Livre blanc

# CIAM : Cultiver des relations de confiance en ligne

Gestion des identités et de l'accès de la clientèle aux services publics



PORTAGE cybertech

portagecybertech.com
info@portagecybertech.com

# CIAM : Cultiver des relations de confiance en ligne

Gestion des identités et de l'accès de la clientèle aux services publics

## Qu'est-ce que la gestion des identités et de l'accès de la clientèle (CIAM)?

La gestion des identités et de l'accès de la clientèle ou « Customer Identity Access Management (CIAM) » en anglais, correspond aux outils et procédures conçus pour assurer des interactions privées, sécurisées et fluides entre les clients et les fournisseurs de services numériques. Les solutions de CIAM offrent des fonctions classiques de gestion des identités et des accès (IAM), dont la gestion des identités, l'authentification des utilisateurs et les permissions d'accès, qui protègent la vie privée des utilisateurs qui se situent à l'extérieur du contrôle direct d'un fournisseur de services et des limites des TI.

## Client? Citoyen?

Les solutions de CIAM ne protègent pas uniquement les acheteurs en ligne. Le terme « client » peut aussi faire référence aux clients de services professionnels, comme des clients de cabinets d'avocats. Il pourrait aussi désigner des citoyens qui interagissent avec des services publics en ligne, comme des services fournis par un organe municipal, provincial ou national.



## Quelle est la différence entre la gestion des identités et de l'accès de la clientèle et la gestion des identités et de l'accès classique?

Les solutions de CIAM et d'IAM aident toutes les deux les organisations à offrir les bons accès aux bonnes ressources aux bonnes personnes, et ce, au bon moment. Les solutions de gestion des identités et de l'accès (IAM) classiques ciblent les utilisateurs qui sont connus de l'organisation et travaillent dans l'environnement TI de celle-ci, c'est-à-dire les membres du personnel. Les solutions de gestion des identités et de l'accès de la clientèle (CIAM) ciblent les utilisateurs potentiels inconnus de l'organisation, du moins au début, qui pourraient se compter par millions. Ces utilisateurs utilisent des identités numériques externes (p. ex. des identifiants sur les médias sociaux) et changent souvent d'appareil et d'emplacement. Ils n'ont pas beaucoup de patience pour les pépins techniques et l'utilisation non autorisée de leurs renseignements personnels.

Pour ces raisons, les solutions de CIAM sont plus poussées que les solutions d'IAM : elles comprennent des dispositifs de protection de la vie privée, de gestion des consentements et de prévention de la fraude plus robustes, ainsi que des politiques dynamiques adaptées aux situations variées de milliers d'utilisateurs. La CIAM favorise les solutions en libre-service, la gestion de profils, le soutien omnicanal et des expériences numériques simplifiées et personnalisées.

### Pourquoi cette différence est-elle importante?

Les clients veulent un accès rapide, facile et fluide aux services numériques. Ils veulent profiter d'une expérience personnalisée, sans pour autant sacrifier leur vie privée ou le contrôle sur leurs renseignements personnels. En parallèle, les fournisseurs de services doivent sécuriser leurs réseaux et protéger les données de leur clientèle tout en respectant les normes de protection des consommateurs comme la *Loi sur la protection des renseignements personnels au Canada* et les lois provinciales de même nature, le *Règlement général sur la protection des données* (RGPD) de l'Union européenne et la *California Consumer Privacy Act* (CCPA).

L'IAM classique n'a pas une visée aussi large. Une bonne solution de CIAM est conçue pour cultiver des relations de confiance avec la clientèle en ligne fondées sur l'identité prouvée, la transparence quant à la collecte et à l'utilisation des données et un équilibre adéquat entre la sécurité et une expérience haut de gamme qui répond aux besoins et aux préférences des utilisateurs.

# Fonctions clés de la CIAM : Enjeux techniques

Pour offrir des services numériques de haut niveau qui surpassent les attentes de la clientèle, il est important d'établir l'identité des personnes avec lesquelles nous interagissons en ligne et de transformer ces interactions en relations de confiance. Les solutions de CIAM permettent d'atteindre cet objectif en offrant des fonctions clés qui favorisent l'engagement de la clientèle en ligne. Les sections ci-dessous définissent ces fonctions clés des solutions de CIAM et présentent comment elles se retrouvent dans CitizenOne[MC].

