ses objectifs, le contexte de son apparition, l'échéancier prévu et son utilité pour les organisations. Elle décrit ensuite les rôles et responsabilités des acteurs impliqués, les renseignements personnels concernés et le cycle de vie de ces données, avant d'évaluer les critères de proportionnalité et de rappeler les principales obligations de conformité applicables.

4.3.1 Définition du projet et ses objectifs dans QuébecConnect

QuébecConnect est un système qui vise à fournir aux citoyens québécois une identité numérique unique et sécurisée leur permettant d'accéder à une multitude de services publics et privés. Il s'agit de créer une plateforme interopérable avec les autres provinces canadiennes et les services fédéraux, tout en répondant aux exigences réglementaires du Québec. Le but principal de QuébecConnect est de faciliter les démarches administratives des citoyens en regroupant leurs identités numériques sous une seule interface tout en leur offrant le contrôle sur leurs données personnelles. Ce projet a également pour ambition de diminuer les risques de fraude, de simplifier la gestion des identifiants et d'améliorer l'expérience utilisateur grâce à une meilleure sécurisation des transactions numériques. QuébecConnect propose aux citoyens québécois un accès simplifié et sécurisé à une large gamme de services, regroupés sous les catégories suivantes :

1. **Administration.** QuébecConnect permet aux citoyens de s'authentifier pour accéder à plusieurs services administratifs en ligne, tels que la déclaration et le paiement des impôts provinciaux auprès de Revenu Québec, la demande ou le renouvellement de documents officiels (passeport, permis de conduire, carte d'assurance maladie via la RAMQ), ou encore le changement d'adresse automatisé auprès de plusieurs ministères grâce au Service québécois de changement d'adresse (SQCA).
2. **Santé.** QuébecConnect donne accès au Dossier Santé Québec (DSQ) et aux démarches liées à l'assurance maladie, comme la demande d'une carte ou l'obtention d'une attestation d'assurance.
3. **Transports.** QuébecConnect permet d'accéder aux services en ligne de la SAAQ, comme la consultation

des points d'inaptitude, le renouvellement du permis ou de l'immatriculation, la déclaration de vente ou d'achat d'un véhicule, ainsi que le paiement des amendes liées aux infractions routières.

4. **Retraite.** QuébecConnect permet aux citoyens de consulter leur relevé de participation au Régime de rentes du Québec (RRQ), d'effectuer des simulations, de déposer des demandes de prestations et d'accéder aux régimes complémentaires administrés par Retraite Québec.
5. **Famille.** QuébecConnect permet aux citoyens de s'authentifier pour accéder à différents services familiaux en ligne. Par exemple, il donne accès à la déclaration de naissance et au livret scolaire numérique, aux prestations familiales (allocations et soutien aux enfants via Retraite Québec), ainsi qu'au carnet de vaccination numérique des enfants.
6. **Travail et activité.** QuébecConnect permet aux citoyens de s'authentifier pour consulter leurs droits sociaux (assurance emploi, aide sociale), accéder aux offres d'emploi via Placement en ligne d'Emploi Québec, ainsi qu'aux programmes de formation et de reconversion offerts par Compétences Québec ou Services Québec.
7. **Logement.** QuébecConnect permet aux citoyens de s'authentifier pour déposer une demande dans le cadre des programmes d'aide au logement, comme le supplément au loyer ou l'accès à un HLM via la Société d'habitation du Québec (SHQ).
8. **Énergie et environnement.** QuébecConnect facilite l'accès aux services liés à la consommation énergétique et à l'environnement. Les citoyens peuvent suivre leurs consommations auprès de fournisseurs comme Hydro-Québec, accéder aux programmes de subventions pour les rénovations écoénergétiques (par exemple Rénoclimat ou Chauffez vert), ainsi que consulter les alertes environnementales et la qualité de l'air diffusées par Environnement Québec.

Contexte de l'apparition du projet. Au Québec, l'accès aux services numériques publics et privés repose aujourd'hui sur une multitude de systèmes d'authentification et de gestion d'identités numériques. Chaque organisme utilise son propre mécanisme, obligeant les utilisateurs à créer et gérer plusieurs comptes pour accéder à différents services. Par exemple, un citoyen doit se connecter à Revenu Québec pour ses déclarations fiscales, à la RAMQ pour gérer sa carte d'assurance maladie, et à Hydro-Québec pour consulter ses factures d'électricité. Cette fragmentation complique les démarches administratives, tout en augmentant les risques d'erreurs et de vulnérabilités, notamment face à l'usurpation d'identité.

Afin de répondre à cette fragmentation, le gouvernement du Québec a mis en place le Service d'authentification gouvernementale (SAG), ayant pour objectif de simplifier l'accès aux services numériques publics en permettant aux citoyens de s'authentifier une seule fois pour accéder à plusieurs services gouvernementaux.

ClicSÉQUR constitue l'un des mécanismes d'accès principaux. *clicSÉQUR* est une solution d'authentification centralisée permettant aux usagers de s'identifier pour accéder à certains services en ligne gouvernementaux. Sur le plan architectural, ce mécanisme s'apparente à un modèle fédéré à fournisseur d'identité unique, dans lequel les ministères et organismes délèguent le processus d'authentification à une entité centrale gérée par l'État, plutôt que de gérer localement leurs propres identifiants.

Bien que clicSÉQUR vise à simplifier les accès, sa portée reste limitée. Il s'agit d'un système utilisé principalement pour les services de l'État provincial. Les systèmes actuels présentent également des limitations importantes en matière de compatibilité avec les services fédéraux et ceux des autres provinces canadiennes. Cette absence d'interopérabilité freine les démarches impliquant plusieurs juridictions, comme l'accès aux prestations fédérales ou la reconnaissance des identités numériques entre provinces. Par ailleurs, les plateformes existantes offrent une expérience utilisateur souvent inefficace, où les utilisateurs doivent répéter les mêmes étapes de vérification et ressaisir leurs informations personnelles auprès de chaque organisme. QuébecConnect répond à ces défis en offrant une solution d'identité numérique interopérable au niveau fédéral. Ce projet centralise et simplifie l'accès aux services, tout en maintenant l'interopérabilité avec les systèmes des autres provinces et du gouvernement fédéral.

Échéancier de mise en œuvre. Le projet QuébecConnect suit un plan de mise en œuvre structuré, permettant une transition progressive vers un système d'identité numérique centralisé :

- **Date de début du projet :** 1er janvier 2025.
- **Durée prévue du projet :** 5 ans, avec des phases clés définies pour assurer une mise en œuvre progressive.
- **Phases du projet :**
  - **Janvier 2025 – Décembre 2025 :** Phase de conception et consultation avec les parties prenantes, y compris les organismes publics et privés.
  - **Janvier 2026 – Juin 2027 :** Développement de l'infrastructure technique, tests de sécurité et intégration des services publics prioritaires.
  - **Juillet 2027 – Décembre 2027 :** Phase pilote dans certaines régions pour tester l'interopérabilité et recueillir les retours des utilisateurs.
  - **Janvier 2028 – Décembre 2029 :** Déploiement généralisé et intégration des services privés et interprovinciaux.

Utilité du projet pour l'organisation. QuébecConnect offre des avantages significatifs aux organisations

publiques et privées impliquées dans la gestion des identités numériques. En centralisant l'authentification et en harmonisant les processus, le projet permet de réduire les coûts liés au maintien de systèmes redondants. Les organismes peuvent se concentrer sur l'amélioration de leurs services plutôt que sur la gestion technique des identités numériques. Le projet améliore également l'efficacité opérationnelle grâce à l'interopérabilité entre les systèmes. Cela facilite la coordination entre les différents ministères et partenaires privés. Sur le plan de la sécurité, le fait de centraliser l'authentification évite aux utilisateurs d'avoir à créer et gérer plusieurs comptes pour chaque service. Cela réduit les risques liés à la réutilisation de mots de passe, à l'oubli d'identifiants ou à la multiplication de points de vulnérabilité. En concentrant l'accès dans un cadre unifié, QuébecConnect permet un meilleur contrôle des accès et une meilleure protection contre les tentatives de fraude ou d'usurpation d'identité.

4.3.2 Définition les rôles et les responsabilités dans QuébecConnect

Identification des responsables du projet dans le contexte de QuébecConnect. Le projet QuébecConnect mobilise plusieurs acteurs clés, identifiés comme suit. Certains sont fictifs, d'autres s'inspirent d'acteurs réels afin de proposer une mise en situation crédible.

