Livre blanc

Identité numérique moderne, Risque minimal

Comment les gouvernements peuvent accélérer leurs résultats grâce à une solution CIAM infonuagique



PORTAGE cybertech

portagecybertech.com
info@portagecybertech.com

Identité numérique moderne, Risque minimale

Comment les gouvernements peuvent accélérer leurs résultats grâce à une solution CIAM infonuagique

Les gouvernements et les organismes publics font face à une pression croissante pour fournir des services numériques aussi rapides et sophistiqués que ceux du secteur privé. Les efforts de modernisation se heurtent à des systèmes de gestion des identités et des accès (IAM) obsolètes, à de lourdes procédures d'approvisionnement et à des ressources limitées, ce qui crée un ensemble de défis complexes pour les décideurs publics.



Sans une base solide en matière de sécurité et de protection de la vie privée, les initiatives numériques risquent de révéler des vulnérabilités susceptibles de compromettre à la fois l'intégrité opérationnelle et la confiance du public. La modernisation se transforme alors en un véritable parcours d'obstacles, souvent orchestré en coulisses dans une succession interminable de concertations avec les parties prenantes, d'audits internes et de séances de planification stratégique, pour aboutir à de longs déploiements exposés à des risques élevés et accueillis avec une adoption souvent limitée une fois les services en ligne.

C'est à ce stade qu'intervient la gestion des identités et des accès client (le « CIAM ») infonuagique : une solution agile et sécurisée qui permet aux gouvernements de gérer efficacement les identités citoyennes à grande échelle. En optant pour une approche basée sur le nuage, les administrations peuvent raccourcir les délais de mise en œuvre, tout en réduisant les risques liés à l'infrastructure. Cette solution facilite également la conformité avec des réglementations en matière de protection de la vie privée, en constante évolution.

Dans ce livre blanc, nous présentons une feuille de route concrète à l'intention des organismes publics qui souhaitent adopter un CIAM infonuagique. Nous y explorons les avantages stratégiques du déploiement en nuage, les garanties de sécurité intégrées aux plateformes modernes conçues pour le secteur public, ainsi que des moyens éprouvés pour accélérer la mise en œuvre et obtenir des résultats tangibles. En adoptant une solution CIAM infonuagique, les gouvernements peuvent rationaliser la gestion des identités citoyennes tout en réduisant les risques, renforçant ainsi la sécurité, la conformité et la confiance du public envers les services numériques.

1

Introduction :
Le défi de l'identité numérique dans l'administration

Partout en Amérique du Nord et dans le monde, les citoyens attendent des services gouvernementaux qu'ils soient aussi accessibles, rapides et intuitifs que ceux offerts par leurs applications préférées ou les grandes plateformes de commerce en ligne. Qu'il s'agisse de renouveler un permis de conduire, de consulter un dossier médical ou de demander une prestation, les citoyens veulent des expériences numériques simples, sécurisées et qui fonctionnent. Si seulement produire une déclaration de revenus était aussi facile que commander une paire de chaussures.

Pourtant, pour de nombreuses administrations publiques, les systèmes de gestion des identités et des accès (IAM) freinent considérablement la modernisation. Ces outils dépassés sont encombrants, coûteux et mal adaptés à la complexité croissante des services numériques. Pire encore, ils exposent les organismes à des cybermenaces, à des brèches de données et à des violations de conformité.

> **Résultat : Les services restent cloisonnés, chaque ministère fonctionnant avec ses propres normes et processus. L'expérience utilisateur s'en trouve fragmentée et souvent frustrante.**

L'inaction n'est plus une option. Elle se traduit par :

- des citoyens confrontés à des méthodes de connexion obsolètes ou incohérentes;
- une baisse de l'utilisation des services et une perte de confiance envers l'administration;
- une exposition accrue aux violations de données et à l'usurpation d'identité;
- un risque de non-conformité avec des lois telles que RGPD, la Loi 25 ou le CCPA.

Pour répondre à des attentes citoyennes croissantes et à un cadre réglementaire changeant, les gouvernements doivent adopter une solution d'identité numérique à la fois sécurisée, évolutive et résolument centrée sur le citoyen.



