Livre blanc

À la rencontre des citoyens

Réinventer l'administration numérique par une gestion stratégique de l'identité



PORTAGE cybertech

portagecybertech.com
info@portagecybertech.com

Résumé

À la rencontre des citoyens

Réinventer l'administration numérique par une gestion stratégique de l'identité



Les citoyens s'attendent de plus en plus à ce que les services publics offrent le même niveau de commodité, de rapidité et de personnalisation que ceux du secteur privé. Pour répondre à ces attentes, les organismes gouvernementaux doivent moderniser la façon dont ils conçoivent et livrent leurs expériences numériques. Au cœur de cette transformation se trouve la gestion des identités et des accès client (CIAM), une base stratégique essentielle pour offrir à grande échelle des services numériques sécurisés, fluides et centrés sur les citoyens.

Le présent livre blanc explore comment les plateformes CIAM conçues pour le secteur public permettent aux administrations de relever des défis majeurs tels que l'obsolescence des infrastructures, la fragmentation des systèmes, la complexité croissante des réglementations en matière de confidentialité et le faible niveau d'engagement numérique. En unifiant l'identité entre les services et les canaux, la CIAM améliore l'expérience utilisateur, réduit la pression sur les services de soutien et renforce la protection des données ainsi que la confiance du public.

Une solution CIAM bien mise en œuvre simplifie l'accès aux services tout en permettant aux organismes de maintenir des pratiques rigoureuses en matière de confidentialité et de conformité. Des fonctionnalités telles que la gestion centralisée des consentements, l'authentification adaptative et l'orchestration automatisée à faible code facilitent un déploiement rapide et une prestation de services plus agile. Grâce à une conception inclusive et à des méthodes d'accès flexibles, les services publics peuvent atteindre un plus large éventail de citoyens, quels que soient leur langue, leur appareil ou leur niveau de littératie numérique.

En comparant trois principaux modèles de mise en œuvre (extension des systèmes d'identité d'entreprise existants, développement de solutions internes personnalisées ou adoption d'une solution CIAM dédiée), ce document guide les décideurs dans le choix de l'approche la plus efficace. Les solutions spécialement conçues se distinguent par leur déploiement rapide, leur évolutivité et leur intégration transparente aux systèmes existants, ce qui permet aux organismes d'innover sans compromettre la sécurité ni les exigences réglementaires.

Des exemples concrets en provenance d'Amérique du Nord illustrent comment le CIAM améliore l'accès aux services, réduit les risques de fraude et renforce la confiance des citoyens. Ils soulignent également l'importance d'harmoniser les initiatives CIAM avec les priorités des différentes parties prenantes — qu'il s'agisse des équipes informatiques, des responsables de la conformité, des spécialistes de l'expérience citoyenne ou de la haute direction.

Au final, les lecteurs comprendront que l'identité dépasse largement le cadre technique : elle constitue un levier puissant de transformation numérique qui façonne la manière dont les citoyens interagissent avec les institutions publiques. Une stratégie CIAM bien pensée permet aux administrations de garantir des services numériques sécurisés, accessibles et fiables, au bénéfice tant des citoyens que des pouvoirs publics.

1 Introduction: l'impératif numérique dans le secteur publique

Dans un paysage numérique en constante évolution, les citoyens attendent désormais des services publics qu'ils offrent le même niveau de commodité, de rapidité et de personnalisation que ceux du secteur privé. Les modèles traditionnels de prestation de services ne suffisent plus.

Les organismes publics sont confrontés à une pression croissante pour se moderniser, tout en composant avec des infrastructures vieillissantes, des réglementations complexes en matière de confidentialité et la nécessité de répondre aux besoins de communautés diverses. Au cœur de cette transformation se trouve l'identité numérique. Plus précisément, la gestion des identités et des accès client (CIAM) constitue le socle stratégique permettant de proposer des expériences numériques sécurisées, simplifiées et centrées sur le citoyen.

En facilitant la gestion centralisée des identités, les plateformes CIAM permettent aux administrations d'accélérer leur transition numérique, en améliorant l'authentification des utilisateurs, la gestion des consentements et l'application des politiques de confidentialité. Lorsqu'elle est bien conçue, une solution CIAM ouvre la voie à des parcours numériques fluides, à un engagement citoyen accru et à une réduction des coûts opérationnels.