- **L'entreprise en charge du projet.** QuébecConnect Inc., par l'entremise de sa Division des solutions numériques sécurisées, agit en tant que prestataire technique principal du projet. Son rôle consiste à concevoir l'architecture technique de la plateforme d'identité numérique, à en assurer le développement, la maintenance continue ainsi que l'intégration avec les systèmes gouvernementaux. Reconnue pour son expertise en cybersécurité et en interopérabilité, l'entreprise met à profit son savoir-faire dans le domaine des solutions numériques destinées au secteur public québécois, ce qui justifie pleinement son implication dans la démarche.
- **La personne responsable du projet.** Le projet est placé sous la responsabilité d'un directeur de projet rattaché à la Division des projets numériques du Ministère de la Cybersécurité et du Numérique. Son rôle consiste à superviser la coordination des différentes parties prenantes, à gérer les budgets et les échéanciers, et à veiller au respect des objectifs fixés. Son implication vise à garantir que la mise en œuvre de la plateforme demeure conforme aux besoins du gouvernement québécois.
- **Les organismes publics ou privés impliqués.** Plusieurs organismes publics et parapublics sont associés au projet afin d'assurer son intégration et son efficacité. Revenu Québec, organisme fiscal du gouvernement du Québec, est chargé d'intégrer les services d'accès aux informations fiscales au sein de la fédération QuébecConnect et d'en garantir la disponibilité. La Régie de l'assurance maladie du

Québec (RAMQ), en tant qu'organisme de gestion de la santé, intervient pour intégrer les services de santé et permettre un accès sécurisé aux dossiers médicaux. Hydro-Québec, participe quant à elle à l'intégration des services énergétiques et à l'accès sécurisé aux données de consommation des citoyens. La CAI assure un rôle de supervision juridique dans le projet. Elle veille à la conformité légale des processus d'évaluation et de traitement des données, en mettant à profit son expertise en matière de protection des renseignements personnels et d'application des lois québécoises. Enfin, le Ministère de la Cybersécurité et du Numérique, en tant qu'organisme porteur du projet au sein du gouvernement du Québec, assure la coordination de l'ensemble des parties prenantes et met à disposition les ressources nécessaires pour le déploiement de QuébecConnect. Son implication est essentielle afin de garantir une gouvernance centralisée et cohérente, ainsi que l'interopérabilité des systèmes utilisés par les différents organismes impliqués.

Identification des responsables de l'évaluation dans le contexte de QuébecConnect. Pour garantir la conformité à la législation sur la vie privée et minimiser les risques liés au traitement des renseignements personnels, les responsables de l'EFVP sont identifiés comme suit. Les noms mentionnés dans cette section sont fictifs et servent uniquement à illustrer le processus.

- **Sophie Martin.** Analyste en protection des renseignements personnels à la Division de l'évaluation des risques du Ministère de la Cybersécurité et du Numérique, elle est chargée de réaliser l'EFVP, d'identifier les risques pour la vie privée et de recommander les mesures d'atténuation. Son implication repose sur son expertise dans l'analyse des impacts sur la vie privée et la conformité réglementaire.
- **Jessica Cooper.** Responsable de la protection des renseignements personnels (RPRP) au Bureau du RPRP du même ministère, elle supervise la conformité globale à la Loi 25, valide l'EFVP et coordonne les actions correctives. Sa participation est motivée par sa responsabilité légale d'assurer que les traitements de données respectent les obligations prévues par la loi.
- **Philippe Lavoie.** Chercheur en cybersécurité à SECUQAM, au Laboratoire de recherche en sécurité informatique de l'Université du Québec à Montréal. Il analyse les mécanismes de sécurité, identifie les vulnérabilités potentielles et propose des solutions techniques fondées sur les dernières avancées scientifiques. Il apporte ainsi une expertise académique sur la robustesse des infrastructures numériques.
- **Hélène Desrochers.** Juriste spécialisée en droit de la vie privée au Service juridique de la CAI, elle vérifie la conformité légale de l'EFVP et formule des recommandations juridiques. Son rôle est essentiel pour garantir le respect des cadres législatifs applicables en matière de protection des renseignements personnels.

4.3.3 Identifier les renseignements personnels concernés dans QuébecConnect

- **Identité et informations personnelles de base.** Les données concernent les attributs d'identité de l'utilisateur, notamment le nom de naissance, le nom d'usage le cas échéant, les prénoms, la date, le lieu et le pays de naissance, le sexe ainsi que l'adresse électronique. Ces informations sont reçues, avec le consentement de l'utilisateur, auprès du fournisseur d'identité (par exemple la RAMQ ou Revenu Québec) au moment de l'authentification. Elles sont utilisées uniquement pour transmettre au service partenaire demandeur les attributs nécessaires, et ne sont partagées qu'avec les services explicitement autorisés par l'utilisateur. QuébecConnect ne conserve pas ces données de manière permanente : elles ne sont utilisées que durant la session d'authentification, tandis que les fournisseurs de services appliquent leurs propres politiques de conservation. La finalité de leur traitement est de permettre un accès sécurisé et personnalisé aux services concernés. L'accès à ces données est limité aux seuls fournisseurs de services partenaires. Ces renseignements concernent toutes les personnes utilisant QuébecConnect pour accéder aux services numériques du gouvernement québécois, citoyens, résidents permanents et temporaires, représentant plusieurs millions de profils d'identification. Ils ne sont disponibles que durant la session et ne sont pas stockés au-delà, leur portée étant restreinte aux services publics provinciaux du Québec.
- **Données de connexion et d'authentification.** Les données traitées incluent les jetons d'authentification conformes au protocole OpenID Connect, l'adresse IP, la date et l'heure de connexion, un identifiant technique unique ainsi que l'historique des services utilisés via QuébecConnect. Ces informations sont recueillies afin de vérifier l'identité de l'utilisateur auprès du fournisseur d'identité lors de l'accès à un service partenaire, de sécuriser et de maintenir la continuité des échanges, et de fournir aux partenaires, uniquement pendant la session, les jetons nécessaires à l'accès autorisé. Contrairement aux attributs d'identité, certains de ces éléments, comme les journaux techniques (incluant l'identifiant pseudonymisé, l'adresse IP, l'horodatage, l'identifiant du service sollicité et les codes d'état de la connexion) peuvent être conservés à des fins de sécurité, d'audit et de détection d'anomalies. Leur finalité est de garantir la sécurité, la traçabilité et la transparence des authentifications et des connexions. L'accès à ces données est strictement restreint aux équipes techniques autorisées du gouvernement, aux fournisseurs d'identité et aux services concernés. Elles concernent tous les utilisateurs actifs de QuébecConnect et génèrent quotidiennement un volume important de journaux de connexion, conservés entre six mois et deux ans. Le stockage est effectué exclusivement au Québec et soumis aux lois québécoises sur la protection des renseignements personnels.

4.3.4 Description du cycle de vie des données dans QuébecConnect

Le cycle de vie des renseignements personnels dans le cadre de QuébecConnect suit les étapes standardisées adaptées aux spécificités des systèmes d'identité numérique. Le tableau 4.1 présente un modèle structurant les méthodes de collecte, les entités impliquées, et les finalités des données dans le système QuébecConnect.

Type de données	**Méthodes de collecte**	**Personnes / partenaires impliqués**	**Finalité de la collecte**
Identité et informations personnelles de Base	Inscription auprès de fournisseurs d'identité partenaires	Utilisateurs, fournisseurs d'identité partenaires	Identification, authentification pour accéder aux services publics et privés
Informations de Connexion et d'Authentification	Interfaces de connexion, protocole OpenID Connect	Utilisateurs, fournisseurs de service, fournisseurs d'identité (responsables de la vérification initiale et de la génération des jetons d'authentification)	Sécurisation des connexions, validation des identités, authentification des utilisateurs auprès des services
Historique des connexions et activités	Journaux de connexion	QuébecConnect, utilisateurs	Traçabilité, sécurité, audit
Données contextuelles (IP, appareil utilisé)	Métadonnées collectées automatiquement lors des connexions	Utilisateurs, administrateurs techniques QuébecConnect	Renforcement de la sécurité, analyse des comportements pour détecter les activités suspectes

Table 4.1 Cycle de vie des données dans QuébecConnect : méthodes de collecte, acteurs impliqués et finalités.

Collecte et accès aux données. Les données personnelles, comme le nom, le prénom, la date de naissance ou l'adresse courriel, sont collectées par les fournisseurs d'identité lors de l'inscription initiale ou au moment de l'accès à un service. QuébecConnect n'en conserve aucune copie permanente : il agit uniquement comme intermédiaire technique pour l'authentification, en s'appuyant sur un identifiant pseudonymisé unique généré pour chaque fournisseur de service. En revanche, certaines métadonnées techniques (telles que l'adresse IP, les journaux de connexion et les horodatages) sont collectées afin d'assurer la sécurité, la traçabilité et l'audit des opérations. Enfin, les données d'authentification sont transmises de manière sécurisée par le protocole OpenID Connect, avec chiffrement en transit.

Catégories de personnes ayant accès. Seuls les administrateurs techniques de QuébecConnect disposent d'un accès limité aux données sous sa responsabilité, en particulier les journaux de connexion et les métadonnées techniques. Cet accès se fait en lecture seule et inclut les identifiants pseudonymisés, les horodatages et les adresses IP. L'objectif est d'assurer la traçabilité des accès, de détecter d'éventuelles anomalies de sécurité et de garantir le bon fonctionnement du service d'authentification.