## Fonctions de base : Gestion des identités

| **Inscription et attribution des comptes** | **Fonctions de CitizenOne[MC]** |
|---|---|
| L'inscription aux services numériques de l'organisation doit être facile et rapide, sans quoi les clients pourraient abandonner le projet. En recueillant seulement un minimum de renseignements personnels nécessaires, vous accélérerez le processus d'inscription et limiterez les frustrations des utilisateurs. | • Création de compte au moyen d'une procédure simple qui recueille uniquement les renseignements essentiels (p. ex. nom d'utilisateur, adresse courriel et mot de passe).<br>• Vérification rapide des comptes par un simple courriel.<br>• Recherche et utilisation de tous les services publics depuis un seul point d'accès convivial dès la première ouverture de session. |
| **Confirmation de l'identité** | **Fonctions de CitizenOne[MC]** |
| Il s'agit du processus par lequel une organisation emploie les renseignements personnels et les preuves d'identité des utilisateurs pour associer une identité numérique à une personne réelle. Cette étape est cruciale pour sécuriser les transactions de nature sensible ou financière (p. ex. services financiers, services juridiques, services médicaux, subventions et prestations gouvernementales). | • Intégration de fournisseurs d'identité et de services de vérification tiers.<br>• Utilisation des meilleures pratiques d'accès à vérification systématique et vérification des données des utilisateurs auprès de toute source fiable à l'extérieur de CitizenOne[MC].<br>• Configuration des règles permettant une vérification et une authentification améliorées de l'identité, pour inscrire les utilisateurs aux services exigeant une assurance de l'identité supérieure.<br>• Gestion des points terminaux d'API et configuration libre-service. |



| Divulgation progressive (profilage) | Fonctions de CitizenOne[MC] |
|---|---|
| La divulgation progressive est une technique de collecte graduelle des renseignements de la clientèle. Plutôt que de demander aux clients de remplir de longs formulaires décourageants dès leur inscription, les organisations qui font appel au profilage progressif amassent de l'information sur leurs clients à mesure que ceux-ci interagissent avec ses services numériques et que leur relation en ligne se construit. Les organisations recueillent seulement des renseignements détaillés lorsque les activités d'un utilisateur l'exigent, ce qui le met en confiance. | • Fonctionnement par fiche de service, qui sert de point d'accès à un service en ligne donné. On demande seulement aux clients de divulguer des renseignements personnels dans le contexte d'un service particulier et des tâches connexes qu'ils veulent accomplir. Grâce à cette approche, les clients contrôlent toujours la nature des renseignements personnels qu'ils partagent et le moment où ils le font. |

> Les clients doivent pouvoir modifier, ajouter ou supprimer des renseignements personnels sans soutien de la part d'une équipe technique.

| Gestion de profils en libre-service | Fonctions de CitizenOne[MC] |
|---|---|
| Les clients doivent pouvoir modifier, ajouter ou supprimer des renseignements personnels sans soutien de la part d'une équipe technique. Idéalement, ils devraient même avoir la liberté de supprimer leur compte et tous les renseignements qui y sont associés.<br><br>Cette fonction offre à la clientèle un contrôle sur ses propres données, tout en réduisant le soutien nécessaire et les risques relatifs aux données incorrectes. | • Les clients peuvent modifier leur nom, leur adresse courriel, le numéro de téléphone et leur adresse depuis leur profil.<br>• Ils peuvent changer leur mot de passe, voir leurs sessions actives et les appareils depuis lesquels ils sont connectés et consulter l'historique des activités du compte.<br>• Ils peuvent configurer leurs préférences en matière de notifications, voir la liste de toutes les notifications dans l'interface utilisateur et définir la langue souhaitée.<br>• Ils peuvent aussi supprimer leur compte; une période de grâce prédéfinie est configurée, s'ils changent d'avis.<br>• CitizenOne[MC] est entièrement accessible et compatible avec les appareils mobiles, conformément aux règles pour l'accessibilité des contenus Web (WCAG) les plus récentes. |

| Consolidation des répertoires d'identités | Fonctions de CitizenOne[MC] |
|---|---|
| La consolidation de plusieurs répertoires en une seule source de renseignements sur l'identité et le profil est nécessaire pour fournir une authentification et un accès fluides aux clients, ainsi qu'une expérience utilisateur uniforme dans tous les services numériques de l'organisation. L'organisation parvient ainsi à mieux gérer les identités des clients et leurs renseignements personnels dans ses différents champs d'activité. | • En plus de permettre l'intégration de fournisseurs d'identité tiers, CitizenOne[MC] joue souvent le rôle de fournisseur d'identité en offrant une source de confirmation pour les profils d'utilisateurs, pour une authentification et un accès fluides. Il assure ainsi une expérience utilisateur riche et personnalisée aux clients qui font appel à d'autres services numériques. |

## Apportez votre propre identité

Apportez votre propre identité ou Bring Your Own Identity (BYOI), en anglais, est une approche à l'authentification numérique selon laquelle l'accès aux services d'une organisation est accordé au moyen d'identifiants émis par un tiers de confiance. En bref, les clients accèdent aux services en réutilisant les identifiants qu'ils possèdent déjà, plutôt que d'en créer de nouveaux. Le tiers est généralement une plateforme de médias sociaux ou une entreprise spécialisée en technologie (p. ex., Facebook, Google, Apple). Toutefois, des identités plus fortes, qui assurent de manière encore plus fiable que l'utilisateur est bien qui il prétend être, voient le jour, émises notamment par des organes gouvernementaux et des entreprises de vérification de l'identité. L'approche BYOI améliore l'expérience client en simplifiant les processus d'inscription et en réduisant le nombre d'identités à gérer. Elle évite aux petites organisations d'avoir à émettre et à gérer des identifiants distincts, ce qui peut représenter un défi. L'approche BYOI peut améliorer la sécurité et la confidentialité, en réduisant le nombre de renseignements personnels qu'un fournisseur de services doit récolter.

