Exemples de critères de sélection pour les plateformes CIAM (Gestion des identités et accès clients)

Un point de départ pour l'évaluation des fournisseurs

Ce document contient une liste d'exemples de questions qui vous aideront à créer un appel d'offres pour une solution CIAM. Ce guide est conçu comme point de départ ; il doit aider vos équipes et parties prenantes à identifier les exigences et les priorités spécifiques de votre entreprise. Nous considérons ces questions comme des critères d'évaluation de base destinés à comparer les solutions et les fournisseurs CIAM.

Informations sur le fournisseur

1. Quel est le nom de votre entreprise ?
2. Veuillez répertorier tous les sites de l'entreprise et le niveau des effectifs de chaque site.
3. Depuis combien de temps l'entreprise est-elle en activité ?
4. Décrivez brièvement l'historique de votre entreprise.
5. Présentez votre portefeuille de produits et de services.
6. Décrivez la disponibilité de votre plateforme à l'échelle mondiale.
7. Fournissez des renseignements concernant les partenariats commerciaux ou techniques avec d'autres organisations.
8. Donnez un aperçu de la situation financière de votre entreprise.

Expérience et références

1. Veuillez décrire l'expérience de votre entreprise en matière de solutions CIAM.
2. Combien de clients avez-vous ?
3. Donnez au moins cinq exemples de déploiements actifs.
4. Parmi vos clients, lesquels sont semblables en termes de taille et de portée à notre entreprise ?
5. Fournissez des rapports d'analystes ou d'autres études indépendantes qui illustrent votre leadership dans le secteur CIAM.
6. Donnez des exemples d'inventions, d'innovations ou d'efforts de votre entreprise en matière de développements liés à la CIAM.

Fonctions CIAM

1. Veuillez décrire en détail votre gamme d'offres CIAM.
2. Quelles sont les fonctionnalités d'enregistrement prises en charge (CAPTCHA, vérification en ligne, validation des données, etc.) ?
3. Prenez-vous en charge plusieurs réseaux sociaux et fournisseurs d'identité pour l'authentification (par exemple, Facebook, Google, Twitter, LinkedIn, etc.) ?
4. Les clients peuvent-ils facilement configurer des formulaires utilisateur pour qu'ils s'adaptent à l'apparence de leur site, et dans quelle mesure ces écrans sont-ils flexibles et personnalisables ?
5. Décrivez le processus d'intégration des formulaires utilisateur dans les sites d'un client.
6. Détaillez les terminaux qui s'intègrent à votre solution. Pensez à inclure les terminaux mobiles, les tablettes et les terminaux IoT/connectés.
7. Fournissez des détails sur la réactivité.
8. Quels kits de développement logiciel (SDK) sont disponibles pour les plateformes standard et mobiles ?
9. Votre système prend-il en charge l'utilisation de différentes langues dans tous les champs (caractères UTF-8/double octet) pour les pays multilingues, et autorise-t-il l'utilisation de caractères spéciaux (par exemple, ñ en espagnol, ö en allemand, ç en français) ?
10. Votre solution est-elle conforme aux normes ouvertes ?
11. Votre service offre-t-il des fonctions de rapports détaillés ?
12. Décrivez les fonctions d'authentification de votre plateforme.
13. Décrivez les fonctions de votre plateforme en matière de contrôle d'accès et de gestion des règles d'accès.
14. Décrivez les fonctions d'administration de votre plateforme.
15. Les clients peuvent-ils créer et gérer d'autres ressources telles que des terminaux, des abonnements ou des sous-profils ?
16. Décrivez comment la gestion déléguée est prise en charge pour les cas d'utilisation consommateur.
17. Les clients peuvent-ils créer des comptes pour leurs amis ou leur famille et les inviter à participer ?
18. Proposez-vous un service d'authentification centralisé pour les utilisateurs finaux ?
19. Les applications Web et pour mobile peuvent-elles se connecter facilement à votre plateforme à l'aide de bibliothèques standard ?
20. Comment la plateforme stocke-t-elle les données de consentement ?
21. Pendant combien de temps l'historique d'audit des consentements est-il conservé ?
22. Le consentement « coarse-grained » et « fine-grained » est-il pris en charge ?
23. Les utilisateurs finaux disposent-ils d'une visibilité et d'un contrôle complets sur leurs données de consentement ?
24. Le consentement peut-il être collecté en contexte si nécessaire ?

