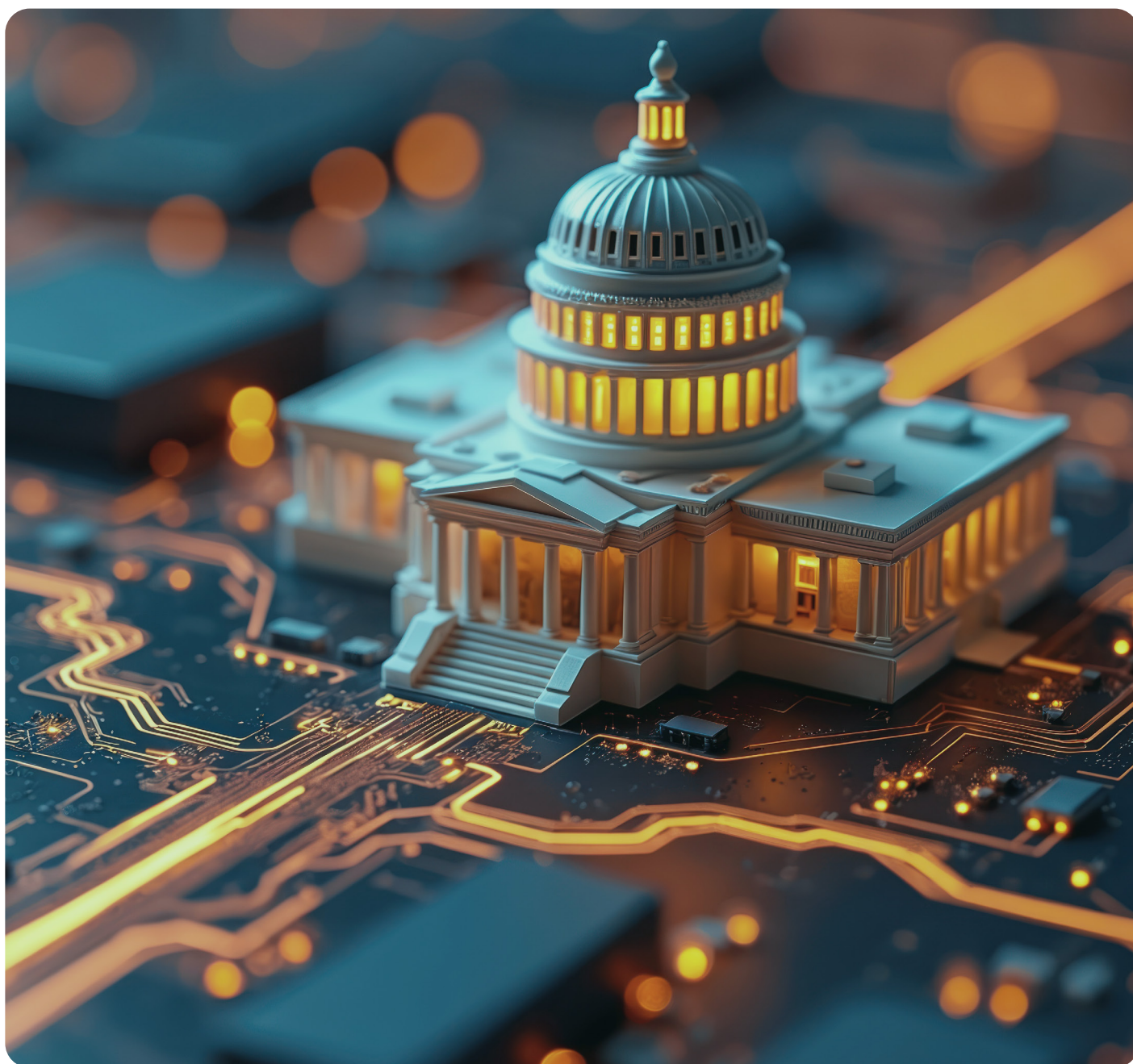


# Guide d'achat des solutions CIAM pour les administrations publiques

Comment choisir la plateforme de gestion des identités et des accès adaptée à votre organisation