Utilisation des données. Les données collectées sont utilisées par les administrateurs techniques de QuébecConnect, au moment de chaque tentative ou succès d'authentification, et sont hébergées exclusivement sur des serveurs sécurisés situés au Québec. Leur usage vise la surveillance du système, la détection des activités suspectes, la production de rapports d'audit ainsi que le maintien de la disponibilité du service.

Communication des données. Les destinataires des données sont les fournisseurs de services partenaires, qui reçoivent uniquement les jetons d'authentification nécessaires à l'accès via le protocole OpenID Connect. QuébecConnect ne transmet donc pas directement de données personnelles. Les communications sont réalisées exclusivement dans la province de Québec et encadrées par le chiffrement des échanges, en recourant à des identifiants pseudonymisés. Toute interconnexion éventuelle avec d'autres juridictions respecte les exigences légales applicables.

Conservation, destruction et anonymisation. Les journaux de connexion, comprenant notamment les identifiants pseudonymisés et les métadonnées, sont conservés pour une durée maximale de deux ans. Ces données sont hébergées sur des infrastructures sécurisées situées au Québec. À l'expiration de ce délai, elles font l'objet soit d'une anonymisation par suppression des identifiants indirects, soit d'une destruction sécurisée. Ce processus est déclenché automatiquement, conformément à une politique interne qui prévoit des événements précis, tels que l'expiration du délai légal ou la fermeture d'un compte.

Moyens utilisés pour traiter et conserver les renseignements personnels. Les traitements de données sont réalisés exclusivement sur des serveurs sécurisés situés au Québec, avec des mécanismes sécurisés de contrôle d'accès, une journalisation systématique des activités administratives et le chiffrement de toutes les communications. QuébecConnect utilise des bases de données techniques destinées à stocker temporairement des journaux de connexion pseudonymisés, comprenant notamment des identifiants techniques, des horodatages et des adresses IP. Afin d'assurer la résilience du système, des copies de sauvegarde chiffrées sont générées régulièrement, avec des politiques d'accès strictement limitées et des

règles de rétention définies à l'avance. Aucun renseignement personnel n'est conservé sous forme papier.

Moyens utilisés pour détruire ou anonymiser les renseignements personnels. Les journaux et métadonnées techniques sont supprimés de manière sécurisée à l'expiration de la période de conservation prévue. Dans certains cas, ces données peuvent être préalablement anonymisées, par exemple pour produire des statistiques internes comme le nombre d'authentifications réalisées sur une période donnée, sans qu'il soit possible d'identifier à nouveau les personnes concernées. Enfin, dans les rares situations où des documents liés à la sécurité ou à l'administration du système ont été imprimés, leur destruction est assurée par déchiquetage, garantissant ainsi la confidentialité des informations.

4.3.5 Évaluation des critères de proportionnalité dans QuébecConnect

Évaluation du degré de sensibilité des renseignements personnels traités. QuébecConnect traite uniquement les renseignements nécessaires pour identifier un utilisateur et vérifier son accès à un service. Les données concernées sont les suivantes : les *jetons d'authentification pseudonymisés* comme les ID Token et Access Token, qui servent à valider une session sans dévoiler directement l'identité de l'utilisateur ainsi que les *métadonnées de connexion* comme par exemple l'adresse IP, le type d'appareil ou l'heure de la connexion. Ces données sont utilisées pour assurer la sécurité et garder une trace des accès. QuébecConnect ne conserve aucune donnée directement identifiable (comme le nom, le prénom ou le courriel). Ces informations restent sous la responsabilité des fournisseurs d'identité. Le tableau 4.2 ci-dessous résume le niveau de sensibilité des principales données utilisées par QuébecConnect, selon leur rôle et les risques en cas de mauvaise utilisation.

Évaluer la finalité de l'utilisation ou de la communication des renseignements personnels. QuébecConnect joue uniquement le rôle d'intermédiaire entre les fournisseurs d'identité et les fournisseurs de services. Il ne traite que les données nécessaires pour faire fonctionner le service. Ces données sont utilisées pour deux finalités principales qui sont l'*authentification*, qui correspond à permettre à un utilisateur de prouver son identité de façon sécurisée à chaque connexion, sans transmettre directement son nom, prénom ou courriel, ainsi que la *traçabilité*, qui vise à garder des journaux pseudonymisés pour pouvoir détecter des problèmes de sécurité ou des comportements suspects. Aucune donnée directement identifiable n'est utilisée par QuébecConnect pour d'autres raisons, et rien n'est transmis à des tiers en dehors des partenaires directement impliqués (comme les fournisseurs d'identité ou de services).

Type de données	Sensibilité	Justification
Jetons d'authentification (ID Token, Access Token)	Élevée	Ces jetons permettent de valider une session et d'accéder aux services. S'ils sont interceptés, quelqu'un pourrait se connecter à la place de l'utilisateur, ce qui pose un risque important pour la sécurité.
Métadonnées de connexion (adresse IP, type d'appareil, heure)	Moyenne	Elles servent à détecter des activités suspectes ou à retracer des connexions. Même si elles ne révèlent pas directement l'identité, elles peuvent parfois permettre d'identifier des habitudes ou des localisations.

Table 4.2 Degré de sensibilité des données traitées dans QuébecConnect.

Évaluation de la quantité de renseignements personnels. QuébecConnect limite la quantité de données traitées en suivant le principe de minimisation : seules les informations strictement nécessaires à l'authentification sont prises en compte. Le système s'adresse à l'ensemble de la population du Québec, soit environ 8,5 millions de personnes, avec la possibilité d'une extension à l'échelle fédérale dans le futur. Le volume de données demeure restreint, puisqu'il se compose essentiellement d'informations pseudonymisées, principalement les jetons d'authentification, et de quelques métadonnées techniques comme l'adresse IP, la date et l'heure de connexion. Même si le nombre total de transactions peut s'avérer très élevé à l'échelle provinciale, la quantité d'informations traitées pour chaque utilisateur reste minimale. En ce qui concerne la conservation, les journaux techniques de connexion sont gardés pour une période limitée, variant entre six mois et deux ans, principalement pour des raisons de sécurité, de traçabilité et d'audit.

Évaluation de la répartition des renseignements personnels. Dans QuébecConnect, les renseignements personnels traités (pseudonymisés) sont répartis selon différents aspects, autant techniques qu'organisationnels. Le tableau 4.3 résume cette répartition en trois dimensions : où les données sont stockées, qui y a accès, et combien de personnes sont concernées.

Évaluation des supports de conservation des renseignements personnels. Dans QuébecConnect, les renseignements pseudonymisés sont conservés uniquement sur des supports numériques. Plus précisément, les

Dimension	Description	Considérations pour QuébecConnect
Spatiale	Localisation des données (centralisée ou décentralisée)	Les données pseudonymisées sont stockées dans des infrastructures sécurisées situées au Québec.
Humaine / administrative	Accès aux données par des entités internes ou externes (ex. : partenaires, prestataires)	Les accès sont limités aux administrateurs techniques de QuébecConnect et aux fournisseurs d'identité et de services, uniquement dans le cadre de leurs rôles respectifs et avec des droits restreints.
Quantitative	Supports de stockage et nombre d'utilisateurs concernés	Les données sont hébergées sur un nombre restreint de serveurs sécurisés, et leur traitement s'applique à l'ensemble de la population québécoise (environ 8,5 millions de personnes).

Table 4.3 Répartition des données dans QuébecConnect.

principaux éléments sont (1) les *serveurs sécurisés* car les données sont stockées sur des serveurs localisés au Québec, qui respectent les normes en vigueur pour protéger les renseignements personnels, et (2) les *mesures de sécurité* mises en place. En pratique, l'accès à ces données est protégé par du chiffrement, des pare-feux et une authentification renforcée pour éviter les accès non autorisés.

4.3.6 Conformité et liste des obligations de protection des renseignements personnels dans QuébecConnect

QuébecConnect doit respecter plusieurs lois sur la protection des renseignements personnels. Cette section présente les principales règles à suivre et les engagements pris pour bien gérer les données. QuébecConnect s'aligne sur deux lois importantes au Québec :

- **Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (Loi sur l'accès).** Cette loi encadre la façon dont les organismes publics doivent gérer les renseignements personnels, en assurant leur confidentialité, leur sécurité et un accès juste à l'information.
- **Loi sur la protection des renseignements personnels dans le secteur privé (Loi 25).** QuébecConnect

applique les principes de cette loi pour encadrer la collecte, l'utilisation, la communication, la conservation et la destruction des données personnelles. La loi impose également la réalisation d'une EFVP pour repérer les risques et mettre en place des mesures de protection.

Ces lois couvrent tout le cycle de vie des données personnelles, et QuébecConnect s'engage à les respecter à chaque étape.

