Livre blanc

Gestion des identités et des accès clients

Avantages de la gestion des identités et des accès client pour les gouvernements nationaux, provinciaux et municipaux

PORTAGE cybertech

portagecybertech.com
info@portagecybertech.com

Gestion de l'identité et gestion des accès

Avantages de la gestion des identités et des accès client pour les gouvernements nationaux, provinciaux et municipaux

Aperçu

Les gouvernements à l'échellenationale, provinciale et municipale sont confrontés à des défis croissants en ce qui a trait à la prestation de services numériques sécurisés, transparents et conviviaux. Le désir d'accélérer la transition des services vers les plateformes en ligne, que ce soit pour répondre à la demande de la clientèle ou pour améliorer l'efficacité opérationnelle, nécessite une stratégie de gestion rigoureuse des identités pour protéger les données sensibles des citoyennes et citoyens tout en garantissant un accès facile aux services essentiels. Les solutions de gestion des identités et des accès client (CIAM) destinées au secteur public, telles que CitizenOne de Portage CyberTech, offrent une plateforme complète pour renforcer la cybersécurité, améliorer l'expérience des citoyennes et citoyens et garantir le respect des règlements stricts en matière de confidentialité. En mettant en œuvre une solution CIAM adaptée à leurs besoins spécifiques, les gouvernements peuvent atténuer de façon efficace les risques de sécurité, rationaliser les processus d'authentification et renforcer la confiance du public envers les services numériques. Le présent livre blanc explique les principaux avantages de la mise en œuvre d'un système CIAM dans le secteur public, en montrant comment il peut renforcer la sécurité, améliorer l'efficacité et accélérer la transformation numérique des activités gouvernementales.

La gestion des identités et des accès client pour le secteur public

La gestion des identités et des accès client destinée au secteur public contraste fortement avec celle destinée au secteur privé, principalement en raison de la diversité des parties prenantes, des objectifs et des cadres réglementaires concernés. Dans le secteur public, l'objectif principal consiste à assurer un accès équitable aux services et à respecter rigoureusement la réglementation gouvernementale et les lois sur la protection des données. Les organisations du secteur public sont au service d'un large éventail de citoyennes et citoyens dont le niveau de littératie numérique et de compétences technologiques varie. Par conséquent, il devient primordial de concevoir des systèmes qui privilégient l'accessibilité, la convivialité et la sécurité, tout en garantissant la transparence et la responsabilité. De plus, les solutions CIAM du secteur public doivent respecter des réglementations strictes, comme le Règlement général sur la protection des données, la Health Insurance Portability and Accountability Act (HIPAA) et d'autres lois sur la protection des données régissant la prestation de services publics.

En revanche, la gestion des identités et des accès client pour le secteur privé est principalement motivée par des objectifs commerciaux, tels que l'amélioration de l'expérience client, l'optimisation des taux de conversion et la croissance des revenus. Elle se concentre généralement sur la personnalisation du parcours de l'utilisateur grâce à des informations basées sur les données, dans le but de fidéliser davantage les clients et d'augmenter leur valeur à long terme. Les entreprises privées peuvent également mettre en œuvre des technologies avancées telles que l'IA et l'apprentissage automatique pour prévoir et influencer le comportement des utilisateurs. Bien que la confidentialité et la sécurité soient des facteurs importants à prendre en considération dans le secteur privé, la pression réglementaire est généralement moins forte, ce qui permet une plus grande flexibilité dans la manière dont les données des clients sont recueillies et utilisées. Par conséquent, la gestion des identités et des accès client dans le secteur privé est souvent axée sur la croissance de l'entreprise, tandis que celle dans le secteur public privilégie l'accessibilité, la sécurité et la conformité réglementaire.