2 Comprendre le citoyen numérique

Qu'il s'agisse de renouveler un permis ou d'accéder à des services de santé, les citoyens s'attendent désormais à pouvoir effectuer leurs démarches administratives en ligne, rapidement et sans difficulté.

Cette évolution des attentes est façonnée par leurs interactions quotidiennes avec des applications, des plateformes de commerce électronique et des services financiers qui offrent des expériences numériques fluides, personnalisées et efficaces. Le secteur privé fixe des standards élevés. Lorsque les services publics ne sont pas à la hauteur, les citoyens se désengagent. Certains se tournent vers des services en personne, ce qui exerce une pression supplémentaire sur des ressources déjà limitées, tandis que d'autres abandonnent tout simplement leurs démarches.

> **Malgré cette évolution, de nombreuses administrations continuent de s'appuyer sur des systèmes fragmentés et des technologies obsolètes, ce qui entraîne des parcours utilisateur incohérents et complique la gestion opérationnelle.**

Pour répondre aux attentes des citoyens numérique, les organismes publics doivent adopter une approche centrée sur l'utilisateur, reposant sur une infrastructure d'identité numérique robuste et respectueuse de la vie privée. Les expériences numériques doivent être aussi simples et intuitives que celles du secteur privé, tout en accordant une attention particulière à la sécurité, à la protection des données, à la transparence et à l'inclusivité.



#3 Répondre aux besoins en matière de commodité, de sécurité et de confidentialité

Commodité

Les citoyens attendent des interactions numériques simples et efficaces. Ils recherchent des interfaces intuitives, une inscription sans friction et une authentification unique pour accéder à l'ensemble des services. Les plateformes CIAM permettent d'unifier ces points de contact, offrant ainsi une expérience fluide et homogène.

> L'accès omnicanal est particulièrement important. Lorsqu'un citoyen met à jour ses coordonnées auprès d'un organisme, ces changements devraient se répercuter dans tous les services connectés, à condition qu'il ait consenti au partage de ses données. Les expériences fragmentées génèrent confusion et abandon, tandis que les systèmes intégrés facilitent une prestation de services rapide et harmonieuse.

Sécurité

La protection des données personnelles est primordiale, mais elle ne doit pas compromettre la convivialité. Les mécanismes d'authentification adaptative permettent aux organismes d'évaluer les risques en temps réel et d'appliquer des mesures renforcées uniquement lorsque cela est nécessaire.

> Des outils supplémentaires comme l'authentification multifactorielle (MFA), la biométrie, l'analyse comportementale et les politiques basées sur les risques permettent de lutter efficacement contre le vol d'identifiants, l'hameçonnage et l'usurpation d'identité. Cependant, l'objectif reste d'assurer un niveau de sécurité optimal avec un minimum de friction pour l'utilisateur.

Confidentialité

Dans un contexte de méfiance croissante envers le numérique, les citoyens exigent transparence et contrôle. Ils veulent savoir quelles données personnelles sont collectées, comment elles sont utilisées et s'ils peuvent choisir d'y consentir ou non.

> Une solution CIAM adaptée permet aux organismes de mettre en œuvre une gestion centralisée des consentements et de respecter les réglementations en matière de confidentialité telles que le RGPD, le CCPA (California Consumer Privacy Act) et les lois provinciales et étatiques sur la protection des données. Grâce à des préférences gérées par l'utilisateur, des demandes de consentement explicites et des contrôles d'accès granulaires, les administrations peuvent démontrer leur responsabilité et instaurer la confiance nécessaire à l'adoption des services numériques.



#4 L'identité comme levier stratégique

L'identité numérique ne se limite pas à une exigence technique : elle constitue un pilier essentiel de la prestation de services modernes. Une infrastructure d'identité robuste facilite l'accès aux services, favorise l'inclusion, réduit les efforts opérationnels et soutient chaque interaction citoyenne.

Grâce à l'orchestration de l'identité, les organismes peuvent intégrer des fonctions clés comme l'authentification, la vérification, la détection des fraudes et la gestion des consentements dans des parcours unifiés. Cette approche renforce l'agilité, limite les redondances et accélère le déploiement de nouveaux services.