Si QuébecConnect devait, à l'avenir, être utilisé dans un cadre plus large (national ou international), il devrait aussi se conformer à d'autres lois comme la LPRPDE (Canada), le RGPD (Europe) ou le CCPA (États-Unis), selon le cas. Cela inclurait des exigences comme le consentement explicite, le droit d'accès ou de suppression des données, et la protection des transferts à l'international. QuébecConnect applique plusieurs pratiques internes pour bien protéger les renseignements personnels. Les politiques internes sur la gestion des données encadrent chaque étape du traitement des renseignements personnels, qu'il s'agisse de leur collecte, de leur utilisation, de leur conservation ou encore de leur suppression. Des procédures documentées sont mises en place afin que les employés disposent de directives claires sur la manière d'appliquer les règles de confidentialité et d'assurer le respect des obligations en vigueur. Un calendrier de conservation précise la durée pendant laquelle les données peuvent être conservées. Une fois ce délai écoulé, elles doivent être détruites ou anonymisées de manière sécuritaire.

Des audits réguliers sont réalisés par QuébecConnect pour vérifier la conformité des pratiques et s'assurer que les règles établies sont bien respectées dans l'ensemble des opérations. Enfin, une documentation technique détaillant l'architecture, les technologies utilisées et les mesures de sécurité mises en œuvre est maintenue à jour. Celle-ci permet de garantir la transparence et facilite les contrôles lors des audits de sécurité ou de conformité. Pour assurer une sécurité optimale, une interopérabilité avec d'autres systèmes et une gestion responsable des renseignements personnels, QuébecConnect s'appuie sur des normes internationales reconnues et sur des cadres de référence adaptés aux systèmes d'identité numérique. Le règlement eIDAS canadien, inspiré du cadre européen, sert de modèle pour établir un cadre commun d'identification électronique et de services de confiance pouvant fonctionner de manière interopérable à l'échelle fédérale.

Sur le plan technique, QuébecConnect repose sur le protocole OpenID Connect, basé sur OAuth 2.0, qui constitue un standard largement reconnu pour l'authentification sécurisée et l'autorisation des accès aux services. Enfin, les niveaux d'assurance (LoA) offrent un mécanisme pour qualifier la fiabilité de l'authen-

tification. Bien que QuébecConnect ne réalise pas l'authentification directement, il peut permettre aux fournisseurs de services de connaître le niveau de garantie de l'identité utilisée, en fonction du fournisseur d'identité choisi, selon un modèle inspiré du règlement eIDAS, qui distingue trois niveaux (faible, substantiel, élevé) selon la fiabilité de l'authentification.

4.4 Identification des risques d'atteinte à la vie privée et évaluation de leurs conséquences dans le contexte de QuébecConnect

Cette section a pour but d'identifier les principaux risques d'atteinte à la vie privée dans le cadre de QuébecConnect, à chaque étape du cycle de vie des données : collecte, utilisation, communication, conservation ou destruction. Pour structurer cette analyse, nous utilisons le modèle PANOPTIC™, une taxonomie développée par MITRE à partir de centaines de cas réels. Elle permet de mieux comprendre les types d'atteintes possibles à la vie privée, leurs causes et conséquences, et de proposer des stratégies concrètes pour les réduire. Chaque sous-section présente un tableau qui résume ces risques selon le modèle PANOPTIC™, avec une attention particulière portée à leur lien avec les obligations légales québécoises.

4.4.1 Risques à la collecte

Le tableau 4.4 présente les principaux risques liés à la collecte des données dans QuébecConnect, en utilisant les codes du modèle PANOPTIC™. Cette taxonomie, développée par MITRE à partir de cas réels, sert à mieux comprendre les atteintes possibles à la vie privée et à évaluer leurs conséquences. Elle permet aussi de structurer les mesures à mettre en place pour réduire ces risques de façon concrète.

Description du risque	**Causes**	**Conséquences**	**Stratégie d'atténuation**
Collecte excessive de données (**PA03.08**)	Absence de principe de minimisation ou collecte de données non nécessaires	Risque de violation des données, non-conformité aux lois québécoises et internationales	Revoir régulièrement les flux d'authentification pour s'assurer que seules les données strictement nécessaires sont demandées. Éviter l'ajout automatique de champs non utilisés dans les appels aux fournisseurs d'identité.

Description du risque	Causes	Conséquences	Stratégie d'atténuation
Collecte non autorisée ou sans consentement(**PA02.03, PA02.06)**	Défaut dans les mécanismes de consentement ou absence d'options d'opt-out	Perte de confiance des utilisateurs, sanctions légales, atteinte à la vie privée	Afficher une demande de consentement claire avant chaque transmission de données (scopes), avec la possibilité pour l'utilisateur de refuser certains champs. Garder une trace du choix de l'utilisateur.
Absence de transparence sur la collecte (**PA01.04**)	Notice insuffisante ou absente pour les utilisateurs	Manque d'information claire sur les données collectées et leur finalité	Présenter, avant la connexion, un résumé clair des données collectées et de leur usage, accompagné d'un lien vers la politique de confidentialité. Fournir également un accès à une documentation technique vulgarisée expliquant le fonctionnement de QuébecConnect (acteurs impliqués, étapes de transmission, règles de sécurité, etc.), afin que les usagers puissent comprendre comment leurs données circulent.
Surveillance non déclarée (**PA03.04**)	Collecte de données techniques (ex. : IP, horodatage) à l'insu de l'utilisateur, sans avis clair	Atteinte à la vie privée, non-conformité aux exigences de transparence et de consentement	Ajouter une mention claire de ces collectes dans la politique de confidentialité.

Description du risque	**Causes**	**Conséquences**	**Stratégie d'atténuation**
Appropriation des identifiants numériques (**PA05.01**)	Utilisation de techniques d'identification implicite, exemple : utilisation de données techniques comme l'adresse IP ou l'appareil pour reconnaître un utilisateur, même sans utiliser son nom.	Profilage involontaire ou suivi de l'utilisateur à son insu, pouvant mener à une réidentification ou à une atteinte à la vie privée.	Limiter l'usage des identifiants techniques à ce qui est strictement nécessaire, anonymiser les données dès que possible et éviter leur réutilisation entre services.
Collecte de données hors du cadre prévu (**PA06.09.01**)	Utilisation des données pour d'autres objectifs que ceux annoncés.	Risque de non-respect de la loi sur la finalité des données, perte de confiance des citoyens.	Définir précisément à quoi chaque donnée peut servir dans la documentation du projet. Interdire toute réutilisation pour d'autres finalités, sauf après un nouvel accord de l'utilisateur.
Données insuffisamment anonymisées (**PA06.07**)	Techniques d'anonymisation faibles ou dépassées, comme l'utilisation d'identifiants techniques partagés entre services	Risque de réidentification, notamment en croisant les données entre services. **Exemple :** Si deux fournisseurs de services utilisent un même identifiant de session, ils pourraient en déduire qu'un utilisateur a accédé aux deux services, même sans connaître son identité.	Utiliser des techniques d'anonymisation sécurisées, éviter les identifiants réutilisables entre services, et tester régulièrement leur efficacité.

Table 4.4: Risques à la collecte des données pour QuébecConnect, intégrant les éléments PANOPTIC avec leurs stratégies d'atténuation.

L'analyse des risques associés à la collecte des données dans QuébecConnect montre que plusieurs menaces proviennent directement de la manière dont les informations sont demandées et utilisées dès les premières étapes du processus d'authentification. Les risques identifiés concernent principalement la collecte excessive de données, l'absence de consentement clair, ainsi qu'un manque de transparence quant aux informations réellement transmises aux différents acteurs du système. Ces situations peuvent mener à des atteintes à la vie privée, à une perte de confiance des utilisateurs ou encore à une non-conformité avec les exigences juridiques applicables.

4.4.2 Risques à l'utilisation

Le tableau 4.5 identifie les principaux risques liés à l'utilisation des données dans l'écosystème QuébecConnect, en s'appuyant sur le modèle PANOPTIC™ pour mieux comprendre les menaces à la vie privée et proposer des mesures concrètes pour y répondre.

Description du Risque	**Causes**	**Conséquences**	**Stratégie d'atténuation**
Accès non autorisé aux données collectées (**PA04.01**)	Sécurité insuffisante (pas de chiffrement, mots de passe faibles, etc.)	Fuite d'informations sensibles ou vol d'identité	Mettre en place un chiffrement de bout en bout (au repos et en transit), activer l'authentification multifacteur pour tous les comptes ayant accès aux données sensibles, et appliquer des règles strictes de gestion des accès fondées sur les rôles. Des audits de sécurité doivent être réalisés régulièrement pour détecter d'éventuels accès non autorisés.
Données interceptées pendant leur envoi (**PA04.02**)	Envoi de données via des connexions non sécurisées ou trop anciennes	Des personnes malveillantes peuvent intercepter les données pendant leur transmission	Utiliser des connexions sécurisées (comme HTTPS ou TLS), tester régulièrement les systèmes pour repérer et corriger les failles.
Préférences de confidentialité ignorées (**PA02.04**)	Les choix de l'utilisateur (ex. : refuser le partage) ne sont pas respectés à cause d'une mauvaise configuration	L'utilisateur peut perdre confiance, sa vie privée peut être atteinte, et l'organisme peut être sanctionné	Configurer les systèmes pour qu'ils respectent toujours les préférences des utilisateurs, et faire des vérifications et des audits régulièrement.

