Livre blanc

CIAM : une solution rentable pour le secteur public

Comment les gouvernements peuvent exploiter pleinement la gestion des identités client



PORTAGE cybertech

portagecybertech.com
info@portagecybertech.com

CIAM: une solution rentable pour le secteur public

Exploiter pleinement la gestion des identités client pour une rentabilité de l'investissement optimale : un avenir numérique sûr, accessible et inclusif pour tous les citoyens



Entre montée des fraudes, attentes croissantes des citoyens et durcissement des cadres réglementaires, les services publics numériques sont à un tournant décisif. Comment les équipes du secteur public peuvent-elles faire face à ces enjeux?

Découvrez la gestion des identités et des accès client (CIAM) — un outil stratégique méconnu, mais essentiel pour garantir des interactions sécurisées, fluides et centrées sur le citoyen.

Résumé

De l'accélération des services numériques pendant la pandémie de COVID-19 aux efforts soutenus pour réduire la fracture numérique, la transformation de l'administration en ligne continue reste au cœur des priorités gouvernementales. Et pour cause.

L'idée d'une administration numérique ne date pas d'hier. Ses premières manifestations remontent aux années 1980 (à l'époque du Commodore 64, pour les nostalgiques). Mais aujourd'hui, la recrudescence des fraudes à l'identité, le durcissement des exigences réglementaires et les attentes croissantes des citoyens en matière de services en ligne sécurisés et fluides rendent cette transformation plus complexe et plus indispensable que jamais.

Une chose est claire : le numérique est le moyen le plus efficace pour les organismes publics d'interagir avec leurs administrés. Cela est particulièrement vrai au niveau local et régional, où

les gouvernements sont souvent le premier point de contact avec les citoyens. En exploitant pleinement leur potentiel numérique, les administrations peuvent améliorer considérablement la vie publique grâce à des services efficaces, cohérents et transparents.

Mais comment y parvenir de manière durable, inclusive et à grande échelle, tout en garantissant la protection des données et la cybersécurité?

> La réponse : en investissant dans une solution d'identité numérique robuste, centrée sur le citoyen.

Ce livre blanc explique comment la gestion des identités et des accès client (CIAM) peut aider les gouvernements à atteindre leurs objectifs numériques tout en :

- réduisant la fraude et les coûts liés aux violations de données;
- améliorant l'expérience citoyenne sur les plateformes numériques;
- assurant la conformité avec des réglementations en constante évolution.

Vous découvrirez pourquoi un système centralisé de gestion des identités et des accès client ne constitue pas seulement une porte d'entrée vers la modernisation des services publics, mais aussi un levier concret pour réaliser des économies, optimiser les budgets et accroître la résilience à long terme.

En mettant en place une stratégie CIAM bien pensée, les gouvernements peuvent renforcer la confiance du public, créer des communautés connectées et bâtir un écosystème numérique où personne n'est laissé pour compte.

Pourquoi le CIAM maintenant

La fraude est en hausse. Les coûts des brèches explosent. Les gouvernements doivent agir.

12,5G $
Pertes liées à la fraude des consommateurs aux É.-U. en 2024

4,88M $
Coût moyen d'une violation de données

6,7 % ↑31 % D/A
Fraude numérique suspectée dans les services publics

6,5M
Incidents soumis à la FTC

2,6M
Impliquant de la fraude

1,1M
Impliquant le vol d'identité

8,1G $
Valeur du marché CIAM en 2023, avec une croissance substantielle prévue jusqu'en 2030

#2 Pourquoi adopter une solution CIAM dans le secteur public

Partout dans le monde, les gouvernements intensifient leurs efforts de transformation numérique. *L'indice de l'administration numérique de l'OCDE* révèle des investissements massifs dans des stratégies visant à améliorer la réactivité et la fiabilité des services publics. La majorité des pays évalués se situent dans la moitié supérieure du classement, preuve qu'une évolution numérique centrée sur l'humain est bel et bien en cours (OECD).

L'enquête 2024 des Nations Unies sur l'administration en ligne confirme cette dynamique. En deux ans seulement, la proportion de la population mondiale se situant en dessous du seuil de référence est passée de 45 % à 22,4 %, grâce à la modernisation des infrastructures et à l'accès élargi à des services internet abordables — des facteurs clés de la numérisation du secteur public (UN DESA).

Mais cette avancée ne va pas sans risques. Une croissance numérique à grande échelle s'accompagne inévitablement d'une série de menaces liées à l'identité numérique, notamment :

- le piratage de comptes,
- les identités synthétiques,
- les attaques par usurpation,
- les fraudes par échange de carte SIM,
- les violations de données.

