Open Sezam

Confidentiel

Fiche Produit

AuthSezam®

CIAM

Sécurisez vos accès clients et partenaires commerciaux avec **AuthSezam**, solution **sans mot de passe** qui simplifie le déploiement d'une stratégie **« MFA et Zero Trust Access - ZTA»** dans vos environnements **BtoB et BtoBtoC.**

Usages recommandés :

AuthSezam® CIAM Start : Idéal pour les organisations qui souhaitent proposer à leurs clients/patients/bénéficières, distributeurs et partenaires commerciaux une expérience d'authentification de confiance fluide, sans mot de passe, et intégrée à leurs services digitaux. La connexion par lien sécurisé ou par biométrie ne nécessite aucune installation logicielle côté utilisateur final. Le MFA est intuitif, les frictions sont éliminées et la console d'administration simplifiée pour accélérer le time-to-market de vos services digitaux tout en réduisant le support lié aux problèmes de mot de passe.

SmartSezam®CIAM – IA & Zero Trust Access : Parfait pour les organisations publiques ou privées qui veulent moderniser rapidement la sécurité des services en ligne avec une sécurité de pointe, robuste et transparente en déployant une protection ZTA « User Centric ». La solution s'adapte en temps réel aux risques grâce à un contrôle continu et à des parcours intelligents pilotés par l'IA, offrant une sécurité transparente qui ne dégrade pas l'expérience utilisateur légitime. Elle intègre des capacités avancées de détection de fraude (IA, ML, LLM) en apprentissage permanent, afin d'anticiper l'évolution des menaces et protéger vos écosystèmes numériques.

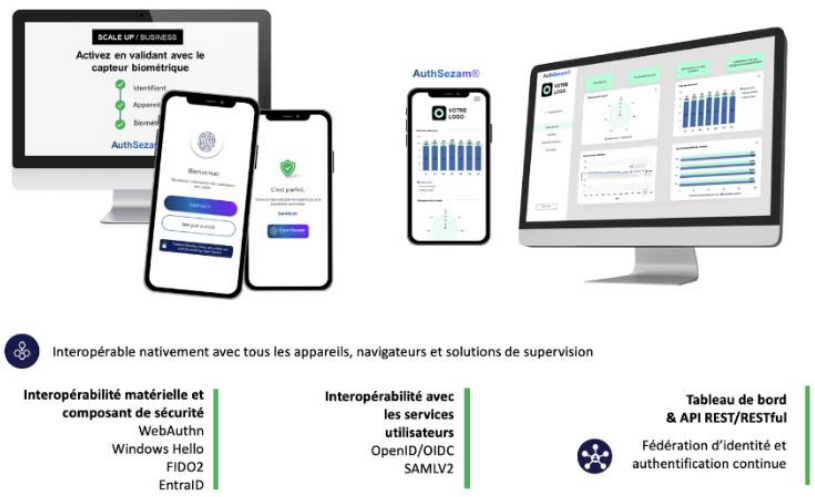
Présentation de la solution

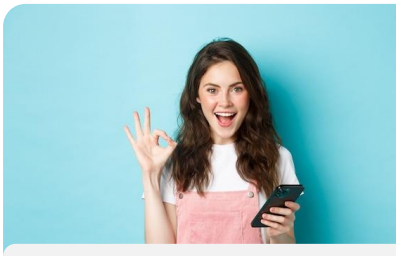
AuthSezam® CIAM est une solution d'authentification forte / MFA / IMFA (Invisible MFA), souveraine et sans mot de passe, conçue pour simplifier et sécuriser la connexion des clients, distributeurs, partenaires ou sous-traitants à vos applications et portails digitaux.

➡️ AuthSezam® combine sécurité, conformité et expérience utilisateur dans une approche Zero Trust Access by Design.

➡️ L'authentification est fluide et sans friction : aucune installation d'application n'est requise, ni sur navigateur ni sur appareil, et le SSO est intégré nativement

➡️ La plateforme est interopérable avec vos services fédérés et vos environnements mobiles ou web, garantissant un parcours client sans rupture.





