UNIVERSITÉ DU QUÉBEC À MONTRÉAL

L'API CITOYEN :
UN FORMAT D'ÉCHANGE POUR LES ORGANISMES PUBLICS

RAPPORT DE PROJET
PRÉSENTÉ
COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN GÉNIE LOGICIEL

PAR
FRANÇOIS DESMARAIS

JUILLET 2019

[Cette page a été laissée intentionnellement blanche]

REMERCIEMENTS

Je tiens à remercier les nombreuses personnes qui ont pris le temps d'écouter mon propos sur le sujet de l'identité citoyenne depuis mars 2017. J'essaie de les nommer tous, en ordre chronologique : Yves Gauthier pour son encadrement et sa vision, Stephen Russet, Morgan Martinet, Jean-François Marcoux, les autres membres du *Comité des APIs* de la Ville de Montréal (Martin Janelle, Malek Chioua, Stéphane Leblanc), Luciana Brusa et Driton Salihu pour leur contribution au concept des organisations, Thomas Chauvet pour sa contribution au concept des validations, Jean-Martin Thibault pour sa grande vision m'amenant à me dépasser et à amener l'API Citoyen plus loin encore, François Boulet de la Ville de Longueuil ainsi que les autres membres du *Comité identité et services numériques*. Je remercie également mes réviseurs, Éric Moreau, Astrid Leclerc et Blandine Émilien. Je remercie aussi Stéphane Guidouin d'avoir insisté pour que je sois présent au *Défi des villes intelligentes*, où j'ai pu creuser les concepts de l'identité décentralisée.

Au niveau académique, je remercie MM. Normand Séguin et Claude Y. Laporte pour leur extrême patience ainsi que l'équipe du Département informatique de l'UQAM pour m'avoir épaulé et avoir répondu à mes nombreuses questions, liées à mon cheminement particulier.

Merci au restaurant *La Petite Marche* pour les nombreux cafés. Merci à mon grand-père, qui est toujours un modèle de curiosité intellectuelle. Merci à mon père qui, dès mon jeune âge, a insisté sur l'importance de l'école, en plus de m'enseigner à toujours bien faire les choses. Je remercie aussi ma mère, sans qui tout ceci n'aurait pas été possible, car en plus de m'encourager à finir la dernière partie de la maîtrise,

elle fut l'une des deux personnes m'ayant incité à me lancer dans des études universitaires en 2004-2005.

Et finalement, un merci tout particulier à ma conjointe, Marianne, qui m'a permis de poursuivre dans cette voie et a tenu le fort de la famille pendant de nombreuses soirées. Sans oublier mes enfants, Antoine et Bastien, que je remercie pour le bonheur qu'ils apportent à ma vie par leur joie de vivre et leurs nombreux encouragements.

AVANT-PROPOS

L'initiative documentée dans ce rapport est issue de la mise en place d'une nouvelle fondation numérique à la Ville de Montréal. Un des objectifs de l'interface de programmation d'applications (API) Citoyen était de ne plus avoir 22 dossiers citoyens différents, un requis émis par le *Bureau de l'expérience client* (BXC) de la Ville de Montréal. Un dossier citoyen représente les renseignements personnels généralement requis par les organismes publics pour offrir un service à un citoyen. Le BXC a commandé une étude à la firme PricewaterhouseCoopers pour obtenir des recommandations sur la mise en place d'un tel dossier (PricewaterhouseCoopers Canada, 2017). La pierre angulaire de ce dossier citoyen intégré – l'API Citoyen – fut réalisée en suivant les principes d'architecture de technologies de l'information (TI) de la Ville de Montréal.

La première difficulté rencontrée au fil du projet fut l'évolution continuelle de l'API Citoyen et du sujet de l'identité numérique. Cela a démontré qu'une représentation numérique constitue un besoin important, et que la solution est évolutive. La seconde difficulté du projet était la possibilité de rencontrer des initiatives parallèles. Cette crainte fut non fondée au moment de finaliser ce rapport, car l'API Citoyen s'est révélé complémentaire aux initiatives parallèles étudiées.

Le présent rapport se veut donc un état des lieux après deux (2) ans et aussi une invitation à divers organismes publics (villes, sociétés d'État, sociétés de transport public, etc.) à utiliser l'API Citoyen proposé pour appuyer leurs projets d'identités et de services numériques. Ce rapport se veut également un point de départ pour l'arrimage avec les autres initiatives donnant appui au mouvement des villes intelligentes et numériques, auquel la Ville de Montréal contribue activement.

De plus, en tant qu'architecte de solutions TI responsable du Dossier citoyen intégré (DCI) de la Ville de Montréal, j'ai eu à discuter de l'API Citoyen avec un grand nombre d'intervenants, de mars 2017 à ce jour. Plusieurs de ces discussions ont été fertiles en nouvelles idées ou en adaptation d'idées existantes. Mon travail consistait donc à centraliser et bien comprendre l'ensemble de ces concepts ou enjeux, tout en supervisant la réalisation des travaux. Le rôle d'architecte de solutions TI implique également d'être l'arbitre devant décider de la façon que le DCI serait réalisé, pour itérer du moment présent vers la cible d'architecture TI, toujours dans le but d'atteindre les objectifs du DCI ou d'enrichir ce dernier.

Au final, j'ai rédigé l'ensemble du présent rapport de projet de synthèse, incluant la préparation des tableaux et des figures, sauf lorsqu'une référence est faite à une autre source. Par souci d'alléger le texte et à la vue du grand nombre de collaborateurs, dont l'identité de certain(e)s doit rester confidentielle, j'ai préparé *l'Annexe A – Générique de document* où je fais la distinction entre ma contribution et celle de l'ensemble des personnes qui ont contribué à l'avancement de l'API Citoyen, que ce soit par une idée, par une question, ou encore, par un bout de code.

[NOTES]

- *Dans ce document, l'emploi du masculin pour désigner des personnes n'a d'autres fins que celle d'alléger le texte.*
- *Dans ce document, les acronymes utilisés sont ceux issus de l'anglais, pour faciliter les liens avec le domaine qui est principalement documenté en anglais.*
- *Bien que l'expression « interface de programmation d'applications (API) » soit un nom féminin, ce document utilise l'expression « API Citoyen » comme un nom propre, au masculin, pour désigner le projet et son implémentation.*
- *Pour respecter la vie privée de mes collègues, leurs noms ont été remplacés par « un collègue » ou « une collègue ».*
- *Finalement, ce rapport de projet de synthèse décrit les ressources de l'API Citoyen d'une façon sommaire, car ce rapport n'est pas une documentation d'API.*

[/FIN DES NOTES]

TABLE DES MATIÈRES

REMERCIEMENTS iii

AVANT-PROPOS v

LISTE DES FIGURES ix

LISTE DES TABLEAUX xi

RÉSUMÉ xiii

ABSTRACT xv

INTRODUCTION 1

CHAPITRE 1 ÉTAT DE L'ART, MANDAT, OBJECTIFS ET HYPOTHÈSES 5

1.1 L'identité citoyenne numérique 5

1.1.1 Quelques définitions 5

1.1.2 État de l'art 8

1.2 Mandat du projet 13

1.3 Objectifs du projet 14

1.3.1 Interopérabilité logicielle entre fournisseurs 14

1.3.2 Interopérabilité entre organismes publics 15

1.3.3 Cas concret envisagé 17

1.4 Hypothèses et limites 18

CHAPITRE 2 DÉMARCHE ET NORMES PERTINENTES 19

2.1 Vue d'ensemble de la démarche 19

2.2 Démarche à la Ville de Montréal 20

2.2.1 Positionnements d'architecture TI 21

2.2.2 Besoins d'affaires de projets concrets 24

2.2.3 Comité des APIs 26

2.3 Démarche au *Comité identité et services numériques* (CISN) 28

2.4 Démarche pour le *Défi des villes intelligentes* (DÉFI) 31

2.5 Normes pertinentes 33

2.5.1 *OpenID Connect* (OIDC) 33

2.5.2 *Système de gestion d'identités interdomaines* (SCIM) 2.0 34

2.5.3 *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ADOP-PRP) 35

2.5.4 *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) 35

CHAPITRE 3 L'API CITOYEN 37

3.1 Contexte de la solution 37

3.1.1 Rappels 37

3.1.2 L'API Citoyen, un service en soi 38
3.1.3 En addition à OIDC 39
3.1.4 En extension à SCIM 2.0 41
3.2 Concepts principaux 42
3.2.1 Individu 43
3.2.2 Organisation 44
3.2.3 Famille 45
3.2.4 Routes et verbes 47
3.2.5 Rôles 49
3.3 Concepts de soutien 50
3.3.1 Consentements 50
3.3.2 Validations 51
3.3.3 Données additionnelles 54
3.3.4 Sécurité 56
3.3.5 Audits et journalisation des accès 58
3.3.6 Historique des adresses et adresses multiples 59
3.3.7 Historique du dossier 61
3.4 Architecture de l'API Citoyen 63
3.4.1 Architecture de haut niveau initiale 63
3.4.2 Arrimage avec la *Fondation pour l'identité décentralisée* (DIF) 64
3.4.3 Arrimage avec le *Cadre de confiance pancanadien* (PCTF) 66
3.4.4 Architecture cible et carte conceptuelle 67

CONCLUSION 69

RÉFÉRENCES 75

GLOSSAIRE 79

ANNEXE A GÉNÈSE DU DOCUMENT 87
1 Éléments paginés 87
2 Éléments conceptuels (non paginés) 97

LISTE DES FIGURES

Figure 1.1 – représentation d'un service multicanal typique 6
Figure 1.2 – flux des renseignements personnels 17
Figure 2.1 – vue d'ensemble de la démarche de l'API Citoyen 20
Figure 2.2 – 1er axe : positionnements d'architecture TI 21
Figure 2.3 – 2e axe : projets concrets 24
Figure 2.4 – 3e axe : comité des APIs (CAPI) de la Ville de Montréal 26
Figure 2.5 – axes du volet CISN de la démarche 28
Figure 2.6 – ligne du temps du Comité identité et services numériques (CISN) 30
Figure 3.1 – interactions typiques entre un fournisseur d'identités et l'API Citoyen 40
Figure 3.2 – relations entre individus, organisations et familles 42
Figure 3.3 – ressources de l'individu 43
Figure 3.4 – ressources de l'organisation 44
Figure 3.5 – ressources de la famille 46
Figure 3.6 – architecture de haut niveau initiale de l'API Citoyen 63
Figure 3.7 – architecture de haut niveau initiale avec un troisième partenaire 64
Figure 3.8 – architecture cible conceptuelle de l'API Citoyen 68

[Cette page a été laissée intentionnellement blanche]

LISTE DES TABLEAUX

Tableau 1.1 – avantages et inconvénients des approches de gestion d'identités numériques 10
Tableau 1.2 – survol des initiatives d'identités numériques gouvernementales 11
Tableau 3.1 – routes et verbes communs des concepts principaux 47
Tableau 3.2 – routes et verbes spécifiques aux individus 48
Tableau 3.3 – routes et verbes spécifiques aux familles et aux organisations 48
Tableau 3.4 – comparaison des rôles prédéfinis entre la famille et l'organisation 49
Tableau 3.5 – principales routes et verbes liés aux consentements 50
Tableau 3.6 – principales routes et verbes liés aux validations 52
Tableau 3.7 – niveau de confiance des renseignements personnels 53
Tableau 3.8 – principales routes et verbes liés aux données additionnelles 54
Tableau 3.9 – principales routes et verbes liés aux audits et aux journaux d'accès 59
Tableau 3.10 – principales routes et verbes liés aux adresses 60
Tableau 3.11 – principales routes et verbes liés à l'historique du dossier 62
Tableau 3.12 – termes et définitions 79

[Cette page a été laissée intentionnellement blanche]

RÉSUMÉ

L'API Citoyen est un format d'échange de style transfert d'état représentationnel (REST) et utilise la notation d'objets JavaScript (JSON). L'API Citoyen vise à faciliter le partage d'identités citoyennes numériques, et les renseignements personnels qu'elles contiennent, entre organismes publics au Québec, lorsqu'un citoyen y consent pour obtenir des services. L'API Citoyen vise aussi à faciliter le transfert d'identités entre systèmes de fournisseurs distincts, à l'intérieur d'un même organisme public, afin de minimiser les coûts de gestion des identités.

Ce projet a émis l'hypothèse que la revue technologique effectuée avant le projet était complète ; revue montrant que les standards existants n'étaient pas suffisants pour les besoins des organismes publics, mais que certains pouvaient servir de points de départ. Afin de minimiser sa complexité, le projet s'est concentré sur les aspects techniques, excluant la gouvernance et l'aspect politique.

L'API Citoyen a été développé à la Ville de Montréal, en collaboration étroite avec le *Comité identité et services numériques* (CISN), issu du *Réseau de l'informatique municipale du Québec* (RIMQ). Il a été conçu pour fonctionner de concert avec le protocole d'authentification *OpenID Connect* (OIDC), en s'appuyant sur le modèle d'extension du *Système de gestion d'identités interdomaines* (SCIM) 2.0. L'API Citoyen bonifie ainsi OIDC avec des capacités requises par les organismes publics, telles la validation des données, le consentement au partage d'identité, l'historique des identités, les audits et la journalisation des accès à l'identité.

Avant de tester le concept de l'identité fédérée, le CISN a adopté une version de l'API Citoyen couvrant les individus et les familles. Une implémentation bonifiée est en préparation à la Ville de Montréal pour supporter les organisations. Dans un objectif à moyen terme, des représentants de la Ville de Montréal discutent avec les membres du *Sous-comité sur la gestion de l'identité* (IMSC) sur l'arrimage possible de l'API Citoyen avec leur projet, le *Cadre de confiance pancanadien* (PCTF).

Mots clés : identité numérique, identité fédérée, organisme public, consentement, API.

[Cette page a été laissée intentionnellement blanche]

THE CITIZEN API: A PROTOCOL FOR PUBLIC ORGANIZATIONS

ABSTRACT

The Citizen API, a protocol based on the JavaScript object notation (JSON) format with the representational state transfer (REST) style, aims to facilitate the sharing of digital citizen identities, including the personal information it contains, among public organizations in Quebec, when a citizen consents to obtain services. The Citizen API also aims to facilitate the transfer of identities between systems of separate vendors within the same organization, to minimize the costs of managing identities.

This project assumed that the technology review conducted prior to the project was complete; this review showed that existing standards were not sufficient for the needs of public organizations, but that some could serve as a starting point. To minimize the complexity of the project, the project focused on the technical aspects and excluded governance and political aspects.

The Citizen API was developed by the City of Montreal, in close collaboration with the *Identity and Digital Services Committee* (CISN), which comes from the *Quebec Municipal Informatics Network* (RIMQ). The Citizen API was designed to work well with the *OpenID Connect* (OIDC) authentication protocol and is based on the extension model of the *System for Cross-Domain Identity Management* (SCIM) 2.0. This enhances OIDC with capabilities required by public organizations, such as validation data, identity sharing consents, identity history, audits and access logs.

Prior to testing the identity federation concept, the CISN adopted a version of the Citizen API covering individuals and families. An enhanced version is also in preparation at the City of Montreal to include support for organizations. The City of Montreal is currently discussing with the *Identity Management Sub-Committee* (IMSC) to assess potential alignments of the Citizen API with their project, the *Pan-Canadian Trust Framework* (PCTF).

Keywords: digital identity, identity federation, public organism, consent, API.

[Cette page a été laissée intentionnellement blanche]

INTRODUCTION

Le domaine de l'informatique municipal au Québec est vaste. Des logiciels participent à la surveillance des traitements de l'eau potable, outillent les équipes des bibliothèques et des ressources humaines, ou encore appuient les équipes de sécurité civile lors d'une situation d'urgence. Un grand nombre de ces systèmes utilisent les renseignements personnels de citoyens pour mettre en application les lois et règlements d'une ville.

Ce projet de synthèse se concentre sur cet aspect, notamment l'identité citoyenne numérique, qui est construite à partir des renseignements personnels généralement requis par les organismes publics pour offrir un service à un citoyen. Le terme « citoyen » est utilisé ici au sens large, incluant les résidents et non-résidents d'une ville, mais aussi les étudiants étrangers, les touristes, les organismes sans but lucratif et les autres formes de personnes morales. De son côté, le terme « organisme public » est utilisé au sens large pour, par exemple, décrire les villes, les sociétés de transport en commun et les autres organismes parapublics, tels que BIXI à Montréal. Ce terme peut aussi s'appliquer aux autres paliers gouvernementaux.

Il n'est pas rare pour un organisme public d'utiliser plusieurs logiciels distincts touchant aux renseignements personnels. La plupart de ces logiciels utilisent une forme de « dossier » qui contient ces données. Toutefois, ces systèmes sont rarement interopérables. Une revue des connaissances effectuée avant le projet a déterminé qu'il n'existe pas de protocole standardisé permettant de facilement transférer les identités citoyennes numériques d'un logiciel à un autre, et encore moins d'un organisme public à un autre. Il existe bien des standards ou techniques pour échanger des profils de personnes, mais ces solutions sont généralement

spécialisées à un domaine d'affaires, ou encore ne permettent pas de représenter les renseignements personnels qu'un organisme public détient avec la finesse ou la précision requise. Par exemple, les standards HL7[1] existent dans le domaine de la santé, mais ne sont pas adaptés au monde municipal où, entre autres, il est requis de qualifier les adresses des citoyens comme ayant été vérifiées ou non.

Une revue des connaissances réalisée avant le projet a montré que la plupart des protocoles d'échanges ont été développés par des organismes privés qui vendent leurs services ou offrent leurs services gratuitement mais avec de la publicité. La nuance est fondamentale, car plusieurs organismes publics offrent des services gratuits ou subventionnés aux citoyens qu'ils desservent. Les organismes publics doivent donc s'assurer de la véracité des renseignements personnels fournis, ce que seuls certains organismes privés réglementés ont l'obligation de faire.

Ces constats ont ouvert la porte au développement d'un format d'échanges d'identités citoyennes numériques qui couvrirait l'ensemble des besoins spécifiques des organismes publics. Le travail a débuté en mars 2017. Une fois établi, ce format d'échange pourrait aider les organismes publics à obtenir de meilleurs prix durant les appels d'offres publics, en incitant certains fournisseurs à se démarquer et à implémenter ce qui pourrait devenir un standard. La porte serait alors ouverte pour une meilleure interopérabilité entre fournisseurs et, par le fait même, entre organismes publics, ce qui pourrait, à moyen terme, minimiser le nombre de fois où un citoyen doit valider ses informations, épargnant des frais de gestion d'identités.

---

[1] Pour en savoir plus, https://www.hl7.org/implement/standards/

Ce rapport de projet de synthèse décrit donc le cheminement ayant mené à l'établissement de l'API Citoyen, une solution de technologies de l'information (TI) répondant à ce besoin des organismes publics. L'API Citoyen a été établi dans le cadre de projets concrets à la Ville de Montréal, en étroite collaboration avec les représentants de plusieurs organismes publics dans le cadre du *Comité identité et services numériques* (CISN). Le mandat de ce comité est d'établir une solution commune, qui inclurait la fédération d'identités.

Ce rapport aborde l'état de l'art, le mandat et les objectifs de la démarche. Le cheminement parcouru durant le projet est décrit, suivi de la description de la solution à proprement parler. Les concepts de la solution sont expliqués, en plus de décrire la preuve de concept réalisée et les liens envisagés avec les autres initiatives recensées, plus particulièrement le *Cadre de confiance pancanadien* (PCTF) (Digital ID and Authentification Council of Canada, 2019).

[Cette page a été laissée intentionnellement blanche]

CHAPITRE 1

ÉTAT DE L'ART, MANDAT, OBJECTIFS ET HYPOTHÈSES

Ce chapitre fait un survol de l'état de l'art lié à l'identité citoyenne numérique dans le contexte des organismes gouvernementaux. C'est l'un des sujets couverts par le mandat du *Comité identité et services numériques* (CISN), qui est un comité de travail du *Réseau de l'informatique municipale du Québec* (RIMQ). Le mandat du projet décrit dans ce rapport est essentiellement le mandat du CISN et est détaillé dans la présente section, suivi des objectifs à atteindre par le CISN, avant d'aborder les limites de ce rapport et les limites du projet lui-même.

1.1 L'identité citoyenne numérique

1.1.1 Quelques définitions

L'identité citoyenne numérique représente l'ensemble des renseignements personnels d'un citoyen, en plus des données permettant d'en attester la véracité pour un organisme public. Un renseignement personnel est une donnée concernant une personne et qui permet de l'identifier. Le terme citoyen est ici utilisé au sens large : les citoyens incluent les individus, les familles et les citoyens corporatifs et autres personnes morales, appelés les organisations. Dans le cas de la Ville de Montréal, il faut y ajouter les touristes, les personnes réfugiées ainsi que les personnes sans papiers, car la Ville de Montréal s'est donné une politique d'accès

sans peur aux services municipaux (Daoust-Brown, 2018). Les organismes publics sont l'ensemble des villes, des sociétés de transport, des sociétés publiques ou parapubliques qui offrent des services aux citoyens.

L'identité citoyenne numérique s'applique aussi dans le mode non numérique, parce qu'un grand nombre d'organismes publics ont l'obligation d'offrir des services de façon multicanale. Un service public multicanal permet au citoyen d'amorcer, de poursuivre ou de compléter une interaction avec un organisme public par le biais de plusieurs canaux de communications, que ce soit via un site Web, une application mobile, par téléphone, en personne, par courriel, par télécopieur ou par la poste, comme le représente la figure ci-dessous.

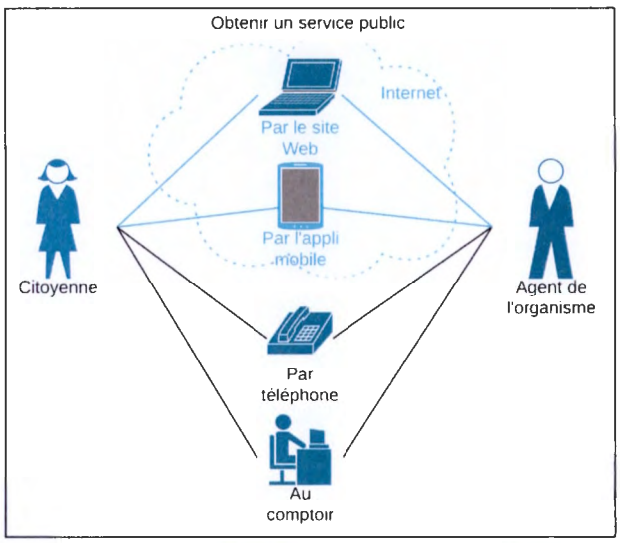

Figure 1.1 - représentation d'un service multicanal typique

Une identité citoyenne doit pouvoir exister sans que le citoyen ait d'accès à l'Internet. L'identité numérique – sans le mot citoyen – peut également servir aux organisations, pour offrir des services commerciaux.