Description du Risque	**Causes**	**Conséquences**	**Stratégie d'atténuation**
Faible sécurité lors de l'utilisation des données (**PA04.05**)	Permissions mal configurées ou trop larges, par exemple : des employés ou systèmes peuvent accéder à des données sensibles sans que ce soit nécessaire	Risque de fuite d'informations, mauvaise utilisation des données, atteinte à la vie privée	Restreindre les accès selon les rôles, chiffrer les données même pendant leur utilisation, et faire des contrôles et audits réguliers pour détecter les erreurs de configuration.
Utilisation des données pour d'autres buts que ceux annoncés (**PA13.02**)	Données utilisées pour des raisons non prévues ou non expliquées aux utilisateurs, sans leur accord	Les personnes perdent confiance, et cela peut violer les lois sur la protection des données	Encadrer strictement les usages des données et exiger un consentement clair avant toute nouvelle utilisation.
Failles d'intégrité des données (**PA04.04**)	Absence de vérification des changements ou de sauvegardes fiables	Altération ou perte de données, perturbation des services	Mettre en place des journaux d'activité, automatiser la détection d'anomalies, et sauvegarder régulièrement les données critiques.
Réidentification des données anonymisées (**PA06.07**)	Utilisation de techniques d'anonymisation insuffisantes	Violation de la vie privée, risques accrus de discrimination	Appliquer des méthodes robustes de dépersonnalisation, évaluer régulièrement leur efficacité.
Ciblage abusif des utilisateurs (**PA11.02**)	Analyse des données pour cibler des utilisateurs spécifiques à des fins discriminatoires ou invasives	Discrimination, perte de confiance des utilisateurs	Établir des audits éthiques pour les algorithmes de ciblage, limiter les données utilisées pour le ciblage.

Description du Risque	**Causes**	**Conséquences**	**Stratégie d'atténuation**
Manipulation des utilisateurs (**PA11.03**)	Utilisation des données pour influencer de manière inappropriée les décisions des utilisateurs	Atteinte à l'autonomie des utilisateurs, exploitation abusive	Prohiber les pratiques manipulatrices dans les interfaces utilisateur, effectuer des évaluations régulières des pratiques.
Vente des données pour des fins commerciales (**PA11.05**)	Utilisation abusive des données pour générer des revenus sans consentement	Perte de confiance des utilisateurs, sanctions légales	Interdire explicitement la vente des données personnelles sans consentement, auditer régulièrement les pratiques pour assurer leur conformité.

Table 4.5: Risques à l'utilisation des données dans QuébecConnect, avec éléments PANOPTIC et stratégies d'atténuation.

L'analyse des risques liés à l'utilisation des données dans l'écosystème QuébecConnect montre que les menaces proviennent principalement de la manière dont les informations sont manipulées, partagées ou exploitées une fois collectées. Les risques identifiés concernent notamment les accès non autorisés, l'interception des données lors de leur transmission, l'utilisation des informations à des fins différentes de celles annoncées ainsi que les failles dans le respect des préférences de confidentialité des utilisateurs.

4.4.3 Risques liés à la communication

La communication des données entre les différents acteurs de QuébecConnect (fournisseur d'identité, fournisseur de service, gouvernement) comporte plusieurs risques techniques et organisationnels. Le tableau 4.6 identifie ces risques, leurs causes, leurs impacts potentiels, et propose des stratégies d'atténuation .

Description du Risque	**Causes**	**Conséquences**	**Stratégie d'atténuation**
Transmission de données d'authentification via des canaux non sécurisés (**PA04.02**)	Failles dans la configuration des connexions HTTPS ou envoi de jetons d'accès sans chiffrement	Interception des identifiants par des tiers malveillants, accès non autorisé aux services	S'assurer que tous les échanges entre les acteurs (fournisseur d'identité, QuébecConnect, fournisseur de service) utilisent des connexions sécurisées (HTTPS, TLS, etc), et effectuer des audits réguliers de la configuration.
Partage non autorisé des données avec des tiers (**PC02.05, PA10.02**)	Accès ou transfert de données sans consentement explicite ou sans encadrement contractuel suffisant	Fuite d'informations sensibles, non-respect des lois sur la protection des renseignements personnels	Limiter les échanges aux tiers autorisés, encadrer les partages par des ententes officielles, et effectuer des audits de conformité réguliers.
Réidentification des données anonymisées (**PA06.07, PA05.01.01**)	Techniques avancées de réidentification appliquées à des données partiellement anonymisées	Violation de la vie privée, divulgation d'identités cachées, risques légaux	Appliquer des techniques d'anonymisation robustes (ex. : confidentialité différentielle, suppression de variables indirectement identifiantes), limiter l'accès aux jeux de données sensibles aux seules personnes autorisées et effectuer régulièrement des tests de réidentification pour évaluer le niveau réel d'anonymat.
Non-respect des exigences légales de communication transfrontalière (**PA13.04**)	Méconnaissance ou non-respect des lois locales et internationales sur les transferts de données	Sanctions légales, perte de confiance des utilisateurs, impact sur les relations internationales	Réaliser des audits de conformité réguliers, se conformer aux lois locales et internationales sur les données.

Description du Risque	Causes	Conséquences	Stratégie d'atténuation
Utilisation des données à des fins non prévues (**PA13.02**)	Partage de données avec des tiers à des fins différentes de celles autorisées	Atteinte à la vie privée, exploitation commerciale non autorisée, perte de confiance	Encadrer strictement les finalités d'utilisation dans la documentation du système, bloquer par défaut toute réutilisation non conforme, et imposer l'obtention d'un nouveau consentement explicite pour tout usage secondaire ou nouveau traitement. Des audits internes doivent vérifier régulièrement le respect de ces finalités.
Absence de traçabilité dans les communications (**PA04.04**)	Manque de journalisation des échanges de données	Impossible d'identifier les abus ou anomalies, manque de transparence	Inclure dans les journaux d'audit non seulement les flux automatisés entre systèmes, mais aussi les actions manuelles des employés ou administrateurs ayant accès aux données personnelles (consultation, export, modification). Ces journaux doivent être stockés de façon sécurisée et accessibles uniquement pour des vérifications internes ou des enquêtes de sécurité.
Liens indirects entre bases de données (**PA10.02.01, PA05.01.01**)	Corrélation entre plusieurs ensembles de données échangés entre fournisseurs de services	Risque de réidentification non autorisée, atteinte à la vie privée des utilisateurs	Utiliser des identifiants pseudonymes différents pour chaque fournisseur et empêcher les recoupements non autorisés.

Description du Risque	Causes	Conséquences	Stratégie d'atténuation
Altération des données pendant la transmission (**PA04.04**)	Absence de mécanismes d'intégrité ou de vérification des données en transit (ex. : version obsolète de TLS, transmission en clair par erreur de configuration)	Modification involontaire ou malveillante des données, perte de fiabilité du système	S'assurer que tous les échanges entre les acteurs (fournisseur d'identité, QuébecConnect, fournisseur de service) sont chiffrés avec TLS 1.2 ou plus, et que les jetons transmis sont signés et vérifiés systématiquement. Implémenter un contrôle d'intégrité sur tous les points de réception des données.
Partage de données pour des usages non prévus (**PA06.09**)	Manque de supervision sur les partages de données	Non-conformité aux finalités annoncées, sanctions légales	Appliquer une politique stricte sur le partage des données et effectuer des audits réguliers.

Table 4.6: Risques à la communication des données dans QuébecConnect, avec éléments PANOPTIC et stratégies d'atténuation.

L'analyse des risques liés à la communication des données dans QuébecConnect montre que plusieurs menaces apparaissent lors des échanges entre les différents acteurs du système. Les risques identifiés concernent principalement la sécurité des transmissions, le partage non autorisé d'informations, ainsi que la possibilité de réidentification ou d'utilisation des données à des fins non prévues. Ces situations peuvent entraîner des atteintes à la vie privée, des sanctions juridiques ou encore une perte de confiance des utilisateurs envers le système.

4.4.4 Risques à la conservation, à la destruction et/ou à l'anonymisation

Les risques associés à la conservation, à la destruction et à l'anonymisation des données dans le contexte de QuébecConnect sont présentés dans le tableau 4.7, en lien avec les catégories du modèle PANOPTIC et leurs stratégies d'atténuation respectives.

