

FICHE D'INFORMATION RADIOMESSAGERIE CRYPTÉE

Q : La norme POCSAG offre-t-elle une option de cryptage ?

R : Non. La norme POCSAG ne prévoit pas le cryptage des données dans le protocole lui-même.

Q : Un message d'échange peut-il être chiffré ?

R : Oui. À cette fin, le texte du message doit être crypté avant d'être transmis au centre de téléappel TELEPAGE ou le service de cryptage TELEPAGE doit être utilisé pour les téléavertisseurs Swissphone.

Q : Le centre de radiomessagerie TELEPAGE chiffre-t-il directement les messages de radiomessagerie ?

R : Non et oui. Étant donné que la norme POCSAG ne fournit pas de cryptage, nous ne sommes pas autorisés à chiffrer tous les messages par défaut. Cependant, il est possible d'envoyer des messages de pagination cryptés du côté du client en mode dit transparent (type de message 4, voir spécification du protocole UCP TELEPAGE). La méthode de cryptage utilisée n'est pas pertinente pour le centre de radiomessagerie. De plus, nous offrons un service de cryptage que le client doit commander spécifiquement. La méthode de cryptage Swissphone IDEA est utilisée, qui n'est compatible qu'avec les pagers Swissphone.

Q : Swissphone propose-t-il des options de cryptage ?

R : Oui. Swissphone propose son propre service de cryptage et ses serveurs de cryptage pour les principaux clients. Les téléavertisseurs Swissphone actuels peuvent être équipés de la fonction de cryptage (également par la suite).

Q : N'importe quel téléavertisseur Swissphone peut-il décoder les messages cryptés ?

R : Non. Vous avez besoin d'un pager de type DE910, DE915, DE925, RES. Q, TRIO, tous les modèles du type s.QUAD. Veuillez noter que la fonction de cryptage doit être activée dans le pager. En outre, le fichier clé utilisé pour le cryptage doit également être programmé dans le pager.

Q : Les téléavertisseurs non-Swissphone peuvent-ils également recevoir et décoder des messages cryptés ?

R : Oui. Toutefois, les téléavertisseurs non-Swissphone ne peuvent pas décoder les messages envoyés via nos services de cryptage. Les fabricants implémentent chacun un protocole propriétaire, puisque la norme POCSAG ne fournit pas de cryptage.

Q : Dois-je programmer les pagers spécifiquement ?

R : Oui. Vous devez activer la fonction de cryptage et programmer le fichier clé utilisé dans le pager. C'est la seule façon pour le pager de déchiffrer et d'afficher les messages reçus.

Q : Les messages de radiomessagerie chiffrés peuvent-ils être pêchés et enregistrés illégalement ?

R : Oui. Cependant, le message n'est plus lisible avec les outils connus, car votre message n'est plus lisible dans le texte en raison du cryptage. Par exemple, le message texte « Hello World » ressemble à ceci : « 2 * 6 26530557 * 650-49] 797---76 », dans lequel l'algorithme que nous utilisons crypte différemment le même message, ce qui rend le décryptage non autorisé encore plus difficile.

Q : Quelle est la méthode de cryptage proposée par Swissphone?

R: Swissphone propose un procédé propriétaire. Ceci est basé sur l'algorithme IDEA 128 bits

Q : La méthode de cryptage IDEA 128 bits est-elle sécurisée ?

R: Nous n'avons pas connaissance à ce jour d'un piratage de la méthode IDEA 128 bits. La méthode de cryptage IDEA 128 bits a été développée par des spécialistes de la cryptographie de l'ETH Zurich et licenciée par Swissphone.

Q : Comment puis-je crypter mes messages ?