Un simple coup d'œil au dernier rapport de la Commission fédérale du commerce suffit à l'ampleur du problème : en 2024, les consommateurs ont signalé 6,5 millions d'incidents, soit une hausse de 20 % par rapport à l'année précédente (FTC).

Le message est clair : si les gouvernements n'agissent pas rapidement pour protéger les données personnelles des citoyens, leurs efforts de transformation numérique risquent d'être compromis, les éloignant de leur objectif d'un environnement numérique fiable et sécurisé.

#3 Quantifier le risque

Le passé est révélateur, et les données de 2024 mettent en lumière des risques concrets et quantifiables que les gouvernements doivent anticiper dans la mise en œuvre de services numériques centrés sur le citoyen.

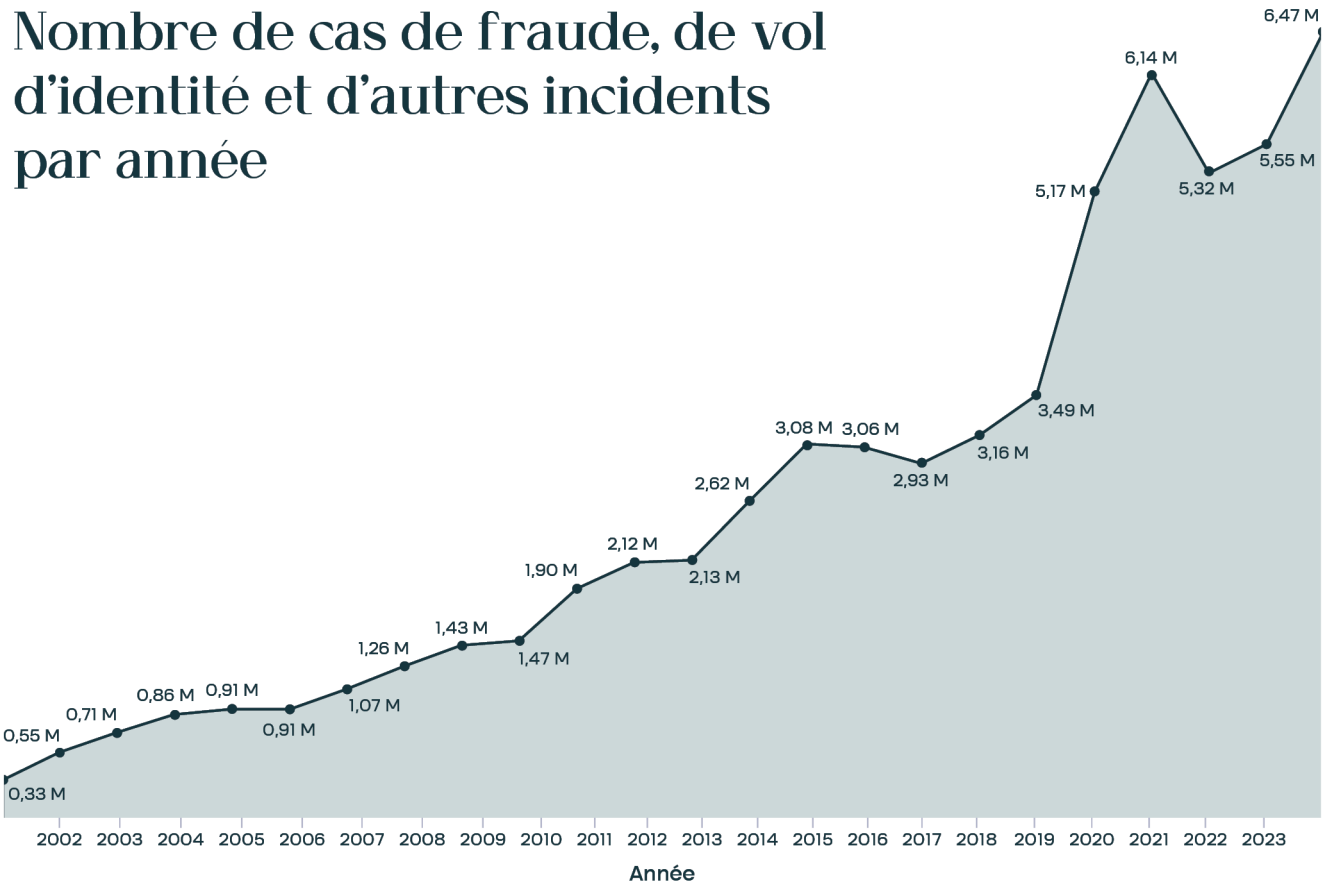
Les chiffres sont révélateurs : en 2024, les consommateurs américains ont déclaré près de 12,5 milliards de dollars de pertes liées à la fraude. Sur les 6,5 millions d'incidents signalés à la la Commission fédérale du commerce, 2,6 millions concernaient des fraudes et 1,1 million des cas d'usurpation d'identité (FTC). À l'échelle mondiale, le coût moyen d'une violation de données a atteint 4,88 millions de dollars (IBM). Dans les services gouvernementaux, le taux de fraude numérique constatée parmi les citoyens a atteint 6,7 %, soit une hausse de 31 % par rapport à l'année précédente, pour atteindre 6,7 % (events.afcea.org). Face à cette réalité, il n'est donc pas surprenant que le marché du CIAM soit en plein essor, avec une valeur estimée à 8,1 milliards de dollars en 2023 et des perspectives de croissance soutenue jusqu'en 2030 (Grand View Research).