Description du Risque	**Causes**	**Conséquences**	**Stratégie d'atténuation**
Conservation prolongée des données (**PANOPTIC : PA12.01**)	Absence de politique claire de rétention	Risque de violation de données et de non-conformité	Mettre en place une politique de rétention claire pour chaque type de donnée, incluant des délais précis. Automatiser l'effacement à l'échéance, y compris dans les sauvegardes et les journaux. Réaliser des audits réguliers pour vérifier que ces règles sont bien appliquées.
Destruction incomplète ou non sécurisée (**PA12.02**)	Procédures de destruction inadéquates ou absence de contrôle	Données récupérables par des tiers, risque de fuite	Standardiser les procédures de destruction, surveiller leur application, et former les responsables.
Anonymisation insuffisante (**PA06.07**)	Techniques obsolètes ou faibles	Réidentification des utilisateurs, atteinte à la vie privée	Appliquer des méthodes avancées d'anonymisation, Tester régulièrement l'efficacité des techniques à l'aide de scénarios de réidentification, former les équipes techniques sur les bonnes pratiques d'anonymisation, et ajuster les approches en fonction des risques identifiés.

Description du Risque	**Causes**	**Conséquences**	**Stratégie d'atténuation**
Stockage dans des environnements non sécurisés (**PA04.02**)	Absence de chiffrement ou de sécurité suffisante	Accès non autorisé, compromission des données sensibles	Mettre en place un chiffrement fort des données, centraliser et sécuriser la gestion des clés, restreindre l'accès aux environnements de stockage, et auditer régulièrement la configuration des serveurs. Former les équipes responsables à la sécurisation des environnements de stockage.
Accès non contrôlé aux sauvegardes (**PA04.05**)	Permissions mal configurées ou absence de contrôle	Divulgation non autorisée, risques accrus pour la sécurité	Appliquer des politiques strictes de contrôle d'accès aux sauvegardes, chiffrer systématiquement les données archivées, et journaliser toutes les opérations d'accès ou de restauration. Réaliser des audits réguliers des droits associés aux sauvegardes et former le personnel concerné aux bonnes pratiques de sécurité.
Non-respect des exigences légales en matière de conservation et de suppression (**PA13.04**)	Ignorance ou mauvaise application des lois encadrant la durée de conservation, la destruction ou l'anonymisation des données	Sanctions juridiques, atteinte à la réputation de QuébecConnect	Former les équipes aux obligations légales applicables, mettre en place un calendrier de conservation validé juridiquement, auditer les pratiques réelles de suppression et destruction, et adapter les politiques internes à l'évolution de la réglementation.

Table 4.7: Risques à la conservation, destruction et anonymisation des données dans QuébecConnect, intégrant PANOPTIC.

L’analyse des risques liés à la conservation, à la destruction et à l’anonymisation des données dans Québec-Connect montre que plusieurs menaces apparaissent lorsque les données sont conservées trop longtemps, supprimées de manière incomplète ou insuffisamment anonymisées. Ces situations peuvent entraîner des violations de données, des risques de réidentification des utilisateurs ou encore un accès non autorisé aux informations archivées, notamment à travers les sauvegardes.

4.4.5 Conclusion de l’EFVP

L’application du modèle d’EFVP au cas fictif de QuébecConnect a permis d’illustrer de manière concrète comment une identité numérique nationale peut être analysée à partir de ses dimensions techniques, organisationnelles et juridiques. Au-delà de la seule identification des risques, cette démarche a aussi permis de préciser les rôles des acteurs impliqués, les catégories de renseignements personnels concernées, leur cycle de vie, ainsi que les exigences de proportionnalité et de conformité applicables dans un tel système.

L’analyse met en évidence que les principaux enjeux ne se limitent pas à la sécurité technique, mais concernent également la gouvernance des données, la transparence des traitements, la limitation des finalités, la qualité des mécanismes de consentement, ainsi que les conditions de conservation, de communication et d’anonymisation des renseignements personnels. Les mesures de mitigation proposées reposent sur une combinaison de garanties techniques, telles que le chiffrement, la pseudonymisation, la journalisation et le contrôle strict des accès, et de garanties organisationnelles et juridiques, comme la documentation des finalités, les audits réguliers, les politiques de conservation et la conformité aux lois applicables.

Ainsi, cette étude de cas montre que l’EFVP ne constitue pas seulement un outil d’identification des risques, mais aussi un cadre structurant pour guider la conception d’un système d’identité numérique respectueux de la vie privée dès ses premières phases de développement. Dans le cas de QuébecConnect, elle permet de rendre visibles les arbitrages nécessaires entre interopérabilité, efficacité administrative, sécurité et protection des droits des citoyens.

CHAPITRE 5
CONCLUSION

5.1 Résumé du mémoire

Ce mémoire explore la mise en œuvre d'une INN respectueuse de la vie privée à partir de l'analyse du projet de loi n°82 et de l'adaptation du modèle d'EFVP au contexte de l'identité numérique. L'objectif principal est de comprendre comment une architecture d'identité peut concilier innovation technologique, efficacité administrative et respect des droits fondamentaux des citoyens.

Le premier chapitre présente les bases de l'INN à la fois sur les plans technique et conceptuel. Il décrit les trois grandes architectures de l'identité numérique : isolée, fédérée et décentralisée, et montre comment chacune influence la gestion des données personnelles et la confiance entre les acteurs. L'architecture isolée sépare les systèmes pour limiter les risques, mais elle manque d'interopérabilité. Le modèle fédéré, comme celui de FranceConnect, unifie la gestion de l'identité, ce qui simplifie l'accès aux services mais crée des dépendances et des risques de corrélation. Le modèle décentralisé, reposant sur les DID, cherche à redonner à l'utilisateur le contrôle sur ses données grâce à des mécanismes de preuve et de divulgation sélective. Toutefois, ce modèle reste encore récent : les technologies qui le soutiennent sont encore en développement et font l'objet de normalisations progressives à l'échelle internationale. Ainsi, l'application des principes de (Allen, 2016) au modèle décentralisé montre que la véritable décentralisation ne dépend pas seulement de la technologie utilisée, mais de la manière dont le pouvoir et la confiance sont répartis entre les acteurs. Peu de systèmes actuels respectent entièrement ces principes, ce qui souligne la difficulté de construire une INN réellement auto-souveraine.

Le mémoire s'est également intéressé à l'intégration de la protection de la vie privée dans la conception des systèmes d'identité numérique. L'adaptation du modèle d'EFVP à ce domaine permet d'analyser l'impact des choix technologiques et organisationnels sur les données personnelles. Cette approche a été illustrée à travers le cas fictif QuébecConnect, inspiré de FranceConnect et du cadre européen eIDAS, afin de montrer comment une province pourrait mettre en place une INN tout en respectant les exigences légales et les principes de protection de la vie privée.

5.2 Contributions principales

Ce mémoire apporte plusieurs contributions à la réflexion sur la mise en œuvre d'une identité numérique nationale respectueuse de la vie privée. Une première contribution réside dans l'analyse des mémoires déposés lors des consultations publiques entourant le projet de loi n°82. Cette analyse a permis d'identifier les principaux enjeux soulevés par les parties prenantes et de dégager les piliers structurants qui devraient guider le déploiement d'une INN, notamment la protection de la vie privée, la sécurité, la gouvernance, l'interopérabilité, l'inclusion et la transparence. Une deuxième contribution concerne l'analyse technique des architectures d'identité numérique et l'évaluation comparative des protocoles d'authentification. Les critères issus de la littérature scientifique ont été adaptés afin de refléter les exigences spécifiques d'un système d'identité numérique fédéré dans un contexte gouvernemental. Une troisième contribution est méthodologique et consiste en l'adaptation du modèle d'EFVP au contexte particulier de l'identité numérique. Cette adaptation permet d'intégrer les enjeux techniques, organisationnels et juridiques dans l'analyse des systèmes d'identité numérique. Enfin, l'application de ce modèle à un cas fictif, QuébecConnect, constitue une contribution supplémentaire en illustrant concrètement comment une EFVP peut être utilisée pour analyser les choix technologiques et organisationnels liés à un projet d'INN.

5.3 Pistes de recherche futures

Cette recherche présente certaines limites. Elle repose principalement sur une analyse documentaire et ne comprend pas de validation empirique. De plus, les critères d'évaluation ont été adaptés au contexte québécois, ce qui peut limiter leur généralisation à d'autres environnements. Ces limites ouvrent plusieurs perspectives de recherche. Des études empiriques pourraient notamment être menées auprès des citoyens afin de mieux comprendre leurs attentes, leurs craintes et les conditions d'acceptabilité sociale d'une INN. De futures recherches pourraient également explorer plus en détail l'implémentation technique des architectures décentralisées et des mécanismes de preuve cryptographique, afin d'évaluer leur applicabilité dans des systèmes gouvernementaux réels. En somme, ce mémoire propose un cadre d'analyse permettant de mieux comprendre les enjeux liés à la mise en œuvre d'une identité numérique nationale respectueuse de la vie privée. Il montre que la conception d'une telle infrastructure nécessite une approche intégrée combinant considérations techniques, juridiques et organisationnelles. Les travaux futurs devront poursuivre cette réflexion en intégrant davantage de données empiriques et en analysant les solutions techniques émergentes dans ce domaine.