Bénéfices pour l'utilisateur

- ✓ Aucun mot de passe à créer, retenir ou protéger
- ✓ Aucune application à installer
- ✓ Utilisation sans assistance
- ✓ UX/UI inclusif, adapté aux personnes en situation de handicap visuel

Bénéfices pour la DSI

- ✓ Interopérabilité native avec vos applications, API et services fédérés
- ✓ Déploiement rapide et administration simplifiée, pour limiter les risques projets et réduire le support utilisateur
- ✓ Réduction des couts directs et indirects

Open Sezam

Le spécialiste européen du ZTA

- ✓ Solution Antibot par essence (transparente pour l'utilisateur)
- ✓ Facteurs complémentaires invisibles et contrôle continu transparent
- ✓ Adaptation et contremesure en temps réel
- ✓ Trace cryptographique, sans rejet possible des signatures.
- ✓ Authentification sans mot de passe & MFA frictionless adaptatif
- ✓ Contrôle d'accès contextuel & adaptatif dynamiquement
- ✓ Évaluation continue du risque utilisateur (Continuous Risk Assessment)
- ✓ Détection de fraude avancée et apprentissage permanent de l'évolution des usages et de la menace
- ✓ **Conforme aux exigences RGPD/CNIL et d'accessibilité**

Open Sezam

Fiche Produit

AuthSezam®

CIAM

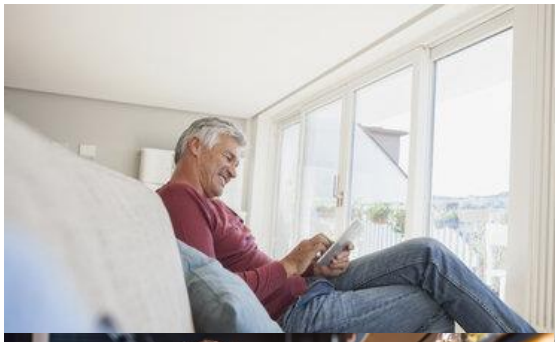
Simplifier l'expérience de vos clients, patients, bénéficières et partenaires avec une navigation sans friction

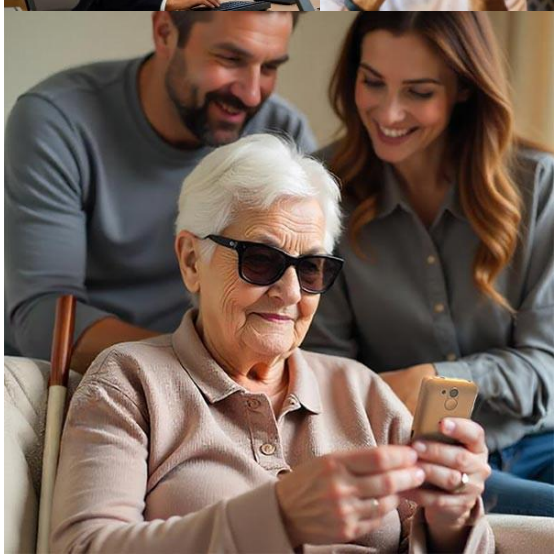
AuthSezam® permet à vos utilisateurs finaux de se connecter facilement, depuis un smartphone, un ordinateur personnel ou même un poste partagé – avec ou sans capteur biométrique.

Intégrée dans vos applications et portails digitaux, AuthSezam® garantit une connexion fluide et sécurisée grâce à des méthodes modernes et fiables de sécurisation ZTA :

- Biométrie multi-modale / détection de menaces par Jumeaux Numériques
- Lien magique sécurisé par trace cryptographique et IA Anti-Fraude
- Signatures cryptographiques non rejouables - Clés FIDO2 / passkeys
- Antibot de pointe « user-centric » / détection de menaces avancées

Bénéfices de la solution CIAM





✅ **Adoption rapide et intuitive**
Expérience fluide pour les clients, partenaires et utilisateurs finaux : aucune app à installer, aucun mot de passe à gérer.

✅ **Déploiement rapide dans vos portails et applications**
Intégration simple via API-first et standards ouverts (OIDC, SAML, FIDO2).

✅ **Réduction des coûts de support**
Suppression des mots de passe = fin des tickets liés aux réinitialisations ou blocages de comptes.

✅ **Conformité RGPD, NIS2**
Souveraineté européenne, traçabilité et respect de la vie privée.

✅ **Protection proactive contre le phishing**
Élimination des mots de passe = élimination des attaques par hameçonnage et vol d'identifiants.

✅ **Anti-bot par essence**
La solution détecte et bloque nativement les tentatives d'automatisation malveillantes (scripts, réseaux de bots) sans ajout de CAPTCHA intrusif qui dégrade l'expérience utilisateur.