Principaux avantages de la mise en œuvre d'un système CIAM pour le secteur public

1. Sécurité renforcée et prévention de la fraude

Les solutions CIAM du secteur public utilisent des mécanismes de sécurité avancés pour protéger les données des citoyennes et citoyens et du gouvernement et empêcher tout accès non autorisé. Des fonctionnalités comme l'authentification multifactorielle, l'authentification unique et les contrôles d'accès adaptatifs renforcent la sécurité tout en préservant la facilité d'utilisation. La mise en œuvre de telles fonctionnalités permet aux gouvernements de réduire considérablement la fraude grâce à des mesures d'authentification strictes, de détecter et atténuer les cybermenaces à l'aide de l'analyse d'identité et de garantir un accès sécurisé aux services numériques. La vérification de l'identité, la détection des fraudes et l'authentification basée sur les risques améliorent davantage les processus de vérification, garantissant que seuls les utilisateurs légitimes y ont accès. De plus, un CIAM adapté aux besoins spécifiques du secteur public prend en charge un modèle de sécurité à vérification systématique, par lequel tous les utilisateurs et les programmes ou systèmes doivent être systématiquement authentifiés afin de minimiser les risques de sécurité. Les gouvernements peuvent également utiliser l'analyse de données afin de détecter les menaces internes et prendre des mesures proactives contre les violations potentielles de données.

2. Une expérience utilisateur améliorée

Une expérience utilisateur positive est essentielle afin de favoriser la confiance et l'engagement envers les services gouvernementaux. Une solution CIAM spécialement conçue pour le secteur public simplifie les processus d'authentification grâce à une gestion unifiée de l'identité des citoyennes et citoyens sur plusieurs services au moyen d'une authentification unique. Cela permet aux utilisateurs d'accéder à divers services gouvernementaux avec un seul ensemble d'identifiants, ce qui simplifie l'expérience utilisateur. Les fonctionnalités en libre-service permettent aux citoyennes et citoyens de gérer leurs comptes, de réinitialiser leurs mots de passe et de mettre à jour leurs profils de manière indépendante, ce qui diminue le recours à l'assistance technique. Les méthodes d'authentification fluides, y compris les connexions tierces, favorisent également la convivialité. L'authentification adaptative et la fédération d'identité permettent de personnaliser l'expérience utilisateur tout en garantissant la sécurité. De plus, ces solutions prennent en charge plusieurs méthodes d'authentification et fournisseurs d'identité, ce qui réduit les obstacles à l'accès. Les fonctionnalités d'accessibilité pour les personnes handicapées garantissent le respect des normes d'inclusion, rendant les services numériques plus équitables, ce qui est essentiel dans le secteur public.

3. Conformité à la réglementation en matière de confidentialité et de sécurité

Les gouvernements doivent se conformer à des réglementations strictes en matière de confidentialité et de sécurité des données, telles que le Règlement général sur la protection des données (RGPD), la California Consumer Privacy Act (CCPA) et diverses politiques régionales. Une solution CIAM correctement structurée facilite la conformité grâce à des cadres de gestion des consentements robustes qui régissent la collecte et le partage des données. Les mécanismes de cryptage sécurisent les renseignements confidentiels des citoyennes et citoyens, tout en respectant les exigences de sécurité standards de l'industrie. Par ailleurs, les solutions CIAM fournissent un registre des audits et des capacités de production de rapports détaillés, garantissant que les gouvernements peuvent respecter et démontrer leur conformité aux obligations réglementaires. La prise en charge des exigences de résidence des données permet de se conformer aux lois locales et internationales sur la protection de la vie privée, tandis que des contrôles d'accès granulaires empêchent le personnel non autorisé d'accéder aux renseignements confidentiels. En améliorant la transparence dans l'utilisation et le stockage des données, les solutions CIAM du secteur public favorisent la confiance du public envers les services numériques gouvernementaux.