Deux éléments essentiels émergent de cette analyse :

1. La valeur lucrative des données compromises incite les cybercriminels à élaborer des stratégies d'intrusion de plus en plus complexes, capables de submerger les administrations si elles ne renforcent pas leurs défenses.
2. Malgré les risques, les citoyens privilégient de plus en plus les interactions numériques pratiques, faisant de l'administration en ligne une attente durable.

Ces deux tendances — la montée des cybermenaces et l'essor de l'engagement numérique — soulignent à la fois l'ampleur du défi et le rôle stratégique des solutions CIAM dans la mise en place de services publics numériques sécurisés et fiables.

Nombre de cas de fraude, de vol d'identité et d'autres incidents par année



#4 Capacités essentielles du CIAM pour répondre aux besoins du secteur public

Pour prospérer à l'ère numérique, les gouvernements doivent opérer un véritable changement de paradigme : abandonner les modèles de services cloisonnés et descendants, qui exposent les données des utilisateurs à des risques, au profit d'une approche connectée et intégrée à l'échelle de l'administration. Dans ce nouveau modèle, les stratégies multicanales traditionnelles sont remplacées par une « porte d'entrée unique », permettant aux citoyens d'accéder à plusieurs services par l'intermédiaire d'un écosystème numérique cohérent. C'est dans ce contexte que le CIAM révèle tout son potentiel, bien au-delà de la simple gestion des identités. Il constitue le socle d'opérations numériques continues, responsables et centrées sur l'utilisateur.

Le CIAM offre ces avantages grâce à un ensemble de fonctionnalités conçues spécifiquement pour le secteur public :

- **Authentification et MFA adaptative :** L'authentification dynamique basée sur les risques permet de garantir un accès sécurisé tout en préservant la fluidité de l'expérience utilisateur. L'identité des citoyens est vérifiée à l'aide de mesures de sécurité adaptatives qui tiennent

compte du comportement, de la localisation et du contexte de l'appareil, réduisant ainsi les risques de prise de contrôle de compte.

- **Vérification d'identité et intégration :** L'authentification dynamique basée sur les risques permet de garantir un accès sécurisé tout en préservant la fluidité de l'expérience utilisateur. L'identité des citoyens est vérifiée à l'aide de mesures de sécurité adaptatives qui tiennent compte du comportement, de la localisation et du contexte de l'appareil, réduisant ainsi les risques de prise de contrôle de compte.
- **Gestion du cycle de vie des comptes, du consentement et de la confidentialité :** Le respect des lois sur la protection des renseignements personnels telles que le RGPD, le PDPA ou d'autres règlements spécifiques à certains secteurs est impératif. Les solutions CIAM centralisent la gestion du consentement, suivent les préférences des utilisateurs et assurent une gestion fluide du cycle de vie des comptes, renforçant ainsi la conformité réglementaire et la confiance des utilisateurs.
- **Détection des fraudes et analyse comportementale :** Grâce à des outils d'analyse avancés, les anomalies sont détectées en temps réel. L'évaluation des risques de session, la surveillance comportementale et la reconnaissance des schémas permettent aux gouvernements de repérer et de bloquer de manière proactive les activités frauduleuses avant qu'elles n'aient des répercussions sur les citoyens.
- **Fédération et interopérabilité :** Les systèmes CIAM modernes s'intègrent aux identités numériques nationales, aux systèmes existants et les services partenaires. Cette interopérabilité assure une expérience uniforme pour les citoyens, tout en garantissant un niveau élevé de sécurité sur l'ensemble des plateformes.
- **API pour développeurs, libre-service et accessibilité :** Les solutions CIAM offrent des outils puissants aux équipes internes et aux utilisateurs finaux. Les API facilitent l'intégration aux applications existantes, les portails en libre-service réduisent le fardeau administratif et les fonctionnalités d'accessibilité permettent à tous les citoyens d'interagir avec les services numériques en toute confiance et de manière autonome.