L'orchestration permet aux équipes de développement de configurer des flux de travail sans expertise approfondie en programmation, à l'aide d'interfaces à faible codage ou sans codage. Cela facilite la mise en œuvre, les essais, l'optimisation et l'évolution des parcours citoyens au sein des différents services et systèmes.

Par exemple, un organisme pourrait créer un flux de travail réutilisable comprenant :

- une authentification renforcée pour les services à forte valeur ajoutée;
- une vérification de l'identité lors de l'inscription de nouveaux utilisateurs;
- des alertes automatisées pour signaler toute activité de connexion inhabituelle aux équipes de sécurité.

> **Ce type d'orchestration réduit le délai de rentabilisation et garantit que la sécurité est intégrée dès la conception.**

Qu'il s'agisse d'une demande d'allocations, d'accéder à des informations de santé publique ou de solliciter une assistance en ligne, l'identité numérique assure la continuité, la personnalisation fondée sur le consentement et la responsabilité tout au long du parcours citoyen.

#5 Surmonter les défis courants grâce au CIAM

Infrastructure héritée

De nombreuses administrations sont confrontées aux limites de systèmes obsolètes ou développés en interne. Les solutions CIAM sont conçues pour s'intégrer aux infrastructures existantes, offrant ainsi des voies de modernisation sans nécessiter de remplacement complet.

Grâce à des interfaces de programmation d'application (API), des connecteurs et des couches d'orchestration, les plateformes CIAM modernes permettent aux organismes de relier les bases de données existantes aux nouvelles applications en nuage. Il est ainsi possible de faire évoluer progressivement les services numériques tout en préservant les systèmes centraux.

Conformité réglementaire

La gestion des réglementations en matière de confidentialité et de protection des données est complexe et en constante évolution. Les agences doivent composer avec des exigences variées selon les juridictions, tout en assurant transparence et responsabilité.

Les plateformes CIAM facilitent la conformité grâce à des fonctionnalités telles que :

- le suivi des consentements;
- les pistes d'audit;
- les politiques configurables;
- les contrôles d'accès basés sur les rôles.

> **La conformité n'est pas seulement une obligation légale : c'est aussi le fondement de la confiance. Une plateforme CIAM bien configurée peut prendre en charge plusieurs cadres réglementaires (comme la HIPAA ou le RGPD) simultanément, ce qui permet aux administrations de développer leurs services numériques tout en respectant les contraintes réglementaires.**

Au service de populations diverses

Les services publics doivent être accessibles à un large éventail d'utilisateurs, quels que soient leur langue, leur appareil ou leurs capacités. Les plateformes CIAM favorisent l'inclusion grâce à des fonctionnalités telles que :

- des interfaces multilingues;
- l'authentification biométrique et la prise en charge de différents fournisseurs d'identité;
- des fonctionnalités d'accessibilité conformes aux normes WCAG.

Une solution CIAM bien pensée et correctement mise en œuvre tiendra également compte d'autres obstacles à l'adoption, comme l'accès à Internet, notamment la disponibilité du haut débit.

> Que les citoyens préfèrent utiliser leur adresse courriel, leur téléphone mobile ou une identité sociale vérifiée, une plateforme CIAM offre des méthodes d'authentification flexibles. Ces fonctionnalités contribuent à réduire la fracture numérique en garantissant l'accessibilité à tous, quels que soient leur profil démographique, leur appareil ou leur niveau de maîtrise du numérique.

Faible engagement et taux d'abandon élevé

Des connexions laborieuses, des parcours utilisateur interrompus et des instructions peu claires peuvent rapidement décourager les citoyens. Les taux d'abandon élevés lors de l'inscription demeurent l'un des principaux obstacles à l'adoption des services numériques. Le CIAM permet de surmonter ces obstacles grâce à une authentification fluide, des expériences personnalisées et des interactions cohérentes sur tous les canaux.

Pour réduire les frictions, les plateformes CIAM proposent des outils tels que :

- des options de connexion proposées par des tiers (par exemple, identifiants sociaux ou mobiles vérifiés);
- une inscription guidée, étape par étape;
- le pré-remplissage intelligent des formulaires.