4. Efficacité opérationnelle et économies

Les anciennes solutions de gestion des identités sont coûteuses et inefficaces, nécessitent souvent une intervention manuelle importante et présentent de nombreux défis en matière d'évolutivité. Lorsqu'elles sont correctement mises en œuvre, les solutions CIAM pour le secteur public peuvent automatiser la vérification des identités et le contrôle des accès, ce qui réduit considérablement la charge de travail des équipes informatiques et les dépenses opérationnelles. Les processus automatisés réduisent les demandes d'assistance liées à la réinitialisation des mots de passe et aux problèmes d'authentification, permettant ainsi aux équipes informatiques de se concentrer sur les tâches prioritaires. Ces solutions s'intègrent facilement à l'infrastructure informatique existante des administrations, garantissant ainsi l'évolutivité et la rentabilité. En remplaçant les systèmes de gestion des identités obsolètes, les administrations peuvent réduire les coûts associés aux failles de sécurité et aux inefficacités. Une interopérabilité accrue entre les services de l'administration permet d'éliminer les processus redondants de vérification des identités, ce qui rationalise la prestation de services. Ainsi, la gouvernance centralisée des identités améliore l'efficacité administrative et assure la cohérence des politiques de sécurité entre les ministères.

5. Soutien aux initiatives de transformation numérique

Alors que les gouvernements adoptent des technologies de ville intelligente et intensifient les initiatives d'administration en ligne, l'utilisation d'un canal Web et d'une solution CIAM axée sur le secteur public joue un rôle essentiel dans la mise en place d'identités numériques sécurisées pour les services en ligne et mobiles. Une interopérabilité transparente et des contrôles appropriés entre les organismes gouvernementaux facilitent le partage efficace des données tout en maintenant les normes de sécurité et de confidentialité. En plus de soutenir les technologies émergentes telles que la vérification d'identité par les utilisateurs et les identifiants basés sur la chaîne de blocs, elles améliorent la fiabilité et l'efficacité de la gestion des identités numériques. En proposant des interfaces d'authentification multilingues et adaptatives, la solution garantit l'inclusion des populations diverses. Par ailleurs, la surveillance continue et les mécanismes de réponse automatisés renforcent la résilience de la cybersécurité, atténuant ainsi les menaces avant qu'elles ne s'intensifient, et établissent une base solide pour les innovations futures en matière de cybergouvernance.

6. Évolutivité et pérennité

Les gouvernements ont besoin de solutions de gestion des identités évolutives pour s'adapter à des bases d'utilisateurs croissantes et à des services numériques en constante évolution. L'approche infonuagique d'une solution CIAM moderne et axée sur le secteur public facilite l'expansion tout en maintenant les performances et la sécurité. Les solutions d'identité fédérée permettent la collaboration entre les organismes publics, ce qui permet une authentification transparente entre plusieurs territoires de compétence. Une solution CIAM orientée vers l'avenir et axée sur le secteur public anticipe la nécessité de s'intégrer aux nouveaux cadres d'identité numérique et aux initiatives nationales d'identification, garantissant ainsi l'adaptabilité aux futurs programmes gouvernementaux. Les protocoles de sécurité prêts pour l'avenir permettent aux gouvernements de faire face de manière proactive à l'évolution des cybermenaces et aux changements réglementaires. Grâce à l'authentification mobile et aux capacités d'accès à distance, les solutions CIAM garantissent l'inclusion numérique pour permettre aux citoyennes et citoyens d'accéder aux services en toute sécurité depuis n'importe quel appareil ou endroit.