En résumé, une plateforme CIAM bien conçu permet aux gouvernements de réduire leur exposition aux risques financiers, de renforcer la confiance du public et de fournir des services numériques fluides, sécurisés et accessibles à grande échelle, favorisant ainsi une gouvernance numérique unifiée et centrée sur le citoyen.

Impact opérationnel et financier du CIAM

Fonctionnalité (capacité CIAM)	**Indicateur opérationnel** (efficacité / prestation de services)	**Indicateur financier** (coût / RCI)
Authentification et MFA adaptative	Réduction des incidents liés au piratage de comptes ; augmentation des taux de connexion réussie	Économies sur les remboursements liés à la fraude ; réduction des paiements liés aux violations
Vérification d'identité et intégration	Réduction des incidents liés au piratage de comptes ; Réduction du temps d'intégration par usager	Réduction des coûts d'enquête/ administratifs liés à la fraude ; moins de paiements erronés de prestations
Gestion du cycle de vie des comptes, du consentement et de la confidentialité	Réduction des exceptions lors des audits de conformité ; meilleure transparence et rapidité dans la réponse aux demandes de données des citoyens	Évitement d'amendes pour non-respect de la vie privée ; réduction des coûts de conformité
Détection des fraudes et analyse comportementale	Réduction de la proportion de transactions frauduleuses (en % du total)	Réduction des coûts liés aux incidents de violation de données (coût moyen de 4,88 M$ par violation évitée)
Fédération et interopérabilité	Nombre de services accessibles via l'authentification unique ; taux d'adoption par les usagers	Gains d'efficacité grâce à la consolidation des systèmes ; réduction des coûts d'intégration
API pour développeurs et portails libre-service	Réduction du nombre de demandes de réinitialisation de mot de passe ; appels au service d'assistance par mois	Réduction des dépenses du service d'assistance (économies calculées selon $/ticket × tickets évités)
Fonctionnalités d'accessibilité	Augmentation de l'adoption numérique par les citoyens ; amélioration du taux de complétion des services	Augmentation des revenus de transactions ; amélioration du RCI des services numériques



#5 Avantages commerciaux et leviers de valeur

Soyons francs : l'expression « gestion des identités » ne suscite pas encore l'enthousiasme dans tous les cercles du secteur public. Pour certains, elle évoque simplement un poste budgétaire informatique de plus, loin d'être un levier stratégique capable d'attirer de nouveaux financements. Pourtant, derrière ce jargon technique se cache un système capable d'influencer les budgets, les réputations et même les cycles électoraux. Une solution CIAM bien conçue dépasse largement le cadre de la cybersécurité. Elle génère une valeur commerciale tangible que les directeurs financiers, les dirigeants principaux de l'information et même les auditeurs les plus sceptiques peuvent reconnaître. Voici comment :

- **Réduction des coûts**
  Les violations de données sont coûteuses. Très coûteuses. Comme mentionné précédemment, le coût mondial moyen d'une violation de données s'élève désormais à 4,88 millions de dollars — un record depuis la pandémie (FTC). Chaque incident évité représente des économies substantielles : moins de frais pour les victimes, moins de juristes mobilisés pour analyser les rapports, et moins de gros titres embarrassants dans les médias. Le CIAM permet de réduire l'incidence des violations et leurs conséquences, en diminuante les dépenses liées à la fraude, la charge des enquêtes, ainsi que les coûts juridiques et de notification.

- **Efficacité opérationnelle**
  Chaque demande de réinitialisation de mot de passe oublié grignote le budget et épuise les équipes. Multipliez cela par des dizaines de milliers, et vous obtenez une facture d'assistance qui pourrait financer un centre communautaire tout entier. Le CIAM allège cette charge grâce à l'automatisation de l'intégration, aux portails en libre-service et aux mécanismes intelligents de récupération, transformant les appels de dépannage en exception plutôt qu'en routine. Moins de vérifications manuelles signifie moins de pression sur les équipes de soutien et un service plus rapide pour les citoyens, qui préfèrent passer cinq minutes en ligne plutôt que 45 minutes en attente.