BIBLIOGRAPHIE

Commission d'Accès à l'Information du Québec (2024). Réaliser une évaluation des facteurs relatifs à la vie privée : Guide d'accompagnement à la démarche et à sa documentation. *Commission d'Accès à l'Information du Québec*.

Aide Pédagogique aux Adultes et aux Jeunes (APAJ) (2025). Mémoire sur le projet de loi n° 82 - loi concernant l'identité numérique nationale et modifiant d'autres dispositions. Mémoire disponible dans la section « Mémoires déposés », consulté le 27 février 2025. Récupéré de https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CFP/mandats/Mandat-52625/memoires-deposes.html

Alaca, F. et Oorschot, P. C. V. (2020). Comparative analysis and framework evaluating web single sign-on systems. *ACM Computing Surveys*.

Allen, C. (2016). The path to self-sovereign identity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

Almeida, J. R., Zúquete, A., Pazos, A. et Oliveira, J. L. (2024). A federated authentication schema among multiple identity providers. *Heliyon*, *10*(7), e28560. http://dx.doi.org/10.1016/j.heliyon.2024.e28560. Récupéré le 2025-09-10 de https://doi.org/10.1016/j.heliyon.2024.e28560

Assemblée Nationale du Québec (2024). Loi concernant l'identité numérique nationale et modifiant d'autres dispositions.

Association québécoise des technologies (AQT) (2025). Positions et recommandations sur le projet de loi n° 82. Mémoire disponible dans la section « Mémoires déposés », consulté le 27 février 2025. Récupéré de https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CFP/mandats/Mandat-52625/memoires-deposes.html

Au, M. H., Susilo, W. et Mu, Y. (2006). Constant-size dynamic k-taa. Dans R. De Prisco et M. Yung (dir.). *Security and Cryptography for Networks*, 111–125., Berlin, Heidelberg. Springer Berlin Heidelberg.

Auth0 (2024). Qu'est-ce qu'oauth 2.0 ? Récupéré le 2025-07-09 de https://auth0.com/fr/intro-to-iam/what-is-oauth-2

Avellaneda, O., Bachmann, A., Barbir, A., Brenan, J., Dingle, P., Duffy, K. H., Maler, E., Reed, D. et Sporny, M. (2019). Decentralized identity : Where did it come from and where is it going ? *IEEE Communications Standards Magazine*, *3*(4), 10–13. http://dx.doi.org/10.1109/MCOMSTD.2019.9031542

Ben Ayed, G. (2011). Digital identity metadata scheme : A technical approach to reduce digital identity risks. Dans *2011 IEEE Workshops of International Conference on Advanced Information Networking and Applications*, 607–612. http://dx.doi.org/10.1109/WAINA.2011.118

Boneh, D., Boyen, X. et Shacham, H. (2004). Short group signatures. Cryptology ePrint Archive, Paper 2004/174. Récupéré de https://eprint.iacr.org/2004/174

BSN Development Association (2024). Realdid official website. Récupéré le 2025-05-06 de https://did.bsnbase.com

Catuogno, L. et Galdi, C. (2014). Interoperability between federated authentication systems. Dans *2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, 493–498. http://dx.doi.org/10.1109/IMIS.2014.71

Chambre des notaires du Québec (2025). Commentaires de la chambre des notaires relativement au projet de loi n° 82 - loi concernant l'identité numérique nationale et modifiant d'autres dispositions. Mémoire disponible dans la section « Mémoires déposés », consulté le 27 février 2025. Récupéré de https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CFP/mandats/Mandat-52625/memoires-deposes.html

Chari, S. B., Ruj, S., Rajarajan, M. et Saxena, N. (2021). The role of trust in oauth 2.0 and openid connect. Dans *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 492–501. IEEE. http://dx.doi.org/10.1109/EuroSPW54576.2021.00057

Comité de parents du Centre de services scolaire de la Capitale (2024). Rapport du comité de parents du centre de services scolaire de la capitale concernant le projet de loi n° 82 - loi concernant l'identité numérique nationale et modifiant d'autres dispositions. Mémoire disponible dans la section « Mémoires déposés », consulté le 27 février 2025. Récupéré de https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CFP/mandats/Mandat-52625/memoires-deposes.html

Commission de l'éthique en science et en technologie (CEST) (2025). Mémoire sur le projet de loi n° 82 - loi concernant l'identité numérique nationale et modifiant d'autres dispositions. Mémoire disponible dans la section « Mémoires déposés », consulté le 27 février 2025. Récupéré de https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CFP/mandats/Mandat-52625/memoires-deposes.html

Commission d'accès à l'information du Québec (CAI) (2025). Projet de loi n°82 - loi concernant l'identité numérique et modifiant d'autres dispositions. Mémoire disponible dans la section « Mémoires déposés », consulté le 27 février 2025. Récupéré de https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CFP/mandats/Mandat-52625/memoires-deposes.html

DIACC's Trust Framework Expert Committee TFEC (2025). *Pan-Canadian Trust Framework : Overview*. Rapport technique, DIACC

Dimova, Y., Van Goethem, T. et Joosen, W. (2023). Everybody's looking for ssomething : A large-scale evaluation on the privacy of oauth authentication on the web. *Proceedings on Privacy Enhancing Technologies*, *2023*(4), 452–467. Récupéré le 2025-09-10 de https://doi.org/10.56553/popets-2023-0119

DINUM (2025). Présentation générale pour les fournisseurs d'identité — documentation franceconnect. Récupéré le 2025-09-10 de https://docs.partenaires.franceconnect.gouv.fr/fi/general/fi-general-presentation/

Dodanduwa, K. et Kaluthanthri, I. (2018). Role of trust in oauth 2.0 and openid connect. Dans *2018 IEEE*

International Conference on Information and Automation for Sustainability (ICIAfS), 1–4. http://dx.doi.org/10.1109/ICIAFS.2018.8913384

Doerner, J., Kondi, Y., Lee, E., Shelat, A. et Tyner, L. (2023). Threshold bbs+ signatures for distributed anonymous credential issuance. Dans *2023 IEEE Symposium on Security and Privacy (SP)*, 773–789. http://dx.doi.org/10.1109/SP46215.2023.10179470

eduGAIN (2024). edugain saml profile. Récupéré le 2025-03-16 de https://technical.edugain.org/doc/eduGAIN-saml-profile.pdf

eIDAS Expert Group (2024). *European Digital Identity Wallet Architecture and Reference Framework*. European Digital Identity Wallet Project

Esther Saurí (2023). Everything you need to know about the eudi wallet. https://gataca.io/blog/eudi-wallet/.

Fantenberg, J. (2022). Single sign-on (sso) vs. federated identity : A complete guide. Récupéré le 2025-09-10 de https://www.pingidentity.com/en/resources/blog/post/sso-vs-federated-identity-management.html

Fett, D., Yasuda, K. et Campbell, B. (2025). *Selective Disclosure for JWTs (SD-JWT)*. Internet-Draft draft-ietf-oauth-selective-disclosure-jwt-17, OAuth Working Group, IETF

France Connect (2024). Présentation du protocole openid connect - franceconnect. Récupéré le 2025-03-16 de https://docs.partenaires.franceconnect.gouv.fr/fi/openid-connect/oidc-presentation/

FranceConnect (2025). Tout savoir sur franceconnect. Consulté le 7 mars 2025. Récupéré le 2025-03-07 de https://franceconnect.gouv.fr/franceconnect

Fédération des cégeps (2025). Projet de loi n°82 - loi concernant l'identité numérique nationale et modifiant d'autres dispositions : Mémoire de la fédération des cégeps. Mémoire disponible dans la section « Mémoires déposés », consulté le 27 février 2025. Récupéré de https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CFP/mandats/Mandat-52625/memoires-deposes.html

Gariépy, F. et al. (2023). Guide sur les conditions et bonnes pratiques pour la mise en place d'une identité numérique nationale. Coordination et rédaction : Félix Gariépy, Comité aviseur : Benoit Dupont, Céline Castets-Renard, Hugo Loiseau, Lyse Langlois, Nadia Tawbi, Pierre-Martin Tardif, Sébastien Gambs, Steve Jacob.

Google Identity (2024). *Using OAuth 2.0 to Access Google APIs*

Gouvernement du Québec (2021). Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (2021, chapitre 25).