25. Les utilisateurs finaux peuvent-ils télécharger une copie de leurs données ?
26. Les données utilisateur final peuvent-elles être supprimées sur demande ?
27. Votre solution offre-t-elle des fonctions d'autorisation configurables ?
28. Quel niveau de granularité votre autorisation prend-elle en charge (RBAC, ABAC, etc.) ?
29. Votre solution prend-elle en charge la recherche dynamique des attributs de règle ?
30. Votre solution prend-elle en charge des règles couvrant plusieurs fournisseurs d'identité ?
31. Votre solution peut-elle fournir des journaux d'audit concernant les décisions d'autorisation ? Et les données sensibles peuvent-elles être chiffrées automatiquement dans ces journaux ?
32. Comment les règles sont-elles créées (c'est-à-dire, disposez-vous d'outils visuels pour créer les règles, ou sont-elles créées via une configuration textuelle/codée) ?
33. Quels outils fournissez-vous pour garantir la validité, l'intégrité et l'analyse de l'impact de vos règles ?
34. Votre solution a-t-elle la capacité de contrôler qui peut créer/modifier/supprimer les règles ?

Intégrations

1. Avec quels navigateurs votre plateforme est-elle compatible ? Veuillez préciser :
    - 1.1 Firefox
    - 1.2 Google Chrome
    - 1.3 Apple Safari
    - 1.4 Microsoft Edge
    - 1.5 Microsoft Internet Explorer
    - 1.6 Navigateur Android
2. Décrivez de quelle manière sont assurées les intégrations avec des plateformes tierces, notamment (mais sans s'y limiter) dans les catégories suivantes :
    - 2.1 Solutions CRM
    - 2.2 Plateformes et services de marketing par e-mail
    - 2.3 Autres plateformes de marketing digital
    - 2.4 Plateformes d'e-commerce
    - 2.5 Solutions CMS
    - 2.6 Solutions de BI et d'analyse
    - 2.7 Solutions SIEM et de surveillance des journaux

3. Votre plateforme prend-elle en charge à la fois les modèles d'intégration par lot et en temps réel ?
4. Décrivez les options de format disponibles pour les données de profil récupérées auprès de votre plateforme.
5. Les données d'événement sont-elles disponibles dans le cadre d'un flux ? Répertoriez tous les événements disponibles.
6. Décrivez les contrôles mis en place pour s'assurer que seules les données autorisées et consenties sont envoyées aux systèmes en aval.

API

1. Veuillez décrire les interfaces de programmation d'applications (API) suivantes de votre plateforme :
    - 1.1 API d'enregistrement (côté client et serveur)
    - 1.2 API d'authentification (côté client et serveur)
    - 1.3 API de mise à jour des comptes (côté client et serveur)
    - 1.4 API d'administration
    - 1.5 API d'interrogation

Architecture de plateforme, stockage de données et infrastructure

1. Veuillez décrire l'architecture de votre plateforme et les méthodes de récupération des données.
2. Proposez-vous une base de données structurée en temps réel et interrogeable pour les données de profil utilisateur collectées au cours du processus d'authentification ?
3. Décrivez la flexibilité de votre schéma de données pour l'ajout et la suppression des champs de données, le passage des champs facultatifs à obligatoires, et inversement.
4. Décrivez la possibilité de supprimer un élément de données d'un enregistrement d'utilisateur (par exemple, si nécessaire pour des raisons juridiques). Décrivez comment cela est possible au sein de votre solution, sous réserve des règles de sécurité relatives à l'accès aux données.
5. Décrivez ce qui se passe lorsqu'un utilisateur supprime son compte de votre solution.
6. Décrivez comment votre solution permet aux utilisateurs d'apporter des modifications aux données de leur profil.
7. Fournissez des détails de la solution sur la réplication des données, la résilience et la disponibilité de l'infrastructure.
8. Donnez des détails techniques sur vos installations de stockage de données et de sauvegarde, y compris l'emplacement géographique, le cadre de sécurité physique et logique approprié et les procédures de sauvegarde.
9. À titre indicatif, combien d'enregistrements d'utilisateur pouvez-vous gérer au maximum ?
10. Comment la disponibilité du système est-elle surveillée par vos clients ?
11. Quel niveau de disponibilité du système sera garanti par votre organisation et quels crédits financiers seront accordés si ce niveau n'est pas atteint ?