7. Renforcer la transparence et la confiance du public

La confiance est fondamentale pour une gouvernance numérique réussie. Une solution CIAM, adaptée aux besoins du gouvernement, renforce la confiance du public en assurant la transparence dans la manière dont les données personnelles sont collectées, conservées et utilisées. Les citoyennes et citoyens peuvent gérer leurs préférences en matière de consentement et d'accès aux données, ce qui renforce leur contrôle sur les informations personnelles. En mettant en place des mesures visibles et transparentes dans le cadre de leur mise en œuvre de la gestion des identités et des accès client, les gouvernements démontrent leur engagement en faveur de la sécurité et de la confidentialité. Le système contribue à réduire le vol d'identité et la fraude, renforçant ainsi la crédibilité des services publics numériques. De plus, des pistes de vérification et des communications claires concernant les politiques de sécurité tiennent les citoyennes et citoyens informés de la manière dont leurs données sont protégées. En incluant judicieusement la transparence dans ses dispositions de sécurité, un gouvernement peut favoriser un écosystème numérique de confiance pour ses services.

Études de cas

Vous trouverez ci-dessous deux études de cas anonymisées illustrant ces avantages.

Un gouvernement d'État améliore les services à la population citoyenne

Selon GovTech, un gouvernement d'État américain a cherché à moderniser ses services numériques afin de fournir à sa population citoyenne un accès sécurisé et transparent à divers programmes de l'État. En mettant en œuvre un système CIAM, l'État a obtenu des améliorations significatives

- Augmentation de l'adoption par les utilisateurs : L'État a connu une augmentation de 25 % des inscriptions d'utilisateurs au cours des six premiers mois, attribuée à la simplification des processus d'intégration et à l'amélioration de l'expérience utilisateur.
- Sécurité renforcée : l'intégration de l'authentification multifactorielle a réduit de 40 % les incidents d'accès non autorisé, renforçant ainsi la confiance des citoyennes et citoyens dans les services numériques.
- Efficacité opérationnelle : les processus automatisés de vérification d'identité ont réduit la charge de travail manuel de 30 %, ce qui a permis au personnel de se concentrer sur des initiatives plus stratégiques.

Ces résultats soulignent l'efficacité des solutions CIAM dans la transformation des services numériques du secteur public.

Une autorité municipale simplifie l'accès de la population citoyenne

GovTech rapporte qu'une autorité municipale visait à fournir aux résidentes et résidents un accès unifié aux services locaux, tels que le paiement des impôts, les demandes de permis et les programmes communautaires. La mise en œuvre d'un système CIAM a donné des résultats remarquables

- Accès unifié : Les résidents pouvaient accéder à plusieurs services par un portail d'authentification unique, ce qui a entraîné une augmentation de 50 % de l'utilisation du portail et une diminution de 35 % des appels d'assistance pour des problèmes de connexion.
- Protection des données améliorée : La conformité au Règlement général sur la protection des données (RGPD) a été atteinte, garantissant que 100 % du traitement des données des utilisateurs répondait à des normes de confidentialité strictes.
- Satisfaction des utilisateurs : Les enquêtes ont indiqué une amélioration de 20 % dans la satisfaction des citoyennes et citoyens à l'égard des services numériques, attribuable à un accès simplifié et sécurisé.

Ces études de cas démontrent que la mise en œuvre de solutions CIAM dans le secteur public contribue à améliorer la sécurité et l'efficacité opérationnelle, et à augmenter la satisfaction des utilisateurs.

Mise en œuvre de la gestion des identités et des accès client dans le secteur public : défis et considérations

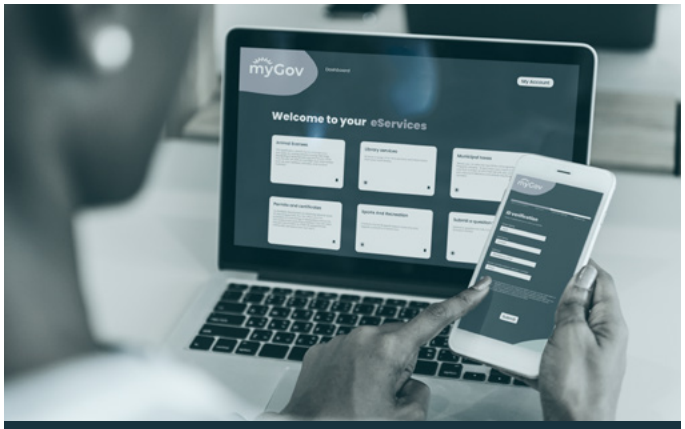
Bien que les solutions CIAM offrent de nombreux avantages, elles présentent plusieurs défis pour les gouvernements. La complexité de l'intégration constitue un obstacle important, qui nécessite une planification minutieuse pour assurer la compatibilité avec les systèmes existants. Il est impératif de choisir la bonne solution de gestion des identités et des accès client, car de nombreux systèmes ne sont pas adaptés aux complexités et aux exigences commerciales uniques des gouvernements.