✅ **Anti-fraude intégré (fraud by design)**
IA & détection comportementale embarquées : surveillance continue des connexions pour contrer en amont les tentatives de fraude (credential stuffing, usurpation de session, anomalies de parcours).

Réduction des coûts indirects grâce à une stratégie Zero Trust Access – User Centric

- Moins d'abandons clients dans les tunnels de souscription/achat grâce à une authentification fluide.
- Moins d'interruptions métiers liées aux réinitialisations de comptes.
- Amélioration de la satisfaction et de la fidélisation client.
- Rationalisation des solutions ZT
- Industrialisation de l'auditabilité et de la formalisation des rapports DPO/SSI

Solution éthique, avec un engagement fort et des efforts R&D continus en matière

- De protection des informations personnelles et respect de la vie privé
- D'inclusion numérique
- De frugalité / optimisation de la consommation énergétique des systèmes

Open Sezam

Fiche Produit

AuthSezam®

CIAM

Fonctionnalités de la solution AuthSezam® CIAM - Start

- IdP (Identity Provider) : Stockage et gestion des identités numériques des utilisateurs
- IdB (Identity Broker) : Délégation vers un ou plusieurs fournisseurs IDP
- SSO (Single Sign On) : Plateforme de fédération, permettant d'utiliser le même service d'authentification sur l'ensemble des applications connectées
- Authentification sans mot de passe : Connexion simplifiée par lien JWT, passkey, Webauthn, FIDO2... (Biométrie, authentification forte)
- Authentification forte sans agent : Système interopérable nativement avec les navigateurs et les équipements compatible (OIDC, SAMLV2, ...), sans enrôlement préalable
- Accès à l'interface d'administration : Accès complet pour la gestion et la surveillance
- Personnalisation du thème : Couleur et logo
- Souveraineté : Développée en France, conformité RGPD assurée et support adapté au contexte local.

Fonctionnalités étendues avec l'offre supérieure AuthSezam® CIAM – IA & Zero Trust Access

Comme indiqué plus haut, **AuthSezam®** peut être complété par un module Zero Trust avec un système de détection de fraude multidimensionnel combinant Intelligences Artificielles (IA), techniques de Mathématiques Avancées (MA) et Big Data.

Ce module intègre la technologie **SmartSezam®**, développée par Open Sezam, qui assure un contrôle continu de l'environnement de connexion avec une évaluation de risque individuelle en temps réel. **SmartSezam®** excelle dans l'identification des menaces avancées, telles que le credential stuffing ou des attaques orchestrées par des réseaux de bots sophistiqués.
Les méthodes d'analyse avancées de **SmartSezam®** minimisent les faux positifs, réduisant l'impact des interruptions pour les utilisateurs légitimes, garantissant ainsi une expérience utilisateur fluide et sécurisée.

En cas de détection de comportement suspect, il est ainsi possible de mettre en place les mesures de sécurité ciblées, comme la suspension temporaire des comptes ou l'activation d'une authentification multi-facteurs renforcée.

- ✓ **Évaluation adaptative continue des autorisations / Assistance automatisée pour l'optimisation des règles de sécurité :** Recommandations en temps réel pour adapter/automatiser les paramètres de sécurité et améliorer en permanence la gestion des faux positifs/négatifs.
- ✓ **Réduction des faux positifs :** Grâce à une analyse humaine précise, minimiser l'impact sur les utilisateurs légitimes.
- ✓ **Mise en place de contre-mesures ciblées :** Suspension temporaire ou MFA renforcé uniquement pour les comptes suspectés.
- ✓ **Détection des menaces complexes :** Identifier et bloquer des menaces humaines ou des réseaux de bots sophistiqués avec une réévaluation continue de la sécurité du contexte de connexion .
- ✓ **IMFA – Invisible MFA :** Ajout de facteurs supplémentaires transparents avec trace cryptographique et évaluation des risques à partir de la biométrie multimodale.

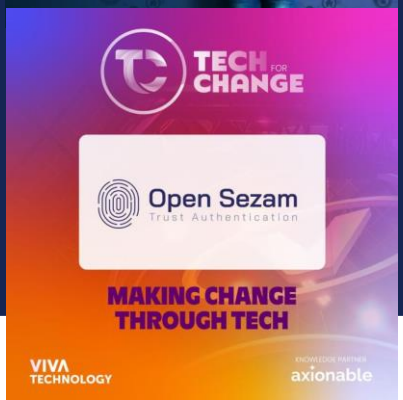
Points forts

Autonomie stratégique et exigences Européenne
100% conforme au RGPD, hébergé dans l'UE — approuvé par des secteurs hautement réglementés (Défense, Santé, Services Publics).