#2 Pourquoi le CIAM en nuage est un impératif stratégique

Commençons par définir en quoi consiste le CIAM

La gestion des identités et des accès client (CIAM) désigne l'ensemble des outils, processus et pratiques qui permettent de gérer la manière dont les utilisateurs s'authentifient et interagissent avec les services en ligne. Elle couvre des fonctions clés telles que la création et la gestion des identités numériques, la vérification des utilisateurs avant l'octroi d'un accès, et la description des ressources que chaque utilisateur peut consulter.

> **Pensez au CIAM comme à un concierge numérique : il sait qui vous êtes, vous guide vers le bon service et garde les intrus à distance, sans jamais vous demander vos clés.**

Contrairement à la gestion traditionnelle des identités et des accès (IAM), conçue principalement pour les utilisateurs internes, comme les employés, le CIAM est pensé pour gérer des millions d'utilisateurs externes, souvent inconnus de l'organisation au départ. Ces utilisateurs accèdent aux services à partir d'une multitude d'appareils, de réseaux et de lieux, et s'authentifient fréquemment par l'intermédiaire de fournisseurs tiers, ce qui complexifie d'avantage la gestion des identités.

Lorsqu'il est correctement mis en œuvre dans le secteur public, le CIAM dépasse largement les capacités de la gestion traditionnelle des identités. Il intègre des mécanismes avancés de protection de la vie privée, de gestion des consentements, de lutte contre la fraude et d'application dynamique des politiques d'accès. Il favorise l'autonomie des utilisateurs grâce au libre-service, assure une prise en charge omnicanale et propose des expériences numériques personnalisées qui renforcent la confiance et encourage l'engagement citoyen.

Les avantages du déploiement d'un CIAM infonuagique

Pour les gouvernements, déplacer une solution CIAM infonuagique ouvre la voie à des avantages considérables. Il s'agit d'une stratégie à l'épreuve du temps qui s'inscrit pleinement dans les objectifs de transformation numérique, d'amélioration de l'expérience citoyenne, d'optimisation opérationnelle et de réduction des risques.

Voici pourquoi le CIAM infonuagique représente un investissement judicieux pour les organisations du secteur public :

- **Déploiement accéléré**
  Une plateforme CIAM soigneusement sélectionnée pour une mise en œuvre rapide. Grâce à des intégrations prêtes à l'emploi et à des composants configurables, elle se connecte facilement aux systèmes existants, ce qui permet de regrouper les services numériques en quelques jours seulement.
- **Réduction des risques liés à l'infrastructure**
  En transférant la gestion des identités vers le nuage, les organismes publics peuvent se libérer des contraintes liées à l'entretien de l'infrastructure sur site. Cela allège la charge des équipes informatiques internes et réduit les risques liés aux pannes, aux logiciels obsolètes et aux ressources limitées.
- **Conformité et sécurité intégrées**
  Les principales solutions CIAM conçues pour le secteur public intègrent des fonctionnalités de sécurité robustes telles que l'authentification multifactorielle (MFA), l'authentification adaptative, la vérification d'identité, la détection des fraudes et le chiffrement des données. Elles facilitent également la conformité aux réglementations sur la protection de la vie privée grâce à des outils de gestion des consentements et de journalisation des accès.
- **Évolutivité adaptée aux services citoyens**
  Les plateformes CIAM infonuagiques évoluent en temps réel. Qu'elles servent des milliers ou des millions d'utilisateurs, elles assurent une performance constante sans nécessiter de mises à jour matérielles coûteuses.

À mesure que les attentes des citoyens évoluent, les stratégies gouvernementales s'orientent de plus en plus vers des modèles centrés sur le citoyen, des infrastructures infonuagiques et des principes de protection de la vie privée dès la conception.

Le CIAM infonuagique, pensé pour le secteur public, répond directement à ces priorités. Il offre un accès sécurisé, évolutif et fluide aux services publics, tout en garantissant la conformité réglementaire, la cohérence des expériences numériques et la capacité de s'adapter rapidement aux besoins changeants des citoyens.



#3 Réduction des risques grâce à un CIAM moderne

À mesure que les organisations migrent vers l'infonuagique, l'identité numérique devient le nouveau périmètre de sécurité. Le modèle traditionnel, fondé sur des pare-feu et des frontières réseau fixes, apparaît désormais dépassé — comme défendre un château à l'ère des drones. Aujourd'hui, l'accès aux services repose sur l'identité vérifiée de l'utilisateur, et non sur sa localisation ou son adresse IP. Si cette identité est compromise, l'acteur malveillant n'a plus besoin de forcer les portes : il est déjà à l'intérieur, avec les clés du royaume.

