

# Nous vous offrons **sécurité, confidentialité** et **anonymat** dans vos communications.

---

## Introduction

Dans ce livre blanc, nous explorerons en détail comment Enigm garantit la protection des informations des utilisateurs, la confidentialité des conversations et l'anonymat au sein de la plateforme. Vous découvrirez comment Enigm redéfinit les normes de la communication numérique en offrant un environnement dans lequel les utilisateurs peuvent se connecter sans crainte d'intrusion ou de surveillance indésirable.

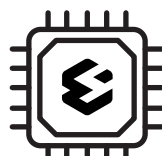
Notre solution repose sur quatre composants essentiels:



App



Serveurs



eSIM



Réseau

# App

## Fonctionnalités

Toutes les fonctionnalités d'Enigm sont conçues pour garantir que vos communications sont sécurisées, privées et anonymes. En mettant l'accent sur l'innovation et la protection, notre application de messagerie vous offre un outil complet pour protéger votre vie privée et garder un contrôle total sur vos données.

L'application vous permet d'envoyer des messages texte et multimédia, tels que des photos, des vidéos et des documents, tous protégés par un cryptage de bout en bout, garantissant que seuls vous et le destinataire pouvez y accéder. De plus, vous pouvez définir la durée de vie des messages, leur permettant de s'autodétruire après une période spécifique, éliminant ainsi toute trace de la conversation. Vous pouvez également joindre des fichiers en toute sécurité, sachant qu'ils sont protégés par le même cryptage robuste qui sécurise vos messages. Pour protéger votre identité, les audios envoyés peuvent être modulés, afin que votre voix ne soit pas reconnue. L'application intègre un système anti-capture d'écran, qui détecte et empêche toute tentative de capture pour protéger la confidentialité de vos messages.

Quant aux appels vocaux et appels vidéo, vous pouvez les passer avec la certitude qu'ils sont cryptés de bout en bout, garantissant ainsi que vos communications sont totalement privées. De plus, pendant les appels et les appels vidéo, vous pouvez moduler votre voix pour protéger votre identité. Nous mettons en œuvre un système qui empêche l'enregistrement des conversations et la capture des appels vidéo, garantissant la totale confidentialité de vos interactions.

L'application permet également la création de groupes de travail, où les communications sont cryptées et l'anonymat des utilisateurs est rigoureusement protégé. Dans ces groupes, les utilisateurs ne peuvent pas voir ou interagir en privé avec d'autres membres qu'ils n'ont pas comme contacts, préservant ainsi l'anonymat. Le créateur du groupe a la possibilité de définir des contrôles d'autorisation stricts, par exemple qui peut envoyer des messages, supprimer des messages, transférer des messages, etc., garantissant ainsi que le groupe fonctionne sous un régime de gouvernance.



Anti-capture



Destruction messages



Modulateur de voix



Inhibiteur d'enregistrements



Gestion de la confidentialité

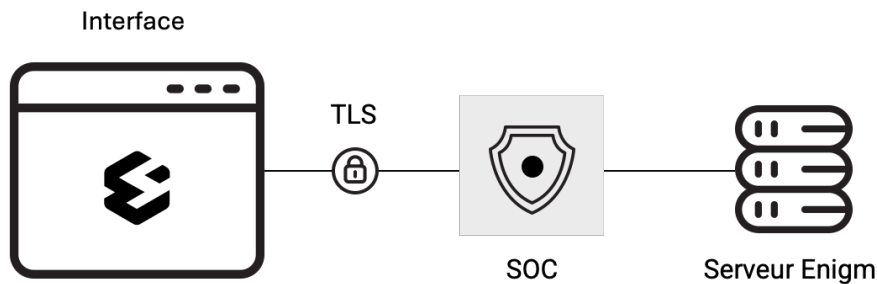


Privacité utilisateurs

“ Enigm **ne stocke aucun message sur le téléphone**, pas même dans la mémoire cache. Enigm empêche la récupération de données par le biais de techniques juridico légales. ”

## Interface

Sur notre plateforme, la sécurité et le contrôle total de votre compte et de vos appareils sont des aspects fondamentaux. C'est pourquoi nous avons développé une interface de contrôle Web intuitif et puissant qui vous permet de gérer tous les aspects de votre compte en toute sécurité et facilement. Du contrôle des appareils connectés à la gestion complète de votre compte, notre panneau de contrôle Web vous fournit tous les outils nécessaires pour garantir votre confidentialité et votre sécurité.