Il n'est pas question de parler d'identités numériques sans parler d'authentification, qui consiste à vérifier l'identité de l'utilisateur en ligne. Pour éviter d'authentifier l'utilisateur à chaque transaction, une connexion permet d'ouvrir une session à l'aide de certaines informations permanentes (renseignement personnel et secrets, le cas échéant) qui sont alors transformées en jeton de contrôle. Les secrets de connexion peuvent être physiques ou numériques. De leur côté, les organisations ne font pas de connexion, ce sont plutôt des personnes – des individus – qui s'authentifient pour agir au nom de la personne morale, l'organisation.

Un autre aspect important est le consentement à l'usage d'un renseignement personnel, pour un service offert par un organisme public donné. Le citoyen peut consentir de façon implicite (en confirmant ses renseignements personnels avant de clairement indiquer le désir d'obtenir le service) ou de façon explicite (en répondant à une question détaillant exactement l'usage qui sera fait des renseignements personnels). Le type de consentement permis varie d'une juridiction à l'autre et il est important pour les organismes publics de respecter ce fait. Du côté de la Ville de Montréal, un consentement implicite a été jugé suffisant, une fois que les conditions d'utilisation des services numériques de la Ville ont été acceptées (Ville de Montréal, 2017c).

Le dernier concept à définir ici est l'audit des identités citoyennes et des renseignements personnels qu'elles comportent. Par ce terme, on comprend autant l'accès en mode modification que l'accès en mode lecture, que ce soit par le citoyen lui-même ou un employé d'un organisme public. Ces données sont importantes pour éventuellement permettre au citoyen de vérifier les usages faits par les organismes publics de ses renseignements personnels, améliorant la transparence des services publics et, par le fait même, la confiance des citoyens dans ces services.

1.1.2 État de l'art

Un état de l'art de l'identité numérique a été réalisé en février 2019 pour le *Chapitre 7 : Technologies* de la candidature finale de la Ville de Montréal (Ville de Montréal, 2019) au *Défi des villes intelligentes* (DÉFI) (Infrastructure Canada, 2018). C'est d'ailleurs dans ce contexte que les quatre approches suivantes de gestion d'identités ont été décrites.

L'**identité sociale,** offerte par plusieurs réseaux sociaux et fournisseurs de courrier électronique gratuits, a permis de démocratiser le concept de connexion unifiée. Les personnes souhaitant utiliser un service en ligne réutilisent leur identité sociale, quand elle est supportée par le service, grâce à un bouton du style « Connectez-vous avec ». Pour la personne, cette approche permet de minimiser le nombre de mots de passe et de rester connecté sur plusieurs sites à la fois (convivialité). Pour un service en ligne, cette approche permet de minimiser la gestion des identités, tels que les mots de passe oubliés ou les comptes verrouillés (minimiser la maintenance identitaire). Une personne peut également se créer plusieurs identités, selon son bon vouloir. L'identité sociale utilise généralement la même technologie que l'identité fédérée, soit *OpenID Connect* (OIDC) (OpenID Foundation, 2014).

L'**identité centralisée** est l'approche où un gestionnaire fort, généralement un organisme public, centralise les renseignements personnels, veille au respect des processus et offre des garanties de validations des données. Dans plusieurs cas, ces dossiers centralisés sont partagés avec d'autres services publics au bénéfice du citoyen, mais la donnée reste centralisée à l'origine. Par exemple, c'est le cas avec la *Société d'assurance automobile du Québec* (SAAQ) qui partage ses données avec la *Régie de l'assurance-maladie du Québec* (RAMQ). Cette approche est lourde à mettre en place et demeure peu flexible, car chaque nouvelle initiative doit être

supportée par le système centralisé. La contrepartie est que cette approche est plus facile à communiquer aux citoyens, car ils y ont été davantage exposés dans le passé.

Un peu comme pour l'identité sociale, l'**identité fédérée** est une approche permettant à un citoyen de choisir un dossier d'origine, qui contiendra ses informations de connexion, à partir duquel sa vie numérique sera bâtie. Lorsque le citoyen interagit avec d'autres organismes publics ou des organisations, appelés partenaires, il peut réutiliser ses informations de connexion avec un bouton « Connectez-vous avec », ce qui donne le consentement au partage d'un ensemble standardisé de données, entre le dossier d'origine et le partenaire offrant le service désiré par le citoyen. Les modifications faites aux données standardisées peuvent être retournées au dossier d'origine, tandis que les différents partenaires peuvent conserver des renseignements supplémentaires, requis pour fournir leurs services respectifs. Par exemple, le gouvernement canadien permet aux citoyens d'utiliser un partenaire, telle leur institution financière, pour s'authentifier à certains services. Cette fédération est limitée, puisqu'elle est à sens unique : les institutions financières ne permettent pas l'authentification avec un compte du gouvernement fédéral. C'est que la fédération d'identités fonctionne sur la base d'une confiance point à point, où chaque organisme public et chaque organisation membre de la fédération doit décider à quels autres organismes il fait confiance. Cette approche, quoique fonctionnelle, montre rapidement ses limites, car sa mise à l'échelle est lourde. Comme l'identité sociale, l'identité fédérée s'appuie principalement sur OIDC.

L'**identité décentralisée** est une approche émergente, où les problèmes d'établissement et de maintenance de la confiance point à point ont été solutionnés

dès le départ. Chaque partenaire interagit avec l'écosystème avec une méthode standardisée, découvrant automatiquement les autres partenaires, ce qui facilite la mise à l'échelle. Les accès et les consentements sont gérés par la personne possédant l'identité. Cette approche est parfois associée avec l'identité souveraine autonome (notre traduction de « Self-Sovereign Identity » (Baars, 2016)), où le citoyen est le seul à posséder les clés vers ses propres données.

Le tableau suivant, bonifié depuis le *Chapitre 7 : Technologies* de la candidature finale de la Ville de Montréal au DÉFI (Ville de Montréal, 2019), résume les avantages et inconvénients des quatre approches décrites précédemment.

Tableau 1.1 – avantages et inconvénients des approches de gestion d'identités numériques

Approche	Avantages	Inconvénients
Identité sociale	Connexion unifiée ; Moins de mots de passe ; Minimise la maintenance identitaire ; Possible d'être quasi anonyme, ou de séparer ses vies privée et professionnelle.	Combine souvent un usage commercial, la publicité, avec les renseignements personnels ; Vérifications volontaires des pratiques de gestion des renseignements personnels (pas d'obligations légales).
Identité centralisée	Uniformité et cohérence de l'information ; Gouvernance et propriété claire des données ; Facile à expliquer.	Modèle de données et d'identités limité à la vision du propriétaire et difficilement extensible ; Centralisation des accès.
Identité fédérée	Certaines données spécifiques sont conservées chez le partenaire, tandis que les données standardisées sont retournées au dossier d'origine.	Lien de confiance point à point : chaque organisme doit faire confiance aux autres organismes de la fédération.

Approche	Avantages	Inconvénients
Identité décentralisée	Identité personnelle intuitive et pratique à gérer ; Contrôle complet de l'utilisation des données ; Flexible, évolutive et supporte la mise à l'échelle.	Nouveaux modèles de gouvernance à définir ; Enjeux de communications pour favoriser l'adoption ; Infrastructure commune à maintenir.

En partant de deux sources existantes (Secrétariat du Conseil du Trésor du Canada, 2018; Ville de Montréal, 2019), le tableau suivant offre un tour d'horizon des initiatives publiques touchant l'identité citoyenne numérique. On remarque que l'approche prédominante est l'identité numérique centralisée. La partie sur les règlements dénote des aspects à ne pas négliger lorsqu'il est question d'identités.

Tableau 1..2 – survol des initiatives d'identités numériques gouvernementales

Identités numériques centralisées	
Estonie (*National ID Card*), **Danemark** (*NemID*), **Royaume-Uni** (*Gov.UK Verify*), **Inde** (UIDAI, *Aadhaar*), **Nouvelle-Zélande** (*RealMe*), **France** (*FranceConnect*), **Québec** (*clicSéqur, clicSéqur entreprises*)	Exemple d'usage : une carte émise par le gouvernement pour l'authentification numérique et/ou servant de preuve pour démontrer que la personne est celle qu'elle prétend en ligne. Sources : https://e-estonia.com/solutions/e-identity/id-card/ https://www.nemid.nu/dk-en/about_nemid/index.html https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify https://uidai.gov.in/ https://franceconnect.gouv.fr/faq https://www.govt.nz/browse/passports-citizenship-and-identity/proving-and-protecting-your-identity/what-is-realme/ https://www.info.clicsequr.gouv.qc.ca/citoyens.html https://www.info.clicsequr.gouv.qc.ca/entreprises.html
Règlements-cadres touchant à l'identité numérique	
Union européenne (*eIDAS*)	*eIDAS* est un **ensemble de règlements** pour régir le marché unique européen, et accroître la confiance des citoyens envers les transactions numériques.

	Source : https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/
Union européenne (*GDPR*)	Le *Règlement général sur la protection des données* (RGPD ou GDPR en anglais) a eu un impact mondial, car il dicte les **mesures de protection des renseignements personnels** des citoyens européens, même ailleurs dans le monde. C'est la référence. Source : https://ec.europa.eu/info/law/law-topic/data-protection_fr
Canada (vie privée)	Les lois et règlements recensés ici sont la référence pour le Canada : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/02_05_d_15/
Approches fédérées, décentralisées ou cadres de certification	
Australie (*Trusted Digital Identity*)	Projet pilote d'un **cadre de certification,** afin d'établir des identités en ligne par le gouvernement et des partenaires. Source : https://www.dta.gov.au/our-projects/digital-identity
Canada (*SecureKey*)	Une initiative de **fédération d'identités**, où un ensemble de partenaires de confiance attestent l'identité d'un citoyen, mais seulement pour obtenir les services du gouvernement canadien (pas de réciprocité avec les partenaires).
Cadre de confiance pancanadien *(PCTF)*	Ce **cadre de certification** vise à faciliter la reconnaissance des partenaires de confiance, pour l'**identité fédérée** d'abord, et pour l'**identité décentralisée** par la suite. Le gouvernement de l'Alberta a complété le processus et a été intégré comme partenaire de connexion à des services fédéraux canadiens. Sources : https://ssimeetup.org/overview-proposed-pan-canadian-trust-framework-ssi-tim-bouma-webinar-19/ https://www.canada.ca/en/treasury-board-secretariat/corporate/news/canada-trusted-digital-identity-vision.html https://account.alberta.ca/
Fondation pour l'identité décentralisée (DIF)	La DIF prépare des spécifications pour gérer et transmettre des **identités décentralisées**. Microsoft travaille à une implémentation de référence, en logiciel libre. Sources : https://identity.foundation https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2DjfY

1.2 Mandat du projet

Le mandat du projet de synthèse décrit dans ce rapport est basé sur le mandat du CISN. Ce dernier consiste à :

1. *[É]laborer une méthode d'authentification commune sécurisée ;*
2. *[É]laborer et tester une interface de programmation [d'applications] (API) commune [permettant] l'échange de données des citoyens.*

(Comité identité et services numériques, 2017)

Pour le présent projet de synthèse, le mandat se limite au deuxième point, soit d'élaborer une interface de programmation d'applications (API) permettant de représenter une identité citoyenne numérique, réutilisable par les divers services d'un organisme public, lorsque le citoyen y consent.

Cet API, appelé API Citoyen, doit permettre à l'organisme public de respecter ses obligations légales liées à la protection des renseignements personnels, tout en facilitant l'expérience des citoyens avec les services qu'ils utilisent, de manière multicanale.

Cet API doit offrir au citoyen un contrôle maximal quant à l'usage de ses renseignements personnels par l'organisme public, et, du même coup, favoriser la transparence des usages que les employés de cet organisme public font de ces mêmes renseignements personnels. Le tout, dans un contexte où certains usages de renseignements personnels sont requis et permis lors de l'application de lois ou de règlements.

1.3 Objectifs du projet

Les objectifs du projet peuvent être résumés comme suit :

- **Interopérabilité entre fournisseurs** : la spécification doit pouvoir être inscrite comme critère dans les appels d'offres publics. Au fur et à mesure que des appels d'offres incluront ce critère, l'interopérabilité sera améliorée entre les logiciels développés par divers fournisseurs d'un même organisme public.
- **Interopérabilité entre organismes publics** : l'initiative doit permettre, lorsque le citoyen y consent, de partager et de valider ses renseignements personnels entre organismes publics distincts, pour minimiser les efforts de gestion d'identités.

Les prochaines sections détailleront chaque objectif, avant d'introduire un cas concret envisagé pour guider la réalisation de l'API Citoyen, dans le cadre d'une approche d'identités fédérées.

1.3.1 Interopérabilité logicielle entre fournisseurs

Une ville utilise de nombreux logiciels pour accomplir sa mission de desservir les citoyens. Allant de déclarations obligatoires, telles les matières dangereuses par les entreprises, à la gestion des divers permis (construction, stationnement, locaux commerciaux, animaliers, etc.), à la taxation municipale des propriétaires, en passant par la gestion de l'eau (propre, en transit, usée), aux bibliothèques, aux sports, aux transports en commun, aux parcs, etc. C'est la même situation pour les autres grands organismes publics, telles les sociétés de transport.

Pour la majorité de ces activités, des logiciels commerciaux existent et peuvent répondre partiellement ou complètement aux besoins des organismes publics. Ces logiciels commerciaux traitent alors un grand volume de renseignements

personnels. Toutefois, plusieurs de ces logiciels ne permettent pas d'extraire facilement les données qui y sont enregistrées, ou encore, ne permettent pas l'extraction de données dans un format compatible avec un autre logiciel. Dans d'autres cas, des frais onéreux d'extraction ou d'importation de données seront facturés aux organismes publics. Selon un avis d'expert[2], de nombreux organismes doivent conjuguer présentement avec cette réalité contraignante et coûteuse.

L'idée est donc d'inclure la spécification comme critère obligatoire dans les prochains appels d'offres publics de logiciels commerciaux traitant des renseignements personnels, dans le but de favoriser **l'interopérabilité logicielle entre fournisseurs**, pour minimiser les ressources utilisées pour ce type d'opération informatique, que ce soit pour une évolution ou une cohabitation.

1.3.2 Interopérabilité entre organismes publics

Pour divers organismes publics, la vérification des renseignements personnels est un requis d'affaires. Par exemple, pour un comptoir de services aux citoyens, la saisie initiale et la vérification des renseignements peuvent prendre jusqu'à :

- 8 minutes par citoyen à saisir en ligne[3] ;
- 1 minute pour un employé à vérifier, lors d'une demande en libre-service, par la concordance entre les photos et les renseignements soumis en ligne[4];
- 30 secondes par employé à vérifier au comptoir, par la concordance entre une pièce justificative présentée par le citoyen et les renseignements du dossier[5].

---

[2] Un collègue, conseiller retraité du Service des TI de la Ville de Montréal.

[3] Source : estimé basé sur le service photo-chèque de la Banque Nationale du Canada.

[4] Source : une collègue du Service de la concertation des arrondissements de la Ville de Montréal.

Il est à noter que pratiquement aucun de ces processus n'inclut de vérification avec l'émetteur original de la pièce justificative, pour savoir si elle est toujours valide, ce qui pose des enjeux pour la sécurité et la protection contre la fraude.

Individuellement, ces délais peuvent sembler courts. Mis ensemble, ils deviennent gigantesques. Avec les 900 000 attestations de dossiers citoyens faites chaque deux (2) ans par les bibliothèques montréalaises[6], l'effort requis pour identifier les citoyens est considérable tout en demeurant sans grande valeur ajoutée, autre que de limiter le service aux citoyens éligibles. En apposant une attestation numérique à un renseignement vérifié, la solution permettra au citoyen de réutiliser ce renseignement plus tard, si l'attestation est suffisamment récente pour les besoins du service public désiré. Par exemple, à la Ville de Montréal, une vérification de moins de deux (2) ans est requise pour les bibliothèques, d'un (1) an pour les permis animaliers et de trois (3) mois pour les permis de stationnement sur rue (à cause des tentatives de fraude plus fréquentes) et les trois sont indépendants. Ainsi, avec un stationnement valide, je peux avoir accès directement à une carte de bibliothèque.

L'objectif **d'interopérabilité entre organismes publics** vise donc à réutiliser des données citoyennes certifiées pour mutualiser les coûts de gestion d'identités. Ce faisant, les citoyens auront des services plus rapidement, même si c'est de la part d'un nouvel organisme public, en autant que ce dernier participe à la fédération d'identités. Évidemment, le citoyen doit consentir au partage de ses renseignements personnels à chaque nouveau service utilisé de chaque organisme public.

---

[5] Source : une collègue du Service de la concertation des arrondissements de la Ville de Montréal.

[6] Source : statistique interne à la Ville de Montréal.

1.3.3 Cas concret envisagé

La figure suivante présente les flux d'informations entre une citoyenne, qui est étudiante à l'université et résidente d'un arrondissement de Montréal, et divers organismes publics de son milieu de vie. Ce cas est une réutilisation des données citoyennes certifiées, où les interactions sont davantage fluides entre les acteurs.

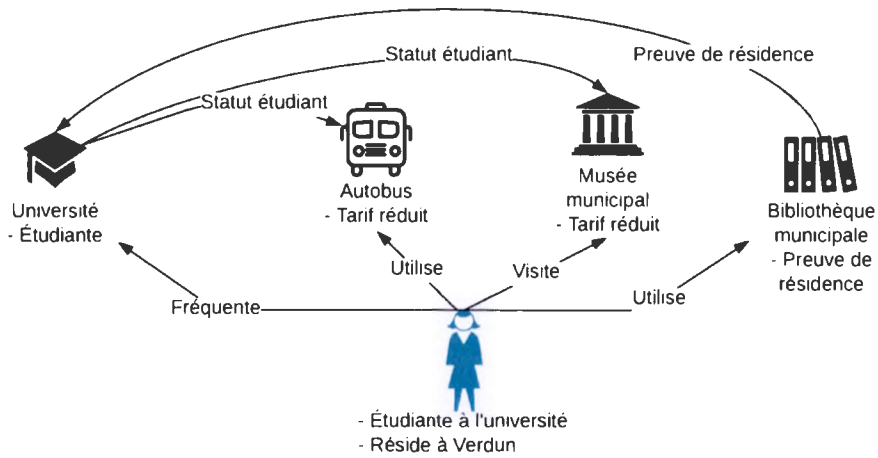

Figure 1.2 – flux des renseignements personnels

- Les flèches du bas représentent les relations entre l'étudiante et les organismes publics ;
- Les flèches du haut représentent les transferts de données citoyennes validées :
  - L'étudiante a initialement prouvé son identité à la bibliothèque ; ce renseignement a été partagé à l'université à la demande de l'étudiante.
  - Le service de transport en commun et le musée obtiennent la confirmation que l'étudiante a bien droit aux rabais qu'ils offrent à cette clientèle.

À noter que ces concepts peuvent être étendus pour offrir des réciprocités de services, comme par exemple, la réciprocité des titres de transport entre deux villes du Québec.

1.4 Hypothèses et limites

- La solution proposée par le présent projet est parfaitement imparfaite ; c'est-à-dire que c'est une base à partir de laquelle on peut comparer d'autres initiatives ou, le cas échéant, itérer vers une solution cible qui serait définie ultérieurement. Cette solution a permis l'avancement d'éléments concrets, tels
  - Une première analyse de l'état de l'art faite préalablement a été révisée ;
  - Un suivi en continu dénote des ajouts au domaine (PCTF, DIF, etc.) ;
  - Une première spécification a été définie par le CISN ;
  - Une implémentation a été faite par des projets concrets à la Ville de Montréal ; ce faisant, l'implémentation comprend certaines divergences de la spécification, car les possibilités de re-travail étaient limitées.
- Ce projet a démarré avec l'hypothèse qu'il n'y avait pas de solution couvrant l'ensemble des besoins, donc le projet a débuté avec pour cible l'utilisation d'OIDC pour l'authentification et d'y ajouter un API spécifique.
- Ce rapport décrit les ressources de l'API Citoyen d'une façon sommaire, sans inclure les définitions détaillées, car ce rapport n'est pas une documentation d'API. Les utilisateurs potentiels ou autres parties intéressées par l'API Citoyen peuvent se référer à la plus récente version de la documentation d'API, en communiquant avec la Ville de Montréal ou un membre du CISN.
- Le présent document se concentre sur un API pour représenter l'identité citoyenne numérique, et non sur les mécanismes possibles d'authentification ; c'est pourquoi les discussions sur l'authentification sont allégées.
- Le mandat du CISN se limite à établir des moyens techniques, car le comité a choisi de repousser la complexité de la gouvernance à un projet distinct.
- Dans le même sens, susciter l'adhésion des organismes publics à l'initiative n'est pas un objectif immédiat du projet.

CHAPITRE 2

DÉMARCHE ET NORMES PERTINENTES

Ce chapitre expose la démarche qui a été utilisée dans le cadre de ce projet de synthèse. Partant de la pratique d'architecture TI mise en place à la Ville de Montréal comme axe initial de la démarche, deux autres axes y ont été adjoints durant le projet, soit le *Comité identité et services numériques* (CISN) mentionné précédemment et les recherches effectuées pour préparer le chapitre sur les technologies de la candidature finale de la Ville de Montréal au *Défi des villes intelligentes* (DÉFI). Enfin, le chapitre se conclut avec le survol des normes ayant guidé la réalisation de l'API Citoyen, dans un contexte gouvernemental.

2.1 Vue d'ensemble de la démarche

Dès le début, la démarche du projet a impliqué plusieurs partenaires, que ce soit des représentants d'organismes publics au CISN ou des employés du *Service des technologies de l'information* (STI) de la Ville de Montréal. Ces personnes ont contribué à l'API Citoyen de diverses façons, dont la principale était de participer à des discussions avec l'auteur du présent document. Cet API est ainsi issu d'une démarche itérative et pragmatique, tout en étant lié à des objectifs concrets d'organismes publics, incluant échéances et contraintes de projet.