> **Face à ces nouvelles menaces, le CIAM moderne s'impose comme une véritable ligne de défense. Il ne se limite plus à une simple interface de connexion, mais devient un pilier de la cybersécurité.**

Fonctionnalités de sécurité intégrées

Les solutions CIAM les plus avancées offrent, dès leur déploiement, des capacités de sécurité de niveau entreprise, notamment :

- L'authentification multifactorielle (MFA);
- Des contrôles d'accès adaptatifs;
- La détection des menaces en temps réel;
- Le chiffrement des données au repos et en transit.

Il ne s'agit pas d'ajouts optionnels, mais de fonctions de base. Elles opèrent discrètement en arrière-plan pour détecter les comportements suspects, bloquer les accès non autorisés et protéger les données sensibles, sans nuire à l'expérience de l'utilisateur. En d'autres termes, le portier numérique est devenu bien plus intelligent.

Identité unifiée, contrôle respectueux de la vie privée

En centralisant les accès au moyen d'une authentification unique et sécurisée, le CIAM contribue à réduire la prolifération des identifiants et l'informatique parallèle. Sans système unifié, chaque ministère a tendance à adopter ses propres plateformes, créant des services cloisonnés, des identifiants dupliqués et des politiques d'accès incohérentes.

Le CIAM consolide les données d'identité des citoyens sur l'ensemble des plateformes, ce qui simplifie la connexion, réduit la surface de cyberattaque et applique le principe « un client, un compte ». Résultat : un accès rationalisé, une visibilité accrue, une réduction des frais administratifs et un renforcement global de la posture de sécurité.

> Déployé dans une logique de protection de la vie privée dès la conception, le CIAM permet aux gouvernements de fournir un accès sécurisé à l'ensemble des services par l'intermédiaire d'un compte unique, tout en limitant la collecte de données personnelles au strict nécessaire.

Il ne s'agit pas de céder le contrôle, mais d'adopter une gouvernance transparente. Les organismes publics conservent la maîtrise des politiques d'accès et des autorisations, tout en offrant aux citoyens une expérience numérique fluide, sécurisée et respectueuse de leur vie privée.

Audit et conformité simplifiés

La conformité est un autre domaine où le CIAM apporte une réelle valeur. Certaines solutions intègrent des outils de gestion des consentements, de journalisation des accès, de tableaux de bord centralisés et d'architecture de protection de la vie privée dès la conception, ce qui permet aux administrations de répondre plus facilement aux exigences de réglementations telles que le RGPD, la Loi 25, le CCPA ou encore la LPRPDE. Plutôt que d'ajouter des couches de conformité après coup, les gouvernements peuvent s'appuyer sur une solution conçue dès le départ pour garantir transparence et responsabilité.



#4 Accélérer la création de valeur

L'évolution vers l'administration numérique est guidée par un objectif central : maximiser la valeur des investissements technologiques pour fournir des services publics qui suivent le rythme d'un monde en évolution rapide. Dans un contexte de ressources limitées, chaque jour compte. Le secteur public doit maximiser la valeur de ses investissements pour répondre rapidement aux attentes des citoyens.

L'un des atouts majeurs du CIAM infonuagique réside dans son efficacité. Il permet aux gouvernements de passer de la planification à la mise en production en une fraction du temps requis par les systèmes traditionnels de gestion des identités et des accès, tout en gagnant en agilité, en réduisant les coûts et en limitant les risques.

- **Intégrations prédéfinies**
  Les plateformes CIAM les plus performantes sont dotées d'API et de connecteurs compatibles avec les systèmes gouvernementaux largement utilisés, ce qui réduit considérablement les besoins en développement sur mesure et accélère le déploiement. Inutile de repartir de zéro : les gouvernements peuvent s'appuyer sur leur infrastructure existante tout en ajoutant de nouvelles capacités. De plus, les meilleures solutions CIAM s'intègrent même aux systèmes existants qui ne reposent pas sur des normes d'authentification modernes, garantissant ainsi que tous les services essentiels demeurent accessibles.
- **Autonomie citoyenne grâce au libre-service**
  Des fonctionnalités telles que l'inscription à des services spécifiques, la réinitialisation de mot de passe, la mise à jour de profil et les contrôles de consentement permettent aux citoyens de gérer leur identité numérique sans avoir recours à un service d'assistance ou à des processus manuels fastidieux, ce qui réduit la charge opérationnelle et rehausse l'expérience utilisateur.
- **Mise en œuvre accélérée**
  Les données du secteur montrent que le CIAM infonuagique peut être opérationnel jusqu'à 70% plus rapidement que les solutions sur site — 1 à 3 mois, contre 9 à 18 mois pour les systèmes traditionnels. Ce gain de temps permet d'accélérer la mise en service des solutions numériques et d'obtenir un retour sur investissement plus rapide.
- **Déploiement agile et progressif**
  Les gouvernements peuvent adopter une approche progressive et itérative : démarrer par un projet pilote au sein d'un service ou d'un ministère, tester la solution, l'ajuster en fonction des retours, puis étendre progressivement le déploiement à d'autres services ou ministères. Cette approche réduit les risques et permet une amélioration continue.