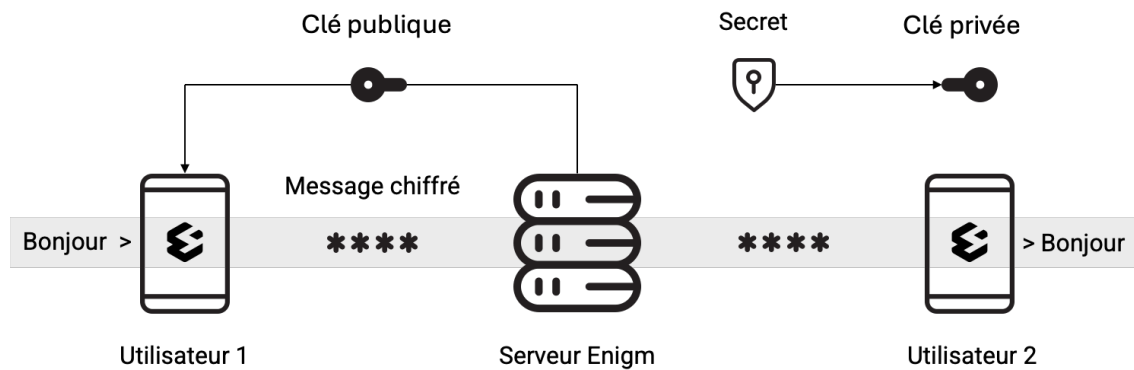
Notre interface de contrôle web vous permet d'avoir un contrôle exhaustif sur les appareils connectés à votre compte. Vous pouvez voir tous les appareils qui ont accès et, si nécessaire, vous déconnecter à distance de chacun d'entre eux, en vous assurant que seuls les appareils autorisés ont accès à votre compte. De plus, vous pouvez activer ou désactiver les notifications push en fonction de vos préférences et de vos besoins en matière de confidentialité, garantissant ainsi de recevoir des alertes uniquement sur les appareils de votre choix.

La gestion de votre compte est également simple et sécurisée via l'interface de contrôle Web. Vous pouvez décider si votre compte est visible sur le serveur public ou si vous préférez qu'il ne soit accessible que sur des serveurs privés, contrôlant ainsi qui peut vous trouver et communiquer avec vous. Si jamais vous avez besoin de récupérer votre mot de passe, vous pouvez le faire en utilisant la phrase secrète générée lors de l'inscription, vous permettant de restaurer votre accès rapidement et en toute sécurité. Vous avez également la possibilité de modifier votre code PIN et votre mot de passe à tout moment pour maintenir la sécurité de votre compte, en les adaptant à vos besoins.

De plus, l'interface vous donne la possibilité de supprimer toutes les données associées à votre compte, y compris les messages et les fichiers multimédias, ne laissant que votre profil et votre liste de contacts si vous le souhaitez. Et si vous décidez que vous ne souhaitez plus être sur notre plateforme, vous pouvez supprimer définitivement votre compte, en disparaissant complètement et sans laisser de trace, comme si vous n'aviez jamais existé.

## Chiffrement

Nous intégrons la technologie de cryptage et de sécurité la plus avancée pour protéger la confidentialité de vos conversations. Du cryptage AES-256 à l'utilisation d'algorithmes post-quantiques et de signatures numériques, notre objectif est de garantir que vos messages restent sécurisés et privés à tout moment.



Dans notre système de messagerie, le chiffrement est la pierre angulaire de la sécurité des données. Nous utilisons le cryptage AES-256 pour garantir que chaque message envoyé est protégé de bout en bout. AES-256 est un algorithme de chiffrement largement reconnu pour sa robustesse et sa sécurité, utilisant une clé de 256 bits pour protéger efficacement les données.