## Fonctions de CitizenOne[MC]

- L'interopérabilité est au cœur de CitizenOne[MC]. Notre solution emploie des normes ouvertes et une approche à l'intégration axée sur les API avant tout. Elle est compatible avec plus de 300 fournisseurs d'identité tiers et fournisseurs de services, et exploite des bibliothèques ouvertes matures pour augmenter les options d'identités numériques offertes à la clientèle.
- La solution permet l'intégration d'applications et de fournisseurs d'identité tiers par la configuration libre-service dans l'application de l'administrateur.

> L'approche BYOI peut améliorer la sécurité et la confidentialité, en réduisant le nombre de renseignements personnels qu'un fournisseur de services doit récolter.



# Fonctions de base : Authentification et autorisation

| **Authentification multifacteur** | **Fonctions de CitizenOne[MC]** |
|---|---|
| Il s'agit d'une méthode de confirmation de l'identité d'un utilisateur qui tente d'accéder à des ressources protégées en utilisant au moins deux facteurs d'identification, comme le nom d'utilisateur, le mot de passe, un code d'accès, une question de sécurité et des données biométriques. L'authentification multifacteur contribue à assurer que les utilisateurs sont bel et bien qui ils prétendent être, tout en empêchant des individus malveillants d'accéder à un compte au moyen d'un seul facteur d'identification (p. ex. le mot de passe d'un utilisateur, alors qu'ils n'ont pas le code envoyé à son numéro de téléphone enregistré). | • Dans CitizenOne[MC], l'authentification multifacteur peut être exigée à l'ouverture de session et, lorsque l'assurance de l'identité est primordiale, dans les contextes d'intégration à des fiches de services individuelles.<br>• Options d'authentification multifacteur à l'ouverture de session :<br>  • texto, courriel, application d'authentification, empreinte vocale (élément projeté).<br>• Les options d'authentification multifacteur lors de l'intégration des services comprennent suffisamment de facteurs pour équilibrer l'expérience de l'utilisateur et les exigences en matière de sécurité, y compris, mais non exclusivement, les éléments suivants :<br>  • codes d'accès envoyés par les canaux mentionnés ci-dessus ou par la poste;<br>  • identifiants ou données provenant de documents d'identification (p. ex. permis de conduite);<br>  • données biométriques (élément projeté). |

| **Authentification adaptative** | **Fonctions de CitizenOne[MC]** |
|---|---|
| Il s'agit d'une méthode d'authentification multifacteur qui varie en fonction de la situation. Si le système détecte un élément inattendu ou étrange, comme un emplacement, un type d'appareil, une heure d'accès ou un type de transaction différent, il invite l'utilisateur à fournir d'autres facteurs d'authentification.<br><br>Ce procédé met des bâtons dans les roues aux individus malveillants qui tenteraient d'accéder à un compte au moyen de facteurs compromis, et améliore ainsi la détection de la fraude. Il simplifie aussi l'expérience des utilisateurs qui s'adonnent à des activités à faible risque, en réservant les facteurs supplémentaires aux services de nature sensible. | • Le système fait le suivi des points de données d'authentification adaptative (p. ex. le système d'exploitation, le navigateur/l'agent et l'adresse IP de l'appareil de l'utilisateur), et consigne l'heure et la nature des incidents. Les utilisateurs sont avisés en cas d'ouverture de session inhabituelle et reçoivent des renseignements sur ces points de données.<br>• L'authentification fondée sur le risque correspond à la mise en place d'une logique pour évaluer les situations auxquelles les utilisateurs font face et leur attribuer un profil de risque. Ce profil déclenche un processus ou une expérience d'authentification adaptative (élément projeté). |