# Résumé

Les administrations publiques sont soumises à une pression croissante pour offrir aux citoyens des services numériques sécurisés, accessibles et dignes de confiance. L'identité est au cœur de cette transformation : elle constitue la passerelle entre les citoyens et les services dont ils dépendent. Le choix d'une plateforme de gestion des identités et des accès clients (CIAM) adéquate est une décision stratégique qui influe sur l'adoption des services, la confidentialité, l'efficacité opérationnelle, la gestion des risques et la confiance du public.

Le présent guide vise à aider les dirigeants du secteur public, les responsables du numérique, les architectes et les équipes d'approvisionnement à :

- comprendre ce qu'est la gestion des identités et des accès clients et pourquoi elle est importante pour les administrations publiques;
- cerner les exigences propres à la gestion des identités dans le secteur public;
- évaluer les solutions CIAM à l'aide de critères clairs et pratiques;
- éviter les pièges courants lors de la sélection d'une plateforme CIAM;
- déterminer avec assurance si une solution axée sur les administrations publiques, comme CitizenOne, convient à leurs besoins.

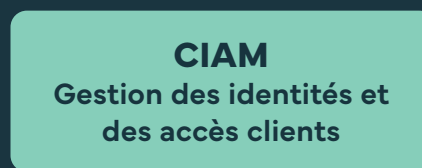
*En comprenant les défis particuliers auxquels les administrations publiques sont confrontées en matière d'identité, les décideurs peuvent choisir une plateforme CIAM capable de soutenir des services numériques sécurisés, inclusifs et évolutifs pour des années à venir.*

## Relier les citoyens aux services grâce au CIAM

L'identité constitue la passerelle entre les citoyens et les services essentiels.



Citoyens et entreprises



# 1 Qu'est-ce que le système CIAM ?

La gestion des identités et des accès clients (CIAM) permet aux organisations de gérer de façon sécurisée les identités d'un vaste bassin d'utilisateurs externes. Dans le secteur public, il s'agit notamment des citoyens, des résidents, des entreprises et d'autres parties prenantes publiques.

Contrairement à la gestion traditionnelle des identités et des accès (IAM), qui est axée sur les employés et les utilisateurs internes, la gestion des identités et des accès

clients (CIAM) est conçue pour :

- une mise à l'échelle massive (des centaines de milliers à des millions d'utilisateurs);
- des services numériques destinés au grand public;
- la gestion de données sensibles et du consentement;
- des expériences utilisateur fluides et sans friction.
- l'instauration de la confiance et la promotion de l'adoption.

# 2 Pourquoi le système CIAM est essentiel pour les administrations publiques

À mesure que les services se numérisent à l'échelle des ministères, des agences et des différents paliers de l'administration publique, l'identité devient le fil conducteur qui assure la cohérence entre l'ensemble des services. En l'absence d'une solution CIAM :

- les citoyens doivent gérer plusieurs identifiants et mots de passe;
- l'adoption des services demeure faible en raison des frictions et de la confusion;
- les canaux de soutien sont surchargés;

- les organismes dupliquent les infrastructures d'identité, ce qui augmente les coûts et les risques;
- la confiance du public s'érode en raison d'une expérience utilisateur déficiente ou de préoccupations liées à la confidentialité.

*Une plateforme CIAM de calibre gouvernemental fournit une assise unifiée, sécurisée et axée sur la confidentialité pour l'accès des citoyens, permettant des interactions fluides et cohérentes entre les différents programmes et services.*

# 3 CIAM gouvernemental et IAM traditionnel

De nombreuses administrations publiques tentent de réutiliser leurs plateformes IAM internes pour des cas d'utilisation destinés aux citoyens ou d'adapter des solutions CIAM commerciales conçues pour le commerce de détail ou les services financiers. Ces approches ne répondent toutefois que rarement aux exigences propres au secteur public.