Cependant, toutes les plateformes CIAM ne se valent pas. Certaines sont prêtes à être déployées rapidement, tandis que d'autres nécessitent des engagements prolongés en services professionnels pour leur conception et leur mise en œuvre. Il est donc essentiel que les organismes évaluent soigneusement la préparation des fournisseurs afin d'assurer une adoption rapide et efficace.

#6 Évaluer les modèles de mise en œuvre : étendre, construire ou acheter

Lorsqu'elles envisagent de déployer des capacités CIAM, les organisations du secteur public ont généralement trois options stratégiques : étendre leurs systèmes IAM d'entreprise existants, développer une solution en interne ou adopter une plateforme CIAM spécialement conçue. Chaque option présente des avantages et des inconvénients selon les ressources disponibles, la tolérance au risque et les résultats attendus.

Option A : étendre les systèmes d'identité d'entreprise existants

Les plateformes d'identité d'entreprise sont généralement conçues pour les utilisateurs internes. Elles présentent souvent des lacunes en matière d'évolutivité, de flexibilité et de fonctionnalités axées sur le client, telles que le libre-service ou l'accès adaptatif. Ces solutions privilégient l'accès des employés aux systèmes internes et ne disposent pas des outils de vérification d'identité avancés ainsi que des capacités de conception de parcours utilisateur nécessaires pour les services destinés au public. Elles sont souvent les plus risquées à mettre en œuvre et les plus coûteuses à long terme.

Si elles peuvent convenir à des environnements petits et stables, elles deviennent rapidement des goulots d'étranglement lorsque les attentes des citoyens et les exigences réglementaires augmentent. L'extension d'une solution IAM d'entreprise peut également engendrer des failles de sécurité et une dette technique, tout en négligeant l'expérience utilisateur. Dans le contexte du CIAM, l'organisation n'a pas le luxe d'imposer ses processus aux utilisateurs : elle doit les convaincre. De nombreuses organisations finissent par investir des efforts disproportionnés pour adapter des solutions qui n'ont jamais été conçues pour répondre aux besoins liés à l'identité des clients.

Par ailleurs, l'extension de ces outils peut freiner l'innovation. Les programmes CIAM reposent sur l'agilité, c'est-à-dire la capacité à itérer, tester et déployer rapidement des mises à jour dans un environnement en interaction constante avec les citoyens. Or, les solutions héritées manquent souvent d'extensibilité et de capacités d'orchestration nécessaires pour soutenir ces écosystèmes dynamiques.

Option B : développer une solution en interne

Créer une solution d'identité sur mesure peut sembler attrayant, notamment pour répondre à des besoins précis. Toutefois, cette approche s'accompagne d'une complexité considérable en matière de gestion des normes, d'intégration et de maintenance, ce qui en fait une initiative à haut risque. Peu d'organisations disposent des ressources ou de l'expertise nécessaires pour mener à bien un tel projet de manière efficace et durable.

Les solutions personnalisées offrent une flexibilité théorique, mais celle-ci a un coût élevé. Les équipes de développement doivent composer avec des normes d'authentification telles que OAuth, SAML ou OpenID Connect, tout en assurant une conformité continue aux lois sur l'accessibilité, aux cadres de confidentialité et aux réglementations régionales en matière de protection des données. Sans oublier qu'elles doivent suivre le rythme des attentes évolutives des citoyens en matière d'expérience utilisateur.

Les systèmes développés en interne exigent des investissements constants en matière de correctifs, de tests et de mises à jour réglementaires. Ils peuvent également enfermer les organismes dans des architectures propriétaires, rendant toute migration future complexe et coûteuse. Plus préoccupant encore, ces projets détournent les équipes internes de leur mission première : innover et améliorer l'expérience utilisateur. Ce qui commence comme une stratégie de réduction des coûts se transforme souvent en une accumulation de dette technique, des retards dans la prestation des services et une exposition accrue à des risques imprévus.

