

Voici un exemple de cahier des charges que vous pouvez utiliser comme point de départ :

1. Introduction

- Objectifs du cahier des charges
- Contexte de la demande (description de l'entreprise, de l'activité, des produits, etc.)
- Présentation de l'environnement technique actuel

2. Besoins fonctionnels

• Gestion des identités :

- Création et modification de comptes utilisateurs
- Gestion des groupes et des rôles
- Gestion des profils utilisateurs

• Gestion des accès :

- Authentification et autorisation
- Gestion des sessions
- SSO (Single Sign-On)

• Gestion des consentements :

- Collecte et gestion des consentements des utilisateurs
- Gestion des préférences utilisateur

• Personnalisation et branding :

- Personnalisation de l'interface utilisateur
- Ajout de logos et d'images personnalisées

• Intégrations :

- Intégration avec les systèmes de CRM
- Intégration avec les applications de marketing
- Intégration avec les systèmes de gestion de contenu

• Évolutivité et extensibilité :

- Capacité à gérer un grand nombre d'utilisateurs
- Capacité à ajouter des fonctionnalités personnalisées

3. Besoins non fonctionnels

• Sécurité :

- Chiffrement des données
- Authentification forte
- Détection des fraudes
- Gestion des vulnérabilités

• Facilité d'utilisation :

- Interface utilisateur conviviale et intuitive
- Support multilingue
- Support de la mobilité

• Performance et évolutivité :

- Capacité à gérer un grand nombre de requêtes
- Temps de réponse acceptable

• Tarification :
<ul style="list-style-type: none"> • Modèles de tarification proposés • Coûts associés à la mise en place et à la maintenance de la solution
4. Exigences techniques
<ul style="list-style-type: none"> • Langages de programmation et technologies utilisés • Architecture logicielle • Prérequis système (serveurs, bases de données, etc.)
5. Exigences de déploiement et de support
<ul style="list-style-type: none"> • Configuration système requise • Formation des utilisateurs et des administrateurs • Support technique (niveaux de support proposés, délais de réponse, canaux de support disponibles, etc.)
6. Exigences légales et réglementaires
<ul style="list-style-type: none"> • Conformité avec les lois et réglementations applicables, telles que le RGPD, la CCPA, etc.
7. Annexes
<ul style="list-style-type: none"> • Glossaire • Références et documents complémentaires • Informations sur l'entreprise prestataire (profil, références, etc.)

Voici un exemple de cahier des charges détaillé pour une solution CIAM :

1. Contexte
<ul style="list-style-type: none"> • Description du contexte dans lequel la solution CIAM sera utilisée : L'entreprise XYZ est une entreprise en pleine croissance opérant dans le secteur de l'e-commerce. Elle cherche à mettre en place une solution CIAM pour gérer les identités et les accès de ses clients sur son site web. • Objectifs de la solution CIAM : La solution CIAM doit permettre à l'entreprise de : <ul style="list-style-type: none"> • Gérer de manière sécurisée les identités et les accès de ses clients • Fournir une expérience utilisateur fluide et personnalisée sur son site web • Offrir des fonctionnalités de SSO pour permettre aux clients de se connecter une seule fois et d'accéder à toutes les applications de l'entreprise
<ul style="list-style-type: none"> • Contraintes et exigences spécifiques : <ul style="list-style-type: none"> • La solution CIAM doit respecter les lois et règlements en matière de protection des données personnelles, notamment le Règlement Général sur la Protection des Données (RGPD)

- La solution CIAM doit être capable de prendre en charge un grand nombre d'utilisateurs et de transactions, car l'entreprise prévoit une croissance rapide de son activité
- La solution CIAM doit être facile à intégrer avec les applications existantes de l'entreprise

2. Fonctionnalités de la solution CIAM

- Gestion des accès :

- Authentification : La solution CIAM doit être capable de prendre en charge différents mécanismes d'authentification, tels que les mots de passe, les certificats, les jetons d'accès, etc. Elle doit également être capable de gérer des règles d'autorisation complexes, en fonction des rôles de l'utilisateur et de l'accès demandé.
- Autorisation : La solution CIAM doit être capable de gérer des règles d'autorisation complexes, en fonction des rôles de l'utilisateur et de l'accès demandé.
- Gestion des sessions : La solution CIAM doit être capable de gérer les sessions utilisateur et de maintenir l'état de l'application tout au long de la session. Elle doit également être capable de gérer des sessions à la fois pour les utilisateurs authentifiés et non authentifiés, de manière à éviter les accès non autorisés et les failles de sécurité.
- SSO (Single Sign-On) : La solution CIAM doit être capable de permettre aux utilisateurs de se connecter une seule fois et d'accéder à plusieurs applications sans avoir à se connecter à chaque fois. Elle doit être capable de prendre en charge différents protocoles SSO, tels que SAML, OAuth, OpenID Connect, etc. Elle doit également être capable de gérer des attributs utilisateur entre les différentes applications et de garantir l'intégrité des données entre les applications.