Domaine	IAM d'entreprise	CIAM gouvernemental
Utilisateurs principaux	Employés	Citoyens et résidents
Échelle	Des milliers	De centaines de milliers à des millions
Priorité à l'expérience utilisateur et à la confiance	Faible	Élevée
Confidentialité et consentement	Limités	Capacités de base
Services assistés	Rares	Essentiels
Accessibilité	Non prioritaire	Exigée par la loi
Interopérabilité	Systèmes internes	Multi-agences, multi-plateformes

Une plateforme CIAM spécialement conçue pour le secteur public reconnaît que les citoyens ne sont pas des employés et ne doivent pas être traités comme tels. Les interactions gouvernementales liées à l'identité doivent accorder la priorité à la confiance, à l'accessibilité, à la transparence, à la sécurité et à l'inclusion.

# 4 Exigences fondamentales d'une solution CIAM gouvernementale

Lorsqu'ils évaluent des plateformes CIAM, les pouvoirs publics doivent examiner les solutions à la lumière d'un ensemble d'exigences fondamentales qui reflètent les réalités de la prestation de services dans le secteur public.

De nombreuses solutions CIAM sur le marché ont été conçues pour soutenir des objectifs commerciaux, tels que la conversion des clients, l'analyse marketing et la croissance du chiffre d'affaires. La solution CIAM gouvernementale doit répondre à un ensemble de résultats très différent. Les plateformes d'identité du secteur public doivent fonctionner à très grande échelle, respecter des obligations strictes en matière de confidentialité et d'accessibilité, soutenir les services assistés et constituer une infrastructure numérique à

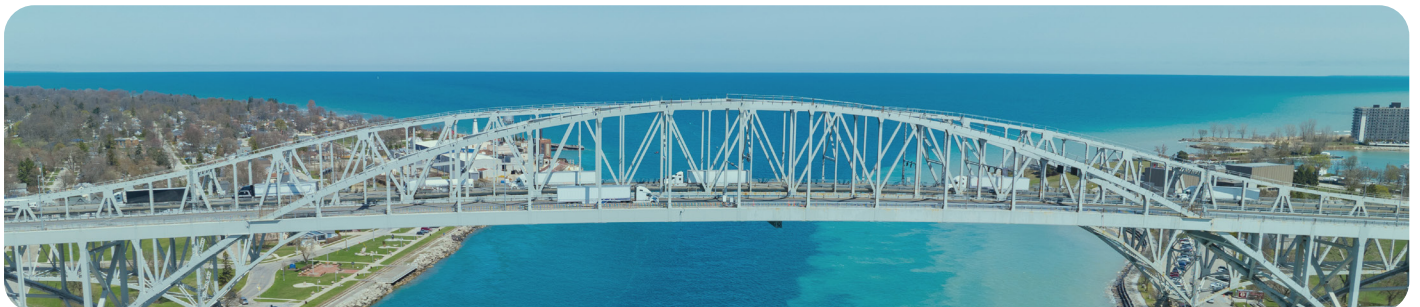
long terme, plutôt que de simples outils d'engagement à court terme.

*Par conséquent, toutes les solutions CIAM ne conviennent pas également aux cas d'utilisation des administrations publiques. Les agences doivent évaluer les plateformes avec rigueur afin de s'assurer qu'elles répondent aux exigences opérationnelles, réglementaires et de confiance associées à la prestation de services aux citoyens, aux résidents et aux entreprises.*

## 4.1 Expérience citoyenne

Une solution CIAM efficace doit réduire les frictions et favoriser l'adoption :