L'adoption par les utilisateurs constitue un autre facteur essentiel : il est primordial d'informer les citoyennes et citoyens des avantages que présentent les identités numériques sécurisées pour favoriser une acceptation généralisée. Les contraintes budgétaires doivent également être prises en compte, car il faut équilibrer l'investissement et d'autres priorités de service. Par ailleurs, l'évolution des cybermenaces nécessite des mises à jour continues et l'intégration de capacités de renseignement sur les menaces. L'accessibilité et l'inclusion devraient être une priorité dans le secteur public pour s'assurer que la solution CIAM s'adresse à toute la population citoyenne, y compris les personnes qui ont un handicap ou une littéracie numérique limitée. Enfin, des politiques de gouvernance des données rigoureuses doivent être établies pour définir la propriété des données, leur conservation et les stratégies de conformité pour obtenir du succès à long terme.

Conclusion et recommandations

L'adoption d'une solution CIAM dans le secteur public offre aux gouvernements à l'échelle nationale, provinciale et municipale une occasion transformatrice de renforcer la sécurité, de rationaliser les interactions numériques et de gagner la confiance du public. En mettant en œuvre des pratiques modernes de gestion des identités, les gouvernements peuvent protéger les données sensibles des citoyennes et citoyens, se conformer aux exigences réglementaires et améliorer l'efficacité opérationnelle. À mesure que les services numériques se développent, une solution CIAM adaptée constitue la base de plateformes gouvernementales sécurisées, évolutives et conviviales. Investir dans cette technologie est une décision stratégique qui permet aux gouvernements de gérer la transformation numérique tout en maintenant les normes les plus élevées en matière de sécurité, d'accessibilité et de satisfaction des citoyennes et citoyens.

De nombreux projets de gestion des identités et des accès client dans le secteur public échouent, souvent avec de graves conséquences. Portage CyberTech offre une solution prête à déployer et de qualité opérateur qui réduit considérablement les risques associés à ces mises en œuvre. Dotée d'une expérience utilisateur avancée et testée par les citoyennes et citoyens, avec des taux d'adoption dépassant 75 % dans les territoires de compétence où elle a été déployée, notre solution garantit une expérience utilisateur fluide. Avec des antécédents démontrés de réussite, elle offre un retour sur investissement rapide. En outre, notre approche permet aux organisations de réaliser rapidement des preuves de concept, de valider des idées et d'affiner efficacement leur stratégie de production.



À propos de CitizenOne

CitizenOne est une solution CIAM de confiance conçue pour répondre aux besoins spécifiques du secteur public.

CitizenOne regroupe tous les services dans un tableau de bord convivial et exploite des fonctionnalités puissantes pour simplifier l'expérience utilisateur et garantir le respect des obligations en matière de confidentialité et de sécurité des données. Grâce à une connexion sécurisée unique, les citoyennes et citoyens peuvent facilement trouver les services et s'y abonner, tandis que ses capacités de configuration en libre-service permettent de regrouper et de fournir rapidement des services par le canal numérique, avec une sécurité sans précédent.

Pour en savoir plus, rendez-vous au https://www.portagecybertech.com/fr/produits/citizenone

Prochaines étapes ?
Des questions ?

En savoir plus sur les solutions de 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.