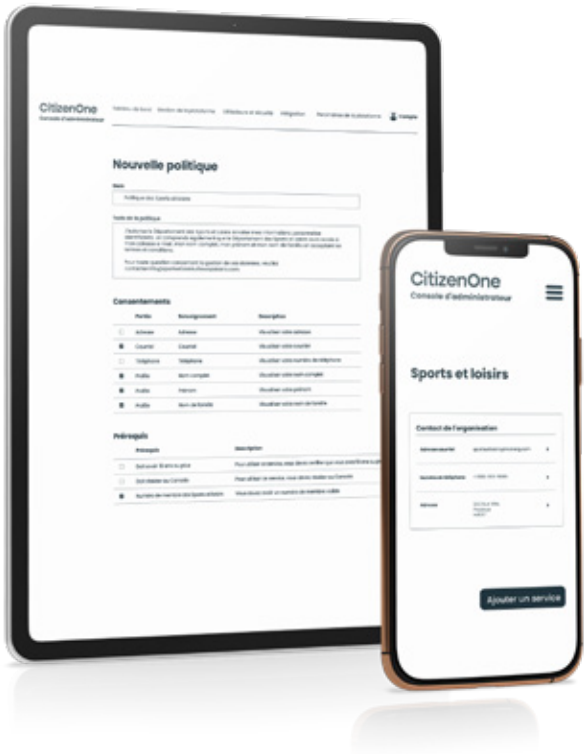
| Contrôle de l'autorisation (des accès) | Fonctions de CitizenOne[MC] |
|---|---|
| Une méthode permettant de déterminer les ressources auxquelles un utilisateur peut accéder et les gestes qu'il peut poser (c.-à-d. lire, modifier, supprimer). Pour les services numériques, l'autorisation est liée à l'authentification, afin de confirmer l'identité de l'utilisateur et de lui accorder l'accès approprié. Les contrôles de l'autorisation garantissent la confidentialité des renseignements personnels. Ils permettent également de limiter les dommages causés par des individus malveillants, en les empêchant d'accéder à plusieurs ressources protégées ou de se déplacer librement d'une cible à l'autre sur le réseau.<br><br>L'une des principales fonctions des solutions de CIAM est de permettre aux clients de gérer des délégués. Les délégués sont autorisés par les utilisateurs à accéder aux ressources et à poser des gestes en leur nom. | • Pour les services destinés à la clientèle, CitizenOne[MC] utilise un modèle de contrôle des accès basé sur les revendications et les identifiants.<br>• Les politiques d'accès sont établies au moyen du moteur de règles de la solution. La configuration des points terminaux d'API permet l'intégration des sources de données externes nécessaires pour vérifier les revendications faites par les utilisateurs.<br>• Ce procédé de gestion des accès produit un ensemble de revendications et d'identifiants vérifiés qui servent à prouver l'identité des utilisateurs durant l'authentification initiale et continue pour accéder aux ressources et services protégés.<br>• Lorsque les utilisateurs prouvent leur identité en respectant une règle d'accès, la suite de leur parcours est déterminée par les « actions » configurées dans l'interface utilisateur; le fournisseur de services les dirige vers les zones d'une ressource protégée qu'il veut qu'ils visitent. Ainsi, l'expérience utilisateur est conçue avec soin.<br>• La délégation de pouvoir permet également aux utilisateurs d'ajouter des collaborateurs et de leur accorder l'autorisation d'accéder aux ressources et d'effectuer des actions en leur nom.<br>• Remarque : Aux fins de l'administration des systèmes, les autorisations pour effectuer des tâches sont régies par un modèle classique de contrôle d'accès basé sur les rôles. |
| **Identification unique** | **Fonctions de CitizenOne[MC]** |
| Il s'agit d'une méthode permettant aux utilisateurs d'accéder à plusieurs applications sans avoir à s'authentifier de nouveau chaque fois. Autrement dit, un nom d'utilisateur et un mot de passe permettent d'accéder à plusieurs applications.<br>Les clients interagissent souvent avec plusieurs systèmes d'arrière-plan ou veulent consolider l'information accessible dans divers systèmes (au moyen d'un tableau de bord ou d'un portail). L'identification unique limite les frustrations et les problèmes de sécurité causés par la gestion de plusieurs identifiants d'ouverture de session.<br><br>Ce procédé permet aussi aux grandes organisations rassemblant plusieurs marques ou unités de services d'offrir des services plus fluides à un même client. | • CitizenOne[MC] prend en charge des protocoles fondés sur des normes ouvertes pour l'authentification et l'autorisation d'accès aux ressources protégées, soit LDAP, OAuth2.0/OIDC et SAML 2.0.<br>• Cette compatibilité permet d'intégrer des fournisseurs d'identité tiers, en jouant le rôle de partie utilisatrice envers ces fournisseurs mais aussi de fournisseur d'identité tiers pour des applications en aval. En supposant que les fournisseurs tiers prennent en charge les mêmes normes que CitizenOne[MC], l'intégration de l'identification unique ne pose pas une grande difficulté technique.<br>• Le modèle schématisé réduit le recours aux fournisseurs et aux ressources techniques, ce qui accélère l'intégration et la prestation des services.<br>• L'expérience d'identification unique en est ainsi optimisée, la satisfaction et la consommation de services numériques sont accrues, et le risque de faille de cybersécurité est réduit. |

# Fonctions de base : Gestion

### Gestion des consentements

Il s'agit du processus consistant à obtenir, à enregistrer et à gérer le consentement des utilisateurs pour la collecte, l'utilisation et la divulgation de leurs renseignements personnels. De plus en plus, les utilisateurs s'attendent à pouvoir refuser la collecte ou la divulgation de données, ou à pouvoir retirer leur consentement préalable.