En plus du cryptage AES-256, nous mettons en œuvre une technologie post-quantique pour renforcer encore notre sécurité. Nous utilisons l'algorithme Kyber pour générer et gérer les clés de chiffrement. Kyber est un système cryptographique spécialement conçu pour résister aux attaques des ordinateurs quantiques, garantissant ainsi la longévité et la sécurité de nos clés dans un environnement technologique de plus en plus avancé.

Pour garantir l'authenticité et l'intégrité des messages, chacun est signé numériquement à l'aide de l'algorithme Dilithium. Cette signature numérique offre une couche de sécurité supplémentaire en garantissant que les messages n'ont pas été modifiés pendant le transit et proviennent de la source attendue.

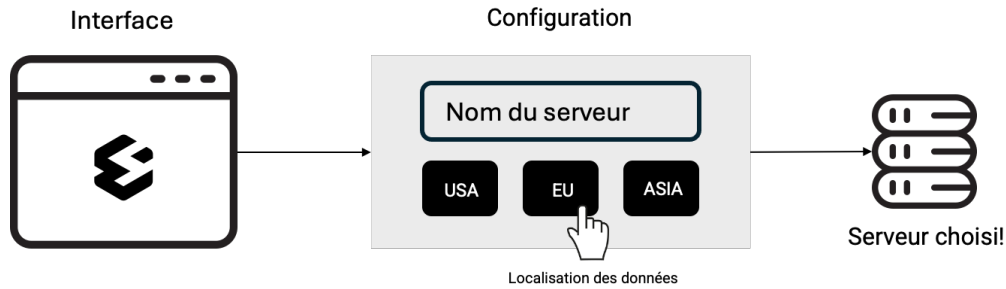
Enfin, pour protéger les clés de chiffrement utilisées dans notre système, nous mettons en œuvre un système de secrets qui distribue des fragments de clés entre différentes entités autorisées. Cette approche garantit que même si un fragment de clé est compromis, la clé entière ne sera pas accessible sans la collaboration de plusieurs parties autorisées.

En résumé, notre système de messagerie utilise une combinaison de cryptage AES-256, d'algorithmes post-quantiques tels que Kyber, de signatures numériques Dilithium et d'un système de secret pour assurer la sécurité et la confidentialité des communications de nos utilisateurs. Grâce à ces mesures en place, nos utilisateurs peuvent communiquer en toute confiance, sachant que leurs données sont protégées à tout moment.

## Serveurs

### Fonctionnalités

Notre plateforme offre également la flexibilité et le contrôle dont vous avez besoin grâce à la possibilité de configurer et de gérer vos propres serveurs. Tout utilisateur d'Enigm peut disposer de ses propres serveurs, permettant une personnalisation et un contrôle complets de son infrastructure de communication. Ces serveurs peuvent être déployés dans l'emplacement géographique souhaité par l'utilisateur, facilitant ainsi le respect des réglementations locales en matière de données et optimisant la vitesse et l'efficacité des communications.



Grâce à ces serveurs, les utilisateurs peuvent demander à l'application de se connecter spécifiquement à leur serveur privé. Cela garantit que l'utilisateur conserve un contrôle total sur ses données, garantissant que les informations sont toujours sous sa supervision et sa gestion. Cette capacité à diriger le trafic des applications vers un serveur spécifique offre une couche supplémentaire de sécurité et de confidentialité.

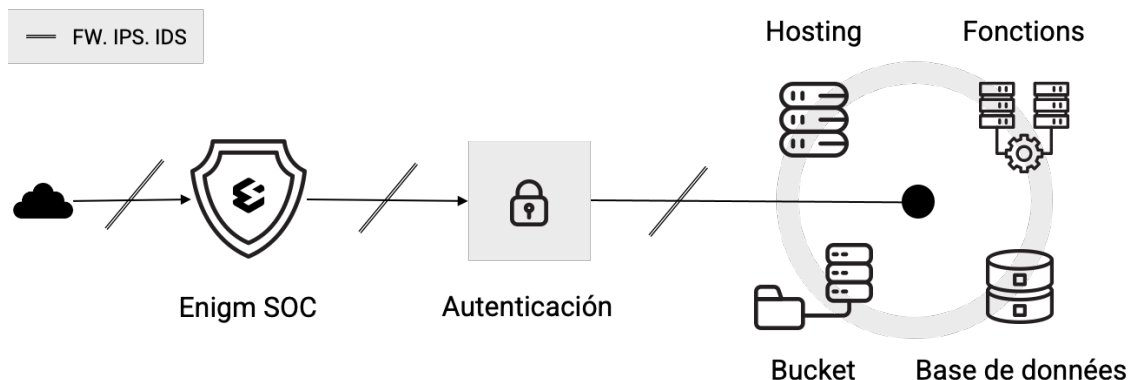
De plus, les utilisateurs ont la possibilité de supprimer des données de leur serveur, y compris tous les messages échangés par les membres appartenant à ce serveur. Cette fonctionnalité est cruciale pour maintenir la propreté et la sécurité des données, permettant à l'utilisateur de gérer efficacement ses informations.