Capacité	Pourquoi est-ce important ?
Inscription et connexion simples et intuitives	La réduction des frictions lors de l'inscription et de la connexion favorise l'adoption des services et réduit les demandes de soutien.
Modèles UX familiers et modernes	Les citoyens s'attendent à une expérience comparable à celle des applications grand public modernes. Une mauvaise expérience utilisateur nuit à la confiance et à l'adoption.
Intégration progressive (recueillir uniquement l'information nécessaire)	La collecte d'un minimum d'information au départ améliore les taux de finalisation des inscriptions et réduit les abandons.
Expérience cohérente entre les services et les canaux	Les citoyens interagissent avec de nombreux programmes gouvernementaux. Une expérience d'identité cohérente réduit la confusion et renforce la confiance.
Interfaces adaptées aux appareils mobiles et accessibles	Bon nombre de citoyens accèdent aux services publics à partir d'appareils mobiles. Une conception accessible garantit le respect des normes d'accessibilité et une prestation inclusive.



## 4.2 Confidentialité, consentement et confiance

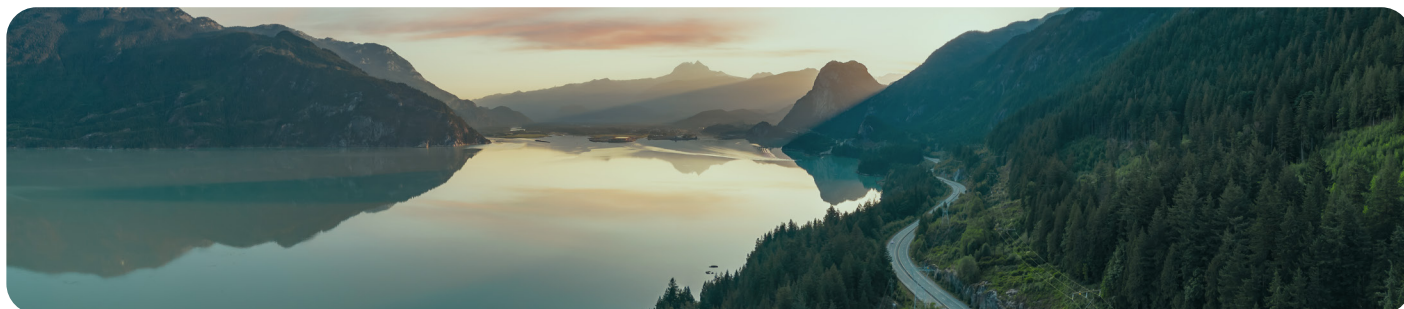
La confiance du public est non négociable. Une solution CIAM doit prendre en charge :

Capacité	Pourquoi est-ce important
Gestion explicite du consentement	Les citoyens doivent être en mesure de comprendre clairement comment leurs données sont utilisées et en garder le contrôle. Un consentement transparent renforce la confiance et favorise la conformité.
Contrôles transparents de l'utilisation des données	La visibilité sur l'utilisation des renseignements personnels aide les gouvernements à maintenir la reddition de comptes et la confiance des citoyens.
Architecture axée sur la protection de la vie privée dès la conception	La protection de la vie privée doit être intégrée dès la conception du système afin d'assurer la conformité aux cadre réglementaires en constante évolution (p. ex., RGPD, CCPA, LPRPDE).
Conformité aux obligations du secteur public en matière de protection de la vie privée	Les gouvernements doivent se conformer à la législation en matière de protection de la vie privée, aux exigences de résidence des données et aux cadres de sécurité qui régissent les renseignements des citoyens.

## 4.3 Sécurité et garantie d'identité

La sécurité doit être robuste, tout en demeurant aussi transparente que possible pour l'utilisateur :

Capacité	Pourquoi est-ce important
Options d'authentification flexibles (authentification multifactorielle, sans mot de passe, etc.)	L'offre de plusieurs options d'authentification permet aux administrations publiques de concilier une sécurité accrue et la facilité d'accès pour les citoyens.
Contrôles d'accès basés sur les risques	Une authentification configurable permet de renforcer la sécurité lorsque le risque est élevé, en ajoutant des contraintes uniquement lorsque la demande l'exige.
Vérification et assurance de l'identité	Certains services publics nécessitent des niveaux élevés d'assurance de l'identité pour protéger les renseignements sensibles et prévenir la fraude.
Détection des fraudes et surveillance des anomalies	La détection d'activités suspectes, comme les tentatives de prise de contrôle de compte ou les attaques automatisées, protège à la fois l'identité des citoyens et les systèmes gouvernementaux.