Agile et modulaire par conception
Conçu pour évoluer : architecture API-first, compatible SIEM (Push/ELK), intégration facile dans les couches de sécurité existantes, dans vos infrastructures ou dans le cloud.

Impact axé sur le business de l'entreprise
Réduit le CAC, les coûts de support et d'exploitation, améliore la conversion et sécurise la croissance numérique à grande échelle.

Flexibilité cloud-native + On Perm
Léger et facile à déployer, tant pour le cloud que pour les environnements réglementés.



Open Sezam

Critères	AuthSezam® CIAM START	AuthSezam® CIAM IA & Zero Trust ACCESS
Méthode d'authentification	Système d'authentification au choix : 1FA, 2FA, MFA, forte et continue Supporte diverses méthodes, sans mot de passe (lien ou biométrique) incluant l'intégration avec Windows Hello pour l'authentification faciale, par empreinte digitale ou PIN	
Sécurité embarquée	Authentification forte par validation cryptographique, sans rejeu possible des signatures biométriques Contrôle des accès par combinaison de facteurs de sécurité de base : • facteur d'authentification : Lien sécurisé avec trace cryptographique ou Signature du capteur d'empreinte ou FIDO • IP filtering • Domaines	Contrôles de sécurité supplémentaires pour vérifier : • l'environnement du navigateur • Le dispositif (notamment sa fréquence d'utilisation) Cette suite offre une sécurité "Zero Trust by Design" : • Dès la première connexion renforcement de la traçabilité des accès et la maîtrise du contexte de connexion • Evaluation de risque de chaque connexion de chaque utilisateur en temps réel tout au long de l'utilisation des services avec les applications compatibles • Contrôle continue et sécurité adaptative • Détection de nouveaux profils de risques et adaptation à l'évolution de la menace • Détection de menaces/fraudes personnalisables pour prendre en compte les besoins ou risques spécifiques de l'organisation • Assistance à l'optimisation des règles de sécurité • Pseudonymisation/Anonymisation des données sensibles par traitement
Déploiement SaaS / Hybride / On Premise et prérequis	SaaS • Nom de domaines • Accès SMTP • Application compatible OpenID-OIDC/ SAMLV2 On-Premise : + Serveurs Ubuntu	• Intégration simple par requête/exécution JavaScript, • ou avancée, par intégration proxy ou applicative pour plus d'options d'analyse (IA sur mesure, IA sophistiquées…)

Open Sezam

Confidentiel

Critères

AuthSezam®

	CIAM START	CIAM - IA & ZERO TRUST ACCESS
Authentification continue	x	oui pour les services compatibles
Orchestration et sécurité adaptative	x	En option
IA Contrôle d'Accès Zero Trust **Sécurité évoluée avec des fonctionnalités de détection de fraude avancées étendue au contrôle continue et à l'authentification adaptative, combinant des techniques de mathématiques avancées ey des IA (ex des ML, des LLM…) en apprentissage permanant pour s'adapter à l'évolution de la menace** Volume de données analysées : quelques centaines à quelques centaines à quelques milliers de données de connexion, issues de 3 sources de données : - Biométrie technique - Biométrie comportementale - Donnée d'authentification (Signature des capteurs biométriques ou lien de connexion) Périmètre Open Once et Always Auth	x	oui
IA d'apprentissage et d'adaptation à l'usage et à la menace Dispositif de sécurité complété par des Intelligences Artificielles d'apprentissage permanent pour renforcer vos stratégies de gestion des accès en fonction des usages et de l'évolution de la menace	x	oui
IA sur mesure Ajout d'intelligences Artificielles et techniques de Mathématiques Avancées (MA) sur mesure pour prendre en compte vos usages et risques spécifiques	x	sur devis (nombres d'IA / nb d'ateliers / dimensionnement d'infrastructure)
Explicabilité technique par log (traçabilité)	oui	oui
Explicabilité approfondie Génération de rapports, analyse automatisée…	x	Sur devis (rapport SaaS / connecteur / support N2)
Installation et interopérabilité Pas de nécessité d'infrastructure serveur local. Aucune application à installer côté client Compatible : OPEN ID/OIDC/OAUTH2, SAMLV2, WEBAUTHN, WINDOWS HELLO, Microsoft EntraID, FIDO2, Yubikey, Gestionnaire de mot de passe…	oui	oui