Livre blanc

Pourquoi les projets CIAM échouent-ils?

Par Bruce Lévis, Gregory Natran, Ed Therriault, Jim Lawson, et Guy Pensa



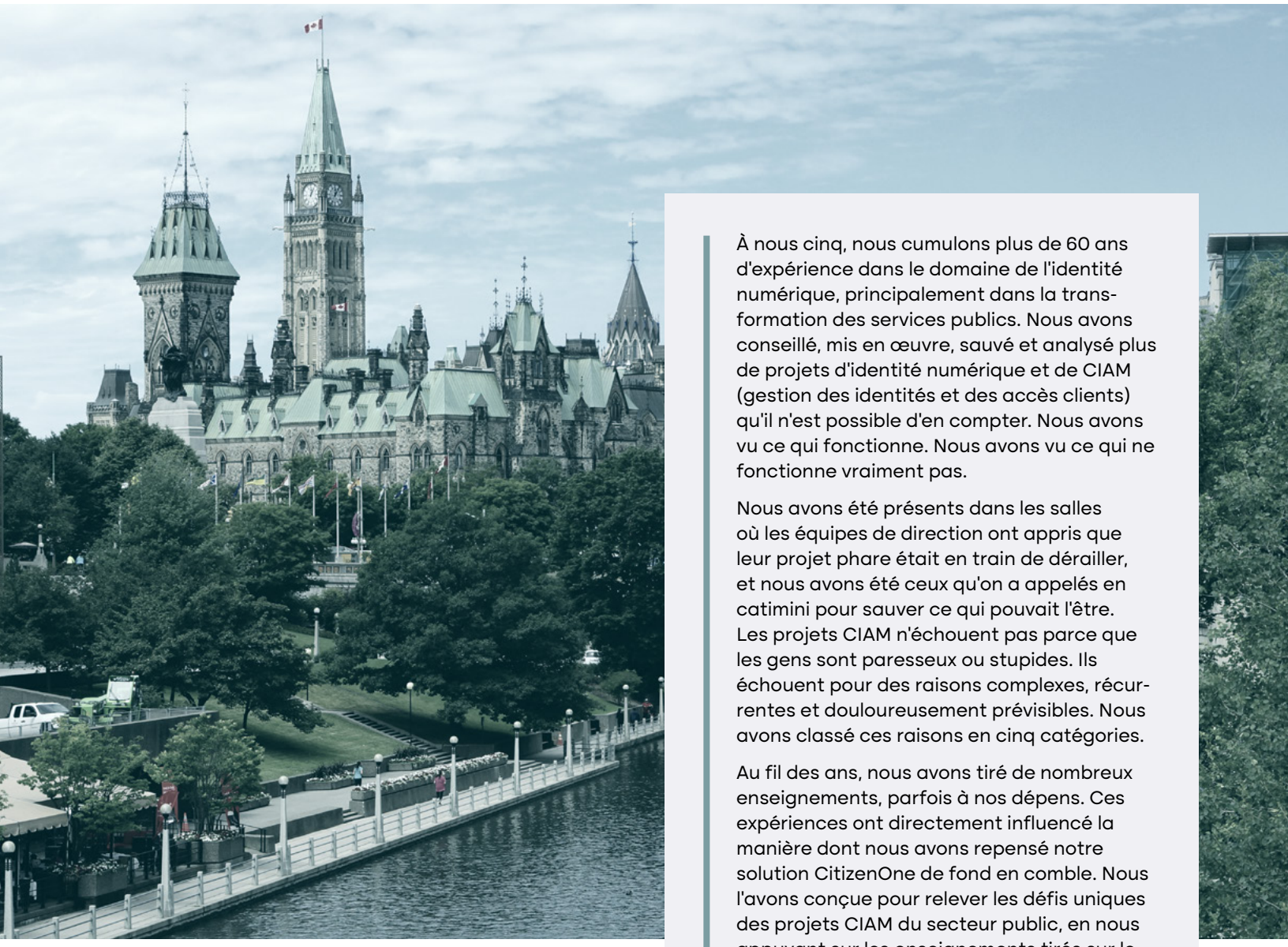
PORTAGE cybertech

portagecybertech.com
info@portagecybertech.com

Introduction :

les dures leçons apprises au fil des décennies

Si vous menez ou êtes sur le point de mener un projet CIAM, nous espérons que cette liste vous aidera à éviter de devenir un autre exemple à ne pas suivre.