La figure suivante illustre la démarche ayant conduit à l'API Citoyen. Cette démarche est constituée de trois volets. Un premier volet englobe des projets concrets à la Ville de Montréal (VILLE), un second volet regroupe les processus du CISN, tandis qu'un troisième volet représente les travaux effectués pour la candidature finale de la Ville de Montréal au *Défi des villes intelligentes* (DÉFI).

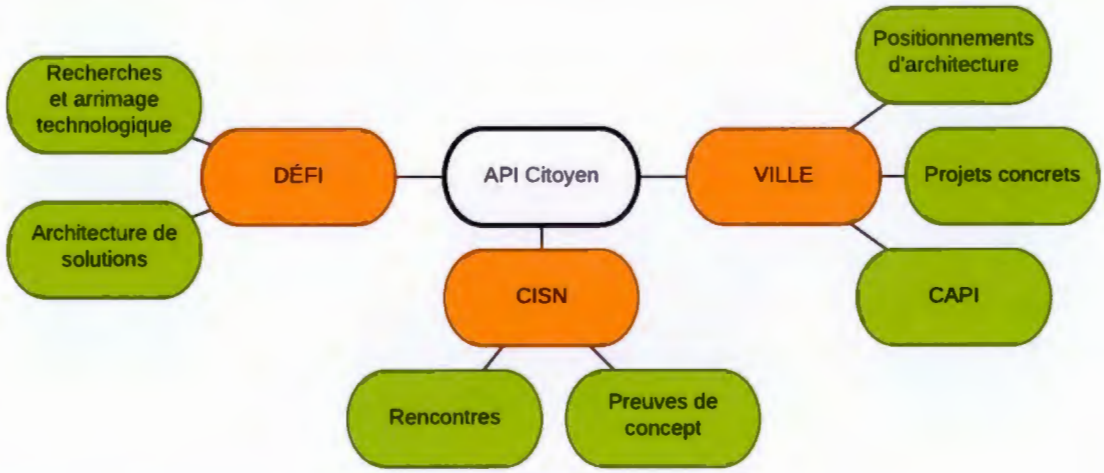

Figure 2.1 – vue d'ensemble de la démarche de l'API Citoyen

2.2 Démarche à la Ville de Montréal

Le volet montréalais de la démarche suit trois axes : les positionnements d'architecture TI, les besoins d'affaires de projets concrets et la contribution de l'équipe du *Comité des APIs* (CAPI) de la Ville de Montréal. Chaque axe couvre plusieurs pratiques. Les prochaines sous-sections détaillent les éléments de chacun de ces trois axes.

2.2.1 Positionnements d'architecture TI

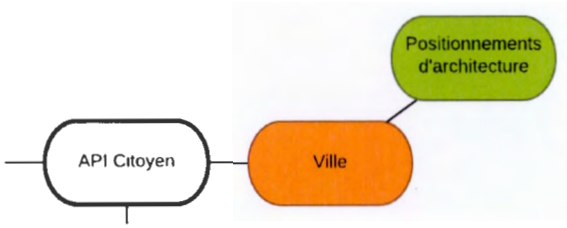

Figure 2.2 – 1er axe : positionnements d'architecture TI

Le *Service des technologies de l'information* (STI) de la Ville de Montréal a mis en place dans les dernières années une pratique d'architecture TI. Avec plusieurs nouveaux employés issus de différents horizons, des positionnements d'architecture TI ont été définis initialement, avant d'être raffinés en principes d'architecture TI (Ville de Montréal, 2018c), toujours pour guider les pratiques de développement et d'acquisitions de logiciels. Certains positionnements, et un principe, sont applicables directement à la démarche de l'API Citoyen et en ont influencé le développement :

- L'approche *API d'abord* (notre traduction de l'anglais « API First ») ;
- L'usage du libre ;
- L'architecture microservices ;
- La réutilisation de normes et standards ;
- Le principe de disponibilité des données de qualité.

L'approche *API d'abord* recommande l'élaboration de la spécification d'un API REST (Fielding, 2000) avant d'amorcer sa réalisation. L'objectif est de rendre parallèle la réalisation des applications frontales et dorsales. Il est question d'une forme de contrat passé entre les développeurs frontaux et dorsaux (RESTlet, 2019). La spécification de l'API est utilisée comme point de référence pour déterminer quel développeur doit effectuer des changements, si l'intégration frontale et dorsale

rencontrait un problème. De façon générale, tous les changements au contrat de l'interface de l'API doivent être acceptés par les deux équipes de développement.

L'API Citoyen a suivi le principe *API d'abord* depuis mars 2017 et la spécification est toujours en avance sur l'implémentation de référence, parfois de plusieurs mois. Cela a soulevé un enjeu : plusieurs différences existent entre la spécification et la première implémentation à la Ville de Montréal, pour diverses raisons : contraintes techniques ou de temps, mauvaise compréhension, ambiguïté de la spécification, spécification incomplète, etc. Lorsque identifiées, ces divergences n'ont pas toujours été corrigées, car les possibilités de re-travail sont limitées dans les projets concrets (la fidélité à la spécification n'étant pas un objectif des projets réalisés à ce jour).

En plus d'un positionnement favorisant **l'usage du libre**, la Ville de Montréal s'est dotée d'une politique de développement et d'utilisation de logiciels libres (Ville de Montréal, 2018b). L'objectif est d'utiliser le libre comme vecteur d'innovation et pour maximiser l'investissement fait avec les dollars publics. De plus, les logiciels développés en libre peuvent être partagés plus facilement avec d'autres organismes publics qui, à leur tour, peuvent y apporter des contributions. L'API Citoyen a été identifié comme candidat à être mis en disponibilité comme logiciel libre.

Une **architecture microservices** sépare les différentes fonctions d'un système en petits morceaux dont les rôles et responsabilités sont bien définis. Cela revient à étendre à l'architecture le principe de responsabilité unique (Martin, 2014; Stine, 2014) qui dicte de faire une chose, mais de la faire bien. Ainsi, chaque morceau de l'architecture microservices se voit confier une responsabilité principale bien définie.

En permettant de centraliser les échanges entre les différents services d'un organisme public et la base de données des dossiers citoyens, l'API agit comme façade devant la solution retenue pour réaliser le dossier citoyen. L'objectif d'une telle façade est de minimiser la propagation des changements, lors d'un changement éventuel de fournisseur ou de technologie.

Le dernier positionnement incite à **une réutilisation de normes et de standards,** lorsque c'est possible. Le but est de ne pas réinventer la roue, de dédier les ressources de développement là où de tels standards n'existent pas pour un besoin. Pour atteindre ce but, un processus de vigie est déclenché avant de débuter un projet. Par vigie, on entend une recherche d'information – principalement via Internet – pour déterminer quels outils, quels systèmes, quelles normes ou quels standards existent et répondent en tout ou en partie aux besoins d'affaires. Les résultats de la recherche sont consignés dans un format standardisé dans les dossiers de la Ville de Montréal, pour référence future ou pour servir de base à une prochaine vigie. C'est en cohérence avec ce positionnement que, en avril 2017, l'API Citoyen a été ajusté afin de s'apparenter à une extension du standard Internet proposé SCIM 2.0 (Hunt, 2015). D'autres normes ou lois ont été considérées pour la réalisation de l'API Citoyen ; voir la section 2.5 pour les détails.

Finalement, le principe d'architecture TI de **disponibilité des données de qualité**, qui inclut notamment la transparence, vise à ce que les données en la possession de la Ville de Montréal soient de la qualité adéquate à leur usage, disponibles aux citoyens lorsque possible, tout en veillant à ce que ces données soient sécurisées correctement. Un exemple d'application concrète est la fonction de l'API Citoyen permettant d'exposer – au citoyen lui-même – les journaux d'accès à son propre dossier par les employés.

2.2.2 Besoins d'affaires de projets concrets

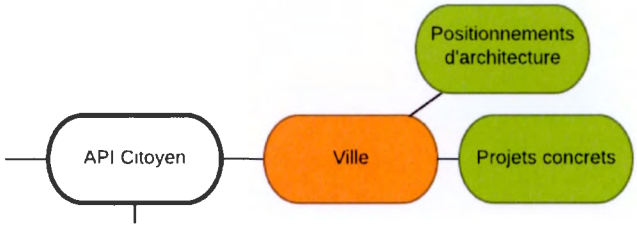

Figure 2.3 2e axe : projets concrets

Le deuxième axe de la démarche à la Ville de Montréal est le développement de projets concrets. Ces projets, priorisés par l'administration, visaient chacun à répondre à des besoins d'affaires différents de la Ville de Montréal. Chaque projet a amené l'API Citoyen, ou l'un de ses composants, à évoluer vers une solution plus complète. La version originale de l'API Citoyen a été développée pour les besoins des projets de *Requêtes 311*[7] et *d'Avis/alertes*[8]. Une version de l'API Citoyen est utilisée depuis l'automne 2017 pour *Requêtes 311*, au bénéfice de l'île de Montréal (Marchal, 2017). Une mise à jour a suivi en novembre 2017 pour *Avis/alertes* (Ville de Montréal, 2017a). Seulement en 2017, plus de 6 000 dossiers citoyens[9] ont été créés en ligne grâce à ces deux projets. Ces dossiers ont été réalisés avec la ressource de base de l'API Citoyen :

- **L'individu**, composé des renseignements personnels du citoyen (ex. : nom, prénom, téléphone(s), adresse(s), etc.).

---

[7] Le service 311, offert par de nombreuses villes, permet de rejoindre un employé de l'administration publique pour signaler un problème ou effectuer un suivi d'une demande. Par exemple, pour signaler l'existence d'un nid-de-poule sur la voie publique, pour signaler la défectuosité d'un lampadaire, etc.

[8] Le service d'avis et d'alertes permet à un citoyen de Montréal de s'abonner à une série de thématiques, et d'être informé par texto ou courriel lorsque quelque chose arrive. Il peut s'agir d'aviser d'un avis d'ébullition d'eau, du début d'une opération de chargement de la neige, etc.

[9] Source : statistiques internes de la Ville de Montréal sur les dossiers créés avant le 1er janvier 2018.

Les projets de *Permis animaliers en ligne*[10] et de *Pétitions en ligne*[11] ont permis de développer plusieurs ressources de soutien, requises pour répondre aux divers besoins d'affaires de ces projets. Là où *Requêtes 311* se satisfaisait d'un relatif anonymat, *Permis animaliers en ligne* et *Pétitions en ligne* ont besoin d'une forte assurance quant à l'identité du citoyen demandeur.

Voici les ressources ajoutées par ces deux projets à l'API Citoyen :

- **Consentements** : informations sur le moment et la méthode utilisée par un citoyen pour consentir à un service (ex. : en ligne, au comptoir, etc.).
- **Journalisation des accès** : liste de toutes les interactions par un employé ou le citoyen lui-même avec son dossier (ex. : date et heure, nom d'usager, lecture ou écriture, etc.).
- **Historique des adresses et adresses multiples** : ajout de champs pour le suivi historique des adresses, ce qui permet aussi le support de plusieurs adresses, par l'ajout de dates de début et de fin de validité des adresses.
- **Validations** : information sur le niveau de validation ou de certification d'une donnée du dossier (ex. : un employé a vu un permis de conduire attestant la date de naissance, etc.).
- **Contacts** : liste des personnes que l'organisme public peut contacter, selon diverses situations pouvant arriver au citoyen (ex. : en cas d'urgence).

---

[10] *Permis animaliers en ligne* est un système disponible depuis avril 2019, permettant d'appliquer le nouveau *Règlement sur l'encadrement des animaux domestiques* (18-042) de la Ville de Montréal. Pour en savoir plus, https://beta.montreal.ca/sujets/patrouille-animale

[11] Les *Pétitions en ligne* sont disponibles depuis février 2019, permettant aux citoyens de se prévaloir de leur droit d'initiatives en consultation publique. Pour en savoir plus, https://beta.montreal.ca/sujets/comprendre-le-droit-dinitiative

- **Données additionnelles** : espace permettant de conserver divers renseignements personnels ou réutilisables par plusieurs services dans le dossier de la personne (ex. : preuve d'absence de casier judiciaire).

Un projet, confidentiel au moment de la préparation du rapport de synthèse, a permis d'ajouter une ressource principale à l'API Citoyen :

- L'**organisation** : une identité distincte sur laquelle agissent une ou plusieurs identités individuelles.

2.2.3 Comité des APIs

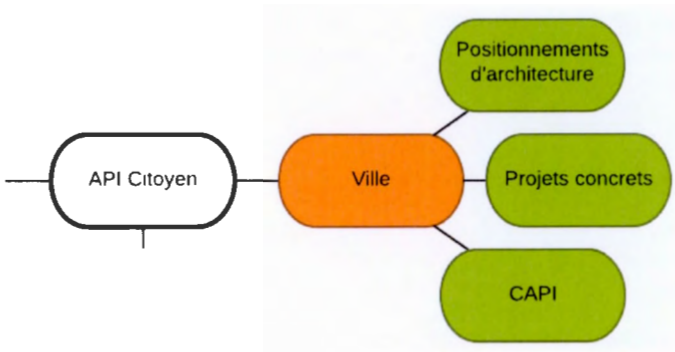

Figure 2.4 – 3e axe : comité des APIs CAPI de la Ville de Montréal

En 2017, un sous-comité d'architecture TI, appelé le *Comité des APIs* (CAPI), a été mis en place pour réviser l'ensemble des APIs REST développé au *Service des technologies de l'information* (STI) de la Ville de Montréal. La mission du CAPI est d'établir, de bonifier et de faire appliquer un guide de style REST lors des développements d'APIs. Ce guide de style est nécessaire, parce que REST n'est pas une spécification, mais plutôt un style architectural (Wodehouse, 2019). Il existe ainsi plusieurs façons valables de décrire une même ressource ou une même donnée.

Le CAPI joue plusieurs rôles, selon l'état d'avancement de l'API qu'il révise :

- Un **rôle cohésif**, où le comité vise à minimiser les dédoublements de ressources d'API et à en maximiser la réutilisation dans divers projets ;
- Un **rôle normatif**, où le comité veille à l'application du guide de style REST et d'une nomenclature (ressources, URI, etc.) en révisant les APIs en développement ;
- Un **rôle consultatif**, où le comité effectue des analyses et émet des recommandations, lors de consultations ponctuelles.

Afin de s'assurer que le CAPI puisse accomplir sa mission, deux jalons obligatoires ont été ajoutés au processus de gestion de projets du STI. Voici une brève description de ces deux jalons obligatoires :

- La **révision de haut niveau** d'un API se déroule idéalement en début de projet, avant que le développement ne commence. L'objectif est d'arrimer les éléments de haut niveau, tels les verbes et les routes choisies, avec le guide de style et les autres APIs, le cas échéant. Même s'il s'agit d'un jalon obligatoire des projets du STI, il est rare qu'un projet soit bloqué à cette étape. Une liste est plutôt dressée faisant état des recommandations et des obligations de changement, le cas échéant ; cette liste sera révisée lors de la révision détaillée.
- Le second passage au comité, appelé **révision détaillée**, a lieu vers la fin de chaque projet de développement d'API. L'objectif est alors de réviser les différentes ressources REST dans le détail. L'accent est mis sur la cohérence entre la définition des ressources entre elles, d'une part, et entre les autres ressources de la Ville de Montréal et le guide de style REST d'autre part. Si une section d'API a substantiellement changé entre les deux étapes, le comité commence par réviser cette partie de haut niveau avant de plonger dans la révision détaillée.

2.3 Démarche au *Comité identité et services numériques* (CISN)

Le CISN est composé d'organismes publics[12]. Au fil des rencontres de 2017 et 2018, deux villes ont cessé d'envoyer des représentants[13], mais deux autres se sont jointes et sont intéressées par l'initiative[14]. Comme mentionné à la section 1.4, le CISN vise une approche apolitique : les participants sont donc majoritairement des spécialistes technologiques, tels des architectes d'entreprises TI ou équivalent. De plus, le CISN est réservé à des organismes publics, permettant de discuter de sujets plus ouvertement que si des fournisseurs technologiques étaient présents, car les clauses d'appels d'offres publics empêchent de parler de certains sujets à l'avance. Le comité travaille à l'avancement de l'API Citoyen selon les axes illustrés ci-dessous :

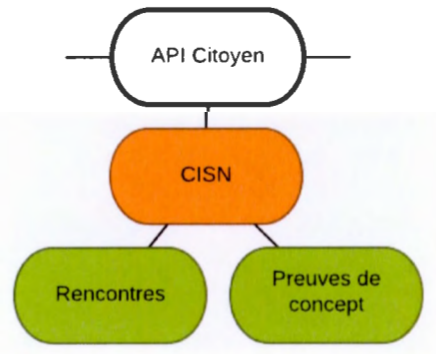

figure 2.5 - axes du volet CISN de la démarche

Les **rencontres** se divisent en deux activités, les tours de tables et les présentations. Le tour de table est le principal engrenage permettant le cheminement du CISN dans l'exécution de son mandat, car, de façon générale, c'est au tour de table que les sujets d'intérêts communs sont identifiés et sélectionnés pour les présentations

---

[12] Les membres originaux du CISN sont (en ordre alphabétique) : les villes de Laval, Longueuil, Montréal, Québec, Saint-Jean-sur-le-Richelieu et la Société de transport de Montréal (STM).

[13] Les villes de Québec et Saint-Jean-sur-le-Richelieu.

[14] Les villes de Gatineau et Sherbrooke.

subséquentes. Quant à elles, les présentations ont couvert un ensemble de sujets pour circonscrire l'identité citoyenne. Ces sujets sont le résumé d'une façon de faire, ou la présentation des bons coups et des leçons apprises sur un sujet donné. L'objectif est de partager ce qui semble être une bonne pratique, de sensibiliser les autres ou encore d'éduquer sur une nouvelle technique ou technologie.

Quant aux **preuves de concepts** (POC), elles sont de mise lorsque des sujets ont été suffisamment recherchés, mais qu'il reste des risques techniques. Le comité peut alors décider d'effectuer une ou plusieurs POCs. La réalisation est généralement confiée à un sous-ensemble du comité, avec une date estimée pour la fin de la réalisation et la présentation des résultats.

La première POC sélectionnée pour réalisation a été la connexion unifiée (de l'anglais « single sign-on », SSO) entre organismes publics avec *OpendID Connect* (OIDC). Cela revient à fédérer divers fournisseurs d'identités entre eux. Cette solution permet de donner confiance au processus de partage de dossiers citoyens, car le citoyen ne se connecte qu'à son dossier d'origine. Cette POC a été réalisée par les villes de Longueuil et Montréal, car OIDC était déjà en utilisation chez elles. L'architecture initiale de l'API Citoyen, décrite à la section 3.4.1, est basée sur cette POC.

La ligne du temps de la page suivante détaille les sujets présentés au CISN, y compris la première POC, les faits marquants et les sujets laissés comme questions en suspens pour une séance ultérieure.

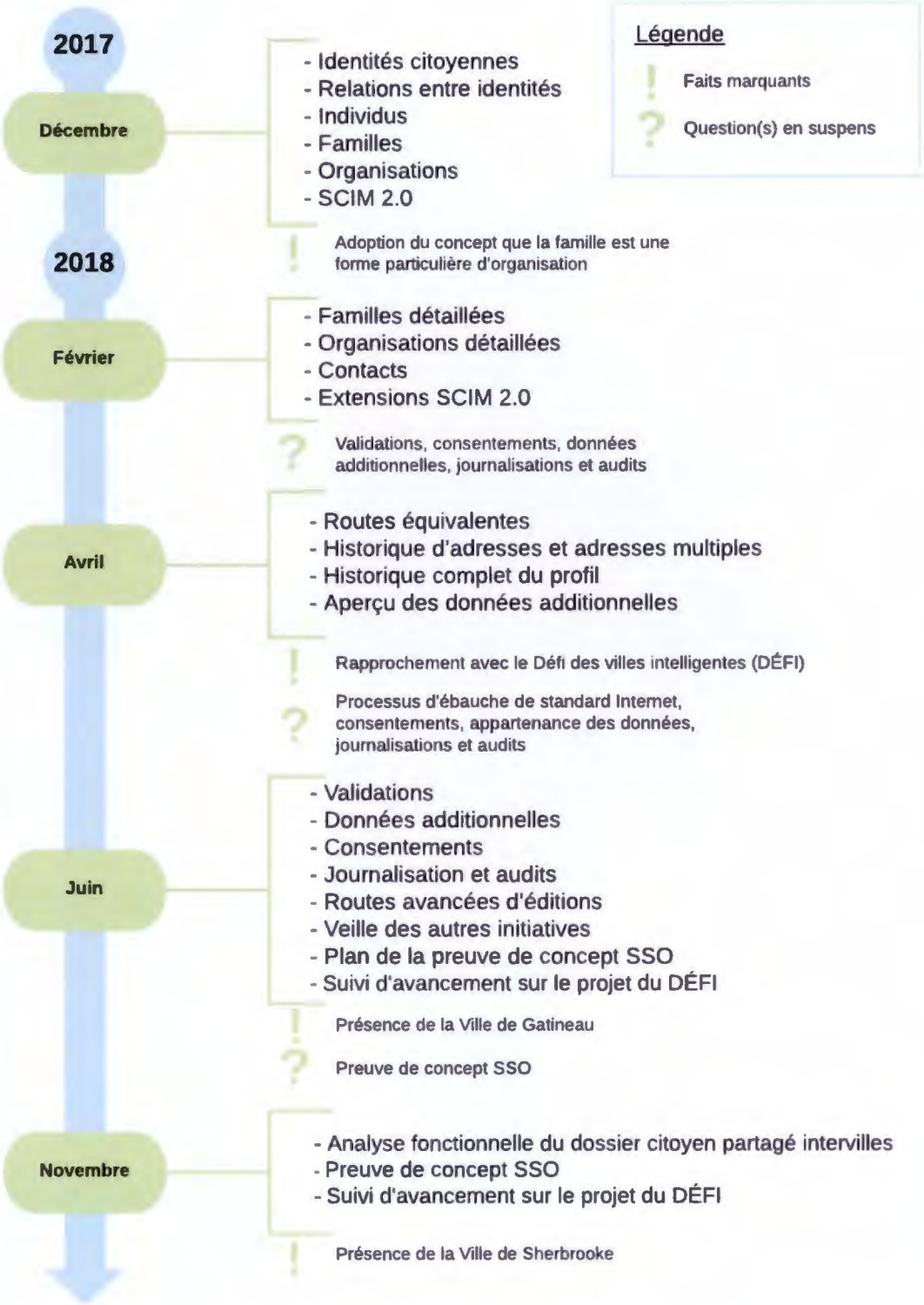

Figure 2.6 – ligne du temps du Comité identité et services numériques (CISN)

2.4 Démarche pour le *Défi des villes intelligentes* (DÉFI)

Le *Défi des villes intelligentes* (DÉFI) est un concours pancanadien (Infrastructure Canada, 2018) ouvert aux villes de diverses tailles, pour les inciter à imaginer des façons de mettre la technologie au service des citoyens et de leur qualité de vie. La Ville de Montréal étant finaliste pour le prix de 50 millions $, elle devait préparer une candidature finale à l'hiver 2019 où elle démontrait comment elle comptait utiliser ce montant dans le sens donné par le DÉFI. L'équipe responsable du DÉFI a alors sollicité l'effort de l'auteur du présent rapport pour étayer le volet des technologies de la candidature, qui s'est fait selon deux axes :

- La **recherche et l'arrimage technologique** de l'API Citoyen avec d'autres initiatives appropriées ;
- La préparation d'**architectures de solutions TI** réalisable (2019) et cible (2023).