- **Expérience citoyenne et conservation des revenus**
  Considérez les services numériques gouvernementaux comme un produit, et les citoyens comme ses utilisateurs. Et les utilisateurs n'aiment pas les frictions. En rendant les services en ligne intuitifs et accessibles, le CIAM améliore l'expérience utilisateur, permettant aux citoyens de finaliser leurs démarches sans frustration. Il en résulte des taux d'adoption plus élevés, un plus grand nombre de demandes traitées et une confiance renforcée. Les recherches de l'OCDE montrent que les citoyens attendent des services publics numériques qu'ils soient aussi simples et fiables que ceux des banques, des compagnies aériennes et des détaillants en ligne (OECD). Quand l'administration numérique fonctionne bien, les citoyens le remarquent et — reviennent.

- **Réduction des risques réglementaires et politiques**
  Rien ne mine la confiance du public plus rapidement qu'un scandale lié à la confidentialité. Le CIAM intègre des outils de conformité aux réglementations fédérales et provinciales en matière de protection des données, réduisant ainsi les risques d'amendes, d'enquêtes et, pire encore, de conférences de presse embarrassantes. Dans l'arène politique, la réputation est capitale. Une seule erreur peut faire basculer une administration de pionnière du numérique à exemple à ne pas suivre.

Qu'il s'agisse d'économiser des millions en coûts liés aux violations de données ou de transformer les services numériques en une expérience agréable plutôt qu'un casse-tête, le CIAM dépasse largement les attentes. Mais les retours sur investissement dans le monde réel n'ont de poids que s'ils peuvent être mesurés. Des données concrètes, des indicateurs de rendement clairs et des mesures exploitables sont essentiels pour démontrer la valeur du CIAM et obtenir les budgets nécessaires à une transformation numérique durable.

#6 Mesurer le rendement de l'investissement : méthodologie et indicateurs de rendement clés

Aussi convaincante que soit la promesse du CIAM du point de vue citoyen, les décisions budgétaires gouvernementales se résument souvent à une question simple : quel est le rendement de l'investissement ? Pour positionner le CIAM comme un pilier incontournable d'une gouvernance numérique moderne, il est essentiel de démontrer sa valeur à l'aide de données concrètes et de métriques claires.

Indicateurs de rendement clés à surveiller

Pour mesurer la portée du CIAM, les agences doivent suivre des indicateurs dans quatre domaines clés, soit la sécurité, les opérations, l'expérience citoyenne et la conformité :

- **Securité :** nombre d'incidents de violation par an, taux de fraude (en pourcentage des transactions), coût moyen par incident.
- **Opérations :** volume mensuel de demandes d'assistance, fréquence des problèmes de mot de passe, délais d'intégration des utilisateurs.
- **Expérience :** taux d'adoption des services numériques, satisfaction des utilisateurs (par exemple, NPS ou sondages), taux de réussite des transactions en ligne.
- **Conformité :** nombre d'exceptions ou de constats lors des audits, délai moyen de traitement des demandes réglementaires.

Données requises

Ces indicateurs de rendement clés prennent tout leur sens lorsqu'ils sont mesurés par rapport à une base de référence établie. Les agences doivent collecter des données sur :

- les incidents passés et leurs coûts associés (ex. : violations de données, remboursements liés à la fraude).
- les coûts actuels du service d'assistance et les niveaux de dotation.
- les volumes d'utilisateurs et de transactions sur les plateformes numériques.
- les coûts estimés de mise en œuvre et d'exploitation du CIAM.

Calcul du rendement de l'investissement (calcul arithmétique)

Pour aider les parties prenantes à visualiser la valeur du CIAM, une simulation basée sur des estimations peut être utile :

Hypothèses :

- Coût moyen d'une violation de données : **4 880 000 $** (IBM)



- Probabilité annuelle d'une violation : **5%** (estimation interne)
- Coût annuel du CIAM : **500 000 $**
- Réduction estimée du risque ou des répercussions d'une violation grâce au CIAM : **30 %**

Calculs :

1. **Coût annuel de référence d'une violation**
   Avec un coût moyen estimé à 4,88 millions de dollars par violation et une probabilité annuelle de survenue de 5 %, le coût annuel attendu pour une agence s'élève à 244 000 dollars.
   4 880 000 × 0.05 = **244 000 $**

2. **Coût annuel estimé après la mise en place du CIAM**
   En supposant que le CIAM permet de réduire de 30 % la probabilité ou la gravité d'une violation, le coût annuel attendu chute à 170 800 dollars.
   244 000 × (1 - 0.30) = 244 000 × 0.70 = **170 800 $**

3. **Économies annuelles liées à la réduction des violations**
   Cela représente une économie directe de 73 200 dollars par an.
   244 000 - 170 800 = **73 200 $**

4. **Comparaison avec les coûts d'investissement CIAM**
   Avec un investissement CIAM annualisé de 500 000 dollars, les économies liées aux violations ne suffisent pas à elles seules à compenser les dépenses, générant un déficit de 426 800 dollars.
   73 200-500 000 = -**426,800 $**