La gestion des membres du serveur est une autre fonctionnalité essentielle. Les utilisateurs peuvent gérer qui a accès au serveur et peuvent expulser et supprimer les membres indésirables. De plus, ils peuvent choisir de supprimer uniquement les informations qu'un membre spécifique a laissées sur le serveur sans avoir besoin de supprimer complètement le membre. Cette flexibilité dans la gestion des utilisateurs et des données garantit que chaque serveur peut être personnalisé selon les besoins spécifiques de son propriétaire.

En bref, vous pouvez facilement déployer des serveurs privés dans des emplacements géographiques spécifiques, connecter l'application à ces serveurs et gérer les données et les membres de manière globale, garantissant ainsi une expérience utilisateur sécurisée, privée et personnalisable.

## Architecture

Notre architecture de serveur est conçue en mettant méticuleusement l'accent sur la sécurité et l'efficacité. Nous mettons en œuvre une série de technologies avancées et de pratiques de sécurité rigoureuses pour garantir que les données de nos utilisateurs sont protégées à tout moment.



Dans notre infrastructure, nous utilisons un système de pare-feu applicatif et un système de détection d'intrusion (IDS) pour protéger nos applications contre les menaces et les attaques. Ce pare-feu agit comme la première ligne de défense, filtrant le trafic malveillant et garantissant que seul le trafic légitime puisse accéder à nos applications. De plus, l'IDS nous permet de détecter et de répondre rapidement à toute activité suspecte susceptible de compromettre la sécurité de nos systèmes.

Notre backend est construit sur une plateforme qui offre des fonctions d'authentification, de bases de données en temps réel, de stockage et de cloud. L'authentification garantit que seuls les utilisateurs autorisés peuvent accéder à nos services. Les bases de données en temps réel nous permettent de gérer et de synchroniser les données efficacement, garantissant une expérience d'utilisation fluide et réactive. Le stockage cloud est utilisé pour gérer les fichiers et autres données utilisateur, tandis que les fonctions cloud nous permettent d'exécuter la logique backend de manière sécurisée et évolutive.

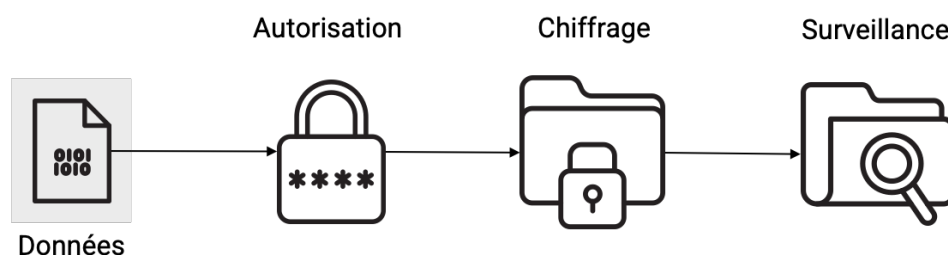
Toute cette infrastructure est protégée sous un système de validation des applications et configurée avec des règles de sécurité strictes. Ces règles s'appliquent à la fois aux compartiments de stockage et aux bases de données, garantissant que les données ne sont accessibles qu'aux utilisateurs et processus autorisés. Cela garantit que les données sont protégées contre tout accès non autorisé et répondent aux normes de sécurité les plus élevées.