Dans le cadre de **l'axe de recherche et de l'arrimage technologique,** la recherche s'est concentrée sur les éléments suivants et, lorsque applicable, un arrimage technologique avec l'API Citoyen a été défini :

- La lecture détaillée des documents publics de la *Fondation pour l'identité décentralisée* (DIF) a permis de creuser le concept de l'identité décentralisée et d'identifier cette approche comme l'évolution naturelle de l'API Citoyen (solutionnant le problème de la confiance point à point) ;
- L'analyse du livre blanc de Microsoft sur l'identité décentralisée (Microsoft, 2018) et le fait que ce soit associé à une implémentation en logicie libre ont montré une faisabilité technique dans un futur rapproché, du moins pour une preuve de concept à la Ville de Montréal ;
- L'analyse du *Cadre de confiance pancanadien* (PCTF) pour en apprendre plus sur l'initiative. Après discussion avec l'équipe derrière cette initiative, l'API Citoyen

et le PCTF seraient compatibles, puisque l'API Citoyen est une approche technologique et le PCTF est plutôt un cadre de certification, voire un futur standard de conformité, prônant des caractéristiques et des processus à mettre en place pour participer au PCTF. Le PCTF est ainsi indépendant des technologies dans le but de rejoindre le plus grand nombre de partenaires.

Pour ce qui est de **l'axe des architectures de solutions TI,** l'équipe de l'API Citoyen a couché sur papier une **architecture initiale** détaillant **l'identité fédérée** entre deux organismes publics, approche décrite dans *l'Analyse fonctionnelle : dossier partagé intervilles* (Ville de Montréal, 2018a). En s'appuyant sur la preuve de concept faite par le CISN sur *OpenID Connect* (OIDC), cette architecture a été inscrite à la candidature comme étant techniquement réaliste dès la deuxième moitié de 2019.

Par la suite, une **architecture cible** a été élaborée avec un horizon de 2023 pour respecter les paramètres du DÉFI. Cette architecture cible s'appuie sur les travaux de la DIF et du PCTF, proposant une approche de gestion **d'identités décentralisées,** incorporant les modules développés par la DIF tels les résolveurs, en plus des modules issus de l'API Citoyen qui n'ont pas d'équivalent dans l'approche actuellement proposée par la DIF ou Microsoft (ex. : les audits, l'historique du dossier et la traçabilité des attestations). La section 3.4.4 survole certains enjeux qui doivent être solutionnés avant la mise en place de cette architecture cible de la gestion d'identités décentralisées.

2.5 Normes pertinentes

Plusieurs normes ou lois ont été prises en considération dans la réalisation de la solution. Pour chacune d'entre elles, une brève description est donnée, avant d'indiquer la ou les section(s) reliée(s) du présent document.

2.5.1 *OpenID Connect* (OIDC)

OIDC est un protocole d'authentification[15] qui permet de fédérer la connexion entre fournisseurs d'identités sur le Web. C'est une évolution de *OAuth* 2.0 qui, lui, est un standard Internet proposé[16]. Les principaux usages d'OIDC sont la connexion unifiée (SSO), la connexion avec un compte Google ou un compte Facebook, etc.

Par l'usage de champs (de l'anglais « scopes »), OIDC permet de spécifier l'intention d'obtenir certains renseignements lors d'une connexion réussie[17]. Une connexion est réussie lorsque l'identifiant (p. ex. un nom d'utilisateur) est contre-validé par la validation des secrets associés, par exemple, la correspondance d'un mot de passe et d'un 2^{e} facteur, tel un appareil physique possédé par l'utilisateur et qui génère des jetons d'accès secrets. Les champs demandés seront alors retournés comme affirmations OIDC (de l'anglais « claims »). Ces affirmations OIDC constituent la méthode utilisée par OIDC pour transmettre des informations identitaires gérées par

---

[15] Pour en savoir plus, http://openid.net/connect/faq/

[16] Pour en savoir plus, https://tools.ietf.org/html/rfc6749

[17] Une connexion est réussie lorsque le nom d'utilisateur et le mot de passe sont reconnus valides par le fournisseur d'identités.

un fournisseur donné d'identités. Ces affirmations OIDC sont généralement signées numériquement[18].

La section 3.1.3 contient davantage de détails sur l'usage de OIDC dans la solution.

2.5.2 *Système de gestion d'identités interdomaines* (SCIM) 2.0

SCIM 2.0 est un standard Internet proposé pour gérer des affectations et des désaffectations de ressources liées à des utilisateurs dans un contexte infonuagique. SCIM 2.0 est décrit dans trois demandes de commentaires, appelées communément RFCs : les RFC 7642, RFC 7643 et RFC 7644[19]. Le premier, RFC 7642, contient la vue d'ensemble de SCIM 2.0, les concepts, les définitions et les différents requis liés à la gestion de ressources dans le nuage. Le second, RFC 7643, contient le modèle de définition de données permettant de décrire des utilisateurs, des groupes d'accès. RFC 7643 contient également un modèle d'extension pour décrire d'autres ressources ou données dans le cadre de gestion des utilisateurs. Ces ajouts, appelés extensions, permettent d'élargir l'usage de SCIM 2.0 à d'autres besoins. Voici deux exemples de telles extensions qui sont en utilisation :

- urn:ietf:params:scim:schemas:extension:2.0[20]

  Non officielle, cette extension ajoute des attributs personnalisés à travers un fournisseur d'identités en logiciel libre basé sur OIDC.

---

[18] Pour en savoir plus, https://connect2id.com/learn/openid-connect

[19] Pour en savoir plus, voir https://tools.ietf.org/html/rfc7642, https://tools.ietf.org/html/rfc7643 ou encore https://tools.ietf.org/html/rfc7644

[20] Pour en savoir plus, https://gluu.org/docs/ce/user-management/scim2/

- urn:ietf:params:scim:schemas:extension:enterprise:2.[21]

  Officielle, cette extension permet de représenter une hiérarchie d'utilisateurs en entreprise.

Finalement, le troisième RFC, RFC 7644, définit les méthodes d'interactions du protocole, permettant d'effectuer les affectations et les désaffectations de ressources à proprement parler. Voir la section 3.1.4 pour la suite de ce sujet.

2.5.3 *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ADOP-PRP)

ADOP-PRP est une loi provinciale du Québec visant à favoriser l'accès aux documents des organismes publics. L'objectif de cette loi est de favoriser la transparence des organismes publics. Cette loi encadre l'accès aux documents des organismes publics et impose des règles particulières à suivre en matière de gestion des renseignements personnels. On y décrit d'ailleurs ce qu'est un renseignement personnel et ce qui ne l'est pas. On y énonce aussi les règles à suivre en matière de consentement lorsqu'il est question de communiquer un renseignement personnel. Les sections 3.3.1 et 3.3.5 détaillent les consentements et la journalisation des accès, deux mécanismes pour aider à la conformité à cette loi.

2.5.4 *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)

LPRPDE[22] est une loi fédérale du Canada qui s'applique aux organisations qui opèrent des activités de nature commerciale au Canada. Dans le cas des organismes

---

[21] Pour en savoir plus, https://tools.ietf.org/html/rfc7643#section-4.3

[22] En anglais, LPRPDE se nomme le *Personal Information Protection and Electronic Documents Act* (PIPEDA).

publics, LPRPDE s'applique seulement si les activités commerciales sont « hors de son activité essentielle » (Commissariat à la protection de la vie privée du Canada, 2017). Un exemple pourrait être la boutique souvenir d'un musée municipal. LPRPDE s'applique également si les renseignements personnels traversent des frontières provinciales ou nationales, ce qui peut être le cas lorsque des outils infonuagiques sont utilisés. Les sections 3.3.4 et 3.3.5 détaillent la sécurité, les audits et la journalisation des accès, qui sont des mécanismes pour aider à la conformité à cette loi.

CHAPITRE 3

L'API CITOYEN

Ce chapitre présente la solution de l'API Citoyen en commençant par la façon dont l'API s'intègre avec les principaux standards techniques reliés. Puis, les concepts principaux sont définis, suivis des concepts de soutien. Par la suite, ce chapitre présente l'architecture TI de haut niveau initiale, les arrimages possibles avec les initiatives parallèles et se termine par une carte conceptuelle donnant une indication du chemin à parcourir avant de finaliser l'architecture TI cible.

3.1 Contexte de la solution

3.1.1 Rappels

Tout d'abord, il importe de rappeler la nature imparfaite de cette solution qui se veut une addition à des standards existants ou déjà proposés. La solution va donc évoluer avec le temps, avec l'arrimage des autres initiatives recensées. C'est là qu'on voit l'importance d'un autre principe d'architecture TI : **l'architecture cible**. Ce principe dicte de développer une architecture cible, à partir de laquelle on déduit une architecture initiale, permettant de progresser vers la cible de façon itérative. Il est également important de réviser la cible annuellement.

3.1.2 L'API Citoyen, un service en soi

L'API Citoyen est la pierre angulaire du dossier citoyen intégré (DCI) de la Ville de Montréal. L'approche d'un DCI vise à donner le contrôle au citoyen sur ce que les organismes publics connaissent de lui. Cette solution lui permet de facilement mettre à jour ses renseignements personnels à un guichet unique, plutôt que de le faire auprès de chaque service de l'organisme public avec qui le citoyen interagit. Cette approche a été recommandée au *Bureau d'expérience client* (BXC) de la Ville de Montréal par la firme PricewaterhouseCoopers (PricewaterhouseCoopers Canada, 2017) pour permettre une situation gagnante-gagnante entre le citoyen et l'organisme public. Avec cette solution, un citoyen a davantage d'occasions (à chaque nouveau service) de réviser et/ou mettre à jour ses renseignements personnels, ce qui fait bénéficier les différents services de l'organisme public de renseignements à jour, accélérant la prestation de services pour tous les citoyens.

L'approche d'un DCI diverge de l'interprétation généralement retenue de *la Loi sur la Protection des renseignements personnels et documents électroniques* (PRPDE) ainsi que de *la Loi sur les renseignements personnels dans les organismes publics* (PRP). Dans ces deux lois, le renseignement personnel est conservé strictement pour rendre un service au citoyen. Dans le cadre d'un DCI – et donc de l'API Citoyen – le renseignement personnel est enregistré de façon centralisée, ce qui devient un service en soi pour le citoyen. Plus précisément, le service offert permet la facilité de réutilisation, le contrôle de la diffusion et la mise à jour des informations personnelles du citoyen. La solution (individu, famille, organisation) respecte PRPDE, car le citoyen doit consentir (implicitement ou explicitement, selon le choix de l'organisme) à utiliser ses renseignements personnels pour un service d'un organisme public donné.

Par définition, un service est numérique ou pas et consiste en quelque chose demandé par l'individu ou fait à sa demande, de façon directe ou indirecte. Un exemple de demande indirecte est le cas d'une transaction immobilière notariée au Québec, où le citoyen est d'accord pour signer l'acte d'achat ou de vente. Ainsi, la ville où se situe la propriété est informée indirectement de la transaction, par le truchement de la *Loi concernant les droits sur les mutations immobilières* (Gouvernement du Québec, 2018a) et de la *Loi sur les bureaux de la publicité des droits* (Gouvernement du Québec, 2018b). Le citoyen a consenti implicitement, car nul n'est censé ignorer la loi[23].

3.1.3 En addition à OIDC

La solution de l'API Citoyen fait partie des approches d'identités fédérées. Le choix dominant de mécanisme d'authentification de cette approche est *OpenID Connect* (OIDC) (voir 2.5.1). OIDC permet de transmettre les renseignements personnels sous deux types d'affirmations OIDC :

- Les affirmations OIDC standards (de l'anglais « claims ») se limitent aux noms, prénoms, courriels, identifiants et à la langue préférée de l'usager.
- Les affirmations OIDC personnalisées (de l'anglais « customs claims ») se limitent à des champs textes.

Après plusieurs considérations, plutôt que de créer des affirmations OIDC personnalisées complexes, transmettant les renseignements personnels manquants, le CISN a choisi OIDC pour l'authentification[24] et de lui ajouter l'API Citoyen, une

---

[23] Pour en savoir plus, https://www.educaloi.qc.ca/jeunesse/capsules/nul-nest-cense-ignorer-la-loi

[24] Rappel : OIDC a été retenu comme forme d'authentification pour la preuve de concept de connexion Longueuil-Montréal, voir section 2.3.

extension philosophique de SCIM 2.0, pour le reste des renseignements personnels. À la différence d'une extension technique, une extension dite « philosophique » a pris certaines libertés par rapport à la spécification des extensions SCIM 2.0 (Hunt, 2015). L'avantage pour le projet a été un développement plus rapide ; par contre, l'inconvénient est qu'un arrimage sera nécessaire avant de pouvoir publier une ébauche de standard Internet (Bradner, 1996) (qui est un mécanisme pour demander à l'industrie des commentaires sur une technique, une technologie ou une pratique liées à l'Internet).

Ainsi, en utilisant les affirmations OIDC standards reçues après une authentification réussie, une application frontale peut afficher ces informations au citoyen, sans avoir à effectuer un appel réseau à l'API Citoyen. Le lien entre OIDC et l'API Citoyen peut ensuite être réalisé à l'aide d'une affirmation OIDC personnalisée, l'identifiant externe[25], qui est transmise en même temps que les affirmations OIDC standards. Fourni préalablement par l'API Citoyen, l'identifiant externe permet de faire le pont entre OIDC et l'API Citoyen, qui sont généralement réalisés par deux implémentations distinctes, tel que l'illustre la figure ci-dessous.

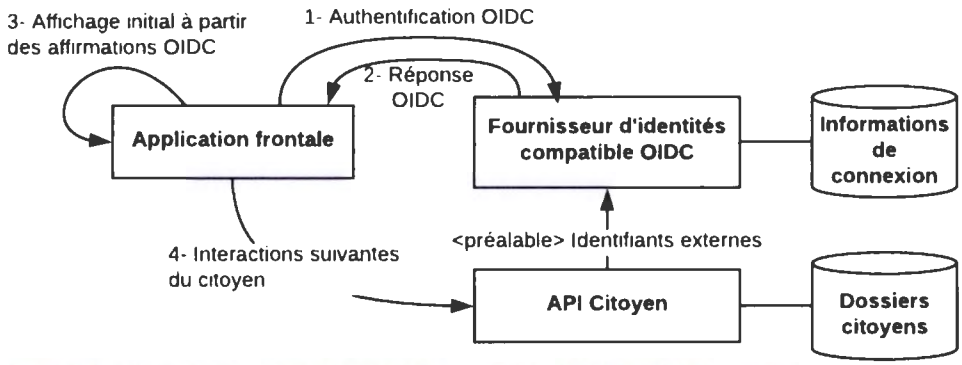

Figure 3.1 - interactions typiques entre un fournisseur d'identités et l'API Citoyen

[25] Fréquemment nommée ainsi dans les implémentations OIDC.

3.1.4 En extension à SCIM 2.0

Tel que mentionné en 3.1.3, l'API Citoyen est une extension philosophique du schéma principal du *Système de gestion d'identités interdomaines* (SCIM) 2.0 (Hunt, 2015). À la base, SCIM 2.0 permet de représenter des utilisateurs et des groupes d'utilisateurs avec la notation d'objets JavaScript (JSON). SCIM 2.0 définit également un mécanisme d'extension (Hunt, 2015) à deux volets :

- **L'indicateur de schéma** à la racine d'une ressource SCIM 2.0, `"schemas":[ ]`, dicte quels schémas gouvernent une ressource SCIM 2.0 en cours. Le tableau JSON doit contenir une ou plusieurs références de schémas.
- L'inclusion **d'éléments d'extension,** soit un élément JSON préfixé de la référence à son schéma SCIM 2.0, permet d'inclure un schéma dans un autre. Par exemple, le type `Enterprise:User` est indiquée par la référence ci-dessous :

  `"urn:ietf:params:scim:schemas:extension:enterprise:2.0:User"`

Par la suite, bien qu'il le redéfinit complètement, l'API Citoyen s'est fortement inspiré du schéma principal de SCIM 2.0 (Hunt, 2015). C'est-à-dire qu'au lieu d'utiliser `"urn:ietf:params:scim:schemas:core:2.0:User"` et des éléments d'extensions, l'API Citoyen a pris l'hypothèse qu'il sera possible d'utiliser uniquement un schéma d'extension comme schéma de base. Cette extension pourrait se nommer :

`"urn:ietf:params:scim:schemas:extension:government:2.0:Identity"`

> *[NOTE]*
> *Les divergences entre l'API Citoyen et SCIM 2.0 ne seront pas davantage décrites dans le présent document ; cette tâche sera faite dans un projet ultérieur.*
> *[/FIN DE LA NOTE]*

3.2 Concepts principaux

Le *Comité identité et services numériques* (CISN) a adopté trois concepts pour classifier l'ensemble des utilisateurs des services des organismes publics participant au CISN : les **individus**, les **organisations** et les **familles**. Le schéma ci-dessous représente les relations entre les concepts, qui seront détaillés par après.

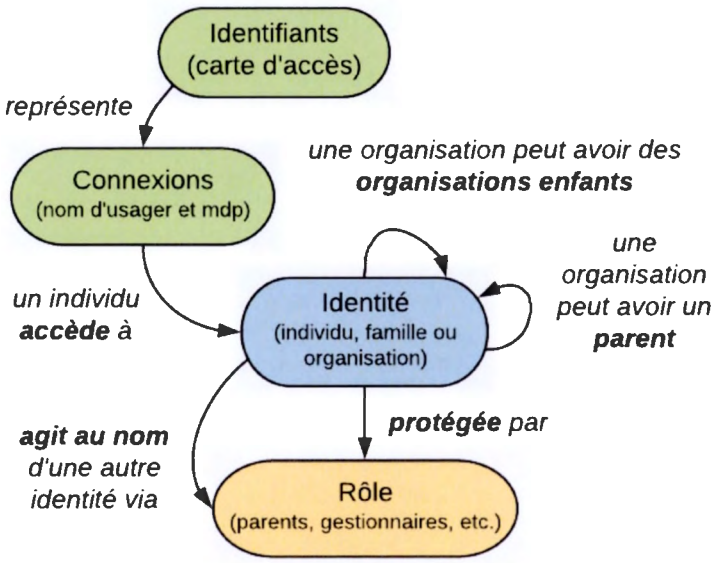

Figure 3.2 - relations entre individus, organisations et familles

Les identifiants et les connexions sont, en fait, des concepts de soutien, mais permettent de mieux expliquer les **concepts principaux** suivants :

- Un **individu** est le seul type d'identité à pouvoir posséder une connexion ;
- Une **organisation** peut avoir des sous-organisations, et donc, une organisation peut avoir une organisation parent ; plusieurs individus peuvent agir au nom d'une organisation, selon leur rôle ;
- Une **famille** est une forme particulière d'organisation, où il n'y a pas de sous-famille ; un individu peut être membre et agir au nom de plusieurs familles.

3.2.1 Individu

L'individu représente la donnée généralement requise pour offrir un service public à une personne physique. L'information recueillie au sujet de cet individu est variée et représentée dans la figure conceptuelle ci-dessous.

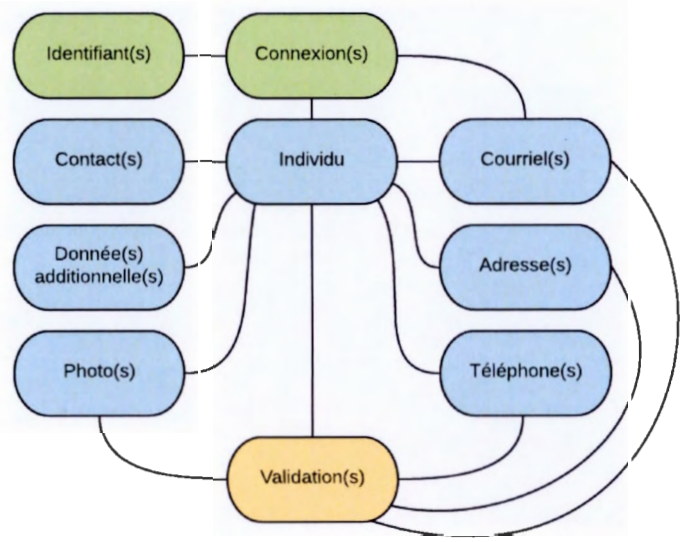

Figure 3.3 -- Ressources de l'individu

- **L'individu** comprend aussi certains renseignements de base (non illustrés), tels : nom, prénom, date de naissance, langue de communication préférée.
- Les **validations**, un concept de soutien qui sera détaillé à la section 3.3.2, qualifie plusieurs autres renseignements.
- Les **connexions** et les **identifiants** sont des éléments de la ressource de type individu, mais seule la connexion a été spécifiée pour le moment.

[NOTE]

L'API Citoyen supporte l'enregistrement de liens sécurisés vers les photos, mais n'offre pas par lui-même de mécanisme de stockage de fichiers. L'implémentation de la Ville de Montréal est compatible avec un hébergement de type S3[26].