5. **Le tableau complet**
   Lorsqu'on tient compte de l'ensemble des avantages quantifiables — notamment les économies réalisées sur le service d'assistance, la réduction des remboursements liés à la fraude, l'augmentation du taux d'adoption des services numériques — la perspective change radicalement.
   Par exemple, si ces bénéfices totalisent 600 000 dollars par an, le rendement annuel net grimpe à 173 200 dollars, ce qui représente un rendement du capital investi de 34,6 %.
   73 200 + 600 000 - 500 000 = **173 200 $**
   RCI = 173 200 / 500 000 = **34.6 %**

Même si la prévention des violations constitue un argument de départ convaincant, c'est l'effet cumulatif de tous les bénéfices — moins d'incidents, des services plus rapides, une plus grande satisfaction citoyenne et une conformité renforcée — qui révèle la véritable valeur du CIAM. En combinant des indicateurs financiers à des résultats qualitatifs, tels que le renforcement de la confiance, l'amélioration de l'accessibilité et la réduction du délai de rentabilisation pour les citoyens, les gouvernements peuvent bâtir un argumentaire irréfutable en faveur d'un investissement durable dans le CIAM.

#7 Considérations et risques liés à la mise en œuvre

Parvenir à la phase de mise en œuvre marque une étape décisive dans tout projet de transformation numérique. Si votre équipe est arrivée jusqu'ici, les prochaines décisions seront parmi les plus stratégiques. Vous avez déjà démontré la valeur du CIAM sur le plan financier, mais maximiser le rendement de votre investissement, il est essentiel d'aborder avec rigueur les dimensions techniques, organisationnelles et réglementaires qui conditionneront le succès du déploiement. Une planification réfléchie dans ces domaines permettra une transition fluide depuis les systèmes existants, tout en limitant les perturbations pour le personnel et les citoyens.

- **Intégration avec les systèmes existants et les référentiels d'identité**
  La plupart des gouvernements s'appuient encore sur un ensemble hétérogène de systèmes hérités. Les solutions CIAM les plus performantes proposent des API et des connecteurs compatibles avec les plateformes gouvernementales et les répertoires d'identité courants, ce qui réduit les besoins en développement sur mesure et assure la continuité des services. Le CIAM approprié offrira également une intégration flexible avec les anciens systèmes qui ne reposent pas sur les normes d'authentification modernes, garantissant qu'aucun service critique ne soit exclu.

- **Confidentialité, résidence des données et contraintes d'approvisionnement**
  La confiance du public repose sur le respect des réglementations strictes en matière de confidentialité, de résidence des données et de souveraineté numérique. Une plateforme

CIAM moderne doit offrir des options flexibles de stockage et de traitement des données, y compris l'hébergement régional ou national selon les exigences locales. Les contraintes liées à l'approvisionnement ajoutent une complexité supplémentaire : les fournisseurs doivent souvent figurer sur des listes de fournisseurs agréés, répondre aux exigences des appels d'offres ou des demandes de propositions, et se conformer à des normes de sécurité rigoureuses.

- **Gestion du changement : migration et sensibilisation des citoyens**
  L'adoption du CIAM ne concerne uniquement la technologie; elle concerne aussi les utilisateurs. La migration des identifiants depuis les systèmes existants, la communication claire autour des nouveaux processus de connexion et l'assurance d'une accessibilité sur tous les points de contact numériques sont des éléments clés. Une intégration fluide et bien pensée réduit les frictions et favorise une adoption rapide.

- **Critères de sélection des fournisseurs**
  Optez pour un partenaire qui possède une expérience avérée dans les déploiements publics et une vision stratégique alignée avec vos objectifs numériques. Priorisez les solutions interopérables, évolutives, sécurisées, respectueuses de la vie privée et inclusives, dotées d'outils intuitifs en libre-service pour les citoyens comme pour les administrateurs. Un fournisseur qui comprend les spécificités du secteur public sera un atout majeur pour garantir le succès du déploiement.

En définitive, la mise en œuvre du CIAM ne relève pas d'un simple exercice technique. Lorsqu'un gouvernement coordonne avec intention ses équipes, ses processus, ses plateformes et l'expérience utilisateur, il jette les bases d'une stratégie d'identité numérique qui résiliente et durable.

#8 Approvisionnement et coût total de possession

Comprendre le coût total de possession d'une solution CIAM est essentiel pour prendre des décisions d'achat éclairées et garantir la viabilité à long terme. Le coût total de possession englobe à la fois les coûts directs et les dépenses récurrentes, ainsi que le modèle de mise en œuvre choisi.