Gouvernement du Québec (2024a). A-2.1 - loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. À jour au 1er octobre 2024. Récupéré le 2025-09-10 de https://www.legisquebec.gouv.qc.ca/fr/document/lc/A-2.1

Gouvernement du Québec (2024b). P39.1 - Loi sur la protection des renseignements personnels dans le secteur privé. Récupéré le 2025-09-10 de https://www.legisquebec.gouv.qc.ca/fr/document/lc/P-39.1

Hardt, D. (2012). *The OAuth 2.0 Authorization Framework*. Rapport technique 6749, Internet Engineering Task Force (IETF)

Hébert, V., Fortin, A., Émilie Michaud, Bourque, R., Cimon, V., Johnson, M. L. et Clerc, I. (2024). La fracture numérique : contexte québécois, pistes d'action et perspectives internationales.

Institut de gouvernance numérique (IGN) (2025). L'identité numérique auto-souveraine : Principe clé de l'identité numérique nationale. Mémoire disponible dans la section « Mémoires déposés », consulté le 27 février 2025. Récupéré de https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CFP/mandats/Mandat-52625/memoires-deposes.html

Institut multidisciplinaire en cybersécurité et cyberrésilience (IMC²) (2025). Mémoire de l'imc² dans le cadre des consultations particulières et auditions publiques sur le projet de loi n°82 - loi concernant l'identité numérique nationale et modifiant d'autres dispositions. Mémoire disponible dans la section « Mémoires déposés », consulté le 27 février 2025. Récupéré de https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CFP/mandats/Mandat-52625/memoires-deposes.html

International Organization for Standardization (2013). ISO/IEC 29115 : Information technology — Security techniques — Entity authentication assurance framework.

International Organization for Standardization and International Electrotechnical Commission (2022). *ISO/IEC 27001 :2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. Rapport technique, International Organization for Standardization

International Organization for Standardization and International Electrotechnical Commission (2024). *ISO/IEC 29100 :2024 - Technologies de l'information — Techniques de sécurité — Cadre privé*. Rapport technique, International Organization for Standardization

Jeyakumar, I. H. J., Chadwick, D., Sporny, M., van Deventer, O., Suzuki, S., Tsabolov, K., Kofoed, L. et Joosten, R. (2025). Verifiable Issuers and Verifiers v0.2. https://www.w3.org/verifiable-iv/.

Kloza, D., Calvi, A., Casiraghi, S., Maymir, S. V., Ioannidis, N., Tanas, A. et van Dijk, N. (2020). Data protection impact assessment in the european union : developing a template for a report from the assessment process. http://dx.doi.org/10.31228/osf.io/7qrfp. Récupéré le 2025-09-10 de https://doi.org/10.31228/osf.io/7qrfp

Leclerc, G. (2025). Notes d'allocution de la vérificatrice générale devant la commission des finances publiques sur le projet de loi n° 82 : Loi concernant l'identité numérique nationale et modifiant d'autres dispositions. Allocution prononcée le 29 janvier 2025 (fait foi). Récupéré de https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CFP/mandats/Mandat-52625/memoires-deposes.html

Ligue des droits et libertés (2025). Loi concernant l'identité numérique nationale et modifiant d'autres

dispositions. Mémoire disponible dans la section « Mémoires déposés », consulté le 27 février 2025. Récupéré de https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CFP/mandats/Mandat-52625/memoires-deposes.html

Loiseau, H., Caron, D. J., Gambs, S. et Brousseau, S. (2025). Pour une identité numérique québécoise au service des citoyens : enjeux et recommandations. Mémoire disponible dans la section « Mémoires déposés », consulté le 27 février 2025. Récupéré de https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CFP/mandats/Mandat-52625/memoires-deposes.html

Micrologic (2025). Projet de loi n°82 - loi concernant l'identité numérique nationale et modifiant d'autres dispositions. Mémoire disponible dans la section « Mémoires déposés », consulté le 27 février 2025. Récupéré de https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CFP/mandats/Mandat-52625/memoires-deposes.html

Milberry, K. et Parsons, C. (2013). *A National ID Card by Stealth ? The BC Services Card : Privacy Risks, Opportunities and Alternatives*. Rapport technique, The British Columbia Civil Liberties Association.

MITRE Corporation (2024). *PANOPTIC Privacy Threat Model : Taxonomy and Applications*. Rapport technique, MITRE Corporation

Mole, C., Chalstrey, E., Foster, P. et Hobson, T. (2023). Digital identity architectures : comparing goals and vulnerabilities. *arXiv preprint*. Récupéré de https://arxiv.org/abs/2302.09988

Mouvement Desjardins (2025). Mémoire du mouvement desjardins : Projet de loi 82 - loi concernant l'identité numérique nationale et modifiant d'autres dispositions. Mémoire disponible dans la section « Mémoires déposés », consulté le 27 février 2025. Récupéré de https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CFP/mandats/Mandat-52625/memoires-deposes.html

National Institute of Standards and Technology (2017). *Digital Identity Guidelines (SP 800-63-3)*. Rapport technique, U.S. Department of Commerce

OASIS Security Services Technical Committee (2005). *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard

OpenID Foundation (2014a). Openid connect core 1.0. https ://openid.net/specs/openid-connect-core-1_0.html.

OpenID Foundation (2014b). *OpenID Connect Core 1.0 – incorporating errata set 1*

Orange Developer (2024). *Mobile Connect*

Parlement Européen et Conseil de l'Union Européenne (2024). Règlement (UE) 2024/1183 du Parlement Européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) no 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R1183. Consulté le 12 mai 2025.

Président-directeur général de la Régie de l'assurance maladie du Québec (2025). *Allocution du président-directeur général de la Régie de l'assurance maladie du Québec à l'intention de la Commission des finances publiques*. Rapport technique, Régie de l'assurance maladie du Québec (RAMQ). Mémoire disponible dans la section « Mémoires déposés », consulté le 27 février 2025

Pöhn, D., Grabatin, M. et Hommel, W. (2023). Modeling the threats to self-sovereign identities. http://dx.doi.org/10.18420/OID2023_07

Regroupement des groupes populaires en alphabétisation du Québec (RGPAQ) (2025). Avis soumis à la Commission des finances publiques dans le cadre des consultations particulières sur le projet de loi 82 : Loi concernant l'identité numérique nationale et modifiant d'autres dispositions. Mémoire disponible dans la section « Mémoires déposés », consulté le 27 février 2025. Récupéré de https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CFP/mandats/Mandat-52625/memoires-deposes.html

RGPD (2024). Qu'est-ce qu'une donnée personnelle ? Récupéré le 2025-09-10 de https://www.rgpd.com/basiques/quest-ce-quune-donnee-personnelle

Roio, D. (2025). The problems in the european digital identity (eudi). Récupéré le 2025-09-10 de https://news.dyne.org/the-problems-of-european-digital-identity/

Roio, D., Selvaggini, R., Bellini, G. et Dintino, A. (2024). Sd-bls : Privacy preserving selective disclosure of verifiable credentials with unlinkable threshold revocation. Dans *2024 IEEE International Conference on Blockchain (Blockchain)*, 505–511. http://dx.doi.org/10.1109/Blockchain62396.2024.00074

Réseau d'informations scientifiques du Québec (RISQ) (2025). Projet de loi n°82 - loi concernant l'identité numérique nationale et modifiant d'autres dispositions. Mémoire disponible dans la section « Mémoires déposés », consulté le 27 février 2025. Récupéré de https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CFP/mandats/Mandat-52625/memoires-deposes.html

Schardong, F. et Custódio, R. (2022). Self-sovereign identity : A systematic review, mapping and taxonomy. *Sensors*, *22*(15), 5641. http://dx.doi.org/10.3390/s22155641

Sharif, A., Ranzi, M., Carbone, R., Sciarretta, G., Marino, F. et Ranise, S. (2022). The eidas regulation : A survey of technological trends for european electronic identity schemes. *Applied Sciences*. http://dx.doi.org/10.3390/app122412679

Steve Waterhouse (2025). Consultations particulières et auditions publiques sur le projet de loi n° 82, loi concernant l'identité numérique nationale et modifiant d'autres dispositions. Mémoire disponible dans la section « Mémoires déposés », consulté le 27 février 2025. Récupéré de https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CFP/mandats/Mandat-52625/memoires-deposes.html

Syndicat de la fonction publique et parapublique du Québec (SFPQ) (2025). Mémoire déposé aux fins du projet de loi 82 - loi concernant l'identité numérique nationale et modifiant d'autres dispositions. Mémoire disponible dans la section « Mémoires déposés », consulté le 27 février 2025. Récupéré de https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CFP/

mandats/Mandat-52625/memoires-deposes.html

Union européenne (2014). Règlement (ue) n° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur. https ://eur-lex.europa.eu/legal-content/FR/TXT/ ?uri=CELEX :32014R0910. Consulté le 6 juillet 2025.

Université de sherbrooke (2022). *Guide d'encadrement sécuritaire de l'identité numérique*. Rapport technique, Université de sherbrooke. Version du 25 mars 2022.

Wu, K. et Yu, X. (2009). A model of unite-authentication single sign-on based on saml underlying web. Dans *2009 Second International Conference on Information and Computing Science*, volume 2, 211–213.