À nous cinq, nous cumulons plus de 60 ans d'expérience dans le domaine de l'identité numérique, principalement dans la transformation des services publics. Nous avons conseillé, mis en œuvre, sauvé et analysé plus de projets d'identité numérique et de CIAM (gestion des identités et des accès clients) qu'il n'est possible d'en compter. Nous avons vu ce qui fonctionne. Nous avons vu ce qui ne fonctionne vraiment pas.

Nous avons été présents dans les salles où les équipes de direction ont appris que leur projet phare était en train de dérailler, et nous avons été ceux qu'on a appelés en catimini pour sauver ce qui pouvait l'être. Les projets CIAM n'échouent pas parce que les gens sont paresseux ou stupides. Ils échouent pour des raisons complexes, récurrentes et douloureusement prévisibles. Nous avons classé ces raisons en cinq catégories.

Au fil des ans, nous avons tiré de nombreux enseignements, parfois à nos dépens. Ces expériences ont directement influencé la manière dont nous avons repensé notre solution CitizenOne de fond en comble. Nous l'avons conçue pour relever les défis uniques des projets CIAM du secteur public, en nous appuyant sur les enseignements tirés sur le terrain, avec une solution adaptée aux réalités du monde gouvernemental.

N° 5 Le piège des statistiques à mi-parcours

Demandez à n'importe quel étudiant en mathématiques ou en ingénierie de vous parler de son cours d'introduction aux statistiques et observez son visage se crisper. Ces étudiants sont habitués à la logique abstraite et aux calculs complexes. Ils comprennent la matière, du moins le pensent-ils. Puis arrive le premier examen de mi-semestre, qui les ramène à la réalité. Les statistiques ne sont pas une question de calculs mathématiques bruts, mais de compréhension et d'application de la bonne logique au bon moment. Il s'agit d'une façon de penser fondamentalement différente.

Le CIAM est très similaire.

> **À première vue, le CIAM semble simple. Authentifier les utilisateurs. Autoriser l'accès. Ajouter l'authentification multifactorielle (MFA) et l'authentification unique (SSO). C'est tout, non ? Pas tout à fait.**

Dans les petites et moyennes entreprises du secteur public en particulier, la CIAM est souvent confiée au service informatique comme un « projet supplémentaire ». Mais la CIAM touche tous les domaines, de l'expérience utilisateur à la confiance des citoyens en passant par la conformité réglementaire. Et lorsque les équipes la considèrent comme « simplement une combinaison de SSO et de MFA », elles passent à côté d'aspects essentiels :

- Donner aux citoyens le contrôle de leur identité grâce à leur consentement
- Simplifier l'expérience en permettant aux citoyens d'utiliser leur propre identité ou justificatif d'identité
- Comprendre les niveaux d'assurance par catégorie de risque de service
- Gérer l'intégration progressive et la vérification d'identité en plusieurs étapes
- Prendre en charge des populations diverses grâce à des méthodes de vérification flexibles
- Intégrer de nouveaux services ou solutions sans introduire de nouvelles vulnérabilités de sécurité
- Respecter des normes strictes en matière de confidentialité, de consentement et d'accessibilité
- Concevoir des solutions de secours robustes pour la récupération des comptes
- Capturer des indicateurs clés de performance exploitables pour améliorer les services
- Planifier des modèles de sécurité zéro confiance et des identités décentralisées

These outcomes underscore the effectiveness of CIAM solutions in transforming public sector digital services.

N° 4 Si vous le construisez... ils ne viendront peut-être pas

La livraison technique n'est pas synonyme de succès. L'adoption est synonyme de succès.

> **Nous avons vu des systèmes CIAM livrés dans les délais, dans le respect du budget et fonctionnellement complets, puis échouer spectaculairement parce que les citoyens ne les utilisaient tout simplement pas.**

Parmi les erreurs courantes en matière d'expérience utilisateur qui nuisent à l'adoption du CIAM, on peut citer :

- Des écrans de connexion encombrés et confus (« quel compte dois-je utiliser ? »)
- Des processus de vérification d'identité longs et complexes
- Des expériences mobiles défaillantes ou incohérentes
- Le retour des citoyens à la vérification d'identité hors ligne (« imprimer ce formulaire »)
- Un manque de cohérence entre les services intégrés
- Des conditions d'utilisation peu claires et intimidantes
- L'absence d'options de secours en cas de réinitialisation du mot de passe, de perte de l'appareil ou d'erreurs
- Absence d'aide à la prise en main pour les nouveaux utilisateurs
- Absence de vue d'ensemble consolidée des services, des avantages et des mises à jour de statut

Les études sur l'expérience utilisateur montrent systématiquement que les systèmes d'identité numérique doivent être intuitifs, transparents et rapides. Si les citoyens rencontrent des difficultés, sont confus ou se méfient, ils abandonneront le processus. Investir dans l'expérience utilisateur n'est pas un luxe. C'est une question de survie.

