Informations concernant la sécurité des **Messages Sécurisées**, proposées par Foxtrot (foxtrot.network).

Sécurité physique

Les serveurs utilisés se situent dans des centres de données ayant la certification suivante : *ISO 27001*.
« Cette certification impose à l'entreprise d'évaluer régulièrement les progrès et les performances de la sécurité de l'information. Ceci est divisé en 3 actions :
La surveillance : l'organisation doit évaluer les performances de la sécurité de l'information et l'efficacité du système de gestion de la sécurité de l'information.
L'audit interne : l'organisation doit effectuer des audits internes à intervalles planifiés pour fournir des informations indiquant si le système de gestion de la sécurité de l'information est toujours adapté à la situation.
L'examen du système : la direction doit examiner le système de gestion de la sécurité de l'information de l'organisation à intervalles planifiés pour s'assurer de son efficacité. »
Pour plus d'informations : *https://www.hetzner.com/unternehmen/zertifizierung*.

Sécurité logicielle

Nous installons et configurons nos serveurs pour être en capacité de résister aux attaques informatiques. Nous utilisons une distribution Linux (Ubuntu) ouverte.
Voici une liste de quelques logiciels et protocoles utilisés :

- SSH, pour communiquer avec nos serveurs de façon chiffrée. L'accès est stricte, et nécessite des mots de passe forts et une authentification à deux étapes (avec un code à six chiffres modifié toutes les 30 secondes).
- IPTables, en tant que pare-feu. Cela permet d'autoriser seulement le trafic légitime.
- Fail2ban, pour contrer les attaques par force brute.

De plus, nous faisons particulièrement attention à faire les mises à jour de sécurité, du système d'exploitation et des logiciels utilisés.

Technologie utilisée

Pour sécuriser le contenu de vos messages, nous utilisons un chiffrement de bout en bout qui s'effectue du côté client en Javascript.
Pour plus d'informations sur les algorithmes utilisés : *https://github.com/wwwtyro/cryptico*.

Procédés cryptographiques

Lors de la connexion, une clé publique (dérivée de votre mot de passe) est générée du côté client et est envoyée au serveur pour vérifier que les identifiants du compte sont corrects. En même temps, la clé privée est également générée et stockée uniquement du côté client avec *sessionStorage* (plus d'informations sur https://developer.mozilla.org/fr/docs/Web/API/Window/sessionStorage). Cette clé privée n'est jamais envoyée au serveur. La clé RSA est de 2048 bits.
Quand vous envoyez un message, en réalité deux messages sont envoyés :

- Un à votre destinataire : chiffrement avec sa clé publique, et votre clé privée (pour la signature, point que nous verrons après). Ce message permet à ce que votre destinataire voit votre message.
- Un à vous : chiffrement avec votre clé publique, et votre clé privée (pour la signature). Ce message permet à ce que vous voyez le message envoyé dans la conversation.

Le déchiffrement lui, nécessite seulement la clé privée. Sans elle, il est mathématiquement impossible de retrouver le contenu initial.

Signatures

Lors du chiffrement des données, nous utilisons (en plus de la clé publique), une clé privée pour vérifier la validité de la signature. De cette façon, si la signature est valide, alors les données ont été manipulées par le propriétaire. En revanche, si elle est invalide, cela signifie qu'une tierce personne a chiffré vos données à partir de votre clé publique.

Attention, nous vous avertissons si une erreur de signature intervient. Cela peut survenir si vous utilisez des caractères spéciaux.

Pour toutes questions supplémentaires, merci d'adresser la demande à l'adresse électronique suivante : *foxtrot.n@protonmail.com*.