12. Décrivez succinctement la procédure de continuité d'activité proposée en cas de perturbations techniques et/ou opérationnelles majeures. Cela peut inclure vos processus de reprise après incident.

13. Votre solution est-elle évolutive de manière dynamique à la demande, par exemple, capable de gérer les promotions d'utilisateur à grande échelle ? Si ce n'est pas le cas, quel serait le délai dont vous auriez besoin pour faire face à un pic attendu ? Avez-vous déjà mis en place l'infrastructure nécessaire pour prendre en charge ce problème ?

14. En outre, votre solution utilise-t-elle une base de données volumineuse avec suffisamment de capacité pour faire face à cette demande ?

15. Quels tests indépendants de performances avez-vous effectués ? Veuillez partager les résultats de ces tests.

16. Votre plateforme exploite-t-elle une architecture de microservices pour faire évoluer les composants de manière indépendante ?

17. Votre plateforme comprend-elle des référentiels distincts pour les profils client et les événements Web ?

18. Votre infrastructure intègre-t-elle les profils client à leur activité Web ?

19. Votre infrastructure comprend-elle un pipeline de données pour rapprocher, transformer et mettre en conformité les données pour la création de rapports sur le stockage de données ?

Cybersécurité et protection des données

Sécurité générale

1. Veuillez fournir un questionnaire entier de collecte d'informations standardisées (SIG) complété.

2. Décrivez votre architecture de sécurité. Intégrez la sécurité des couches réseaux, des bases de données et des applications.

3. Disposez-vous d'un aperçu de la sécurité et de la confidentialité ?

Programmes de sécurité

1. Disposez-vous d'un programme de gestion de la sécurité de l'information (ISMP) ? Si oui, comment son efficacité est-elle évaluée ?

2. Disposez-vous d'un programme de risque ?

    2.1 Décrivez l'approche que vous avez adoptée pour suivre les risques connus et veiller à ce qu'ils soient gérés.

    2.2 Décrivez vos procédures formelles d'évaluation des risques. À quelle fréquence ces opérations sont-elles effectuées et dans quel périmètre ?

3. Comment gérez-vous la défense antivirus ?

Contrôle d'accès

1. Comment gérez-vous l'accès de vos employés aux systèmes de production ?

2. Utilisez-vous l'authentification multifactorielle ?

Gestion des modifications

1. Disposez-vous d'une règle de gestion des modifications ?
2. Comment vous assurez-vous que les procédures de gestion des modifications sont respectées ?
3. Comment la gestion des modifications est-elle opérationnalisée pendant le développement technique de vos principales offres de produits ?
4. Décrivez votre processus de gestion des modifications pour les configurations d'applications client.
5. Décrivez votre processus de gestion des modifications pour les personnalisations client.
6. Comment informez-vous vos clients de la maintenance et des correctifs ?
7. Comment informez-vous vos clients des sorties de produits ?

Protections des données

1. Indiquez si vos données stockées sont chiffrées et de quelle manière.
2. Indiquez si vos données sont chiffrées en transit et de quelle manière.
3. Votre solution fournit-elle des contrôles d'accès de sécurité granulaires sur des champs de données individuels afin que nous puissions contrôler quels champs d'autres systèmes, sites Web, sites pour mobile et parties externes peuvent afficher, lire, modifier et supprimer ?
4. Votre solution offre-t-elle plusieurs niveaux de sécurité pour les applications et les personnes accédant aux données stockées ? Ces niveaux de sécurité peuvent-ils être appliqués par application ou par rôle ?
5. Quels mécanismes de détection d'intrusion avez-vous mis en place ?