De plus, nous mettons en œuvre des systèmes de surveillance de la sécurité par l'Intelligence Artificielle pour surveiller en permanence l'état de notre infrastructure et détecter d'éventuelles vulnérabilités. Cependant, il est important de souligner que ces systèmes de surveillance ne stockent ni n'analysent aucune donnée permettant d'identifier nos clients. Nous nous concentrons sur le maintien de la confidentialité de nos utilisateurs, en veillant à ce que toutes les informations personnelles restent confidentielles et sécurisées.

En bref, notre architecture de serveur est soigneusement conçue pour allier haute sécurité et efficacité opérationnelle. De la protection périmétrique au backend sécurisé et à la surveillance continue, chaque composant de notre infrastructure fonctionne ensemble pour fournir un environnement sécurisé et fiable pour nos applications et les données de nos utilisateurs.

## Protection des données

La protection des données sur nos serveurs est l'une de nos principales priorités. Dans un environnement numérique où les menaces de sécurité sont de plus en plus sophistiquées et persistantes, nous avons mis en œuvre une série de mesures avancées pour garantir que les informations de nos utilisateurs restent sécurisées et privées à tout moment.





## Autorisation

Pour garantir une sécurité et une confidentialité maximales des données hébergées sur nos serveurs, nous avons mis en place un système de contrôle d'accès rigoureux au niveau des enregistrements dans notre base de données. Ces règles, méticuleusement définies et gérées via notre plateforme backend, jouent un rôle essentiel dans la protection des informations sensibles. Chaque fois qu'une opération de lecture ou d'écriture est effectuée, ces règles sont minutieusement évaluées, garantissant que seuls les utilisateurs authentifiés et correctement autorisés peuvent accéder aux données correspondantes. Cette approche permet non seulement de contrôler précisément qui peut accéder à quelles informations, mais permet également une adaptation dynamique à mesure que les exigences d'accès évoluent. De cette manière, nos systèmes garantissent l'intégrité et la confidentialité des données, garantissant que seules les personnes disposant des autorisations appropriées peuvent interagir avec elles, renforçant ainsi la sécurité et la confidentialité à toutes les étapes de la gestion des données.

## Chiffrement

Pour protéger les données sur nos serveurs, nous utilisons une approche de cryptage avancée. Les données au repos sont cryptées au niveau des données avec AES-256, puis bénéficient d'un deuxième niveau de cryptage appliqué par notre plateforme backend, offrant une double couche de sécurité. De plus, au niveau du disque, nous appliquons un cryptage supplémentaire, garantissant que les données sont protégées sur toutes les couches de stockage. Ce triple cryptage garantit que même si un niveau de cryptage était compromis, les données resteraient protégées.

Pour les données qui n'ont pas besoin d'être réversibles, nous utilisons un processus de hachage avec des sauts dynamiques générés aléatoirement pour augmenter la résistance aux attaques par force brute. Chaque hachage est en outre crypté avec AES-256, augmentant ainsi sa sécurité.

Les données en transit sont protégées à l'aide de TLS 1.3 et nous appliquons un cryptage transactionnel supplémentaire pour protéger les données de la payload et empêcher les attaques par Sniffing. Cela garantit une sécurité maximale à toutes les étapes de la transmission et du stockage des informations.

De plus, nous mettons en œuvre une politique de rotation régulière des clés via notre système de secrets, ce qui augmente encore la sécurité. Nous effectuons des audits réguliers de nos systèmes de cryptage et de sécurité pour garantir leur efficacité et mettons à jour nos pratiques pour inclure des algorithmes résistants aux attaques quantiques, renforçant ainsi la protection des données à long terme.

**“ Les données stockées sur nos serveurs ne peuvent être déchiffrées qu'avec les mots de passe de votre téléphone et notre système de secrets. Enigm ne peut pas les déchiffrer. ”**

## Surveillance

Pour renforcer encore la sécurité d'Enigm, nous disposons d'un système de surveillance soutenu par l'intelligence artificielle, conçu pour détecter et répondre de manière proactive aux nouvelles menaces. Ce système garantit la protection continue de notre environnement contre tout risque potentiel. De plus, nous avons mis en place une conservation maximale des Logs de 30 jours pour garantir la disponibilité des Logs nécessaires aux analyses et audits de sécurité ultérieurs. Il est important de noter qu'aucune donnée permettant d'identifier nos utilisateurs n'est stockée dans nos journaux et que toutes les métadonnées sont anonymisées avant d'être enregistrées par nos systèmes de surveillance de sécurité et notre équipe des opérations de sécurité (SOC). Cette mesure ajoute une couche supplémentaire de protection de la vie privée de nos utilisateurs, garantissant que leurs données personnelles sont totalement sécurisées et protégées contre tout risque potentiel d'exposition.