La gestion des consentements est obligatoire dans de nombreux territoires. Qu'elle soit requise ou non, la gestion des consentements est intégrale à la création de relations de confiance en ligne : elle montre l'engagement du fournisseur de services envers la transparence et le respect de la vie privée de la clientèle.




### Fonctions de CitizenOne[MC]

- Conformément aux principes de protection de la vie privée dès la conception, CitizenOne[MC] offre un mécanisme de consentement mené par l'utilisateur. L'utilisateur garde le contrôle sur les données qui sont communiquées avec le gouvernement et les fournisseurs de services, ainsi que sur le motif et le moment de ce partage.
- La minimisation des données est au cœur du modèle de données de CitizenOne[MC]. Le système ne stocke que les données relatives au profil de l'utilisateur, généralement pas plus que celles nécessaires à la création d'un compte (c.-à-d. le prénom, le nom, l'adresse courriel et le mot de passe).
- Le processus d'intégration commence par le consentement au partage des données. Les conditions générales du service sont présentées à l'utilisateur en toute transparence. Y figurent le motif de la collecte des données, des références aux lois applicables en matière de protection de la vie privée, ainsi qu'un point de contact, comme une adresse courriel, pour permettre à l'utilisateur de communiquer avec le fournisseur de services s'il a des questions sur le traitement des données.
- Au cours du processus d'intégration d'un service en particulier, l'utilisateur consent au partage des attributs des données de base de son profil et de toute donnée supplémentaire configurée dans le cadre de la politique du service.
- L'utilisateur peut refuser la collecte de données à tout moment, en retirant son consentement. CitizenOne[MC] peut demander aux applications et aux fournisseurs de services en aval de retirer des données de leurs systèmes. Notez que ces demandes doivent respecter les politiques de conservation des données et les réglementations relatives à la suppression des données.
- CitizenOne[MC] assure le suivi de tous les consentements et changements liés à ceux-ci, et peut générer des rapports pour les professionnels de la protection de la vie privée (par exemple, en cas d'audit).
- La combinaison de ces fonctionnalités garantit la conformité aux lois sur la protection des données en vigueur et aux obligations des fournisseurs de services à l'égard de leurs clients et des citoyens.

À propos de la protection des données :

Toutes les données stockées dans CitizenOne[MC] sont dépersonnalisées, donc il n'est pas possible de suivre l'activité d'un utilisateur ni de deviner l'identité d'une personne d'après ses identifiants.

- Toutes les données sont chiffrées lorsqu'elles sont en transit et inactives, en dans le respect des meilleures pratiques de chiffrement de l'industrie.

| Analyse dans les solutions de CIAM | Fonctions de CitizenOne[MC] |
|---|---|
| Il s'agit de la capacité à mener des évaluations et à produire des rapports pour comprendre les comportements de la clientèle et lui fournir un environnement sécurisé. La solution de CIAM choisie devrait être compatible avec les programmes de sécurité et de conformité de l'entreprise, et offrir des renseignements sur les procédés liés à l'identité, comme l'authentification, l'authentification multifacteur/les mesures adaptatives, l'accès aux systèmes, les modifications aux renseignements personnels et les changements à la configuration du système. | • Le système comprend des fonctions d'analyse intégrées qui permettent au fournisseur de services de produire des rapports sur les statistiques des utilisateurs, notamment sur l'utilisation d'un service en particulier, qui est évaluée en fonction d'indicateurs prédéterminés.<br>• Il tire parti de l'intégration d'outils d'alerte et de suivi comme NewRelic, Zabbix et Sentry pour offrir des fonctions avancées d'enregistrement, de suivi et d'alerte. Par son système d'API, il peut représenter visuellement les données et les résultats d'analyse de ces outils dans l'application de l'administrateur de CitizenOne[MC].<br>• Il est compatible avec des outils de gestion des informations et des événements de sécurité et de renseignement sur les cybermenaces de haut calibre qu'utilisent les fournisseurs de services. |