N° 3 Ignorer la conformité et la cybersécurité jusqu'à ce qu'il soit trop tard

Dans le secteur public, la conformité et la cybersécurité ne sont pas des exercices consistant à cocher des cases. Ce sont des disciplines vivantes qui doivent être prises en compte dès le premier jour.

La conformité ne se limite pas aux lois sur la confidentialité. Elle englobe les normes informatiques, les règles d'approvisionnement, les exigences en matière d'accessibilité et la souveraineté des données juridictionnelles. La cybersécurité ne se limite pas aux pare-feux : elle concerne la gestion du cycle de vie des identifiants, la réponse aux incidents, les obligations de notification des violations et la garantie de l'intégrité continue des services gouvernementaux.

Ne pas s'engager dès le début crée un risque énorme :

- Les évaluations d'impact sur la vie privée (PIA) peuvent révéler des cas de non-conformité systémique
- Les politiques en matière d'identifiants peuvent ne pas respecter les normes NIST ou ISO
- Les audits d'accessibilité peuvent mettre en évidence une conception non inclusive
- Les examens juridiques peuvent rejeter les conditions d'utilisation ou les modèles de consentement
- Les audits internes peuvent révéler des lacunes en matière de gouvernance
- Les audits de sécurité peuvent révéler des vulnérabilités inacceptables
- Les données sensibles des citoyens pourraient être exposées
- L'intégration de services interjuridictionnels peut enfreindre la loi

> **Ce n'est pas théorique. Nous l'avons constaté de nos propres yeux. Nous avons aidé des clients qui ont pris les bonnes mesures dès le début à éviter des problèmes majeurs. Nous sommes également intervenus tardivement dans des projets, après que ces problèmes aient entraîné des retards importants, une surveillance publique, des coûts de refonte considérables, voire l'arrêt total du projet.**

Ignorer la conformité et la cybersécurité peut transformer un projet prometteur en un exemple à ne pas suivre dans le secteur public et c'est souvent le cas. À lui seul, ce problème pourrait facilement occuper une place encore plus élevée dans notre classement.





N° 2 Devenir involontairement un fournisseur de logiciels

De nombreux acheteurs publics pensent acheter un « produit » CIAM. Trop souvent, ils achètent en réalité une « plateforme », et la distinction est cruciale.

Prenons l'exemple des entreprises leaders dans le domaine du « SaaS-to-PaaS » :

- Office 365 se situe à l'extrémité pure du SaaS : entièrement fonctionnel, prêt à l'emploi, sans codage requis.
- Wix et Squarespace se situent légèrement plus à droite : principalement de la configuration avec une flexibilité mineure.
- Shopify se situe encore plus à droite : puissant, mais nécessitant souvent des partenaires de mise en œuvre pour une personnalisation plus poussée.
- De nombreux concurrents du CIAM se situent encore plus à droite : ils proposent des plateformes où, malgré des listes de fonctionnalités étendues, les acheteurs doivent créer eux-mêmes les parcours utilisateurs, gérer le renforcement du système, concevoir l'expérience utilisateur des citoyens et intégrer les services critiques.
- À l'extrême opposé, vous achetez essentiellement une machine virtuelle, un serveur d'applications, du stockage, de la mémoire, et vous construisez tout à partir de zéro.

Les acheteurs du secteur public ne disposent pas des structures budgétaires, des profils de personnel ou de la flexibilité opérationnelle nécessaires pour fonctionner comme les éditeurs de logiciels du secteur privé. Ils ne devraient d'ailleurs pas essayer de le faire.

Les gouvernements existent pour fournir des services publics, pas pour concurrencer la Silicon Valley. Leurs ressources sont optimisées pour la conformité, la prestation de services et l'engagement des citoyens, et non pour le développement continu de produits, les correctifs de sécurité ou les cycles de publication de nouvelles fonctionnalités. Attendre des institutions publiques qu'elles agissent comme des entreprises de logiciels agiles est voué à l'échec.