NOS CERTIFICATIONS

## Confidentialité et conformité

Enigm se conforme aux réglementations applicables en matière de confidentialité et de sécurité des données, telles que le Règlement général sur la protection des données (RGPD) de l'Union européenne et du California Consumer Privacy Act (CCPA). Nous nous engageons à respecter les lois et réglementations en vigueur pour protéger les droits et la vie privée de nos utilisateurs dans le monde entier.

Avec Enigm, les utilisateurs peuvent communiquer en toute tranquillité d'esprit, sachant que leurs données sont protégées par une infrastructure de sécurité de pointe qui donne la priorité à la confidentialité.

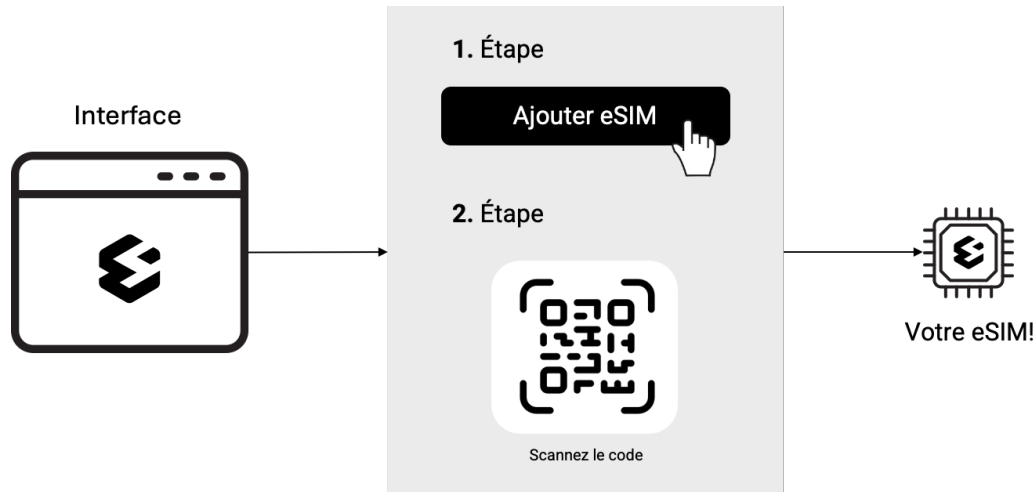
“ Nous ne **compromettons** ni ne vendons les données des utilisateurs à des tiers. ”



# eSIM

## Fonctionnalités

Notre eSIM anonyme offre un certain nombre de fonctionnalités uniques qui garantissent la sécurité et la protection de vos données en ligne.



En utilisant cette eSIM, votre fournisseur de réseau mobile local ne connaît pas votre véritable numéro de mobile, puisque vous êtes en itinérance. Cela garantit que des attaques telles que SimToolKit Attack ne peuvent pas être menées, garantissant ainsi l'intégrité et la confidentialité de vos communications.

De plus, notre application dispose d'un VPN intégré qui ajoute une valeur significative à la sécurité de vos données. Le VPN crypte toutes les communications sur votre appareil, garantissant ainsi que votre activité en ligne est protégée contre les intrusions et les attaques malveillantes, même sur les réseaux Wi-Fi publics ou non sécurisés. Cela fournit une couche de sécurité supplémentaire lors de l'utilisation de notre eSIM, garantissant que vos données sont protégées à tout moment.

Notre eSIM protège également contre la surveillance de la localisation des abonnés et la journalisation des appels, des messages et des sessions de données, garantissant ainsi la confidentialité de vos activités en ligne. En bref, notre eSIM anonyme combinée à notre VPN intégré à l'application offre une solution complète pour protéger vos données et assurer votre sécurité en ligne.