## 4.4 Prestation de services assistée et inclusive

Les pouvoirs publics doivent servir l'ensemble de la population, y compris les personnes ayant un accès limité aux services en ligne ou un faible niveau de littératie numérique :

Capacité	Pourquoi est-ce important ?
Accès délégué sécurisé (aidants, parents, avocats)	De nombreux citoyens comptent sur des représentants de confiance pour gérer des services en leur nom. Les systèmes CIAM doivent soutenir ces relations de manière sécurisée.
Processus de récupération d'identité	Il est inévitable que des citoyens oublient leur mot de passe. Des mécanismes simples et sécurisés sont essentiels pour maintenir l'accès aux services tout en évitant les prises de contrôle non autorisées.
Conformité aux normes d'accessibilité (WCAG, ADA, AODA, etc.)	Les pouvoirs publics sont légalement tenus d'assurer l'accessibilité des services numériques aux personnes handicapées.
Prise en charge multilingue	Les administrations publiques servent des populations diversifiées et peuvent avoir plus d'une langue officielle. Des interfaces multilingues améliorent l'accessibilité et l'adoption.

## 4.5 Intégration et évolutivité

Les environnements informatiques des administrations publiques regroupent de multiples plateformes, générations et technologies :

Capacité	Pourquoi est-ce important
Architecture axée sur les API	Les systèmes d'identité modernes doivent s'intégrer facilement aux services et applications numériques existants.
Prise en charge des normes d'authentification et d'intégration	Les administrations publiques gèrent des environnements informatiques complexes; les intégrations prêtes à l'emploi et le respect des normes accélèrent le déploiement des services.
Compatibilité avec les systèmes hérités et modernes	Les systèmes gouvernementaux s'appuient sur des technologies couvrant plusieurs décennies; les plateformes CIAM doivent fonctionner aussi bien avec les infrastructures modernes qu'avec les infrastructures héritées.
Évolutivité éprouvée pour des millions d'utilisateurs	Les services publics doivent soutenir de vastes populations sans compromettre la performance.
Haute disponibilité et reprise après sinistre	Les systèmes d'identité constituent une infrastructure essentielle; toute interruption peut empêcher l'accès des services critiques.
Identité citoyenne unifiée pour l'ensemble des services	Une base d'identité unifiée réduit les doublons, améliore la prestation des services et permet une gestion cohérente de la confidentialité et du consentement entre les agences.

## 5 Pièges courants de la mise en œuvre de solutions CIAM dans le secteur public

Les administrations publiques rencontrent fréquemment des difficultés lors de la mise en œuvre de solutions CIAM. La compréhension de ces pièges courants peut permettre d'éviter les erreurs suivantes, qui pourraient être coûteuses :

- choisir une plateforme CIAM commerciale conçue pour la vente au détail ou les services bancaires non adaptés au secteur public;
- sous-estimer les exigences en matière de confidentialité et de consentement;
- négliger les canaux de services assistés et les mécanismes d'accès délégué;
- privilégier les fonctionnalités au détriment de l'adéquation opérationnelle à long terme;
- considérer le système CIAM comme un outil autonome plutôt que comme une composante centrale de l'infrastructure numérique.

## 6 Comment évaluer les fournisseurs CIAM

Les fournisseurs de CIAM se distinguent par leur capacité à répondre aux besoins propres au secteur public. Amorcer le processus par une série de questions générales et évaluer l'expérience de chaque fournisseur dans des environnements gouvernementaux peut contribuer à simplifier et à structurer la sélection.