[FIN DE LA NOTE]

---

[26] Pour en savoir plus https://docs.aws.amazon.com/AmazonS3/latest/API/Welcome.html

3.2.2 Organisation

L'organisation est généralement une personne morale (The Canadian Encyclopedia, 2013), c'est la reconnaissance du droit à une identité juridique propre (possession, responsabilité, etc.). Le terme « organisation » a été retenu, car il y a de nombreuses variantes de la personne morale[27] et l'API citoyen les supporte sans distinction (entreprise individuelle, société par actions, personne morale sans but lucratif, etc.).

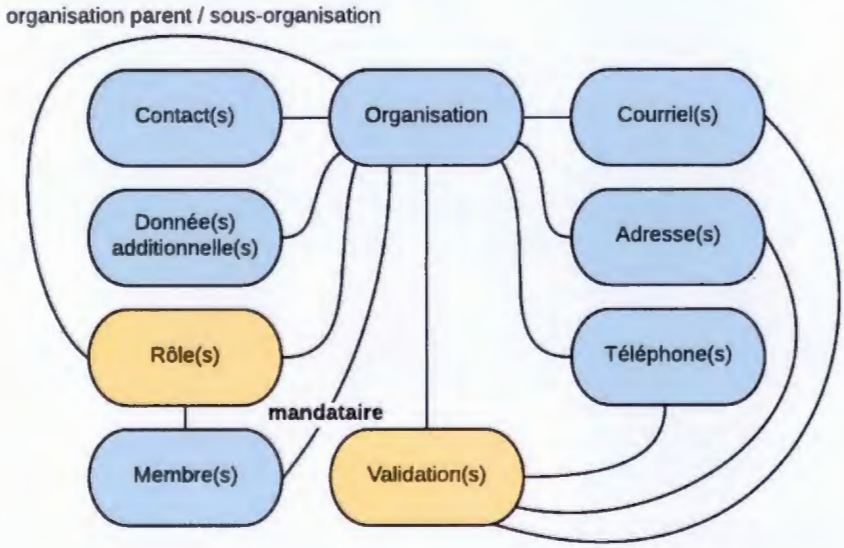

Figure 3.4 – ressources de l'organisation

On remarque que les ressources sont similaires à celles de l'individu, auxquelles on ajoute les **rôles**, les **membres** et le **mandataire**, qui est un membre particulier. Les organismes publics, comme la Ville de Montréal, offrent une panoplie de services aux organisations, tels les rapports d'accident[28], les certificats d'occupation commerciale[29], etc. Toutefois, ces personnes morales sont par définition

---

[27] Pour en savoir plus, http://www.registreentreprises.gouv.qc.ca/fr/demarrer/differentes-formes-juridiques/

[28] Pour en savoir plus, https://servicesenligne.ville.montreal.qc.ca/sel/accidents/bienvenue.do

[29] Pour en savoir plus, http://ville.montreal.qc.ca/portal/page?_pageid=7297,74297646&_dad=portal&_schema=PORTAL

immatérielles ; on ne peut donc pas prendre une photo de la personne morale, ni lui émettre de pièce d'identité. L'API Citoyen permet donc qu'une personne physique serve de **mandataire** à une personne morale, c'est-à-dire qu'elle a le pouvoir de la représenter auprès de l'organisme public et d'engager la responsabilité civile de l'organisation. Par la suite, le mandataire peut donner des accès à d'autres individus, sans que l'organisme public n'y regarde ; ce sera de la responsabilité du mandataire.

À noter que le mandataire est un administrateur particulier de l'organisation, qui ne peut pas supprimer son compte et ne peut pas être retiré de l'organisation, tant que celle-ci existe numériquement ; il peut seulement déléguer son mandat à un autre utilisateur. La section 3.2.5 sur les rôles détaille ces interactions davantage. Un individu peut être membre ou mandataire de plusieurs organisations à la fois. Si un mandataire n'est plus apte à transférer son rôle par lui-même (démission, maladie, mortalité, etc.), un mécanisme permet aux employés de l'organisme public d'assigner un autre mandataire, sans perdre le contenu du dossier de l'organisation.

Parce que l'API Citoyen traite toutes les identités comme des types de données similaires, il est possible d'implémenter les liens entre les organisations comme des rôles particuliers ; c'est un choix d'implémentation.

3.2.3 Famille

La famille est une spécialisation du concept d'organisation, c'est-à-dire une variante d'organisation à la structure limitée. Ainsi, une famille n'a pas de sous-famille, ni donc de rôle d'administrateur, mais comporte le concept de parent-enfant. De son côté, le **mandataire** d'une famille sera simplement dénommé être le **parent principal** (ou créateur, selon la terminologie souhaitée) et pourra transférer ce rôle à l'un des autres parents, au besoin. La différence entre le parent principal et les

autres parents est qu'un autre parent ne peut pas évincer d'une famille le parent principal. Un employé de l'organisme public peut par contre le faire, advenant une situation le requérant (mortalité, divorce, etc.). Voici la figure décrivant la famille.

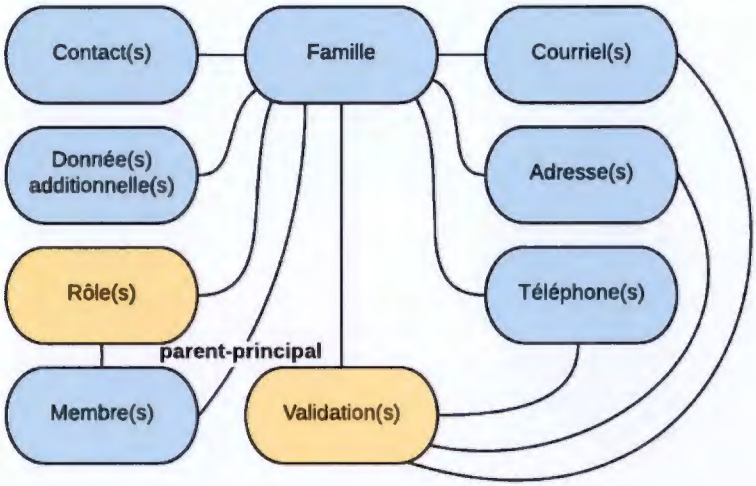

Figure 3.5 – ressources de la famille

Comme un individu peut être membre de plusieurs organisations, il peut être membre ou mandataire de plusieurs familles. C'est ainsi que le modèle retenu ne pose pas de contrainte sur les formes de familles supportées par l'API : des familles monoparentales jusqu'aux familles reconstituées, les diverses formes sont permises.

[NOTES]

- *Les concepts de curatelle*[30] *et de famille d'accueil*[31] *sont des concepts qui existent au Québec, mais qui ne sont pas inclus dans la spécification actuelle.*
- *Le concept de* famille *n'est pas encore présent dans l'implémentation de la Ville de Montréal, car la portée du projet* confidentiel *qui devait ajouter la famille à l'implémentation a été revue à la baisse avant le présent projet de synthèse.*

[FIN DES NOTES]

Particularité : la famille n'a pas d'existence juridique propre au Canada, mais le CISN a décidé de réutiliser les mécanismes de l'organisation, car le concept d'une famille

---

[30] Pour en savoir plus, https://www.educaloi.qc.ca/capsules/la-curatelle-au-majeur

[31] Pour en savoir plus, http://www.centrejeunessedemontreal.qc.ca/famille_demarches.htm

qui a ses propres données facilite beaucoup l'implémentation et l'utilisation des services. Par exemple, la famille peut détenir a priori des actifs ou, lorsque disponible, payer toutes les factures des inscriptions aux sports et loisirs de la famille en une seule opération. Si applicable, un parent pourrait obtenir un seul reçu fiscal pour l'ensemble des services utilisés par les membres de la famille.

3.2.4 Routes et verbes

Les **routes et verbes** suivants sont disponibles pour les concepts principaux. On remarque que la route est polymorphique, permettant d'agir sur les divers types d'identités par le même point d'accès.

[NOTE]

- *Ce tableau représente une vue de haut niveau de l'API, un peu comme celle que le Comité des APIs (CAPI) de la Ville de Montréal utilise lors de son premier passage. Se référer à la documentation d'API pour les détails.*
- *Les routes et verbes sont en anglais dans l'API pour favoriser la réutilisation hors-Québec.*

[FIN DE LA NOTE]

Tableau 3.1 – routes et verbes communs des concepts principaux

Verbes	Routes	Usages
GET	`/identities?type=individual`	Rechercher un individu selon plusieurs filtres.
GET	`/identities?type=organisation`	Rechercher une organisation selon plusieurs filtres.
GET	`/identities?type=family`	Rechercher une famille selon plusieurs filtres.
GET	`/identities/:id`	Accéder au dossier d'une identité ; le type spécifique sera trouvé dans le champ `ressourceType`.
POST	`/identities`	Créer une identité ; le type dépendra du corps de la requête.
PUT	`/identities/:id`	Modifier une identité.
DELETE	`/identities/:id`	Effacer ou désactiver une identité ; initialement, l'API Citoyen ne permet pas la suppression d'une identité ayant utilisé un service.

Les routes et verbes suivants sont propres aux identités du type **individu**.

Tableau 3.2 – routes et verbes spécifiques aux individus

Verbes	Routes	Usages
GET	/identities/:id/logins	Accéder à la liste des connexions de la personne.
POST	/identities/:id/logins	Associer une connexion à cette personne.
DELETE	/identities/:id/logins	Désactiver une connexion à cette personne ; il est possible d'enlever la dernière connexion, signifiant que la personne doit interagir avec son dossier par l'intermédiaire d'un employé : au comptoir, par téléphone, par la poste, selon les règles d'affaires prévues par l'organisme public.

Les routes et verbes suivants sont propres aux identités du type **famille** ou **organisation**. On remarque la présence de la variable « cleRole » : c'est une clé textuelle unique, associée au tableau des rôles prédéfinis dans l'API Citoyen ; voir la section 3.2.5 pour plus de détails sur les rôles.

Tableau 3.3 – routes et verbes spécifiques aux familles et aux organisations

Verbes	Routes	Usages
GET	/identities/:id/roles	Obtenir la liste des rôles définis pour cette identité ; un rôle regroupe d'autres identités qui peuvent agir au nom de la présente identité (:id).
POST	/identities/:id/roles	Créer un nouveau rôle pour cette identité, comprenant au moins un membre.
GET	/identities/:id/roles/:cleRole	Obtenir un rôle particulier, y compris la liste des membres.
PUT	/identities/:id/roles/:cleRole	Modifier un rôle particulier, généralement pour en changer la liste des membres.
DELETE	/identities/:id/roles/:cleRole	Retirer un rôle et l'accès de tous les membres de ce rôle à la présente identité ; cela ne fait que supprimer la relation.

3.2.5 Rôles

Les **rôles prédéfinis** dans l'API Citoyen sont des rôles liés aux relations entre les identités et aux autorisations d'accès au nom d'une autre identité. Ce mécanisme supporte également des **rôles spécifiques** à un service d'un organisme public donné. Ces rôles spécifiques ne sont pas partagés lors de la fédération d'identités. Le parent principal/mandataire peut donner accès à sa famille/à son organisation à d'autres individus qu'il invitera.

Le parent principal/mandataire est responsable de l'attribution des rôles, que ce soit par lui-même ou parce qu'il a délégué ce pouvoir en confiant un rôle de parent/gestionnaire à un autre. Le terme « parent » est utilisé au sens large, pouvant dénoter un parent biologique, des grands-parents, un tuteur légal, etc. Le tableau ci-dessous décrit les rôles ; remarquez que la plupart sont partagés entre famille et organisation, facilitant une implémentation commune.

Tableau 3.4 – comparaison des rôles prédéfinis entre la famille et l'organisation

Famille	Organisation	Caractéristiques
Parent principal	**Mandataire**	Le parent principal/mandataire est un parent/administrateur qui ne peut pas être démis de ses fonctions ; il peut transmettre son rôle à un autre membre.
n. a.	**Administrateur**	L'administrateur, c'est un gestionnaire qui peut créer, détruire ou transférer des sous-organisations ; ce rôle est hérité dans les sous-organisations.
Parent	**Gestionnaire**	Le parent/gestionnaire est un membre qui peut ajouter des membres ou d'autres parents/gestionnaires à la même famille/organisation ou sous-organisation que lui-même.
Membre	**Membre**	Un individu qui peut agir au nom de l'identité.
Invité	**Invité**	Un individu invité à rejoindre la famille/l'organisation dans un certain rôle, mais qui n'a pas encore répondu à l'invitation.

Famille	Organisation	Caractéristiques
Enfant	n. a.	Un individu, généralement sans connexion, qui ne peut pas agir au nom de la famille, mais qui en fait partie.
Rôle(s) spécifique(s)	**Rôle(s) spécifique(s)**	Un individu qui a un rôle pour un service donné, d'un organisme public donné (ex. : contact en cas d'urgence).

3.3 Concepts de soutien

[NOTE]

- *Dans un souci d'alléger le texte des prochaines sections, le lecteur est avisé que le terme « identité » représente à la fois les ressources individus, familles et organisations ; se rappeler que le terme « citoyen » est utilisé au sens large.*
- *Certains concepts de soutien (connexions, identifiants, contacts) ne sont pas détaillés, car n'ayant pas de particularités significatives par rapport au reste du domaine de l'identité numérique.*

[/FIN DE LA NOTE]

3.3.1 Consentements

L'API Citoyen inclut le consentement à l'utilisation des renseignements personnels. Les consentements régissent l'accès et le partage des renseignements personnels entre le citoyen, d'une part, et les services des organismes publics avec lesquels il interagit, d'autre part. L'idée des consentements vient originalement d'un rapport de la firme PricewaterhouseCoopers (PricewaterhouseCoopers Canada, 2017) préparé pour la Ville de Montréal. Ce rapport recommandait d'établir un dossier citoyen central, intégré, tel que décrit à la section 3.1.2.

Tableau 3.5 – principales routes et verbes liés aux consentements

Verbes	Routes	Usages
`GET`	`/identities/:id/consents`	Obtenir la liste des consentements actifs pour cette identité.
`POST` ou `PUT`	`/identities/:id/consents`	Créer (POST) ou modifier (PUT) un consentement pour cette identité, ciblant au moins un champ.
`GET`	`/identities/:id?expand=consents`	Route raccourcie, pour obtenir le détail de l'identité, incluant les consentements.

Verbes	Routes	Usages
GET	/identities/:id/consents?serviceType=pet-licensing	Route raccourcie, permettant de récupérer ce consentement spécifique, s'il existe.
DELETE	/identities/:id/consents/:idConsent	Retirer un consentement.

Chaque consentement spécifie un ou plusieurs champ(s) concerné(s), autorisés par le citoyen. Lorsqu'un service tente d'accéder au dossier de l'identité, seuls les champs consentis, et l'identifiant de l'identité, seront retournés.

Les consentements peuvent être révoqués, mais cela n'empêche pas le service ou l'organisme public d'accéder aux données consenties dans le passé. Cela va simplement bloquer les accès aux mises à jour des renseignements personnels. En contrepartie, le citoyen ne pourra plus bénéficier du ou des services concernés.

Le consentement tient toujours compte de la personne qui note le consentement au dossier, que ce soit un individu ou un employé au bénéfice de cette identité. De plus, à l'instar des individus, l'API Citoyen conserve des consentements pour les familles et les organisations. Même si les informations ne sont pas strictement des renseignements personnels, ces consentements notent que la responsabilité civile de l'organisation ou des parents de la famille a été encourue pour un service donné.

3.3.2 Validations

Lorsqu'il est question des renseignements personnels d'une identité citoyenne, il est également question du niveau de validations de ces données. Le mot « validations » a été choisi, car il peut inclure les certifications et d'autres méthodes d'établir le degré de certitude qu'un renseignement est vrai. Il faut aussi noter la façon dont il a été vérifié : avec une preuve ? Si oui, par quel type de preuve et par quel moyen ?

Que ce soit un API ou par l'action d'un employé, l'API Citoyen note ces informations lorsqu'une validation est apposée sur un renseignement personnel.

Un champ ou un groupe de champs peuvent être la cible d'une validation. Par exemple, les courriels sont validés individuellement. Par contre, les champs noms et prénoms doivent être validés ensemble, incluant optionnellement la date de naissance.

Il est important de se rappeler que le niveau de confiance des validations peut diminuer avec le temps, par exemple en ce qui a trait aux adresses de résidence. Ce n'est pas le rôle de l'API Citoyen de dicter la durée de validité d'une information. Le mécanisme de validation fournit l'information sur le moment où la validation a eu lieu, sur les champs concernés, sur le niveau de confiance et, finalement, sur la méthode utilisée. Il revient aux services de déterminer l'âge maximal des validations qu'ils acceptent, avant d'exiger une revalidation par le citoyen.

Tableau 3.6 – principales routes et verbes liés aux validations

Verbes	Routes	Usages
GET	/identities/:id/validations	Obtenir la liste des validations pour cette identité.
POST	/identities/:id/validations	Créer une validation ou une demande de validation manuelle d'informations (selon le contenu).
PUT	/identities/:id/validations/:idValidation	Modifier le statut d'une demande de validation manuelle pour approuver ou rejeter.
GET	/identities/:id?expand=validations	Route raccourcie, pour obtenir le détail de l'identité, y incluant les validations.
GET	/identities/:id/validations/:idValidation	Obtenir une validation.
DELETE	/identities/:id/validations/:idValidation	Annuler une validation ou une demande de validation.

Une fois validée, on peut dire qu'une forme d'attestation numérique est émise, incluant des éléments de sécurité assurant la non-répudiation, c'est-à-dire qu'il n'est pas possible pour un employé de contester le fait d'être l'auteur d'une validation.

Certaines validations peuvent être complétées en libre-service. Par exemple, la validation d'un courriel ou d'un numéro de téléphone mobile ne peut être pratiquement effectuée que par un code envoyé par courriel ou par message, que l'individu utilise pour confirmer la validation.

Certaines validations ne sont pas aussi fortes que d'autres. Par exemple, avoir validé l'existence d'une adresse de façon numérique auprès d'un référentiel d'adresses n'est pas une preuve que le citoyen y demeure, mais simplement que l'adresse est réputée existante. Le tableau suivant est tiré d'un exercice fait à la Ville de Montréal en 2017 (Ville de Montréal, 2017b) et explicite divers niveaux possibles de confiance envers les validations.

Tableau 3.7 – niveau de confiance des renseignements personnels

Niveau de confiance	**Description**
Déclarée	Le citoyen fournit l'information.
Inférée	Niveau de confiance déduit à partir d'autres informations.
Mesurée	Niveau de confiance provenant d'un instrument de mesure de confiance (GPS, biométrie, etc.).
Certifiée/validée	Avec un processus formel (numérique ou avec un processus humain), lequel cas requiert généralement une photo du document.
Formelle	Un humain confirme l'identité, le lieu, la possession, l'authenticité ou la conformité. Par authenticité, nous entendons que les pièces justificatives sont vérifiées auprès de l'émetteur du document utilisé comme preuve pour s'assurer que ce dernier soit toujours valide.

3.3.3 Données additionnelles

Le concept des données additionnelles est là pour couvrir tous les cas où un organisme public doit conserver davantage d'information sur un citoyen par rapport à ce qui avait été prévu initialement par l'API Citoyen. La structure envisagée est similaire à un dictionnaire de données, c'est-à-dire que chaque information est codifiée. Un service peut donc consulter une donnée ajoutée par un autre service, comme c'est déjà le cas pour d'autres informations du dossier citoyen.

Tableau 3.8 – principales routes et verbes liés aux données additionnelles

Verbes	Routes	Usages
GET	`/identities/:id/additionalInfos`	Obtenir la liste des données additionnelles pour cette identité, qui me sont présentement accessibles (en tant que citoyen ou en tant qu'employé dans le cadre d'un service donné).
POST	`/identities/:id/additionalInfos`	Créer une donnée additionnelle d'un certain type (selon le contenu fourni).
PUT	`/identities/:id/additionalInfos/:idInfo`	Modifier une donnée additionnelle ; à noter que les validations spécifiques sont le fait de l'API Citoyen de chaque organisme public.
GET	`/identities/:id?expand=additionalInfos`	Route raccourcie, pour obtenir le détail de l'identité, y incluant les données additionnelles.
GET	`/identities/:id/additionalInfos/:idInfo`	Obtenir une donnée additionnelle.
DELETE	`/identities/:id/additionalInfos/:idInfo`	Supprimer une donnée additionnelle ne fait que lui adjoindre un statut particulier et la masquer ; elle sera accessible dans l'historique du dossier (via le paramètre « `expand=additionalInfos` »).

Dans cette version de l'API Citoyen, les données additionnelles ne sont pas transmises entre les organismes publics, car, mis à part la structure les définissant, il n'y a pas de convention d'usage de ces données. Une liste des données

additionnelles bien connues sera établie ultérieurement pour en faciliter l'échange entre les organismes publics, sans pour autant limiter l'extensibilité du concept.

Des exemples de données additionnelles sont les suivantes : les preuves de non-possession de casier judiciaire, les commentaires entre employés sur un citoyen pour un service donné (ex. « le citoyen passera demain avec la balance du paiement »), etc.

Les données additionnelles sont typées par une clé au format texte. Par exemple : `clean-record-certification`, ou encore, `pet-licensing-recent-homeless-shelter-user`. Remarquer qu'un organisme public peut décider de spécifier une portée limitée à une donnée additionnelle, en précisant le champ optionnel `scope` et une clé de service (ex. `pet-licensing`). Cette restriction n'est pas recommandée, car les citoyens s'attendent qu'un même renseignement demandé par plus d'un service puisse être réutilisé (avec le consentement approprié). De plus, les données comportent un champ identifiant leur structure (`schemaVersion`) qui, une fois combinée avec le `type`, permet de valider la structure des données (entier, chaîne de caractères, date, etc.).

Certaines données additionnelles ont une visibilité limitée : le citoyen lui-même seulement, les employés seulement ou ouvert à tous ceux pouvant consulter l'identité. Évidemment, une donnée additionnelle invisible à un acteur ne peut pas être modifiée par ce dernier.

Les données additionnelles ne sont pas exposées à un service, ou aux employés d'un service, sans le consentement du citoyen. La section 3.3.4, sur la sécurité, parle plus spécifiquement de cet aspect. Par exemple, pour éviter que des employés n'ayant

accès qu'au service de permis de stationnement sur rue n'accèdent par inadvertance à des renseignements sensibles (comme une donnée additionnelle relative au casier judiciaire) les implémentations de l'API Citoyen doivent respecter la portée et la visibilité des données additionnelles.