## Fonctions stratégiques

| Soutien omnicanal | Fonctions de CitizenOne[MC] |
|---|---|
| Le soutien omnicanal correspond à la capacité de la solution de CIAM à offrir une expérience constante et familière aux clients, qu'ils utilisent un site Web, un centre d'appels ou un comptoir de services. Une bonne solution de CIAM consolide les renseignements sur l'identité, les préférences et d'autres données de base utiles dans toutes les interactions avec la clientèle. Elle rend ensuite ces données accessibles dans l'ensemble des canaux de service de l'organisation, tout en conservant le consentement et en assurant la confidentialité et la sécurité. | • CitizenOne[MC] tire parti d'un modèle de courtage et d'un système d'API puissants. À titre de source principale de confirmation des données du profil des utilisateurs, CitizenOne[MC] peut jouer un rôle primordial dans la gouvernance et le courtage des données et des renseignements de confiance sur l'identité à travers l'infrastructure de service de l'organisation. Voici certains de ses avantages :<br>  • permettre les interactions de service dans des contextes numériques, en personne et hybrides;<br>  • favoriser des ententes de partage des données interservices;<br>  • adopter un modèle de gestion des identités numériques plus décentralisé. |



| Architecture moderne fondée sur les API | Fonctions de CitizenOne[MC] |
|---|---|
| C'est bien connu : les API sont les éléments fondamentaux des logiciels modernes. Les clients, les partenaires et les unités fonctionnelles s'attendent à ce que les données et les services soient accessibles sur l'ensemble des plateformes, appareils et réseaux; ces attentes sont à la base d'une solution de CIAM. Les architectures modernes axées sur les API offrent les capacités évolutives, le rendement et les coûts-avantages nécessaires pour intégrer une solution de CIAM à l'environnement informatique d'une organisation. | • Doté d'une architecture modulaire, le système privilégie une approche à l'intégration fondée sur les API et les normes. Cette pratique permet au fournisseur de participer à un écosystème de services et d'accéder à un maximum de possibilités d'intégration d'applications tierces, pour accroître la valeur offerte aux utilisateurs au moyen de services interconnectés.<br>• Il permet une configuration en libre-service pour la gestion des points terminaux, la configuration des règles et l'intégration des fournisseurs de services, ce qui réduit la dépendance à l'égard des fournisseurs. |

| Modèle de déploiement flexible | Fonctions de CitizenOne[MC] |
|---|---|
| Un déploiement flexible permet à la solution de CIAM d'être mise en œuvre de manière à répondre aux besoins et aux préférences des fournisseurs de services, tout en respectant les règlements et politiques en vigueur.<br>Pour plus de souplesse, la solution de CIAM devrait permettre un déploiement dans des environnements locaux et infonuagiques, notamment les environnements à nuages multiples et à nuage hybride. | • Options de déploiement<br>• Fonctionnement local<br>• Nuage public ou privé<br>• Compatibilité avec plusieurs fournisseurs de services infonuagiques<br>  • Les déploiements actuels emploient Azure comme fournisseur.<br>  • Digital Ocean est aussi utilisé<br>• Mono-locataire (dans la majorité des déploiements)<br>• Multilocataire prêt-à-l'emploi<br>  • Plusieurs fournisseurs de services (p. ex. associés à un gouvernement municipal) peuvent être locataires de la même instance, chacun avec son URL et son image de marque distinctes, ce qui permet de réaliser des économies et de profiter d'autres avantages d'une infrastructure partagée. |



### Utilisation de normes ouvertes

Les normes ouvertes définissent des exigences, spécifications ou recommandations techniques que n'importe qui peut consulter et utiliser. Dans le contexte des solutions de CIAM, ces normes permettent la cohérence et l'uniformité nécessaires pour assurer l'interopérabilité, la compatibilité et la sécurité entre les systèmes et composantes, et à l'intérieur de ceux-ci. Elles aident à établir la confiance requise pour mettre en œuvre les approches BYOI et d'identification unique, tout en évitant le verrouillage des fournisseurs et des technologies.

### Fonctions de CitizenOne[MC]

- CitizenOne[MC] prend en charge des protocoles fondés sur des normes ouvertes pour l'authentification et l'autorisation d'accès aux ressources protégées, soit LDAP, OAuth2.0/OIDC et SAML 2.0.
- Ces normes favorisent aussi la mise en place de meilleures pratiques d'accès à vérification systématique, rehaussant le niveau de sécurité de manière à respecter les architectures et normes de cybersécurité modernes les plus rigoureuses.