Gestion des clés

1. Comment gérez-vous les clés de chiffrement ?
2. Pouvons-nous utiliser notre propre clé ?

Gestion des mots de passe

1. Effectuez-vous le hachage des mots de passe ?
2. Quel facteur de coût utilisez-vous pour votre algorithme de hachage ?
3. Fournissez-vous un salage unique à chaque utilisateur final ?
4. Comment les salages sont-ils traités lors d'une réinitialisation de mot de passe ?
5. Les clients peuvent-ils choisir leurs propres règles de mot de passe (c'est-à-dire leur propre expression régulière de mot de passe) ?

Durabilité

1. Quelle durabilité fournissez-vous aux données client ?

Surveillance

1. Fournissez-vous une surveillance 24 h/24, 7 j/7 et 365 j/an ?
2. Informez-vous vos clients en temps réel sur l'état de votre plateforme ?
3. Effectuez-vous une surveillance des tendances sur les applications client ?
4. Comment gérez-vous les attaques distribuées persistantes avancées ?
5. Comment gérez-vous les attaques par déni de service (DoS) ?
6. Pouvez-vous bloquer les adresses IP ?
7. Votre solution permet-elle l'exportation d'événements de sécurité vers une plateforme SIEM ou de gestion de la sécurité ?

Protections réseau

1. Décrivez vos pare-feu.
2. Utilisez-vous des groupes de sécurité ?
3. Utilisez-vous des clouds privés virtuels (VPC) ?
4. Votre solution est-elle conçue pour Zero Trust ?
5. Quels sont les éléments que vous renforcez ?

Continuité des activités et reprise après incident (BCDR)

1. Possédez-vous une règle de continuité des activités ? Veuillez préciser.
2. Mettez-vous régulièrement en pratique vos plans BCDR ?
3. Écrivez-vous simultanément les données client dans un autre centre de données ?
4. Combien de sauvegardes faites-vous des données client ?
5. Combien de sauvegardes faites-vous de votre plateforme principale ?
6. Testez-vous les restaurations à partir de la sauvegarde ? Si oui, à quelle fréquence et sont-elles vérifiées par des organismes d'audit externes ?
7. Avez-vous déjà mis en œuvre vos plans de reprise après incident ou de continuité des activités dans une situation réelle ? Si oui, décrivez cette situation.

Tests de pénétration et de vulnérabilité

1. À quelle fréquence effectuez-vous un test de pénétration du réseau ?

Conformité

1. Parmi les certifications de conformité suivantes, lesquelles ont été vérifiées par un cabinet d'audit externe accrédité ?
    - 1.1 SOC 2 Type 2, Sécurité (critères communs) – Si oui, veuillez fournir le rapport.
    - 1.2 SOC 2 Type 2, Disponibilité – Si oui, veuillez fournir le rapport.
    - 1.3 SOC 2 Type 2, Vie privée – Si oui, veuillez fournir le rapport.
    - 1.4 SOC 2 Type 2, Intégrité du traitement
    - 1.5 SOC 2 Type 2, Confidentialité
    - 1.6 ISO 27001:2013 – Si oui, veuillez fournir le rapport.
    - 1.7 ISO 27018:2014 – Si oui, veuillez fournir le lien de certification.
    - 1.8 HIPAA – Si oui, veuillez fournir le rapport.
    - 1.9 HITECH – Si oui, veuillez fournir le rapport.
    - 1.10 CSA Star niveau 2 certifié – Si oui, veuillez fournir le lien de certification et le rapport d'attestation.
    - 1.11 Pratiques en matière de confidentialité – Si oui, veuillez fournir une preuve de l'évaluation.
    - 1.12 Politique de protection Privacy Shield – Si oui, veuillez fournir une preuve de l'évaluation.