3.3.4 Sécurité

Parce que ces renseignements personnels sont des données sensibles, l'API Citoyen tient compte que certaines données ne sont pas nécessairement disponibles ou modifiables, selon les droits d'accès de la personne qui y accède. Par disponibilité, on entend « visibilité ». Ce mécanisme est en supplément du mécanisme de visibilité des données additionnelles.

Ainsi, certains champs sensibles (date de naissance, numéro d'assurance-maladie, etc.) supportés par l'API Citoyen ne sont pas retournés dans les réponses de base, même si l'utilisateur y a accès. Ces champs doivent être demandés spécifiquement par un second appel à l'API, où l'option `fields` est spécifiée dans les paramètres de l'URL (ex. `?fields:birthdate`). Ces appels supplémentaires seront journalisés et pourront être enquêtés, selon les règles de l'organisme public.

En bref, ce sont les implémentations de l'API Citoyen qui sont responsables de supporter les droits d'accès et la visibilité au niveau des champs individuels (de l'anglais « field level security »). Ce concept est bien expliqué par IBM (IBM, 2019). Le format d'échanges prévoit des mesures de sécurité, mais chaque implémentation se doit de les appliquer.

Par la suite, l'approche de sécurité proposée assume que tous les employés de service à la clientèle auront accès aux données des citoyens, mais que tous les accès

et/ou modifications seront journalisés. Cela peut apparaître contradictoire, mais les organismes publics doivent maintenir un équilibre entre la protection de la vie privée et l'accessibilité des services. Tel que mentionné plus haut, les champs sensibles, tels la date de naissance, ne seront pas retournés initialement. L'employé doit insister, par une action supplémentaire, pour y avoir accès. Dans le cas de données additionnelles dont la portée est liée à un service, la session de l'employé doit être accompagnée d'une session valable du compte de service du service associé. À noter qu'un compte de service est similaire à un utilisateur, mais qu'il représente un système d'information ; utile, par exemple, pour la gestion des reprises en cas d'incidents tels qu'une coupure d'accès réseau. La combinaison de deux sessions (employé et compte de service) permet de s'assurer que l'employé a les droits requis pour offrir le service (c'est le devoir du service métier). Par exemple, à la Ville de Montréal, les permis de transformation de bâtiment ne sont pas une compétence des employés du service à la clientèle de première ligne ; les données additionnelles qui sont associées à ce service seront donc limitées aux employés pouvant délivrer de tels permis de transformation.

Il revient aux organismes publics utilisant l'API Citoyen de définir des stratégies finales de sécurité, d'audits des procédures, et de vérification de l'usage que les employés font des renseignements personnels. L'implémentation de la Ville de Montréal permet une visibilité et des accès variés à chaque service. Cela permet à un service donné de restreindre encore davantage les accès des employés aux données du dossier citoyen, limitant ainsi la libre circulation des renseignements personnels des citoyens.

3.3.5 Audits et journalisation des accès

Par souci de transparence, l'initiative de l'API Citoyen doit permettre aux citoyens de connaître l'usage qui est fait de leurs renseignements personnels, de consulter facilement les services consentis et de connaître **les raisons** pour lesquelles des employés utiliseraient leurs données. Parce que le projet se concentre sur le volet technologique, et non la gouvernance, nous n'aborderons pas la gestion du changement qui serait requise pour que chaque employé d'un organisme public spécifie les raisons d'accéder au dossier d'un citoyen ; l'API Citoyen se limite à offrir la capacité technique de le faire.

L'audit (utile pour connaître qui a modifié des champs) et la journalisation des accès (permettant d'identifier celles et ceux ayant consulté des champs) sont essentiels pour assurer la confidentialité des renseignements personnels. Tout accès par un employé ou un compte de service est journalisé, incluant la liste **des champs accédés**. Comme certains champs sensibles ne sont pas retournés dans la réponse de base de l'API, l'accès à un champ sensible est journalisé séparément, lors de l'appel réseau supplémentaire mentionné précédemment.

La spécification n'impose pas de méthode pour conserver de façon sécuritaire les journaux, seulement une façon minimale de les consulter. Une version sécuritaire est proposée par le biais de l'implémentation de référence de la Ville de Montréal. Cette implémentation exigera la présence d'une deuxième base de données où tous les accès seront en ajout seulement, dans le but d'y enregistrer les audits et d'y journaliser les accès. Ces droits, plus restreints, représentent le début d'une approche sécurisée.

Tableau 3.9 – principales routes et verbes liés aux audits et aux journaux d'accès

Verbes	Routes	Usages
`GET`	`/identities/:id/audits`	Obtenir la liste des audits et des journaux d'accès pour cette identité.
`GET`	`/identities/:id?expand=audits`	Route raccourcie, pour obtenir le détail de l'identité, y incluant les audits.
`GET`	`/identities/:id/audits/:idAudit`	Obtenir une entrée d'audit.

Ces ressources sont en lecture seulement (verbe `GET` seulement), car ce sont des ressources générées automatiquement par l'implémentation ou à partir d'informations reçues en entête HTTP des messages. Un mécanisme similaire a été publié récemment par Google, pour sa suite applicative *G Suite*[32].
Chaque entrée d'audit contient le moment, la raison d'accès, l'identité qui y accède (l'employé, le citoyen lui-même ou un membre de sa famille) et les champs concernés.

L'inclusion de la famille est importante ici, car les parents peuvent agir au nom des enfants et ces accès seront journalisés, tel un employé qui accèderait au dossier d'un adulte à sa demande.

3.3.6 Historique des adresses et adresses multiples

L'historique des adresses est une fonction de l'API Citoyen essentielle, voire obligatoire puisque la plupart des services des organismes publics municipaux sont liés au lieu de résidence ou à une adresse donnée, tel un bâtiment. L'historique des adresses permet aux citoyens de consulter facilement la liste des services qu'ils

[32] Pour en savoir plus, voir https://gsuiteupdates.googleblog.com/2019/04/access-transparency-cloud-data-security-trust.html

utilisent à chacune de leurs adresses. L'historique des adresses est une fonction permettant implicitement le support des adresses multiples. Une adresse multiple concerne une personne possédant plus d'une adresse encore valide, c'est-à-dire sans date de fin et qui peut être située à Montréal ou ailleurs dans le monde.

L'API Citoyen permet de spécifier des dates de début et de fin de validité pour chaque adresse ; c'est du ressort des règles d'affaires des différents organismes publics de décider si un citoyen peut ajouter une adresse à l'avance (service de changement d'adresse à l'avance). C'est aussi du ressort des organismes publics de décider du mécanisme permettant à leurs divers services d'être mis au courant d'un changement d'adresse. Par exemple, une ville fictive pourrait décider d'envoyer un courriel lors du changement d'adresse d'un citoyen avec permis de stationnement sur rue, pour rappeler au citoyen son devoir de confirmer son changement d'adresse dans les 30 jours, si le citoyen veut se prévaloir d'un droit de transfert gratuit de son permis de stationnement, s'il y a lieu.

Tableau 3.10 – principales routes et verbes liés aux adresses

Verbes	Routes	Usages
GET	/identities/:id/addresses	Obtenir la liste des adresses pour cette identité.
POST	/identities/:id/addresses	Créer une nouvelle adresse pour cette identité.
PUT	/identities/:id/addresses/:idAddress	Modifier une adresse, en mettant une date de fin sur la version précédente.
GET	/identities/:id?expand=addresses	Route raccourcie, pour obtenir le détail de l'identité, y incluant les adresses.
GET	/identities/:id/addresses/:idAddress	Obtenir une adresse.
DELETE	/identities/:id/addresses/:idAddress	Route raccourcie pour mettre une date de fin à une adresse.

L'API Citoyen n'est pas un référentiel d'adresses. Même si deux identités distinctes utilisent la même adresse, chacune aura sa propre copie qui évoluera distinctement. Cette fonction est nécessaire, car les adresses sont un sujet complexe où des adresses sont ajoutées ou enlevées continuellement, au rythme des constructions et des transformations de bâtisses. Seule une adresse de famille sera implicitement partagée avec les membres de cette même famille, s'ils n'ont pas actuellement d'adresses (par exemple, les enfants).

Pour permettre de réconcilier plus facilement les adresses de l'API Citoyen avec les autres systèmes d'un organisme public, chaque adresse d'un dossier peut porter une mention du **référentiel d'origine** et **d'identifiant d'origine**. Par exemple, si une adresse a été retrouvée dans le référentiel d'adresses de la Ville de Montréal, l'identifiant associé à cette adresse sera conservé avec les informations de l'adresse de cette identité. L'historique des adresses aurait pu être reconstitué à partir de l'historique du dossier (prochaine section), mais le choix a été fait de le maintenir séparément, car l'adresse est centrale dans les prestations des services municipaux au Québec.

3.3.7 Historique du dossier

Un autre volet de la spécification couvre les besoins d'accéder à la version historique des renseignements personnels d'un citoyen. Par exemple, l'historique peut servir pour des vérifications *a posteriori* de la conformité de délivrance de rabais pour des permis animaliers. L'historique du dossier permet de garantir aux divers services d'un organisme public que toutes les données que ces services ont pu consulter d'un dossier citoyen seront encore disponibles ultérieurement, pour autant que ces services notent le numéro de version du dossier, présent dans la représentation reçue de la ressource. L'objectif est d'éviter l'éternelle duplication des

renseignements personnels, qui est monnaie courante dans les systèmes d'organismes publics ; c'est la racine d'un dossier citoyen intégré et centralisé, et des bénéfices associés pour le citoyen (mentionnés en 3.1.2).

Parce que l'accès à une version historique d'une identité est aisé (un simple numéro de version à conserver), les équipes de développement des services d'un organisme public sont encouragées à se conformer à la pratique recommandée de l'API Citoyen (ne pas conserver de copie des données ; toujours se référer à l'origine). En utilisant l'historique du dossier, les équipes TI s'épargnent du travail, car elles n'ont pas à réaliser les audits et la journalisation des accès qui sont requis par les lois (voir 2.5.3 et 2.5.4).

Tableau 3.11 – principales routes et verbes liés à l'historique du dossier

Verbes	Routes	Usages
GET	`/identities/:id/history`	Obtenir la liste des versions du dossier de cette identité.
GET	`/identities/:id/history/:version`	Obtenir une version du dossier en historique ; à noter que la version actuelle est également disponible sur la route de l'historique.
GET	`/identities/:id/history/5 ?expand=validations`	Les mécanismes normalement disponibles sur l'identité actuelle, sont généralement disponibles sur une version historique. Ici, les validations de la version 5.

On remarque que, comme pour les audits et la journalisation des accès, l'historique est généré automatiquement au fil des interactions avec le dossier de l'identité. Dans la version actuelle de l'implémentation de la Ville de Montréal, les accès à l'historique sont les mêmes que les accès à la version courante. Parce que cette implémentation ne supporte pas (encore) la révocation des consentements, cette approche ne pose pas de problèmes. Lorsque la révocation d'un consentement sera

supportée, l'historique devra être bonifié pour limiter l'accès aux versions de l'identité qui ont existé entre la date de début du consentement et la date de sa révocation (inclusivement). Finalement, les accès à l'historique du dossier sont journalisés par le mécanisme d'audit et de journalisation des accès (voir section 3.3.5) ; par contre, les informations d'audits et de journalisation des accès **ne sont pas** dans la portée du mécanisme d'historique du dossier.

3.4 Architecture de l'API Citoyen

3.4.1 Architecture de haut niveau initiale

Cette architecture de haut niveau découle de la preuve de concept (POC), décrite à la section 2.3. Chaque partenaire y déploie son instance d'API Citoyen, incluant la base de données, et un module d'authentification compatible avec *OpenID Connect* (OIDC) supportant la fédération d'identités.

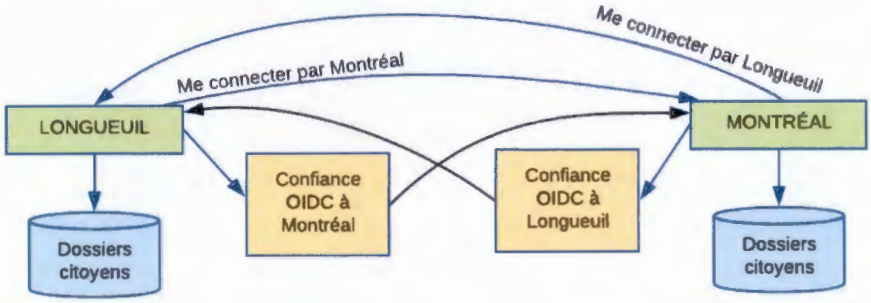

Figure 3.6 – architecture de haut niveau initiale de l'API Citoyen

Lorsqu'un citoyen clique le bouton « Me connecter par », il est redirigé sur le site partenaire, où il peut saisir ses informations de connexion. Le lien de confiance est requis, car OIDC requiert des informations de la part du demandeur (l'origine), lors d'une demande d'authentification pour s'assurer que ce partenaire est de confiance. En général, cette information est un secret partagé. Le citoyen est alors retourné au site d'origine, accompagné d'un jeton de session.

Quoique fonctionnelle, cette approche se complique rapidement avec l'ajout d'un troisième partenaire. La figure suivante décrit, avec des lignes grasses, les interactions qui s'ajoutent avec un troisième partenaire : chacun doit faire confiance aux autres, de façon point à point.

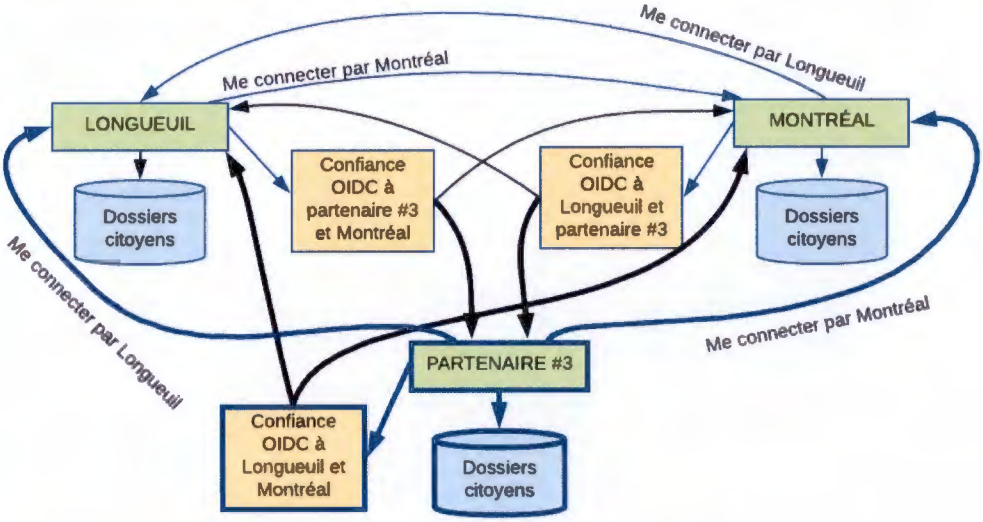

Figure 3.7 – architecture de haut niveau initiale avec un troisième partenaire

On constate donc pourquoi la mise à l'échelle de l'identité fédérée est un problème complexe. Une alternative reste de créer les liens de confiance de façon unidirectionnelle, c'est-à-dire où seul un des deux partenaires est audité par l'autre, comme le fait le gouvernement canadien avec l'initiative de *SecureKey* (voir 1.1.2).

3.4.2 Arrimage avec la *Fondation pour l'identité décentralisée* (DIF)

La *Fondation pour l'identité décentralisée* (DIF)[33] est une initiative qui a été identifiée comme partie intégrale de l'architecture cible de l'API Citoyen dans le cadre du *Défi des villes intelligentes* (voir 2.4). Les travaux de la DIF sont coordonnés par plusieurs groupes de travail, qui avancent chacun un volet des spécifications requises. Ces travaux touchent, entre autres, à la gestion de plaques tournantes

[33] Pour en savoir plus, https://identity.foundation

d'identités (de l'anglais « identity hub »), à la découverte dynamique des participants grâce à des résolveurs, à l'émission et au suivi des attestations qu'un renseignement est vrai, ou encore à la façon d'enregistrer des preuves publiquement dans les chaînes de blocs. Cette initiative est à l'avant-garde de la recherche sur l'identité, tout en solutionnant intrinsèquement le problème de confiance point à point de l'approche de gestion d'identités fédérée.

Lors de l'analyse de l'initiative de la DIF dans le cadre du *Défi des villes intelligentes* (DÉFI), un arrimage ultérieur est apparu nécessaire, car certains concepts présents ou prévus dans l'API Citoyen n'y ont pas (encore) d'équivalents :

- Les **audits et la journalisation des accès,** permettant de connaître quels usages les employés d'organisme ont faits des renseignements personnels après avoir reçu un consentement.
- La **non-révocation des accès** à l'historique du dossier, permettant aux organismes publics de conserver un accès aux dossiers des citoyens qui ont bénéficié d'un service public. C'est-à-dire, même si le citoyen révoque le consentement donné, l'organisme public continue d'avoir accès à l'historique du dossier, tel qu'il était entre la date du consentement et la date de sa révocation.

Le concept suivant, prévu dans la cible de l'API Citoyen, n'y existe pas non plus :

- La **traçabilité des attestations**, c'est-à-dire un mécanisme inhérent à la récupération d'une attestation numérique d'un dossier, grâce auquel il est possible, en ayant une attestation numérique en main, de tracer par quel employé de quel organisme cette attestation a été originalement extraite du dossier citoyen. Ce mécanisme permettrait donc de retracer rapidement l'origine d'une fuite de renseignements personnels, permettant de prendre action.

Un dernier enjeu avec la DIF est que, dans une approche décentralisée, chaque partie utilisatrice (de l'anglais « relying parties ») doit déterminer à qui elle fait confiance et la DIF ne semble pas (pour l'instant) avoir de mécanisme pour en faciliter la réalisation. De son côté, l'implémentation de Microsoft (Microsoft, 2018) semble adresser ce cas par le biais d'une infrastructure décentralisée de clés publiques (DPKI). C'est aussi pourquoi le *Cadre de confiance pancanadien* (PCTF) est en développement, tel que décrit à la section suivante.

3.4.3 Arrimage avec le *Cadre de confiance pancanadien* (PCTF)

À l'ère des échanges numériques de plus en plus fréquents et variés entre citoyens, organisations et organismes publics, il devient important de pouvoir déterminer à qui faire confiance, et jusqu'à quel point. Ce n'est pas une problématique propre à l'approche de gestion d'identités décentralisées, car ce problème a été identifié au tournant des années 2010, avec la création en 2011 du *Sous-comité sur la gestion de l'identité* (IMSC) (Institut des services axés sur les citoyens, 2019) qui œuvre depuis sur le sujet, avec pour résultat la naissance du *Cadre de confiance pancanadien* (PCTF) (Digital ID and Authentification Council of Canada, 2019).

Tel que mentionné en 2.4, le PCTF est un cadre qui définit des critères de conformité qui peuvent être appliqués comme un standard ou comme un guide lors de l'utilisation de technologies. Ces critères visent à définir un nombre d'éléments clés, dans le but de faciliter l'échange de représentations numériques fiables (de l'anglais « trusted digital representations »), soient :

- Les **identités numériques fiables** (de type **individu**) ;
- Les **identités numériques fiables** (de type **organisation**) ;
- Et les **relations numériques fiables**.

On peut ainsi remarquer que les concepts du PCTF sont très proches de ceux de l'API Citoyen, sans être identiques, ce qui invite à effectuer un arrimage entre les deux initiatives dans le futur. Par cette compatibilité et la complémentarité déjà identifiée en 2.4, le PCTF facilite l'atteinte des objectifs de l'API Citoyen. En effet, le PCTF ajoute la possibilité de certifier l'usage dont fait un organisme public de l'API Citoyen, incluant les processus d'affaires liés à la gestion d'identités que l'organisme public mettra en place. De plus, parce que le PCTF vise à établir des ponts avec d'autres pays pour établir des liens de confiance internationaux (Secrétariat du Conseil du Trésor du Canada, 2018), une installation de l'API Citoyen certifiée avec le PCTF pourra éventuellement reconnaître et faire usage d'identités de confiance fournies par d'autres organismes publics, au Québec et ailleurs dans le monde.

3.4.4 Architecture cible et carte conceptuelle

L'architecture cible de l'API Citoyen n'a pas été finalisée dans le cadre de ce projet de synthèse, car cette cible était en dehors de la portée du projet. Par contre, nous avons trouvé approprié d'établir une carte conceptuelle de la situation actuelle, sachant que ces concepts nous apparaissent faire partie de la cible éventuelle. La figure suivante présente donc cette carte conceptuelle de l'API Citoyen L'idée d'établir cette carte vient des discussions sur l'arrimage avec les autres initiatives et des chevauchements déjà identifiés des concepts qui les composent. Un projet ultérieur pourra donc démarrer à partir de cette carte conceptuelle, la mettre à jour, effectuer l'arrimage restant pour amener une superposition des bulles pour, finalement, obtenir une architecture cible complète.

[NOTE]

L'arrimage des quatre initiatives de la figure suivante n'a pas été complété ; cet arrimage est hors de la portée du présent projet de synthèse (l'API Citoyen).