### 6.1 Questions clés d'évaluation

Utilisez les questions suivantes pour orienter l'évaluation des fournisseurs et définir les critères de l'appel d'offres :

- La solution est-elle spécialement conçue pour les cas d'utilisation dans le secteur public ?
- Comment garantit-elle la protection de la vie privée, la gestion du consentement et la confiance du public ?
- Peut-elle s'intégrer aux systèmes d'identité et aux plateformes de services existants ?
- Prend-elle en charge à la fois les parcours citoyens en libre-service et les parcours avec services assistés ?
- Comment s'adapte-t-elle à l'augmentation du nombre d'utilisateurs et à l'élargissement de l'offre de services ?
- Intègre-t-elle les autres composantes nécessaires pour répondre aux demandes des citoyens (p. ex., notifications, gestion des profils) ?
- La solution est-elle hautement configurable pour s'adapter à l'évolution des politiques et des services publics ?
- Peut-elle être mise en œuvre rapidement et facilement ?
- À quelle vitesse de nouveaux services peuvent-ils être intégrés sans coût ni complexité supplémentaires ?

### 6.2 Preuve à demander

Demandez aux fournisseurs de fournir des éléments concrets permettant d'étayer leurs affirmations :

- des références propres au secteur public;
- de la documentation sur l'architecture et les capacités d'intégration;
- une présentation de la conception en matière de sécurité et de confidentialité;
- des démonstrations de parcours citoyens réels;
- des exemples de processus liés aux services assistés et à la récupération d'identité;
- des indicateurs de performance et de disponibilité.

## 7 Considérations relatives à l'approvisionnement et à la mise en œuvre

Lors de la planification du déploiement d'une solution CIAM, il est recommandé de :

- définir clairement les résultats attendus en matière de services et d'expérience citoyenne avant de déterminer les fonctionnalités;
- prévoir un déploiement progressif, en commençant par des services à faible risque, avec une approche axée sur un déploiement rapide et une amélioration continue;
- mobiliser dès le départ les équipes responsables de la confidentialité, de la sécurité, des affaires

juridiques et de la prestation des services;

- considérer la solution CIAM comme une infrastructure numérique stratégique à long terme;
- ne pas sous-estimer l'effort requis pour adapter une plateforme CIAM commerciale, un processus coûteux et à haut risque.

*Les mises en œuvre réussies mettent l'accent sur la création de valeur, et pas uniquement sur le déploiement technologique.*

## 8 Pourquoi les administrations choisissent CitizenOne

CitizenOne est une plateforme CIAM de calibre gouvernemental conçue expressément pour soutenir la transformation numérique du secteur public.

Capacités de CitizenOne

- portail citoyen unifié pour l'ensemble des services;
- intégration progressive et gestion des identités;
- contrôles de consentement axés sur la protection de la vie privée;
- soutien aux services assistés et intégration avec les centres d'appels;
- architecture modulaire axée sur les API;

- conception assurant une évolutivité sécurisée et durable;
- solution offerte en mode service, et déployable en quelques semaines plutôt qu'en plusieurs mois ou années, éliminant ainsi les risques de mise en œuvre souvent associés à d'autres approches.

*CitizenOne permet aux administrations publiques de moderniser leurs services numériques tout en préservant la confiance du public, l'inclusion et la conformité réglementaire.*

## 9 Prochaines étapes

L'administration numérique repose sur une identité digne de confiance.

Le choix de la plateforme CIAM appropriée constitue une décision stratégique qui influence l'ensemble des services numériques offerts par une administration.

Pour aller de l'avant en toute confiance :

- cernez vos besoins actuels et futurs en matière d'identité numérique;

- définissez des critères d'évaluation alignés sur les exigences du secteur public;
- effectuez une analyse du marché en vous appuyant sur les questions et les critères présentés dans le présent guide;
- demandez des démonstrations axées sur des parcours citoyens réels, plutôt que sur des présentations génériques de produits.