Option C : adopter une plateforme CIAM spécialement conçue

> **Les plateformes CIAM dédiées, conçues pour répondre aux besoins spécifiques du secteur public, offrent une alternative robuste et éprouvée. Elles permettent un déploiement rapide, une évolutivité native et une prise en charge intégrée des exigences de conformité. Grâce à des API, des outils d'orchestration et des modules preconfigures, elles accélèrent la transformation numérique tout en réduisant les risques liés au développement sur mesure.**

Ces solutions visent à offrir aux citoyens une expérience fluide, sécurisée et conforme aux normes internationales en matière de protection des données et de cybersécurité. Elles prennent en charge des fonctionnalités avancées telles que l'authentification biométrique, l'authentification unique (SSO) et la synchronisation multi-appareils, assurant une continuité de service sur l'ensemble de l'écosystème numérique public.

Les fournisseurs spécialisés proposent également des intégrations avec des outils d'analyse tiers, des systèmes de détection de fraude, des plateformes d'engagement citoyen, des systèmes de gestion de contenu et des services d'assistance à la clientèle. Cette approche écosystémique facilite le lancement rapide de nouveaux services, leur adaptation continue et leur évolution en fonction des besoins. Elle permet avant tout aux organismes de rester concentrés sur leur mission essentielle : offrir aux citoyens des services publics fiables, accessibles et de haute qualité.

Une plateforme CIAM soigneusement sélectionnée et axée sur le secteur public doit offrir une extensibilité, des interfaces sans code pour l'automatisation des flux de travail et une intégration transparente avec les environnements informatiques existants des administrations publiques, afin d'intégrer l'identité numérique à chaque étape du parcours utilisateur.

#7 Élaborer un dossier stratégique en faveur du CIAM

Pour obtenir un soutien transversal aux initiatives CIAM, les responsables du secteur public doivent adapter leur proposition de valeur aux priorités spécifiques de chaque groupe de parties prenantes. Le CIAM a une portée organisationnelle étendue : il touche à l'informatique, à la cybersécurité, à l'expérience citoyenne, à la prestation de services, à la conformité et à l'innovation.

Équipes axées sur l'engagement (expérience citoyenne, services numériques)

Ces équipes sont évaluées en fonction de la satisfaction des citoyens, de l'utilisation des portails, des taux d'adoption et de la fidélisation. Elles recherchent des plateformes qui réduisent les frictions, permettent une personnalisation fine et renforcent l'engagement. Le CIAM répond à ces attentes en accélérant l'inscription, en simplifiant la connexion et en adaptant l'accès en fonction du comportement et des préférences des utilisateurs. Ces équipes privilégient également la rapidité d'exécution et accordent une importance particulière au délai de rentabilisation.

> Grâce au CIAM, elles peuvent tester différentes variantes de parcours (par exemple, des tests A/B sur les flux d'inscription), diffuser du contenu localisé et personnaliser les alertes ou rappels selon le profil des citoyens. Il en résulte une amélioration de la prestation de services et une hausse des niveaux de satisfaction.

Acteurs de l'informatique, de la sécurité et de la conformité

Pour ce groupe, la priorité est l'intégrité opérationnelle. Ils doivent s'assurer que les nouvelles plateformes n'introduisent pas de vulnérabilités ni ne compromettent les données sensibles des citoyens. Une solution CIAM robuste applique les principes du « zéro confiance », chiffre les données sensibles, enregistre les tentatives d'authentification et permet un contrôle d'accès granulaire.

Le CIAM contribue également à alléger la charge des services d'assistance en réduisant les demandes de réinitialisation de mot de passe et le volume des appels. Des mécanismes d'authentification adaptative limitent les risques d'usurpation d'identité, tandis que les journaux d'audit facilitent les enquêtes de conformité et la gestion des incidents. Ces parties prenantes attendent aussi des garanties en matière de respect de la vie privée : limitation de la collecte de données, respect des préférences de consentement et application des principes de confidentialité dès la conception dans tous les flux d'identité.

Dirigeants et décideurs politiques

Pour les dirigeants, le CIAM ne doit pas être perçu comme un simple projet technologique, mais comme un levier stratégique de transformation. Il doit être présenté comme un vecteur de réduction des coûts, d'amélioration de l'efficacité des programmes, de promotion de l'équité numérique et de renforcement de la confiance citoyenne. Positionner le CIAM comme un investissement dans la confiance du public est souvent plus percutant que de mettre l'accent uniquement sur ses aspects techniques. Il contribue directement à la réalisation des objectifs de la politique numérique, notamment en améliorant l'accessibilité, en élargissant la portée des services en ligne et en garantissant une gestion de l'identité dans l'ensemble des programmes.