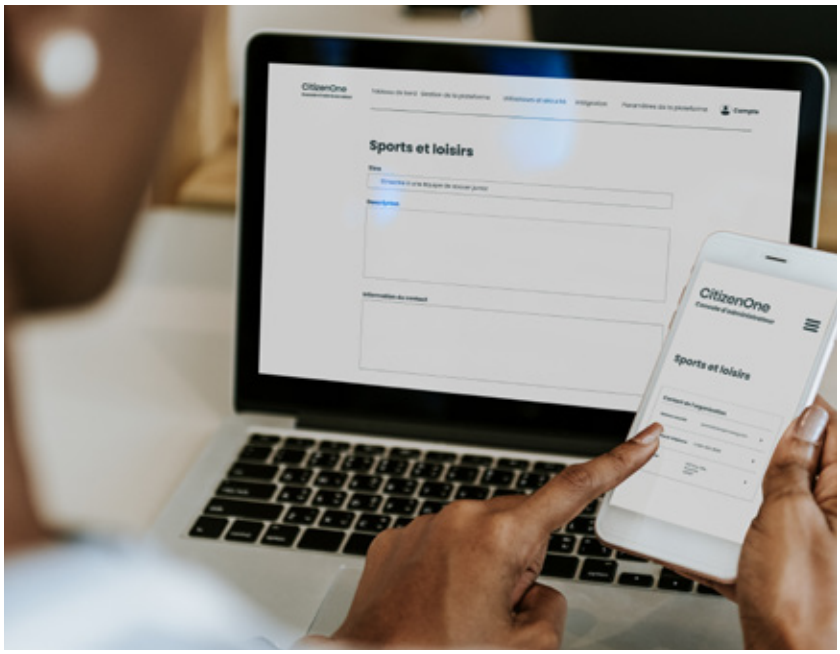
### Contrôle de la résidence des données

La résidence des données est le territoire où les données des clients sont stockées. Pour être conforme aux exigences légales et garantir l'autorité sur les renseignements personnels, la solution de CIAM doit faire en sorte que les renseignements personnels d'un citoyen sont uniquement collectés, traités et stockés dans son territoire d'origine (généralement au niveau national).

### Fonctions de CitizenOne[MC]

- Bien que nous soyons agnostiques en matière de fournisseur de services infonuagiques, CitizenOne[MC] a utilisé Microsoft Azure pour nos plus grands déploiements à ce jour, en veillant à ce que les données demeurent résidentes au Canada dans les centres de données de Toronto et de Québec. Nous pouvons travailler avec n'importe quel fournisseur d'hébergement, y compris le client lui-même, pour satisfaire aux exigences de résidence des données et aux besoins d'infrastructure.

> Une bonne solution de CIAM consolide les renseignements sur l'identité, les préférences et d'autres données de base utiles dans toutes les interactions avec la clientèle.



# Fonctions tournées vers l'avenir

### Données de confiance (identifiants vérifiables)

Pour servir les clients et tisser des relations à long terme avec eux, la clé est d'utiliser leurs renseignements personnels pour vérifier leur identité, leur fournir les services dont ils ont besoin et personnaliser leur offre afin de répondre à leurs besoins uniques. La vérification de toutes ces données est souvent un processus coûteux et long, qui repose sur des procédures manuelles et hors ligne. Les solutions de CIAM se veulent la solution à ce problème, et adoptent de nouveaux moyens d'obtenir les données de confiance nécessaires, tout en minimisant les risques d'entrave à la sécurité et à la vie privée. Dans bien des cas, ces nouvelles méthodes s'appuient sur la technologie d'identifiants vérifiables.

Les identifiants vérifiables utilisent des technologies cryptographiques avancées pour s'assurer que l'authenticité de l'identifiant numérique d'un utilisateur peut être retracée jusqu'à son émetteur et que les données contenues dans l'identifiant n'ont pas été manipulées. Cette technologie permet une vérification numérique des données des clients, pour éviter de compter uniquement sur des revendications et des données qui pourraient s'avérer erronées.

### Fonctions de CitizenOne[MC]

- Le moteur d'identifiants *Credential Engine* de CitizenOne[MC] est une fonction native permettant d'émettre et de vérifier des identifiants vérifiables.
- Émission d'identifiants vérifiables de sources de confiance aux utilisateurs :
  - de la part de toute agence gouvernementale ou organisation privée;
  - à n'importe qui;
  - pour tout cas d'utilisation ou attribut, en limitant les données au strict minimum.
- Hautement interopérable, le moteur d'identifiants prend en charge tous les types d'identifiants vérifiables et de spécifications utilisés dans les portefeuilles numériques grand public.

> Le moteur d'identifiants *Credential Engine* de CitizenOne[MC] est une fonction native permettant d'émettre et de vérifier des identifiants vérifiables.

### Identités de clients décentralisées

Les données de clients s'accumulent souvent dans des bases de données fragmentées; le risque de fuite de données et de non-respect des règlements relatifs à la protection de la vie privée est donc bien réel. L'utilisation de technologies comme les identifiants vérifiables atténue ces problèmes, grâce au stockage de renseignements personnels dans des portefeuilles numériques contrôlés par les clients. Les identités et les renseignements personnels sont alors décentralisés, c'est-à-dire qu'ils ne sont pas entreposés dans un seul système ni placés sous un contrôle unique. Le fournisseur de services ne recueille qu'un minimum de données personnelles : il demande seulement aux clients de lui fournir des données de confiance lorsque nécessaire, plutôt que de créer des bases de données internes volumineuses.