Principales catégories de coûts

Les agences doivent prendre en compte l'ensemble des coûts tout au long du cycle de vie du CIAM :

- **Licences :** abonnements logiciels ou licences perpétuelles nécessaires à l'utilisation de la plateforme.
- **Intégration et déploiement :** services de mise en œuvre, configuration des API et connexion aux systèmes ou répertoires existants.
- **Vérification et authentification d'identité :** coûts liés à la validation des documents, à l'authentification basée sur les connaissances ou à l'utilisation de la biométrie.
- **Exploitation et soutien continu :** ressources dédiées à la maintenance, à la surveillance et au soutien technique.
- **Surveillance des fraudes :** abonnements à des outils d'analyse avancée, de suivi comportemental et de détection des anomalies.

Modèles et mises en oeuvre

Le choix du modèle de mise en œuvre a une incidence sur le coût et la complexité de la mise en œuvre. Chacun présente ses propres avantages et inconvénients :

- **SaaS par abonnement :** offre un déploiement rapide, des coûts prévisibles et des mises à jour automatiques. Idéal pour les agences qui recherchent un déploiement rapide avec un

investissement initial minimal.

- **Solutions gérées ou hébergées :** offrent un équilibre entre contrôle et assistance du fournisseur. Utile pour les juridictions nécessitant une certaine personnalisation tout en réduisant la charge opérationnelle.
- **Déploiement sur site :** garantit un contrôle maximal sur les données sensibles, mais s'accompagne d'une complexité accrue, des délais plus longs et des coûts de maintenance plus élevés.

En évaluant soigneusement les catégories de coûts en fonction du modèle de mise en œuvre, les agences peuvent éviter les pièges cachés et choisir une approche CIAM qui équilibre les besoins de l'organisation et ceux des citoyens qu'elles servent. L'option la plus économique n'est pas toujours la plus judicieuse. Le CIAM est plus qu'un logiciel. C'est un levier de transformation, un outil d'engagement citoyen, et un investissement durable qui portera ses fruits pendant de nombreuses années.

#9 Études de cas et cas d'utilisation

L'intégration du CIAM dans des contextes réels révèle toute sa capacité à moderniser les services publics. Les exemples suivants illustrent les résultats observés avant et après la mise en œuvre.

Qu'il s'agisse d'agences fiscales, de services sociaux ou de soins de santé, le CIAM renforce la sécurité, améliore l'expérience des citoyens et optimise l'efficacité opérationnelle dans l'ensemble du secteur public.

Portail fiscal citoyen

Avant la mise en place du CIAM : les demandes frauduleuses et les usurpations d'identité entraînaient des retards dans le versement des prestations et une hausse des coûts d'enquête.

Après la mise en place du CIAM : la vérification avancée de l'identité et l'analyse comportementale ont permis de réduire les demandes frauduleuses de 35 %, accélérant ainsi la distribution des prestations légitimes et diminuant les dépenses opérationnelles.

Prestations sociales

Avant la mise en place du CIAM : les demandes en double ou les identités synthétiques entraînaient des erreurs dans l'attribution des prestations et une surcharge administrative.

Après la mise en place du CIAM : la vérification d'identité dès l'inscription a permis d'éliminer 90 % des demandes en double, améliorant ainsi la précision, la conformité et la confiance des citoyens.

Portails santé/patients

Avant la mise en place du CIAM : les patients rencontraient des difficultés de connexion, la gestion des consentements était incohérente et les données sensibles étaient exposées à des risques.

Après la mise en place du CIAM : l'authentification sécurisée et la gestion centralisée des consentements ont augmenté l'adoption du portail de 40 %, réduit les appels de réinitialisation de mot de passe de 25 %, et renforcé la conformité aux réglementations en matière de confidentialité.

S'il y a une leçon à tirer des données et des exemples partagés, c'est que les chiffres parlent ne mentent pas. Avec les bons outils CIAM en place, les organismes publics peuvent aller bien au-delà de la simple gestion des risques : ils peuvent améliorer activement leurs services, protéger les citoyens et produire des résultats concrets qui font une réelle différence dans la vie des gens.

#10 Cadre stratégique pour les décideurs

La réussite d'une mise en œuvre du CIAM repose sur une approche méthodique. Les gouvernements peuvent s'appuyer sur un cadre structuré pour orienter leurs décisions, évaluer les résultats et évoluer avec assurance :

- **Étape 1 : Recenser les services liés à l'identité et les points de friction**
  Commencez par dresser l'inventaire de tous les services numériques qui s'appuient sur la vérification d'identité, l'authentification ou la gestion des accès. Repérez les processus actuels qui créent des obstacles, des risques ou des inefficacités tant pour le personnel que pour les citoyens. Ces points de friction, souvent sous-estimés, peuvent freiner considérablement l'adoption des services numériques.