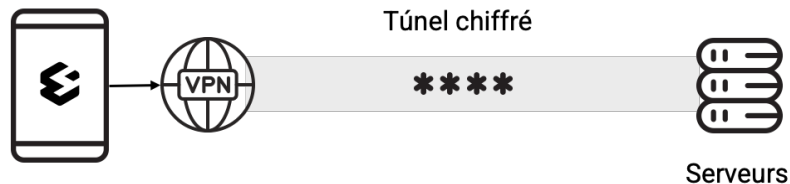
## Confidentialité et anonymat

Notre technologie eSIM se distingue par le fait d'offrir un service exclusivement axé sur les données, éliminant complètement le numéro de téléphone. Cette solution innovante vous permet de connecter instantanément votre appareil au réseau Global Mobile Data, vous offrant ainsi un accès rapide et fiable aux données mobiles dans presque tous les pays du monde, sans nécessiter de vérification d'identité, de carte SIM ou de documents. Notre service se distingue par sa totale confidentialité, puisque nous ne collectons aucune donnée utilisateur.

# Réseau

## Fonctionnalités

Chez Enigm, nous nous engageons à vous fournir non seulement une plateforme de communication sécurisée, mais également une couche de protection supplémentaire grâce à notre VPN intégré et à notre réseau de proxys qui protègent votre anonymat complet entre vous et nos systèmes.



Notre VPN offre une variété de fonctionnalités pour répondre aux besoins de sécurité et de confidentialité de chaque utilisateur. L'une des fonctionnalités clés est la possibilité de choisir si vous souhaitez que seule notre application utilise le canal VPN sécurisé ou si vous souhaitez que toutes les applications installées sur votre appareil bénéficient de cette protection supplémentaire.

De plus, notre VPN est conçu pour rester actif à tout moment, garantissant ainsi que toutes vos communications sont protégées à tout moment. Même si vous vous déconnectez du serveur pour quelque raison que ce soit, notre application se connectera automatiquement et immédiatement à un autre serveur, assurant une protection constante et ininterrompue.

En cas d'urgence, notre VPN intégré dispose d'une fonction Kill Switch, qui agit comme un interrupteur de sécurité dans les situations où la connexion VPN est perdue. Cette fonctionnalité bloque automatiquement tout le trafic sur votre appareil pour protéger votre identité et vos données en ligne, empêchant ainsi toute exposition indésirable en cas de déconnexion inattendue.

## Confidentialité et anonymat

Nous ne stockons aucun enregistrement ou Logs d'aucune sorte sur nos serveurs. Cela signifie que nous n'avons pas accès aux détails sur les connexions ou les activités de navigation de nos utilisateurs. Vos informations, y compris vos communications et votre activité en ligne, restent totalement privées pendant que vous utilisez ce service.





De plus, nos serveurs sont situés à l'étranger pour maximiser la confidentialité et la protection des données. Cela signifie qu'ils sont soumis à des lois et réglementations qui favorisent la confidentialité des données, offrant ainsi un environnement sûr et sécurisé pour stocker les informations.

L'utilisation de notre VPN ajoute une couche supplémentaire de cryptage au transport de données, garantissant une plus grande sécurité de vos communications en ligne et empêchant votre fournisseur de services de connaître vos destinations de connexion, préservant ainsi davantage votre confidentialité en ligne.

# Annexe

## Comparaison avec la concurrence

Dans cette comparaison, nous examinerons les fonctionnalités clés et les aspects de sécurité de notre application par rapport à certains des principaux concurrents du marché. Cela vous aidera à prendre une décision éclairée quant à la meilleure option pour vos besoins en matière de sécurité et de communication en ligne.

				
Aucune donnée requise	✓	✗	✓	✗
Message anti-récupération	✓	✗	✗	✗
Chiffrement de bout en bout	✓	✓	✓	✓
Cryptographie post-quantique	✓	✓	✗	✗
Service VPN intégré	✓	✗	✗	✗
Modulateur de voix	✓	✗	✗	✗
Inhibiteur d'enregistrement	✓	✗	✗	✗
Anti-capture d'écran	✓	✓	✗	✗
Serveurs privés	✓	✗	✓	✗
Conformité RGPD	✓	✗	✓	✗