Règlement général sur la protection des données (RGPD)

1. Votre solution fournit-elle des flux de travail pour prendre en charge les demandes des personnes concernées en vertu du RGPD ?
2. Si des données personnelles sont transférées au-delà des frontières du pays, identifiez les mécanismes de transfert appropriés, tels que la certification Privacy Shield, les règles d'entreprise contraignantes (BCR) ou les clauses contractuelles standard, que votre entreprise peut respecter ou fournir pour légitimer le transfert.
3. Quelle formation RGPD avez-vous mise en œuvre ?
4. Disposez-vous d'un responsable de la sécurité de l'information ?
5. Disposez-vous d'un vice-président en charge de la confidentialité ou d'un directeur de la confidentialité ?
6. Votre solution offre-t-elle une fonction de gestion du consentement ?

Support et services

1. Veuillez fournir un aperçu du processus de déploiement de votre solution, des fonctions de support qui seront disponibles pour les clients au cours du déploiement et du délai moyen de mise sur le marché.
2. Décrivez vos services de support technique, notamment les options 24 h/24 et 7 j/7 et les accords de niveau de service (SLA).
3. Décrivez les services de conseil et de stratégie proposés par votre entreprise.
    3.1 Votre entreprise dispose-t-elle d'une expertise en matière d'intégrations tierces ou de meilleures pratiques en matière d'architecture d'entreprise ?
4. Décrivez les services de formation ou le programme de formation proposés par votre entreprise.
5. Quel est le profil d'embauche d'un ingénieur de support technique ?
6. Où se trouvent les équipes de support technique ?
7. Comment les équipes de support technique sont-elles formées ?
8. Comment les équipes de support technique sont-elles évaluées et encadrées en matière de qualité des tickets ?
9. Comment l'équipe de support technique mesure-t-elle la réussite ?
10. Quelle est la relation entre le support technique et l'ingénierie ?
11. Quels processus sont utilisés pour protéger le client contre les éventuelles erreurs de configuration par l'équipe de support technique ?
12. Comment protégez-vous les clients des demandes ou modifications de configuration non autorisées ?
13. Quels types de données le client reçoit-il de l'équipe de support technique tous les mois ou tous les trimestres ?
14. Quel est le processus de remontée des problèmes de support technique ?
15. Quelle est la conformité des SLA pour vos clients actuels ?
16. Comment mesurez-vous la satisfaction des clients vis-à-vis des tickets de support technique ?
17. Votre entreprise propose-t-elle des services de conseil en architecture de solution ?
    17.1 Ces services incluent-ils des conseils sur l'intégration de la gestion des identités dans notre écosystème d'informations existant, y compris la capture de données, l'automatisation du marketing, la création de rapports opérationnels, l'analyse commerciale et d'autres processus informatiques ?

Akamai sécurise et fournit des expériences digitales pour les plus grandes entreprises du monde. La plateforme de périphérie intelligente d'Akamai englobe tout, de l'entreprise au cloud, afin d'offrir rapidité, agilité et sécurité à ses clients et à leurs entreprises. Les plus grandes marques mondiales comptent sur Akamai pour les aider à concrétiser leur avantage concurrentiel grâce à des solutions agiles qui développent la puissance de leurs architectures multi-cloud. Akamai place les décisions, les applications et les expériences au plus près des utilisateurs, et au plus loin des attaques et des menaces. Les solutions de sécurité en bordure de l'Internet, de performances Web et mobiles, d'accès professionnel et de diffusion vidéo du portefeuille d'Akamai s'appuient également sur un service client exceptionnel, des analyses et une surveillance 24 h/24 et 7 j/7, 365 jours par an. Pour savoir pourquoi les plus grandes marques internationales font confiance à Akamai, visitez www.akamai.com/fr/fr/, blogs.akamai.com/fr ou suivez @Akamai_FR sur Twitter. Vous trouverez nos coordonnées dans le monde entier à l'adresse www.akamai.com/fr/fr/locations.jsp. Publication : 04/19.