Dans un contexte ou la rapidité, l'évolutivité et la simplicité d'exécution sont essentielles, un CIAM bien conçu permet d'obtenir des résultats sur tous les plans, sans compromis sur les coûts, la sécurité ni la gouvernance.

#5 Facteurs clés de succès pour la mise en œuvre

La mise en œuvre d'un CIAM dans le secteur public ne se résume pas à une simple mise à niveau technologique. Elle exige une mobilisation collective : direction, TI, équipes de service et citoyens. Une planification rigoureuse, une coordination interfonctionnelle et une approche centrée sur le citoyen sont les fondements d'une transformation réussie.

- **Parrainage exécutif et collaboration**
  Un leadership fort et une coordination entre les organismes gouvernementaux sont essentiels. L'identité numérique touche tous les ministères. Il est donc crucial que le personnel comprenne bien le nouveau système et ses avantages. Des formations ciblées peuvent améliorer la prestation de services et favoriser l'adoption du système par les citoyens.
- **Choisir le bon partenaire**
  Tous les fournisseurs de CIAM ne sont pas conçus pour répondre aux exigences des administrations publiques. Il est important de choisir un partenaire ayant une expérience avérée dans le secteur public, dont la vision cadre avec vos objectifs à long terme. Privilégiez les solutions qui s'intègrent facilement à votre infrastructure existante, qui respectent les normes de sécurité, de confidentialité et d'accessibilité, et qui offrent une interface conviviale avec des outils en libre-service intuitifs. Un fournisseur qui comprend parfaitement les besoins spécifiques du secteur public peut faire toute la différence.
- **Résidence des données et souveraineté**
  Les gouvernements doivent s'assurer que les données des citoyens sont collectées, traitées et stockées conformément aux lois en vigueur. Une plateforme CIAM moderne doit offrir des options de déploiement flexibles, y compris l'hébergement spécifique à une région ou à un pays. Certains fournisseurs, opérant à l'international, peuvent conserver des droits d'accès aux données, ce qui pose un risque pour la résidence et la souveraineté des données. Une véritable souveraineté signifie un contrôle juridique et opérationnel absolu, sans ingérence étrangère. De plus, la disponibilité d'un soutien technique local devient un critère de plus en plus déterminant.
- **Architecture axée sur la protection de la vie privée**
  Les plateformes CIAM conçues pour le secteur public doivent intégrer les principes de la protection de la vie privée dès la conception et promouvoir une hygiène numérique rigoureuse, notamment la minimisation des données, l'usage limité à des fins précises, et une gestion transparente des consentements. Les utilisateurs doivent pouvoir consulter, modifier ou supprimer leurs données personnelles facilement. Ces pratiques renforcent la conformité réglementaire et la confiance du public. En outre, les analyses dépersonnalisées fournies par les plateformes de CIAM permettent d'optimiser la prestation de services et d'orienter les décisions stratégiques sur l'attribution des ressources.
- **Migration des systèmes existants**
  La modernisation des solutions d'identité dans le secteur public implique souvent le remplacement de solutions existantes. Une stratégie de migration bien orchestrée est essentielle pour éviter les interruptions de service et assurer une transition fluide pour les utilisateurs internes comme pour les citoyens. Il est recommandé de commencer par des services non critiques, puis d'élargir progressivement le déploiement. Les étapes clés comprennent l'intégration des annuaires existants, la conversion des identifiants et la réduction des frictions pour les utilisateurs. L'objectif est de garantir une transition sécurisée, sans rupture de service ni perte de confiance des utilisateurs.