Les décideurs doivent disposer de données claires sur le retour sur investissement, notamment :

- réduction du nombre de tentatives de connexion infructueuses et de réinitialisations de mot de passe;
- augmentation du temps passé sur les portails numériques;
- amélioration des scores de conformité lors des audits;
- diminution des incidents liés à l'usurpation d'identité;
- délai de lancement de nouveaux services numériques;
- réduction globale des risques en matière de sécurité et de conformité.

L'alignement précoce entre les équipes clés est essentiel pour passer efficacement de la planification à la mise en œuvre. Les organismes qui réussissent cette transition s'appuient sur des programmes pilotes, des tableaux de bord d'identité et des boucles de rétroaction citoyenne pour bâtir des analyses de rentabilité solides. Le succès repose sur l'implication dès le départ des responsables de la conformité, des DSI, des équipes chargées de l'expérience citoyenne et des responsables de la gouvernance des données. Rassembler ces expertises dès les premières étapes permet de créer un élan collectif et d'obtenir plus rapidement des résultats mesurables.

Résultats concrets



le CIAM en action

Les administrations publiques nord-américaines poursuivent leur modernisation, mais beaucoup restent confrontées à des systèmes fragmentés et à des approches traditionnelles en matière de gestion de l'identité. Cette fragmentation entraîne des expériences numériques dégradées, source de frustration pour les citoyens et de vulnérabilité pour les systèmes. Une solution CIAM conçue pour le secteur public comble cette lacune en offrant des parcours utilisateurs modernes, sécurisés et unifiés à grande échelle.

Le CIAM génère de la valeur en facilitant l'intégration sécurisée des utilisateurs, la gestion efficace des accès et l'analyse en temps réel des comportements, permettant ainsi la personnalisation des services et la détection proactive des fraudes. Une authentification fluide améliore non seulement l'expérience utilisateur, mais réduit également la charge des services d'assistance et le taux d'abandon des sessions. Les plateformes CIAM offrent une visibilité précieuse sur les comportements des utilisateurs, permettant aux organismes d'optimiser leurs services et de diffuser des communications ciblées favorisant l'engagement et l'inclusion.

> **Aux États-Unis, par exemple, plusieurs gouvernements d'État ont adopté le CIAM pour unifier les portails disparates de leurs organismes sous un cadre d'identité unique. Les citoyens bénéficient d'un accès simplifié, tandis que les équipes internes gagnent en contrôle centralisé, en conformité et en rapidité de déploiement des services. Au Canada, un gouvernement provincial a utilisé le CIAM pour soutenir les services liés au passeport vaccinal. En exploitant les capacités de gestion du consentement et de reconnaissance des appareils, il a pu délivrer en toute sécurité des identifiants numériques à des millions de résidents en quelques jours seulement.**

Lors d'un webinaire GovTech en 2023, l'urgence d'adopter le CIAM a été clairement mis en évidence. Les intervenants ont souligné que la fragmentation des connexions entraînait une désaffection des citoyens et exposait les systèmes à des attaques par force brute. En mettant en œuvre une authentification adaptative et une gouvernance des identités fondée sur le consentement, plusieurs États ont observé une hausse significative du taux de réussite des connexions et une baisse des signalements de fraude.

Une idée clé ressort de ces expériences : le CIAM dans le secteur public doit se différencier des modèles utilisés dans le secteur privé. Alors que les entreprises visent avant tout la conversion commerciale, les gouvernements doivent prioriser l'inclusion, l'accessibilité et l'équité numérique. Les meilleures plateformes CIAM pour le secteur public intègrent notamment :

- le respect des normes linguistiques et d'accessibilité;
- une conception intuitive adaptée aux utilisateurs peu familiers avec les outils numériques;
- plusieurs options de connexion (mobile, biométrie, courriel, etc.).