### Fonctions de CitizenOne[MC]

- Les fournisseurs de services peuvent utiliser la gestion de points terminaux d'API en libre-service de CitizenOne[MC] pour mettre en place des processus d'émission d'identifiants vérifiables dans le portefeuille numérique des utilisateurs.
- Les politiques de gestion des accès peuvent être définies plus en profondeur au niveau du service ou de la ressource pour vérifier des attributs de l'utilisateur qui emploie l'identifiant stocké dans son portefeuille, avant qu'il obtienne l'accès au service.
- Avec le temps, ces pratiques contribuent à la création d'un modèle de plus en plus décentralisé pour le stockage de données de confiance sur les appareils appartenant à l'utilisateur.

# CitizenOne[MC]: Associer la CIAM et la prestation de services

CitizenOne[MC] offre des fonctions de CIAM robustes qui permettent aux fournisseurs de services de recueillir et de gérer l'identité et les données du profil des utilisateurs en toute sécurité, tout en contrôlant l'accès des utilisateurs aux applications et services. Ces fonctions accélèrent et diversifient l'accès aux services numériques par les moyens suivants :

- Établir des procédures d'inscription des utilisateurs, de confirmation de l'identité, d'authentification et d'autorisation uniformes pour l'ensemble des services et des partenaires d'affaires.
- Fournir un mécanisme de confirmation de l'identité numérique pour veiller à ce que les utilisateurs qui tentent d'ouvrir une session soient bien qui ils prétendent être.
- Offrir aux utilisateurs un compte unique qu'ils peuvent gérer de façon autonome, et qui agit comme source unique de données des utilisateurs.
- Séparer les données relatives à l'identité de celles relatives aux services pour faire en sorte que le compte d'utilisateur unique contienne uniquement des données partagées ou communes.
- Améliorer les contrôles de gestion des consentements et de protection de la vie privée qui permettent aux utilisateurs d'accepter l'utilisation d'un service numérique, et aux fournisseurs de services de définir des politiques de consentement à accepter pour accéder à un service en particulier.
- Remplacer des solutions d'IAM fragmentées, coûteuses et risquées par une solution moderne et fondée sur les normes, applicable dans l'ensemble des secteurs d'activité.

Grâce à ses fonctions de CIAM, CitizenOne[MC] relève un défi majeur auquel les fournisseurs de services numériques sont confrontés : fournir un accès numérique de confiance aux services de manière sécurisée, collaborative et axée sur les utilisateurs.

Les fonctions de CIAM seules, quel que soit le fournisseur, ne sont pas suffisantes pour régler un autre problème majeur touchant les fournisseurs de services numériques, c'est-à-dire le fait qu'il est difficile de mettre les clients ou



citoyens en contact avec les services dont ils ont besoin, surtout ceux dont ils ne connaissent pas l'existence, dans un environnement Web surchargé.

Pour relever ce deuxième défi, CitizenOne[MC] associe des fonctions de CIAM à une expérience axée sur l'utilisateur permettant de trouver des services numériques, d'y accéder et de gérer les relations en ligne.

CitizenOne[MC] regroupe tous vos services dans un seul tableau de bord convivial et offre des fonctionnalités puissantes qui simplifient votre travail et assurent votre conformité aux politiques et règlements en vigueur. Les utilisateurs peuvent accéder et s'inscrire aux services avec un seul identifiant sécurisé, pendant que les fournisseurs de services centralisent la gestion des identités, consentements et accès aux services.

En ce sens, CitizenOne[MC] agit comme contrôleur d'accès de confiance pour toutes les applications destinées aux citoyens au sein de votre écosystème. Lorsque les utilisateurs interagissent avec un service donné, CitizenOne[MC] les soumet aux procédés de confirmation de l'identité, d'authentification et de vérification des accès nécessaires, tout en protégeant leurs renseignements personnels et en obtenant leur consentement au besoin. À titre de contrôleur d'accès de confiance, CitizenOne[MC] offre des fonctions clés qui assurent une expérience utilisateur supérieure et fiable :

- Un seul compte d'utilisateur pour accéder à l'ensemble des services en ligne.
- L'identification unique et la gestion des sessions de l'utilisateur.
- La gestion des identifiants des utilisateurs.
- Une source unique de profils gérés par les utilisateurs qui contiennent des renseignements personnels pouvant être transmis à des applications Web.
- Des rappels de données qui favorisent la personnalisation des services.

# La prochaine étape?

Découvrez les solutions de Portage CyberTech.

Prenez rendez-vous pour discuter de ce que pourrait être une mise en œuvre stratégique du CIAM pour votre organisation.

Tous les droits réservés | Portage CyberTech 2024