L'adoption d'un CIAM repose sur l'harmonisation des personnes, des processus, des technologies et de l'expérience utilisateur. Avec la bonne stratégie et le bon partenaire, les gouvernements peuvent moderniser la gestion des identités, renforcer la confiance du public et offrir des services numériques sécurisés et transparents.



Étude de cas concrète



Refonte du CIAM dans une province canadienne

Une province canadienne de taille moyenne faisait face à une insatisfaction croissante de ses citoyens au sujet de ses services numériques. Les utilisateurs devaient jongler avec plusieurs identifiants, naviguer dans des interfaces complexes et subir des interruptions fréquentes — autant de signes d'une infrastructure d'identité dépassée.

Défis rencontrés :

- Systèmes de gestion des identités et des accès obsolètes et cloisonnés
- Coûts d'assistance élevés et pannes fréquentes
- Difficultés croissantes à respecter les règlements sur la protection de la vie privée

Solution mise en œuvre :

La province a opté pour une plateforme CIAM infonuagique, conforme aux exigences de résidence des données au Canada et intégrant des outils de conformité aux lois fédérales et provinciales sur la vie privée. Un projet pilote a été lancé dans les services fiscaux en ligne, avec des intégrations préconfigurées et une interface en libre-service conviviale pour réaliser un déploiement presque quatre fois plus rapide que les projets précédents.

Résultats obtenus :

- Déploiement réalisé en moins de 4 mois
- Diminution de 40 % des demandes d'assistance liées à la connexion
- Réduction de 30 % des coûts opérationnels
- Moins d'incidents de sécurité grâce à l'authentification multifacteur et aux contrôles de confidentialité granulaires
- Satisfaction accrue des utilisateurs et confiance renouvelée du public

Fort de ce succès, la province a étendu en toute confiance le CIAM aux secteurs de la santé et des prestations sociales. Cette approche progressive et centrée sur le citoyen a permis d'obtenir des résultats rapides tout en posant les bases d'une transformation numérique durable. Une belle réussite, malgré les défis inhérents à ce type de mise en œuvre.

Recommandations et bonnes pratiques

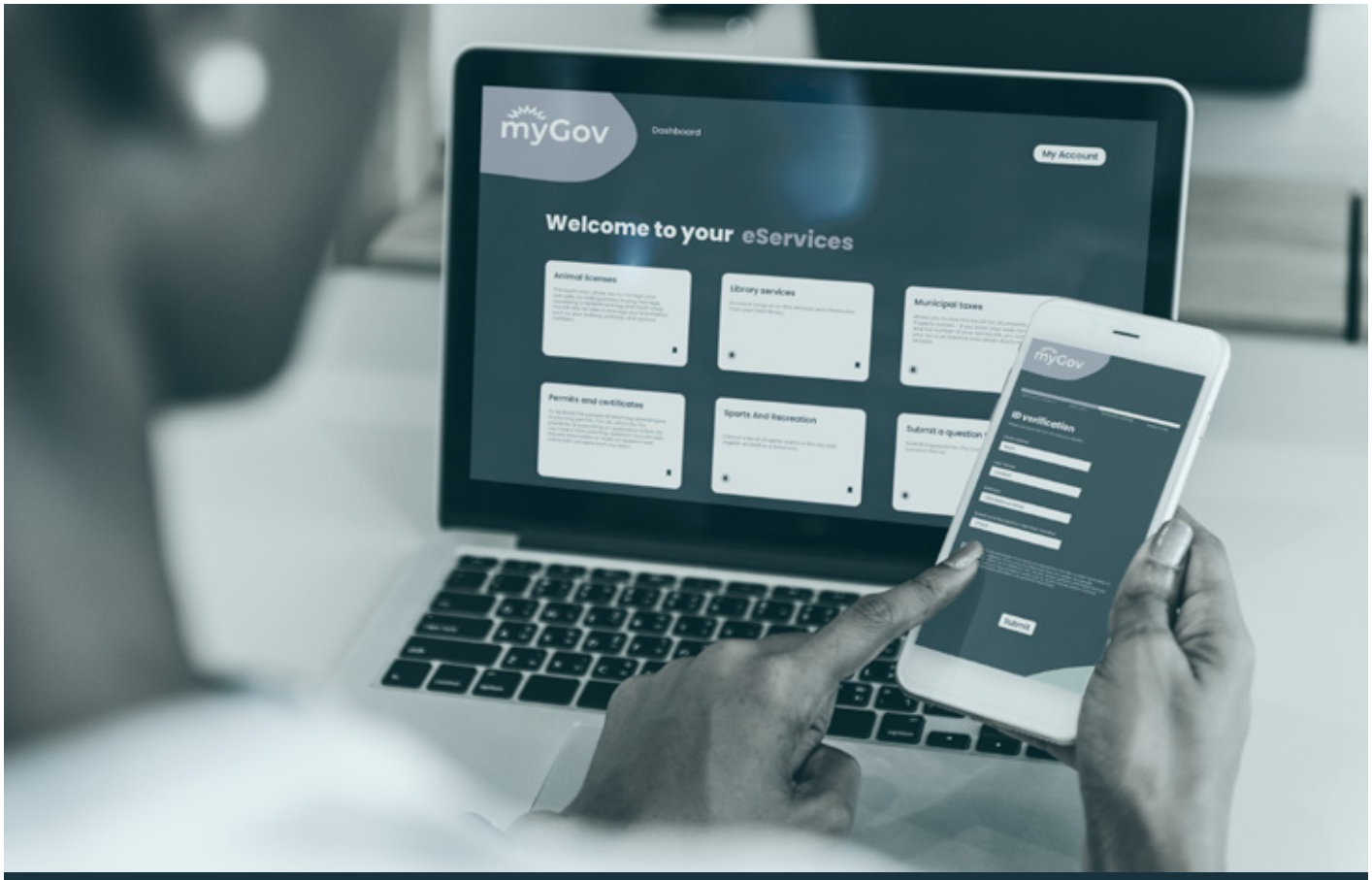
Pour maximiser les avantages du CIAM en nuage, les équipes du secteur public doivent adopter une approche stratégique, structurée et axée sur le long terme. Voici les étapes à suivre :