[FIN DE LA NOTE]

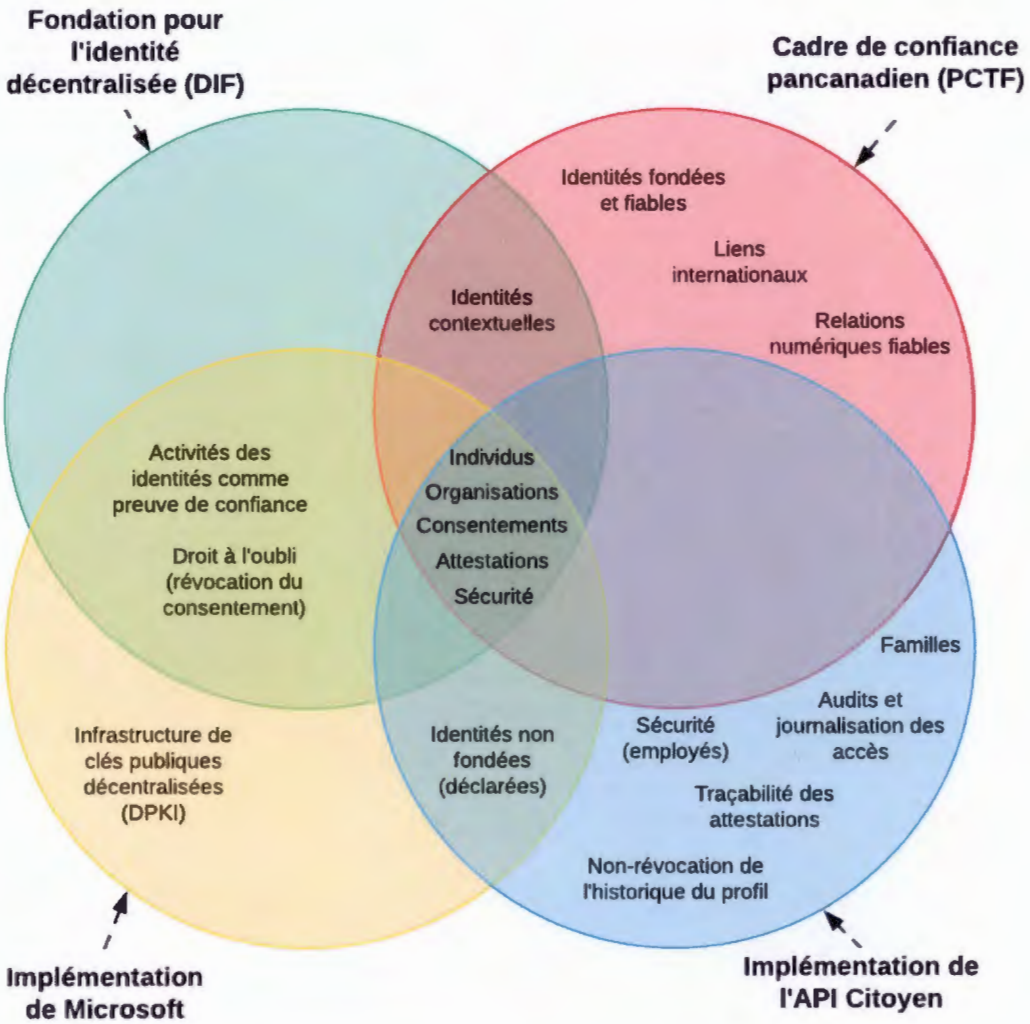

Figure 3.8 – architecture cible conceptuelle de l'API Citoyen

Quelques remarques :

- « Sécurité (employés) » (API Citoyen) est un mécanisme spécifique à la gestion des droits des employés, en plus de la sécurité générale trouvée au centre.
- L'initiative de la DIF, le PCTF ou l'API Citoyen pourraient évoluer distinctement pour devenir chacun un standard.
- L'API Citoyen et le PCTF se concentrent présentement sur l'approche de fédération d'identités ; les quatre initiatives tendent vers l'approche de l'identité décentralisée dans leur cible respective, d'où l'intérêt d'un arrimage ultérieur.

CONCLUSION

Le but du projet documenté dans ce rapport de synthèse était de faciliter le partage de renseignements personnels de citoyens entre logiciels d'un même organisme public, d'une part, et entre organismes publics d'autre part, dans le domaine de l'informatique municipale au Québec, et ce de façon sécuritaire tout en conservant un haut niveau de confiance de la part des citoyens. Amorcé à la Ville de Montréal, ce projet a eu des échos auprès d'autres organismes publics qui faisaient face à des problématiques similaires. Le *Comité identité et services numériques* (CISN) a ainsi vu le jour avec le présent mandat, dans le cadre du *Réseau de l'informatique municipale du Québec* (RIMQ).

Une veille technologique, faite avant le début du projet de synthèse, a été résumée verbalement à l'équipe du projet à la Ville de Montréal et indiquait qu'il n'y avait pas de standard existant couvrant les besoins ciblés, mais que certains pouvaient servir de blocs de départ, tel *OpenID Connect* (OIDC). OIDC a été choisi dans un projet distinct à la Ville de Montréal, mais également par d'autres partenaires du CISN, faisant d'OIDC le choix évident pour le volet authentification du projet.

Puisque OIDC est un protocole d'authentification, et non pas une interface de programmation d'applications (API), OIDC ne pouvait pas remplir l'entièreté du présent mandat. Il faut comprendre que plusieurs protocoles liés à l'Internet sont avancés par des entreprises privées, qui n'ont pas souvent les mêmes besoins ou contraintes que les organismes publics. Par exemple, l'entreprise privée sur Internet cherche fréquemment à vendre ses services, ou encore, à les offrir gratuitement en échange de quelque chose, généralement les renseignements personnels pour mieux cibler des clients potentiels avec de la publicité. De leur côté, les organismes

publics ont des missions où ils se doivent d'offrir des services à des populations données, généralement gratuitement ou à peu de frais ; c'est pourquoi, quand il est question d'organismes publics, il est généralement question de la population éligible à recevoir le service discuté.

En cherchant à développer un API pour répondre aux besoins du mandat et des membres du CISN, le projet visait à complémenter OIDC avec des capacités et fonctions requises par les modèles d'affaires des organismes publics. Pour y parvenir, les travaux du projet furent itératifs et collaboratifs, que ce soit au fil des rencontres du CISN pour creuser des sujets, présenter des avancées ou effectuer une preuve de concept. Ou encore, que ce soit par les travaux effectués à la Ville de Montréal, qui étaient répartis en trois volets : les positionnements d'architecture TI (tels l'approche *API d'abord*, l'usage du libre, l'architecture microservices, la réutilisation de normes et standards et le principe d'architecture TI de la disponibilité des données de qualité – qui inclut la transparence – d'où un besoin clair d'audits), des projets concrets qui faisaient avancer le développement de l'API selon leurs besoins respectifs et, finalement, avec l'aide du *Comité des APIs* (CAPI) de la Ville de Montréal, qui offrait son aide par la supervision d'un guide de style et des conseils sur les bonnes pratiques de ressources d'APIs. Finalement, le mois de février 2019 a vu le projet évoluer grandement en lien avec des sujets d'avant-garde dont, entre autres, l'identité décentralisée et le *Cadre de confiance pancanadien* (PCTF), par la participation de l'auteur du présent document au *Défi des villes intelligentes* (DÉFI).

Le résultat de cette démarche est l'API Citoyen qui complémente le protocole OIDC en y ajoutant une séquence d'échange de données supplémentaires, via une extension philosophique[34] du *Système de gestion d'identités interdomaines* (SCIM) 2.0. À noter que SCIM 2.0 est un standard Internet proposé dans une série de demandes de commentaires (RFCs).

En agissant comme extension qui bonifie SCIM 2.0, l'API Citoyen offre l'accès à des concepts que OIDC ne supporte pas, comme les liens familiaux, l'appartenance à une organisation, les consentements, les validations, les données additionnelles (un mécanisme d'extension propre à l'API Citoyen), les audits et la journalisation des accès, l'historique des adresses, les adresses multiples et l'historique du dossier du citoyen.

Tout n'est pas parfait pour autant, car malgré le fait que l'API Citoyen ait bénéficié des efforts consentis par des projets concrets de la Ville de Montréal, les contraintes de temps et de budget ont eu des impacts sur la réalisation de la première implémentation de l'API Citoyen. Ainsi, malgré l'intention que l'API Citoyen soit une extension SCIM 2.0, il faut plutôt dire qu'il en est une extension *philosophique*, car des divergences se sont glissées dans sa réalisation et un arrimage sera nécessaire avant de pouvoir songer à soumettre une ébauche de standard Internet.

L'initiative de l'API Citoyen a tout de même permis de démontrer la faisabilité technique d'une solution partagée entre organismes publics, idéalement via le logiciel libre. Le projet a aussi démontré que les organisations ont la même

[34] À la différence d'une extension technique, une extension philosophique prend certaines libertés par rapport à la spécification des extensions SCIM 2.0 ; un arrimage sera requis avant de considérer l'API Citoyen comme une véritable extension de SCIM 2.0.

différence qu'une famille par rapport à un individu. Ce sont divers individus agissant au nom d'une autre identité – un autre individu, une famille ou une organisation – selon certains rôles d'accès.

Un autre constat, au fil des discussions du CISN, est que chaque composant d'une identité est géré et attesté par un organisme distinct. Par exemple, le nom, le prénom et la date de naissance proviennent ultimement du *Directeur de l'état civil du Québec*[35]. Du côté de l'adresse de résidence, elle est prouvée par un acte notarié de transfert de propriété pour les propriétaires et, pour les locataires, par la possession d'une facture adressée à la personne par un service public, tel un fournisseur de téléphonie ou d'électricité. C'est ainsi qu'on peut dire qu'un ensemble d'organismes publics et d'organisations privés participent à établir une identité complète, unique et – si l'effort est mis sur la technologie, les processus et la gouvernance – réutilisable, pour l'ensemble de la vie numérique du citoyen.

Finalement, bien que susciter l'adhésion des organismes publics à l'initiative n'était pas un objectif immédiat du projet, la prochaine étape naturelle reste l'arrimage avec les autres initiatives, prioritairement le *Cadre de confiance pancanadien* (PCTF). Le PCTF est un cadre de certification permettant de juger si une utilisation d'une solution technique, telle l'API Citoyen et les processus qui l'entourent, permet d'établir des identités numériques fiables. L'équipe de l'API Citoyen pourrait y contribuer en réalisant une preuve de concept avec certains outils publiés en logiciel libre tel, par exemple, que l'implémentation par Microsoft des standards en développement de la *Fondation pour l'identité décentralisée* (DIF). L'API Citoyen évoluerait ainsi pour supporter l'identité décentralisée et cette dernière

[35] Pour en savoir plus, http://www.etatcivil.gouv.qc.ca/fr/default.html

bénéficierait de capacités supplémentaires, qui sont recherchées pour répondre aux besoins spécifiques des organismes publics, tout en démontrant que le PCTF est apte à supporter l'approche novatrice de l'identité décentralisée.

Pour conclure, ce projet aura eu pour effet bénéfique de suggérer des échanges interorganismes sur le sujet de l'identité citoyenne numérique, les organismes ayant tout avantage à joindre leurs forces pour réduire les faiblesses de leurs initiatives respectives, en travaillant de concert vers une solution d'identité unique au Québec, voire au Canada.

En ce sens, voici une liste survolant les prochaines étapes possibles pour le CISN et l'API Citoyen :

- S'arrimer avec le *Cadre de confiance pancanadien* (PCTF) ;
- S'arrimer avec la *Fondation pour l'identité décentralisée* (DIF) ;
- Déterminer la pertinence de préparer une ébauche de standard Internet, décrivant l'API Citoyen comme extension SCIM 2.0 ;
- Analyser et résoudre les écarts entre l'API Citoyen et les requis d'une extension SCIM 2.0 ;
- Analyser et résoudre les écarts entre la spécification de l'API Citoyen qui inclue les organisations et l'implémentation de la Ville de Montréal ;
- Finaliser la mise en logiciel libre de l'implémentation de l'API Citoyen de la Ville de Montréal.

[Cette page a été laissée intentionnellement blanche]

RÉFÉRENCES

Baars, D. (2016). *Towards Self-Sovereign Identity using Blockchain Technology.* Université de Twente, Pays-Bas. Récupéré de https://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf

Bradner, S. (1996). *The Internet Standards Process -- Revision 3.* (RFC2026). Internet Engineering Task Force. Récupéré de https://tools.ietf.org/html/rfc2026#section-2.2

Bray, T., Ed. (2017). *The JavaScript Object Notation (JSON) Data Interchange Format.* (RFC8259). Internet Engineering Task Force. Récupéré de https://tools.ietf.org/html/rfc8259

Comité identité et services numériques. (2017). *Projet de standardisation des échanges de données citoyennes.*

Commissariat à la protection de la vie privée du Canada. (2017). *Aperçu des lois sur la protection des renseignements personnels au Canada*. Récupéré de https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/02_05_d_15/

Daoust-Brown, S. (2018). Montréal : un accès aux services municipaux pour les personnes sans statut. *Journal de Montréal*. Récupéré de https://www.journaldemontreal.com/2018/12/05/montreal--une-ville--responsable-et-engagee--mais-pas-sanctuaire

Digital ID and Authentification Council of Canada. (2019). *Request for Review and Comment: PCTF Model Overview Discussion Draft V0.02 Review*. Récupéré de https://diacc.ca/2019/02/12/pctf-model-overview-discussion-draft-v0-02/

Gouvernement du Québec. (2018a). *Loi concernant les droits sur les mutations immobilières* Récupéré de http://legisquebec.gouv.qc.ca/fr/ShowDoc/cs/D-15.1

Gouvernement du Québec. (2018b). *Loi sur les bureaux de la publicité des droits* Récupéré de http://legisquebec.gouv.qc.ca/fr/ShowDoc/cs/B-9/

Hunt, P., Ed., Grizzle, K., Wahlstroem, E., Mortimore, C. (2015). *System for Cross-domain Identity Management: Core Schema*. (RFC7643). Internet Engineering Task Force. Récupéré de https://tools.ietf.org/html/rfc7643

IBM. (2019). *Field level security*. Récupéré le 2019-04-14 de https://www.ibm.com/support/knowledgecenter/en/SSFUEU_8.0.0/op_grc_admin/c_adm_fieldlevelsecurity.html

Infrastructure Canada. (2018). *Défi des villes intelligentes : Les finalistes*. Récupéré de https://www.infrastructure.gc.ca/cities-villes/index-fra.html

Institut des services axés sur les citoyens. (2019). *Sous-comité sur la gestion de l'identité (IMSC)*. Récupéré de https://iccs-isac.org/councils/joint-councils/identity-management-sub-committee

Kolkman, O., Bradner, S., Turner, S. (2014). *Characterization of Proposed Standards*. (RFC7127). Internet Engineering Task Force. Récupéré de https://tools.ietf.org/html/rfc7127 - section-3

Marchal, M. (2017). L'application mobile pour signaler nids-de-poule et graffitis entre en fonction. *Métro*. Récupéré de http://journalmetro.com/actualites/montreal/1200552/signaler-les-nids-de-poule-grace-a-une-application/

Martin, R. C. (2014). *The Single Responsibility Principle*. Récupéré le 2019-03-20 de https://blog.cleancoder.com/uncle-bob/2014/05/08/SingleReponsibilityPrinciple.html

Microsoft. (2018). *Decentralized Identity*. Récupéré de https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2DjfY

Office québécois de la langue française. (2006). Récupéré de http://granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=500185

Office québécois de la langue française. (2018). *logiciel libre*. Récupéré le 2019-03-20 de http://granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8389988

OpenID Foundation. (2014). *OpenID Connect Core 1.0 incorporating errata set 1*. Récupéré de http://openid.net/specs/openid-connect-core-1_0.html

PricewaterhouseCoopers Canada. (2017). *Revue des livrables du mandat de recherche*.

Réseau de l'informatique municipale du Québec. (2018a). *Le RIMQ*. Récupéré le 2018-11-27 de http://rimq.com/

Réseau de l'informatique municipale du Québec. (2018b). *Les comités*. Récupéré le 2018-11-19 de http://rimq.com/a-propos-du-rimq/les-comites/

RESTlet. (2019). *What are the key activities in an API-First Project?* Récupéré le 2019-01-13 de https://restlet.com/use-cases/activities/

Secrétariat du Conseil du Trésor du Canada. (2018, 7 novembre). Digital Identity in Canada. *FWD50* (p. 23).

Stine, M. (2014, 2019-01-14). *Microservices are solid*. Récupéré le 2019-01-14 de http://www.mattstine.com/2014/06/30/microservices-are-solid/

The Canadian Encyclopedia. (2013). Corporation Law. Récupéré de https://www.thecanadianencyclopedia.ca/en/article/corporation-law

Ville de Montréal. (2017a). *Avis et alertes*. Récupéré de https://beta.montreal.ca/avis-et-alertes

Ville de Montréal. (2017b). *Inventaire des services numériques.*

Ville de Montréal. (2017c). *Politique de confidentialité*. Récupéré de https://beta.montreal.ca/sujets/politique-de-confidentialite

Ville de Montréal. (2018a). *Analyse fonctionnelle : Dossier citoyen partagé inter-villes | Preuve de concept.*

Ville de Montréal. (2018b). *Politique sur l'utilisation et le développement des logiciels et du matériel libres* Récupéré de http://ville.montreal.qc.ca/pls/portal/docs/PAGE/PRT_VDM_FR/MEDIA/DOCUMENTS/politique_materiel_libres_fr.pdf

Ville de Montréal. (2018c). *Principes d'architecture TI.*

Ville de Montréal. (2019). *Chapitre 7 : Technologies*

Wodehouse, C. (2019). SOAP vs. REST: A Look at Two Different API Styles. *Upwork*. Récupéré de https://www.upwork.com/hiring/development/soap-vs-rest-comparing-two-apis/

GLOSSAIRE

Les termes définis dans le tableau ci-dessous ont une signification particulière dans ce document.

Tableou 3.12 – termes et définitions

Terme	Définition
Affirmations OIDC	Dans le cadre du protocole OIDC, se disent des informations retournées comme véridiques par un fournisseur d'identités. De l'anglais « claims ».
Affectation de ressources, Désaffectation de ressources	Dans les systèmes infonuagiques, se dit de l'action d'ajouter ou d'enlever des droits à un utilisateur donné, sur des ressources informationnelles données. Par exemple, ce peut être d'accéder à un outil de traitement de texte dans le nuage.
Appels d'offres publics	Mécanisme réglementé utilisé par un organisme public pour se procurer des biens ou des services.
Architecture, Architecture TI	Se dit de la pratique d'organiser une solution TI dans le but de minimiser les redondances et les liens aux autres systèmes informatiques, tout en maximisant les capacités fonctionnelles ainsi que les qualités non fonctionnelles réalisées par la solution TI. La version écourtée, sans le « TI », est utilisée dans ce document pour alléger le texte.
Architecture microservices	Style d'architecture favorisant la réalisation des fonctions d'affaires dans plusieurs services Web, chacun ayant son rôle et sa responsabilité bien définis. Chaque microservice doit être utile par lui-même et potentiellement réutilisable.
Authentifier	Action de vérifier qu'un utilisateur peut accéder à un dossier ou à une ressource. De façon générale, en fournissant un nom d'utilisateur et un mot de passe.
Champs OIDC	Dans le cadre du protocole *OpenID Connect* (OIDC),

	se disent des informations demandées à un fournisseur d'identités durant le processus d'authentification. De l'anglais « scopes ».
Citoyen	Utilisé à son sens très large, représente une personne physique ou morale pouvant utiliser ou bénéficier des services de l'administration publique. Ce peut être un touriste, un organisme sans but lucratif, un étudiant étranger en stage, une entreprise, un propriétaire non résident, etc.
Comité des APIs de la Ville de Montréal (CAPI)	Comité d'architecture TI dont la mission est de soutenir et veiller à la mise en place d'une pratique uniforme dans le développement d'API à la Ville de Montréal.
Comité des grandes villes du Québec (GVQ)	Comité de dix des plus grandes villes du Québec se réunissant de temps à autre sous le chapeau du Réseau de l'informatique municipale du Québec (Réseau de l'informatique municipale du Québec, 2018b). Plusieurs dirigeants et élus y échangent sur divers sujets, dont les pratiques en technologies de l'information.
Comité identité et services numériques (CISN)	Comité initié à l'automne 2016 pour faciliter l'adoption d'identité et de services numériques.
Connexion unifiée (SSO)	Mécanisme utilisé pour minimiser le nombre de fois où un utilisateur authentifié doit saisir son mot de passe, lors de l'accès à diverses ressources informatiques. L'acronyme SSO vient de l'anglais « single sign-on ».
Consentement	Accord donné par une personne à l'usage de ses renseignements personnels, pour un obtenir un bien ou un service. Dans l'API Citoyen, les consentements peuvent être donnés de façon verbale à un employé, qui fait l'inscription au dossier citoyen, ou de façon numérique, à l'aide des informations d'authentification du citoyen.
Demande de commentaires (RFC)	Document officiel d'un format prédéfini décrivant une solution technique en lien avec l'usage de l'Internet. Certains RFCs sont des standards, mais ils

	peuvent aussi être des ébauches pour discussion.
Dossier citoyen intégré (DCI)	Représentation centralisée de tous les renseignements personnels d'un citoyen que possède à la Ville de Montréal. On le dit « intégré », car si deux services de l'organisme utilisent la même donnée, ce sera le même champ dans le DCI. C'est un exemple de mise en pratique des bénéfices de l'API Citoyen dans un organisme public donné.
Dorsale	Se dit d'une application exposant principalement des APIs pour une ou plusieurs applications frontales ; invisible à l'utilisateur, mais qui reçoit l'information et la gère dans le temps.
Façade	La façade est un patron de conception logicielle[36] qui vise à masquer les détails techniques sous-jacents à une solution TI, pour en faciliter le changement, le cas échéant.
Fédération d'identités	Action d'interconnecter plusieurs fournisseurs d'identités entre eux pour les accès à une ressource informatique.
Fournisseur d'identités	Sur Internet, se dit d'une entité qui agit comme source de données, avec un certain niveau de confiance, pour montrer qu'un identifiant donné correspond à une personne donnée.
Frontale	Se dit d'une application proposant une interface utilisateur ; c'est la vue utilisée par le citoyen, c'est l'interface utilisable.
Gestion d'utilisateurs	Pratique permettant de voir à l'affectation et la désaffectation de ressources informatiques à une personne ou une autre, en général à l'aide de groupe d'accès.
Groupes d'accès	Technique permettant de regrouper des utilisateurs selon leurs besoins, leur travail ou sur une autre