Les avantages dépassent largement la seule expérience utilisateur. Grâce à une conformité réglementaire intégrée, les plateformes CIAM permettent de respecter les obligations telles que le RGPD et le CCPA, ainsi que les normes telles que le NIST et le PCTF, sans recourir à des processus manuels complexes. Des outils centralisés de gestion du consentement et des journaux d'audit sécurisés renforcent la transparence et la responsabilité, tout en aidant les organismes à maintenir la confiance du public et à réduire les risques de non-conformité.

#9 L'avantage pour le secteur public

Le CIAM ne se limite pas à une solution d'accès : c'est un véritable levier stratégique qui permet aux gouvernements de fournir des services inclusifs, conformes et centrés sur les citoyens, à grande échelle.

Avec une plateforme CIAM adaptée, les organismes peuvent :

- réduire les frictions à la connexion et favoriser l'adoption des services numériques;
- diminuer les coûts liés au soutien technique en limitant les échecs de connexion et les réinitialisations de mot de passe;
- exploiter les données comportementales pour orienter la conception des politiques et des programmes;
- respecter les normes de confidentialité et de sécurité sans ralentir les cycles de développement;
- faciliter la collaboration entre les organismes grâce à des profils citoyens partagés, fondés sur le consentement.

> **Plus important encore, le CIAM offre aux administrations publiques la souplesse nécessaire pour s'adapter à l'évolution des besoins, qu'il s'agisse de déployer des programmes d'identification numérique, de délivrer des permis ou de distribuer des prestations. Une infrastructure identitaire solide garantit des interactions sécurisées, confidentielles et simples avec les citoyens.**

En plaçant l'identité au cœur de leur stratégie numérique, les organismes publics peuvent transformer non seulement la manière dont les services sont fournis, mais aussi la manière dont ils sont perçus, renforçant ainsi la confiance et l'engagement citoyen à chaque interaction.

Conclusion: l'identité, catalyseur de la transformation numérique

L'avenir de la prestation des services publics repose sur la capacité à offrir des expériences numériques sécurisées, fluides et centrées sur l'utilisateur. Les citoyens ne jugent plus leur gouvernement uniquement en fonction des services offerts en personne ou des délais d'attente au téléphone. Ils évaluent désormais la facilité d'accès aux services, la rapidité de connexion et la qualité du service de soutien en ligne.

L'identité numérique est la pierre angulaire de cette transformation. En adoptant le CIAM, les organismes peuvent fournir des services conformes, accessibles et fiables, tout en favorisant l'innovation au sein des institutions publiques. Ils ne se content plus de répondre aux attentes des citoyens — ils les dépassent.

> **Une stratégie CIAM robuste, conçue pour le secteur public garantit que la sécurité n'est pas un compromis, mais une composante essentielle de chaque interaction. La confidentialité n'est pas une considération secondaire, mais un droit fondamental intégré dès la conception. La commodité n'est pas un luxe, mais une exigence de base.**

Prochaines étapes



Explorez des plateformes CIAM conçues spécifiquement pour le secteur public et adaptées aux objectifs stratégiques de votre organisme. Pour aller de l'avant :

- Lancez un projet pilote ciblant un service essentiel pour les citoyens (par exemple, l'inscription aux prestations sociales, l'octroi de licences commerciales ou l'accès aux soins de santé).
- Collectez des données sur les taux d'inscription, les performances de connexion et les niveaux de satisfaction. Ajustez votre approche en fonction des commentaires des citoyens.
- Mobilisez les parties prenantes des domaines clés (politique, informatique, conformité, services numériques) pour élaborer conjointement votre stratégie identitaire.
- Appuyez-vous sur l'expérience de vos pairs en consultant des guides pratiques et des études de cas d'organismes qui ont mis en œuvre le CIAM avec succès.

Et surtout, restez centré sur les citoyens. L'identité n'est pas simplement une capacité technologique. C'est un engagement à gagner et à conserver la confiance des personnes que vous servez.

L'avenir numérique des administrations publiques ne commence pas par de meilleures applications, mais par un meilleur accès. Et cet accès commence par une identité fiable et sécurisée, une vision que Portage CyberTech s'engage à concrétiser.

Prêt à vous lancer ?

Découvrez les solutions de Portage CyberTech ou réservez une consultation pour discuter des avantages d'une mise en œuvre stratégique du CIAM pour votre organisation..

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