- **Étape 2 : Évaluer les coûts des incidents et les indicateurs de friction**
  Évaluez les effets des systèmes existants à l'aide d'indicateurs clés : nombre d'incidents de sécurité, pertes liées à la fraude, volume des demandes au service d'assistance, taux de réussite des transactions en ligne. Ces données de référence fournira un point de comparaison solide pour démontrer la valeur ajoutée du CIAM.

- **Étape 3 : Lancer un projet pilote ciblé**
  Choisissez un service à fort enjeu et déployez un projet pilote CIAM sur une période de 3 à 6 mois. Définissez des indicateurs de rendement clairs avant le lancement, notamment en matière de sécurité, d'efficacité opérationnelle et d'expérience utilisateur. Ce projet pilote permettra de valider les approches d'intégration, de tester les stratégies de gestion du changement et d'optimiser les flux de travaux.

- **Étape 4 : Déployer, mesurer et communiquer les résultats**
  Déployez progressivement la solution à d'autres services, en assurant un suivi continu des indicateurs de rendement clés et en ajustant les paramètres au besoin. Partagez les résultats en interne pour favoriser l'adhésion, consolider les arguments financiers et opérationnels et positionner le CIAM comme un pilier de la transformation numérique gouvernementale.

Commencez modestement, mesurez rigoureusement, et suivez une démarche structurée. Grâce à des données probantes à l'appui, les gouvernements peuvent transformer le CIAM d'un concept prometteur en une réalité, en intégrant une gestion des identités sécurisée et centrée sur les citoyens dans l'ensemble de leur écosystème numérique.

Conclusion :

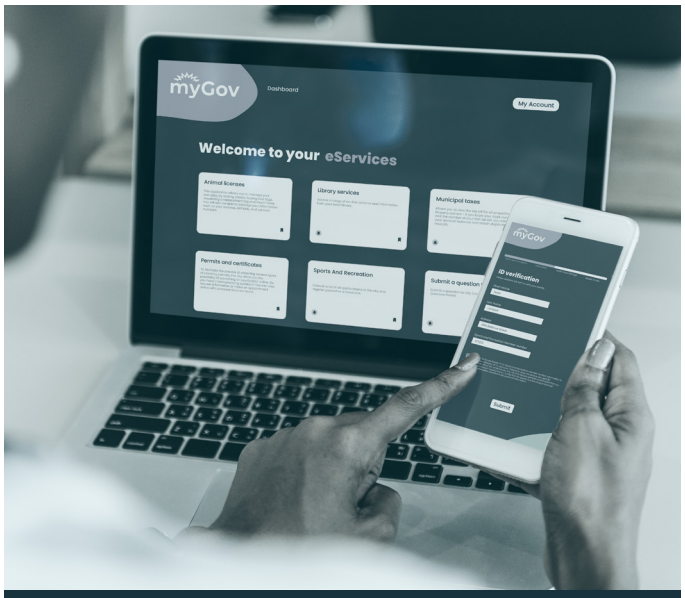
Comme tout parcours de transformation, celui des services publics numériques comporte son lot d'obstacles, d'enseignements et de scepticismes. Mais c'est la volonté de servir le bien commun qui fait avancer l'histoire. En misant sur un avenir numérique sûr, équitable et accessible à tous — et en investissant intelligemment — les agences peuvent faire du CIAM non plus un héros méconnu, mais un véritable moteur de la modernisation gouvernementale.

La question est simple : votre agence est-elle prête à franchir le pas ?

> **Contactez-nous pour découvrir les solutions de Portage CyberTech et amorcer votre propre transformation numérique grâce à une mise en œuvre stratégique du CIAM.**

Annexe :
Sources de données et lectures recommandées

- IBM – Rapport sur le coût moyen des violations de données. (IBM)
- Commission fédérale du commerce – Données sur les signalements de fraude et les pertes associées. (Federal Trade Commission)
- Grand View Research – Prévisions du marché pour le CIAM (taille et croissance). (Grand View Research)
- TransUnion – Statistiques sur la fraude d'identité dans le secteur public (taux de fraude présumé de 6,7 % en 2024). (TransUnion)
- Nations Unies – Enquête sur l'administration en ligne 2024. (UN DESA)
- OCDE – Indice de l'administration numérique 2023. (OECD)



Prêt à vous lancer ?

Explorez des plateformes CIAM conçues spécifiquement pour le secteur public et adaptées aux objectifs stratégiques de votre organisme.

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