[36] Pour en savoir plus, http://www.latece.uqam.ca/wp-content/uploads/2012/08/Les-patrons-de-conception-Repr%C3%A9sentation-et-mise-en-%C5%93uvre.pdf

	base pour faciliter la gestion des utilisateurs.
Infonuagique	Se dit des techniques et pratiques informatiques permettant de délocaliser des traitements informatiques dans le nuage.
Individu	Ressource de la présente API représentant une personne physique.
Interface de programmation d'applications (API)	Couche ou application logicielle facilitant l'interconnexion de deux solutions TI. De l'anglais « Application Programming Interface ».
JavaScript	Langage de programmation généralement utilisé dans les solutions TI pour réaliser les interactions complexes d'une page Web.
Logiciel libre	*Logiciel livré avec son code source de manière qu'il puisse être copié, modifié et redistribué [...] dans un esprit de développement coopératif et communautaire.* (Office québécois de la langue française, 2018)
Mandataire	*Une personne physique ou morale qui est autorisée à agir au nom d'une autre personne, ou encore à la représenter en vertu d'un contrat de mandat.* (Office québécois de la langue française, 2006)
Micro-services REST	Style de microservices favorisant l'usage des verbes et routes de base du protocole HTTP pour réaliser des services numériques sous forme d'API. De l'anglais « Representational State Transfer ».
Non-répudiation	Garantie significative qu'il n'est pas possible de renier une chose ou une information.
Notation d'objets JavaScript (JSON)	Format d'échange de données fortement inspiré de la déclaration d'objets dans le langage JavaScript. Ce format, relativement léger et structuré, est un standard Internet proposé[37]. De l'anglais « JavaScript Object Notation » (Bray, 2017)

[37] Pour en savoir plus, https://tools.ietf.org/html/rfc7159

Nuage	Se dit d'un ensemble de composants logiciels et matériels qui sont destinés à être utilisés via l'Internet, plutôt que sur leur emplacement physique.
Multicanal	Se dit d'un service public qui peut être amorcé, poursuivi ou complété par le biais de divers moyens de communication.
Organisation	Synonyme de personne morale ou de regroupement de personnes dans les ressources du présent API.
Organisme public	Organisation dont l'objectif principal est de desservir les citoyens. Dans ce rapport, cela inclut les organismes privés dont le propriétaire est majoritairement l'état (parapublics).
Personne morale	Regroupement nommé de personnes ayant ses droits et obligations propres[38].
Photo-chèque	Terme utilisé par diverses institutions financières pour parler de l'action de déposer un chèque de façon numérique, c'est-à-dire sans que l'institution ne voie le document physique. Seules des photos sont envoyées par l'utilisateur.
Renseignement personnel	Un renseignement personnel est une information permettant d'identifier un individu. Les lois et règlements ajoutent parfois d'autres informations dans ce groupe, dont l'âge, le poids, la taille, les dossiers médicaux, le groupe sanguin, etc.[39]
Réseau de l'informatique municipale du Québec (RIMQ)	Association[40] qui « [...] regroupe l'ensemble des intervenants du milieu informatique municipal du Québec. » et dont « [...] la mission est de soutenir l'échange et l'amélioration des connaissances des

[38] Pour en savoir plus, http://www.justice.gc.ca/fra/pr-rp/sjc-csj/redact-legis/juril/no91.html

[39] Pour en savoir plus, http://www.ci.com/web/company/questions.jsp?lang=FR

[40] Pour en savoir plus, https://rimq.com

	responsables de la gestion des ressources informationnelles dans les municipalités du Québec [...] » (Réseau de l'informatique municipale du Québec, 2018a)
Ressource	Dans le contexte d'un API REST, se dit d'une donnée ou d'un concept qui peut être représenté de plusieurs manières, par exemple en JSON ou en HTML.
Services numériques	Dans les organismes publics, se dit de rendre un service à un utilisateur sans requérir sa présence physique.
Solution, **Solution TI**	Volet informatique de la solution globale à un problème d'affaires. La version écourtée, sans le « TI », est utilisée pour alléger le texte.
Standard Internet, **Standard Internet proposé**	*Un standard Internet est caractérisé par un haut degré de maturité technique et offre, selon une pensée généralisée, un bénéfice significatif à la communauté Internet.* *Quant à lui, un standard Internet proposé est une spécification stable, qui a résolu les choix de design connu, qui a été significativement révisée par la communauté [...] sans avoir nécessairement d'implémentation ou d'expérience [...].* Notre traduction de (Kolkman, 2014)
Système de gestion d'identité interdomaines (SCIM) 2.0	Standard Internet proposé permettant de gérer des identités entre solutions TI, à travers Internet. De l'anglais « System for Cross-Domain Identity Management ».
Technologies de l'information (TI)	Se dit de l'ensemble des outils et pratiques permettant de traiter l'information de façon numérique et/ou à l'aide d'un ordinateur.
Ville d'origine	Ville où résident les données maîtres du dossier du citoyen, dont le mot de passe plus particulièrement.
Ville partenaire	Ville dans laquelle le citoyen bénéficie d'un service.

ANNEXE

[Cette page a été laissée intentionnellement blanche]

ANNEXE A

GÉNÈSE DU DOCUMENT

Cette annexe a pour but de distinguer ma contribution à ce projet de la contribution de mes collègues à la Ville de Montréal. Concentrés en deux sections : les éléments paginés et les éléments non paginés (conceptuels). Cette annexe décrit ainsi l'origine de chaque élément du rapport ainsi que ma contribution. Il est à noter que je suis l'auteur de l'entièreté du présent rapport, exception faite de certaines citations (phrases ou tableaux).

1 Éléments paginés

Les éléments paginés sont la description des éléments du présent document ; c'est-à-dire, l'origine du contenu ou de la forme d'une ou plusieurs pages spécifiques. Le tableau ci-dessous décrit ma contribution à chacun de ces éléments, en se basant sur l'ordre concret des pages du document où le chiffre « 1 » représente la page titre.

Tableau A-1 – origine et contribution aux éléments paginés

Pages	Section(s) ou concept(s)	Origine	Ma contribution
1, 2, 3, 4, 5, 6, 10, 12, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 35, 52, 53, 86, 87	Style visuel des pages liminaires et des pages d'entrée des chapitres, avec mini résumé de chapitre.	Inspiré de la thèse « Le développement du leadership partagé dans les équipes de projet » par Isabelle Bonneau, décembre 2015.	Tel que mentionné, j'ai rédigé les textes de chacune des sections, tout en m'inspirant de ce document comme exemple d'application du style « UQAM ».

7, 8, 9, 11, 13	Style des tables des matières, des tableaux et des figures.	Guide de style des mémoires et des thèses de l'UQAM, version de décembre 2017.	
24, 25, 26	État de l'art	Cette section est basée sur le document du gouvernement du Canada, enrichi et bonifié par moi-même et deux collègues. Un tableau a été bonifié à partir de celui finalisé par le *Laboratoire de l'innovation urbaine* de Montréal (LIUM), dans le cadre du *Défi des villes intelligentes* (DÉFI).	De mon côté, j'ai lu et internalisé le document du Canada, fourni par une collègue. J'ai également dû traduire et bonifier le tableau pour mieux l'expliquer aux membres du LIUM, qui eux-mêmes l'ont synthétisé davantage, avant que je le bonifie à nouveau.
15	Abstract	Traduction originale par Google Translate.	Révisé par moi-même, puis par une collègue.
29	Mandat du projet, mission du CISN, incluant l'idée de le mettre comme critère d'appels d'offres	Un collègue du *Comité identité et services numériques* (CISN) a proposé le mandat.	J'ai participé à la révision du mandat, à ma première présence au CISN ; les objectifs du CISN pré-dataient mon arrivée.
30, 31, 32	Objectifs	Tiré du mandat du CISN	J'ai reformulé les objectifs dans mes mots pour mieux les expliquer et les

			arrimer avec le reste du discours.
33	Cas concret	Mon imagination ; ce cas est le cas classique alimentant mes discussions de corridor.	Ce cas a été avalisé par la découverte que l'UQAM partage des informations avec la STM pour le statut étudiant (j'ai reçu un courriel que j'ai mentionné au CISN).
34	Hypothèses	Mes hypothèses, sauf l'expression « parfaitement imparfait » qui vient d'un collègue d'un autre palier gouvernemental, à propos du *Cadre de confiance pancanadien* (PCTF).	Moi-même.
36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 47	Démarche	Moi-même.	Cela résume ma démarche. Le dossier citoyen étant ma responsabilité ; j'ai tout de même abondamment sollicité mes collègues architectes de solutions TI, vu l'importance du dossier.
46	Ligne du temps du CISN	Version originale par un collègue, réalisé à ma demande pour illustrer une présentation (qui n'a	J'ai retravaillé la ligne du temps pour qu'elle soit verticale et s'affiche sur une seule page.

		pas eu lieu)	
49, 50, 51	Normes pertinentes	OIDC identifiée par la direction d'Infrastructures et plateformes du *Service des technologies de l'information de* la Ville de Montréal (STI) ; SCIM 2.0 identifié par un collègue. Certaines des lois identifiées par un autre collègue et la section légale du site de la Ville de Montréal.	J'ai résumé les lois et écrit le texte ; une grande révision par Éric Moreau a rendu la section bien plus digeste.
54, 55	Le concept que l'API Citoyen est un service en soi ; Le concept de Dossier citoyen intégré.	Une création commune du *Bureau de l'expérience client* (BXC) de la Ville de Montréal, de plusieurs collègues, dont moi-même, en s'inspirant des travaux commandés à PWC Canada.	Après digestion du rapport PWC, j'ai défendu l'importance d'un dossier intégré pour la suite des projets avec la collaboration indéfectible d'une collègue.
55, 56	« Claims » trop complexes	Un collègue d'une autre ville a effectué une recherche et des tests pour le CISN ; un autre collègue me les a également expliqués.	J'ai résumé l'approche et les limitations.

57	Extension SCIM 2.0	C'est mon idée originale, à la suite de la lecture de SCIM 2.0.	J'ai relancé mon projet de synthèse une 4e fois, sur le sujet de l'extension SCIM 2.0, devenue le présent rapport.
58, 59, 60, 61, 62	Concepts principaux et schéma ; Individus, familles et organisations	Un collègue recommandait le terme organisation dès nos premières discussions ; un autre collègue m'a inspiré par la phrase célèbre au STI : « Les familles et les organisations, c'est la même différence d'un individu. »	Il m'a fallu un mois de réflexion en novembre 2017 pour arriver au modèle initial (connexions-identités-rôles), incluant les boucles ; un collègue a révisé et repositionné le concept d'identifiants.
60	Organisation	Besoin identifié par une collègue et moi-même, à la suite d'une demande de deux autres collègues.	Je suis reparti du concept de famille et j'ai réfléchi à la phrase mentionnée précédemment pour me rendre compte que c'était pareil ; J'ai validé avec le *Comité des APIs* (CAPI) et un autre collègue.
61	Familles et rôles	Le besoin venait d'un projet, Sports et loisirs. Comme à mon habitude, j'ai réfléchi à la situation idéale pour me faire une tête. Le fournisseur a ensuite	Je suis parti de la discussion avec un collègue et je me suis forcé à retravailler les volets entreprises et familles. Découverte : ça fonctionnait. J'ai repris les

		expliqué son implémentation, et la complexité des relations familles au Québec.	cas complexes cités par le fournisseur pour valider mon concept.
63, 64	Routes et verbes	Mon design d'APIs, pour la présentation de décembre 2017 au CISN.	Révisé par deux collègues.
65	Rôles	Inspiré par le compte entreprise de Apple ; bonifié par le CISN.	Adaptation des concepts de Apple au contexte Ville. J'ai eu à maintenir le fort quand tous voulaient séparer les deux types de comptes. J'ai imaginé le concept de sous-organisation, pour supporter un cas réel rapporté par un collègue, sur une situation dans une précédente grande organisation.
66	Concepts de soutien	Connexions et identifiants précisés avec l'aide d'un collègue. J'ai fait le design (simplifié) des contacts selon les besoins des projets.	J'ai proposé un format de contacts basé sur les besoins d'affaires de Permis animalier ; deux collègues ont ensuite vérifié.

66	Consentements	Inspiré de la Ville d'Ottawa pour l'explicite ; l'équipe de design de la Ville de Montréal, pour les étapes.	Moi pour les signatures et le lien entre révocation et historique, avec l'assistance de deux collègues.
67, 68	Validations	Moi pour avoir identifié le besoin ; un collègue pour avoir lancé l'idée de regarder la structure JWT ; un autre collègue pour la réalisation actuelle.	J'ai révisé les suggestions de l'autre collègue, dont le design devait répondre aux besoins que j'avais exprimés ; j'ai moi-même choisi le terme « validation » plutôt que « certifications » (et le CISN a révisé).
69	Niveau de confiance	Un collègue a fait un document initial en 2016-2017.	Avec l'aide d'une collègue, nous avons fait une simplification pour une première version de Requêtes 311 ; niveaux approuvés par la représentante des arrondissements du moment et un collègue.
70, 71	Données additionnelles	Mon idée, inspirée de *Open311* qui a lui-même servi d'inspiration pour les Requêtes au 311, avec la flexibilité que cette approche donne.	J'ai créé le format pour faire entrer des données spéciales requises par Permis animalier ; le CISN a approuvé le concept ; ce concept fut le plus difficile à faire approuver par le CISN.

72, 73	Sécurité	Inspiré de l'approche d'extensions de SCIM 2.0. S'appuyant sur les positionnements d'architecture TI de la Ville (fait par l'équipe d'architecture avant mon arrivée).	J'ai fait un résumé des principales considérations.
74, 75	Journalisation des accès ; audits accessibles aux citoyens	Moi-même, basé sur les requis du Greffe de la Ville de Montréal. L'idée de l'historique des accès est un rêve d'un collègue pour améliorer la transparence des organismes publics.	J'ai gardé ce rêve en tête depuis le printemps 2017 ; approche validée par le Greffe.
75, 76, 77	Historique des adresses et adresses multiples	Inspiré des adresses SCIM 2.0 (une liste, une adresse primaire pour les communications).	J'ai créé l'historique d'adresses ; un collègue m'a suggéré l'origine ; un autre collègue a imaginé la solution pour mon problème de gestion des adresses multiples.
77, 78, 79	Historique du dossier	Concept que j'appelle gentiment « photo-historique ». J'ai imaginé la solution, qui a été révisée par trois collègues, pour minimiser les duplications de dossiers citoyens.	J'ai défendu mon point de vue, et les avantages, que les systèmes distants ne devaient pas faire des copies multiples (reproduisant le problème classique de dossiers en double à la Ville de Montréal).

			J'ai proposé la spécification du concept, qui a été révisée par le CISN (entre autres, amenant le passage au numéro de version plutôt que la date pour la garantie d'historique).
80, 81	Architecture initiale	J'ai suivi les préceptes de la fédération OIDC.	J'ai préparé les illustrations pour les présentations au CISN.
81, 82, 83	Arrimage avec la *Fondation pour l'identité décentralisée* (DIF) et Microsoft.	Un collègue m'a lancé l'idée que chaque morceau d'identités appartient à un organisme distinct, en plus de l'idée que la décentralisation était requise (en décembre 2017). Merci à un autre collègue pour son support sur les questions de la chaîne de blocs.	J'ai suivi l'idée d'une identité basée sur la chaîne de blocs pendant 1 an, jusqu'à ce qu'un collègue m'envoie la référence à la DIF et au livre blanc de Microsoft à l'automne 2018. J'ai assimilé les concepts du livre blanc et la documentation de la DIF, pour remarquer les concepts manquants par rapport à l'API Citoyen. Avec un collègue, nous avons rencontré Microsoft pour réviser la solidité de l'initiative.
83, 84	Arrimage avec le *Cadre de confiance pancanadien*	Issue d'une rencontre de deux collègues et d'un représentant du gouvernement fédéral	En tant que responsable du dossier citoyen, j'ai révisé les différents documents que ces trois

	(PCTF)	à l'automne 2018.	personnes m'ont transmis cet hiver, pour faire valoir les commentaires de la Ville de Montréal.
84, 85	Architecture cible et carte conceptuelle	Décision d'un collègue d'entériner la DIF (avec mes bonifications) comme cible d'architecture 2023.	J'ai fait la carte conceptuelle, selon ma compréhension du moment, en notant que cette carte va changer, car les 4 initiatives sont en constante évolution.
87, 88, 89, 90, 91	Conclusion	Je suis parti du gabarit du guide de l'UQAM. J'ai regardé plusieurs références sur « une bonne conclusion », notamment pour découvrir que c'est la section qui laisse l'idée finale dans la tête du lecteur.	J'ai rédigé la conclusion de nombreuses fois, avant d'arriver à la mouture actuelle. L'ordonnancement des étapes a été suggéré par un réviseur, pour être plus facile à comprendre d'un point de vue externe.
92, 93, 94	Références	Guide de style de l'UQAM	J'ai utilisé le logiciel *Endnote* fourni par l'UQAM, pour recenser et appliquer le Guide. Un grand merci à une bibliothécaire de l'UQAM pour la gestion des références vers les personnes morales qui apparaissent maintenant correctement.

95, 96, 97, 98, 99, 100	Glossaire	Je me suis basé sur un format que j'utilisais dans mon précédent travail, inspirés d'un gabarit d'un ancien collègue de travail que j'ai souvent utilisé par le passé.	Ordonnancement suggéré par M. Normand Séguin.

2 Éléments conceptuels (non paginés)

Les éléments conceptuels, ou non paginés, sont des éléments liés directement ou indirectement à l'API Citoyen. Ces éléments sont mentionnés dans le document, ou sont des concepts fréquemment discutés autour du sujet du Dossier citoyen intégré (DCI) à la Ville de Montréal. Ces éléments sont classés selon le début de la période couverte par l'élément. En plus de la description de l'origine et de ma contribution, les personnes de références sur le sujet sont indiquées.

Tableau A-2 – origine et contribution aux éléments conceptuels (non paginés)

Période	Section(s) ou concept(s)	Origine et contribution	Personne(s) référence(s)
Automne 2016	Serveur d'authentification	J'ai demandé la configuration requise pour tester l'identité fédérée ; j'ai fait une installation maison pour apprendre sur le concept.	Trois collègues architectes de solutions TI
Hiver 2017	Guide de style des APIs de la Ville de Montréal	J'ai participé à la révision finale du guide à mon arrivée à la Ville de Montréal	Les membres fondateurs du *Comité des APIs*, dont moi-même, et les autres

			contributeurs.
Hiver 2017	Rôles du comité des APIs	Ma compréhension de la mission du Comité.	Moi-même
Hiver 2017	CISN	Le comité des Grandes villes du Québec (GVQ) a lancé le CISN avec l'appui d'un collègue ; un autre collègue m'a invité à y être membre permanent. Je fais plusieurs présentations depuis décembre 2017 ; je présente en moyenne 2 h par rencontre du CISN (littéralement).	Deux collègues, le, CISN et le GVQ
Mars 2017	API Citoyen de base	La mission d'un dossier citoyen au sens large m'est donnée par un collègue. J'ai fait un design préliminaire des pages du dossier citoyen et des interactions avec l'API sur des feuilles brouillonnes (mes « napkins »). J'ai énuméré sur « napkins » tous les types d'identités potentielles, du touriste ou propriétaire non résident, à l'organisme sans but lucratif, en passant par la fondation religieuse et la base militaire.	J'ai fait l'exercice seul avec l'aide de recherches Google. Cet exercice a mis la table pour la suite de mes travaux sur l'API Citoyen. Six collègues différents, développeurs, architectes TI ou gestionnaires, m'ont aidé à finaliser

			l'approche.
Mars-avril 2017	Individus	Un collègue m'a donné la référence de SCIM 2.0, qui parle d'utilisateurs et de groupes.	J'ai fait la spécification de la ressource, champ par champ, en suivant le Guide de style des APIs de la Ville de Montréal.
Avril-septembre 2017	Implémentations 0.1 à 1.0 de l'API Citoyen à la Ville de Montréal	Le code de ces versions de l'API a été fait par l'équipe de développement ORO Platform à la Ville, en PHP. Je réalisais les spécifications en mode *API d'abord*. J'avais délégué la conformité de l'API à un collègue à cette étape.	Quatre collègues développeurs.
Juillet 2017-Printemps 2018	Ajustements des concepts pour Permis animaliers	À partir des ressources existantes de l'individu, j'ai ajouté les ressources contacts, données additionnelles, validations, etc.	Deux collègues et le CISN.
Septembre 2017	Document d'API Citoyen 0.9.17	J'ai rédigé l'entièreté de la documentation à l'aide de l'outil Restlet Studio (compatible au format *Swagger* 2.0).	Moi-même.
Décembre	Le présent	Amorcé à la suite de la	Moi-même.

2017 – mars 2019	rapport de synthèse	rencontre du CISN de décembre 2017, où j'ai présenté l'identité citoyenne pour la première fois.	
Janvier 2018 – février 2019	Implémentation 2.0 de l'API Citoyen à la Ville de Montréal	J'ai supervisé la réalisation de l'API en Node.js.	Cinq collègues développeurs.
Janvier 2018 à ce jour	Spécifications Google Docs pour la V2 de l'API	J'ai rédigé le document pour mieux décrire les ajouts et les cas d'usage (moins limitatif que *Swagger* ou *OpenAPI 3.0*)	
Juin-novembre 2018	Preuve de concept du CISN sur l'identité fédérée	Demande du CISN à un collègue qui me l'a délégué ; j'ai fait le plan et les tests locaux avant de coordonner la réalisation avec l'équipe d'Infrastructures et plateformes de la Ville de Montréal.	Trois collègues et des membres du CISN.
Été 2018	Routes multiples	Un collègue m'a convaincu de m'inspirer de JIRA pour diminuer la complexité de certaines routes de l'API Citoyen. J'ai fait l'approbation du principe au CISN.	Un collègue et le CISN.
Octobre-novembre 2018, mars 2019	Cohérence du document et notes pour aider le lecteur	Merci à un réviseur pour sa grande assistance dans la recherche de la cohérence entre les sections.	Un réviseur.

Janvier, février 2019	*Défi des villes intelligentes* du Canada (DÉFI)	Idée originale et concepts technologiques de base mis en place par le *Laboratoire d'innovation urbaine* de Montréal (LIUM). J'ai retravaillé le volet technologique de la soumission avec trois collègues. Une quatrième collègue m'a mis en contact avec un collègue du gouvernement du Canada. J'ai fait la recherche sur la DIF et le PCTF. J'ai travaillé à une architecture cible, qui a été bonifiée par un autre collègue. Une collègue et moi avons rencontré l'équipe du PCTF à Ottawa.	Six collègues différents.
Février 2019	Traçabilité des attestations	Mon idée de filigranes numériques, mieux nommée par l'équipe de la sécurité informatique de la Ville de Montréal.	Deux membres de l'équipe de la Sécurité de l'information et un autre collègue.
Mars 2019	Qualité du français	Le texte du présent rapport est de moi, mais ne serait pas aussi précis et formel sans l'assistance de mes trois réviseurs, pour leur apport indéniable.	Trois réviseurs.