- **Commencer petit, voir grand**
  Lancez un projet pilote ciblé, limité à un seul service ou ministère. Ce premier succès servira de tremplin pour affiner votre stratégie, mobiliser les parties prenantes et obtenir l'adhésion de la direction. Il s'agit d'un marathon, pas d'un sprint.
- **Prioriser les services à haut risque**
  Une fois la dynamique enclenchée, concentrez-vous sur les services qui traitent des données sensibles ou qui génèrent un volume élevé d'interactions avec les citoyens. Ce sont ces domaines qui bénéficieront le plus de la valeur ajoutée du CIAM.
- **Renforcer la confiance des citoyens**
  La protection de la vie privée est au cœur de votre réputation. La transparence, le consentement et le respect de la vie privée dès la conception doivent être des principes fondamentaux. Il est essentiel que les citoyens comprennent clairement l'usage de leurs données et puissent en garder le contrôle. Ce défi est de taille, mais un CIAM conçu pour le secteur public peut grandement faciliter cette démarche.
- **Planifier la gestion du cycle de vie**
  L'identité numérique évolue constamment. Prévoyez une maintenance continue et engagez-vous dans une démarche d'amélioration continue. Les besoins des citoyens changent avec le temps : votre plateforme CIAM doit pouvoir suivre le rythme. Ce n'est pas un investissement ponctuel, mais un engagement durable.

L'adoption intelligente du CIAM ne consiste pas en des lancements spectaculaires, mais en des étapes réfléchies qui permettent de gagner du terrain, de réduire les risques et de placer les citoyens au cœur de votre transformation numérique.



Conclusion



La modernisation de l'identité numérique est un processus holistique qui englobe la technologie, les politiques publiques, le financement et, surtout, les personnes. Qu'il s'agisse de décideurs élaborant une stratégie nationale ou d'une famille demandant un permis pour un animal de compagnie, l'accès aux services gouvernementaux touche tous les aspects de la vie publique.

Un CIAM infonuagique, conçu pour le secteur public, permet aux gouvernements de mieux servir leurs citoyens. Grâce à sa sécurité intégrée, sa capacité d'évolution et sa conformité aux normes, il offre un rare équilibre entre impact élevé et risque maîtrisé. Il est rapide à déployer, facile à gérer et prêt à répondre aux exigences actuelles en matière de confidentialité et d'accès.

Mais le facteur temps est crucial. Chaque jour passé à se débattre avec des systèmes obsolètes est une occasion manquée d'améliorer les services, de réduire les risques et de renforcer la confiance du public. Plus les gouvernements attendent, plus il leur est difficile de répondre aux attentes croissantes des citoyens et aux normes réglementaires en constante évolution.