En réalité, lorsque les organisations du secteur public achètent des plateformes plutôt que des solutions finies, elles se retrouvent souvent responsables de :

- Définir et mettre en place des flux de travail d'intégration et d'authentification
- Concevoir et maintenir les composants de l'expérience utilisateur destinés aux citoyens
- Gérer la délivrance complexe des identifiants, la fédération et le cycle de vie des identités
- Rédiger, héberger et mettre à jour en permanence les mentions légales et les flux de consentement
- Gérer les mises à niveau, les correctifs, le déploiement de nouvelles fonctionnalités et les audits de conformité

> **Du jour au lendemain, l'organisation se retrouve confrontée à des exigences de gestion de produits qu'elle n'a jamais été structurée ni financée pour gérer. Ce qui semblait être un achat gérable devient rapidement un scénario de propriété de produit coûteux, fragile et politiquement délicat.**

C'est exactement là que de nombreux projets CIAM s'effondrent sous leur propre poids, et c'est pourquoi il est essentiel de bien comprendre ce que vous achetez avant de signer le contrat. Lorsque nous avons conçu le nouveau CitizenOne, nous avons gardé cette réalité à l'esprit et avons positionné la solution plus près d'un Shopify dans le spectre, éliminant ainsi une grande partie des risques techniques et liés au projet.

N° 1

Les personnes et le pouvoir

C'est le défi le plus dangereux et le plus difficile à relever.

Dans la plupart des administrations publiques, le CIAM est initialement détenu par une organisation informatique centralisée. Cette centralisation a souvent fait suite à des années où chaque département, agence ou service public disposait de sa propre équipe informatique et de sa propre feuille de route. La centralisation a apporté de l'efficacité, mais elle a également créé du ressentiment et de la méfiance.

Pire encore, de nombreux programmes et services sont fournis par différentes agences, ministères ou même des entités juridiquement distinctes telles que les services publics, les autorités de transport public ou les entreprises publiques (ou la Couronne au Canada).

Ils ont leurs propres services de conformité, leurs équipes de cybersécurité, leurs responsables de programmes et leurs propres priorités.

Lorsqu'un système CIAM centralisé est proposé, il suscite souvent un profond scepticisme :

- Les agences craignent de perdre le contrôle des relations avec les citoyens et des données.
- Les équipes informatiques locales craignent d'être marginalisées.
- Les responsables de programmes résistent à l'intégration parce que « nos besoins sont uniques ».
- Les parties prenantes utilisent les politiques d'approvisionnement, les normes techniques ou les processus de gouvernance comme armes pour ralentir ou empêcher le déploiement.

> **Si les gens veulent résister, ils peuvent le faire, et ils le feront, sans jamais être officiellement blâmés. Ils peuvent « respecter les règles » tout en sapant la dynamique.**

Lorsque les projets échouent, ce sont rarement les résistants internes qui en subissent les conséquences. Ce sont les fournisseurs externes, le service informatique central ou les responsables du projet qui sont blâmés.
Sans une gestion du changement de classe mondiale, un engagement sans faille des parties prenantes et un soutien indéfectible de la direction, même le meilleur système CIAM au monde peut échouer, et c'est souvent le cas.



Conclusion : c'est pourquoi nous avons créé CitizenOne

Après des décennies d'enseignements difficiles, nous ne nous sommes pas contentés de créer une nouvelle plateforme d'identité. Nous avons repensé CitizenOne pour résoudre précisément ces problèmes.

Nous avons rejoint des organismes de normalisation. Nous avons contribué à la conception de cadres de confiance nationaux. Nous avons interrogé plus de 400 organisations gouvernementales par l'intermédiaire d'IDC. Nous avons collaboré étroitement avec des prestataires de services de première ligne. Nous avons établi des partenariats avec des instituts de recherche expérimentés dans les systèmes de niveau opérateur.



CitizenOne est le premier CIAM véritablement prêt à l'emploi pour les gouvernements, spécialement conçu pour :

- Respecter la conformité, la confidentialité et la cybersécurité dès le premier jour
- Offrir une expérience utilisateur centrée sur le citoyen
- Éviter à nos clients de tomber dans le piège des « fournisseurs de logiciels accidentels »
- Permettre une intégration transparente et évolutive
- Favoriser la flexibilité des programmes tout en protégeant la confiance des citoyens

Nous ne pouvons pas changer la nature humaine. Mais nous savons comment travailler avec elle.

Si vous vous lancez dans la mise en place d'une solution CIAM, nous serions ravis de vous aider à la concevoir correctement, de la première décision au déploiement final

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.

© Copyright Portage CyberTech 2025