**Si votre organisation évalue actuellement des solutions CIAM, découvrez comment une plateforme conçue spécifiquement pour le secteur public peut vous aider à atteindre vos objectifs.**

**Pour découvrir comment CitizenOne soutient la transformation numérique des administrations publiques :**

- demandez une démonstration personnalisée de CitizenOne;
- parlez à un spécialiste des solutions CIAM pour le secteur public.

## Annexe:

# Tableau comparatif d'évaluation des fournisseurs de solutions CIAM

Cette fiche de travail propose une approche structurée et indépendante des fournisseurs pour évaluer les plateformes CIAM au regard des exigences propres au secteur public. Elle favorise une prise de décision transparente, reproductible et justifiable.

## 1 Catégories d'évaluation et pondération

Les catégories ci-dessous correspondent directement aux critères présentés aux sections 4 et 6 du présent guide. Les pondérations reflètent leur importance relative dans les programmes CIAM du secteur public et peuvent être ajustées pour tenir compte des priorités propres à chaque juridiction.

Catégorie d'évaluation	Description	Pondération (%)
Expérience citoyenne	Inscription, connexion, expérience utilisateur, intégration progressive, cohérence entre les services, prise en charge mobile	15
Confidentialité, consentement et confiance	Gestion du consentement, transparence, protection de la vie privée dès la conception, conformité réglementaire	15
Sécurité et assurance de l'identité	Authentification multifactorielle (MFA), vérification d'identité, surveillance de la sécurité	20
Prestation de services assistée et inclusive	Accès délégué, procédures de récupération, accessibilité, soutien multilingue	15
Intégration et évolutivité	Architecture axée sur les API, prise en charge des normes, approche d'intégration aux systèmes existants, disponibilité	15
Gouvernance et pérennité opérationnelle	Administration, auditabilité, configurabilité, opérabilité à long terme, faible risque de mise en œuvre	10
Expérience dans le secteur public	Expérience avérée auprès de clients du secteur public	10
Total		100

## 2 Barème de notation

Chaque fournisseur est évalué selon la même échelle normalisée afin d'assurer la cohérence entre les évaluateurs.

Définition	Note
Ne répond pas aux exigences	0
Répond partiellement aux exigences ; des lacunes importantes subsistent	1
Répond aux exigences	2
Dépasse les exigences ; capacités démontrées et éprouvées	3

### 3 Fiche de comparaison des fournisseurs

Les évaluateurs attribuent une note de 0 à 3 pour chaque catégorie et pour chaque fournisseur.

Catégorie d'évaluation	Pondération (%)	Fournisseur A	Fournisseur B	Fournisseur C
Expérience citoyenne	15			
Confidentialité, consentement et confiance	15			
Sécurité et assurance de l'identité	20			
Prestation de services assistée et inclusive	15			
Intégration et évolutivité	15			
Gouvernance et pérennité opérationnelle	10			
Expérience dans le secteur public	10			
<b>Note finale pondérée</b>	<b>100</b>			

### Méthode de calcul de la note finale

1. Note pondérée = note × pondération
2. Note totale = somme de l'ensemble des notes pondérées (note totale maximale = 300)
3. Note finale en % = (note totale / note maximale) × 100

### 5 Interprétation de la note

Le pourcentage obtenu permet d'évaluer l'adéquation globale d'une solution aux exigences gouvernementales en matière de CIAM.

Score Range	Interpretation
80 à 100 %	Très bonne adéquation avec les exigences gouvernementales en matière de CIAM
70-79%	Solution viable, mais comportant certaines lacunes
50-69%	Limitations importantes
Below 50%	Solution non adaptée aux exigences gouvernementales



# Prochaines étapes ?

## Des questions ?

Découvrez les [solutions de Portage CyberTech.](#)

Ou [réservez une consultation](#) avec l'un de nos experts pour explorer comment nos solutions peuvent bénéficier à votre municipalité.

© Portage CyberTech, 2026. Tous droits réservés