- Gestion des identités :

- Création et gestion des profils utilisateurs : la solution doit permettre de créer et de gérer les profils des utilisateurs de manière efficace et intuitive.
- Processus de validation d'inscription : la solution doit permettre de vérifier l'identité des utilisateurs lors de leur inscription, par exemple en utilisant des mécanismes de validation d'adresse email ou de numéro de téléphone portable.
- Modification des données personnelles : les utilisateurs doivent pouvoir modifier leurs informations personnelles facilement et en toute sécurité.
- Désactivation des comptes : la solution doit permettre aux administrateurs de désactiver les comptes utilisateurs en cas de

besoin, par exemple en cas de violation de la politique de sécurité de l'entreprise.

- Suppression des comptes : la solution doit permettre aux utilisateurs de supprimer leur compte et de supprimer toutes les données personnelles associées à ce compte.

4. Gestion des données utilisateur

- La solution doit permettre la collecte, la gestion et la sécurisation des données personnelles des utilisateurs conformément aux réglementations en vigueur telles que le RGPD.
- La solution doit permettre la gestion des consentements des utilisateurs pour l'utilisation de leurs données personnelles.
- La solution doit permettre la suppression ou la modification des données personnelles des utilisateurs sur demande.

5. Personnalisation de l'interface utilisateur

- La solution doit permettre la personnalisation de l'interface utilisateur en fonction des besoins de l'entreprise, tels que l'ajout de logos, la personnalisation des couleurs et des polices.
- La solution doit permettre l'ajout de fonctionnalités personnalisées pour répondre aux besoins de l'entreprise.

6. Intégration avec d'autres systèmes

- La solution doit être capable de s'intégrer facilement avec les autres systèmes utilisés par l'entreprise tels que les systèmes de gestion de contenu, les systèmes de gestion de la relation client, les systèmes de marketing et les applications mobiles.
- La solution doit fournir une API ouverte pour permettre une intégration facile avec d'autres systèmes.

7. Reporting et analyse

- La solution doit fournir des rapports et des analyses sur les activités des utilisateurs tels que la fréquence d'utilisation, les données d'inscription et les comportements d'achat.
- La solution doit permettre la personnalisation des rapports en fonction des besoins de l'entreprise.

8. Support et maintenance

- La solution doit fournir un support technique efficace pour aider l'entreprise en cas de problèmes avec la solution.
- La solution doit fournir des mises à jour régulières pour améliorer les fonctionnalités et la sécurité de la solution.

9. Sécurité

- La solution doit fournir un niveau de sécurité élevé pour protéger les données des utilisateurs.
- La solution doit être conforme aux normes de sécurité telles que ISO 27001.

- La solution doit fournir des outils pour détecter et prévenir les attaques de sécurité telles que les attaques par déni de service.

10. Coûts

- Les différents modèles de tarification proposés, tels que l'abonnement mensuel, annuel, ou par utilisateur actif.
- Les coûts associés aux fonctionnalités supplémentaires telles que la personnalisation, l'intégration, le support premium, etc.
- Les coûts liés à la mise en œuvre et à la configuration de la solution, ainsi que les coûts de formation pour les utilisateurs et les administrateurs.

11. Planification et mise en œuvre

- La solution doit fournir une planification claire pour la mise en œuvre de la solution, y compris les délais et les ressources nécessaires.
- La solution doit fournir une assistance à l'entreprise pour la mise en œuvre de la solution.

12. Formation et documentation

- La solution doit fournir une formation pour les utilisateurs de la solution et pour les administrateurs de la solution.
- La solution doit fournir une documentation complète pour aider l'entreprise à utiliser et à administrer la solution.

13. Conditions contractuelles :

- Les termes et conditions de l'accord de service, y compris les garanties, les niveaux de service, les clauses de résiliation, les obligations de confidentialité, etc.
- Les conditions de paiement, de facturation, et de renouvellement de l'accord de service.
- Les dispositions relatives à la propriété intellectuelle, à la responsabilité, à la juridiction compétente, etc.

14. Références et témoignages :

- Les références de clients similaires ayant déjà utilisé la solution, avec des cas d'utilisation et des témoignages de satisfaction.
- Les certifications ou les prix remportés par le fournisseur pour la qualité de sa solution ou de son service.
- Les avis d'experts ou les analyses indépendantes de la solution et du fournisseur.

14. Évolution future

- La solution doit être évolutive pour répondre aux futurs besoins de l'entreprise.
- La solution doit fournir une feuille de route claire pour les futures mises à jour et les nouvelles fonctionnalités.