La voie à suivre est claire. Une approche gouvernementale unifiée de la gestion des identités, qui harmonise les services, simplifie l'expérience utilisateur et place la conformité au premier plan, commence par une première étape. Évaluez dès aujourd'hui votre environnement identitaire. Car l'avenir de l'administration numérique n'est pas pour demain. Il est déjà là.

Prêt à franchir le pas ? Découvrez les solutions de Portage CyberTech ou réservez une consultation pour explorer une mise en œuvre stratégique du CIAM en nuage pour votre organisation.

Glosssaire des termes clés

- **CIAM (Customer Identity and Access Management) :** Gestion des identités et des accès client
- **Données dépersonnalisées :** Informations traitées de manière à ne plus permettre l'identification d'une personne.
- **Données dépersonnalisées :** Informations traitées de manière à ne plus permettre l'identification d'une personne.
- **FIDO2 (Fast Identity Online) :** Norme d'authentification sans mot de passe, renforçant la sécurité tout en simplifiant l'expérience utilisateur.
- **IAM (Identity and Access Management) :** Gestion des identités et des accès
- **Sprawl de l'identité :** Multiplication non contrôlée des identités numériques d'un même utilisateur dans différentes applications.
- **Gestion du cycle de vie :** Gestion des identités numériques tout au long de leur parcours : création, mise à jour, désactivation.
- **Authentification multifactorielle :** Méthode d'authentification combinant plusieurs facteurs (mot de passe, appareil, biométrie) pour renforcer la sécurité.
- **OIDC (OpenID Connect) :** Protocole d'authentification basé sur OAuth 2.0, permettant une gestion sécurisée de l'identité.
- **Privacy by Design (PbD):** Approche proactive intégrant la protection de la vie privée dès la conception des systèmes et processus.
- **Progressive Profiling:** Collecte graduelle d'informations sur les utilisateurs, au fil de leurs interactions, pour améliorer l'expérience sans intrusion.
- **SAML (Security Assertion Markup Language) :** Protocole standardisé pour l'échange sécurisé de données d'authentification entre systèmes.
- **SSO (Single Sign-On) :** Mécanisme permettant aux utilisateurs d'accéder à plusieurs services avec une seule authentification.
- **Zéro confiance :** Modèle de sécurité dans lequel aucun utilisateur ou appareil n'est présumé fiable.

Liste de contrôle technique pour l'évaluation des fournisseurs de CIAM

- Prise en charge de la résidence et de la souveraineté des données
- Authentification multifactorielle, chiffrement et authentification adaptative intégrés
- Gestion du consentement et de la confidentialité (privacy by design)
- Intégrations préconfigurées avec les plateformes gouvernementales (impôts, santé, services sociaux)
- Architecture évolutive et infonuagique (prise en charge de plusieurs régions, mise à l'échelle élastique)
- Compatibilité avec SSO, OIDC et SAML
- Contrôle d'accès basé sur les rôles et administration déléguée
- Outils de journalisation des accès et de rapports de conformité
- Gestion en libre-service des profils d'utilisateurs et des consentements
- Prise en charge de la localisation (interface bilingue, conformité à l'accessibilité)
- Intégration sécurisée avec des sources de données fiables pour la vérification de l'identité
- Accès à l'API et extensibilité pour les intégrations futures
- Transparence du fournisseur (accords de niveau de service clairs, politiques de traitement des données bien définies)

Tableau de référence réglementaire

Réglementation	Juridiction	Points clés
GDPR	UE	Protection des données et de la vie privée
Loi 25	Québec	Consentement, transparence, gouvernance des données
CCPA	Californie	Droits des consommateurs, accès et suppression des données
PIPEDA	Canada	Traitement équitable des renseignements personnels
HIPAA	États-Unis (santé)	Confidentialité et sécurité des informations sur la santé
NIST 800-63	États-Unis (fédéral)	Lignes directrices sur l'identité numérique et niveaux d'assurance

Prochaines étapes ?
Des questions ?

En savoir plus sur les solutions de Portage CyberTech. Ou prenez rendez-vous avec l'un de nos experts si vous êtes prêt à explorer comment nos solutions peuvent bénéficier à votre municipalité.

© Portage CyberTech, tous droits réservés 2025