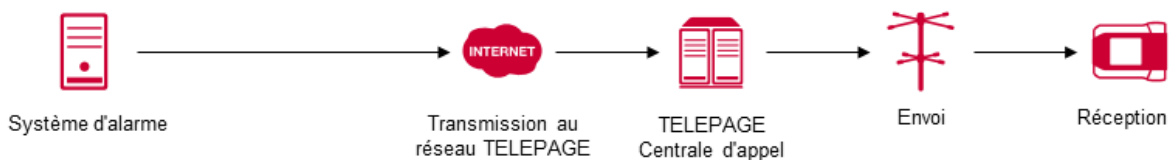
R : Nous offrons trois options :

1. Vous utilisez le service de cryptage de Swissphone. Vous envoyez les messages au centre de radiomessagerie TELEPAGE. Selon les besoins, cette transmission peut également être sécurisée TLS. Le centre de radiomessagerie chiffre ensuite les messages de pagination en fonction du numéro de téléphone. C'est la procédure la plus simple que nous recommandons, car il n'y a pas d'interfaces supplémentaires à développer ou de serveurs à construire.
2. Chiffrement à l'aide de serveurs de chiffrement PNC. Le PNC est installé sur le site du client et peut également être utilisé de manière redondante. Après le chiffrement des messages, le PNC envoie automatiquement le message de pagination au centre de radiomessagerie TELEPAGE. Cela correspond au chiffrement de bout en bout.
3. Si vous utilisez un serveur d'alarme de type I.SERACH, vous pouvez déjà chiffrer les messages de pagination dans I.SEARCH et les transmettre au centre de radiomessagerie TELEPAGE. Ainsi, vous avez également la possibilité de cryptage de bout en bout.

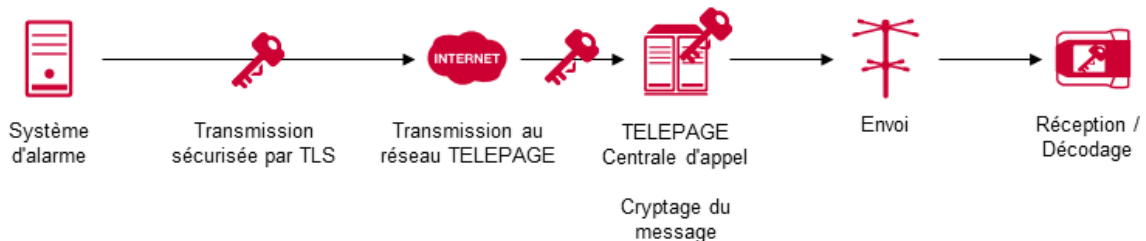
Q : Qu'est-ce que le cryptage de bout en bout ?

R : Avec le chiffrement de bout en bout, le message est chiffré avant d'être envoyé dans l'environnement client. Le message reste crypté sur tous les chemins de transmission et n'est déchiffré et lisible que sur le pager.

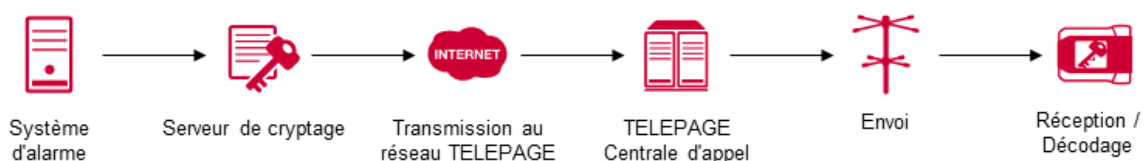
Envoi de la radiomessagerie non cryptée



Envoi crypté de la radiomessagerie avec le service de cryptage TELEPAGE



Envoi de paging crypté de bout en bout



Q: Quel est le niveau de sécurité du service de cryptage de Swissphone?

R: Si vous utilisez le service de cryptage de Swissphone, vous devez vous assurer que les messages de votre point de déclenchement vers le serveur de cryptage sont sécurisés. Cela peut être fait, par exemple, en utilisant des certificats TLS (anciennement certificats SSL). Des connexions via des réseaux virtuels privés (VPN) sont également envisageables.

Q : J'utilise IMASYS Messaging Gateway. La pagination peut-elle chiffrer les messages ?

R : IMASYS ne chiffrera pas les messages de pagination. Cependant, le service de chiffrement du réseau de radiomessagerie TELEPAGE peut alors chiffrer le message.

Q : Quand puis-je commencer à utiliser les fonctionnalités de cryptage ?

R: Les services de cryptage sont introduits sur le marché et peuvent être commandés à tout moment.

Q : Comment puis-je introduire le cryptage ?

R: Il est préférable de contacter votre partenaire commercial ou notre service client. Nous sommes heureux de prendre rendez-vous pour clarifier vos besoins et de faire une offre adaptée à vos besoins.

Nos options de contact:

Swissphone Wireless SA
Fälmisstrasse 21
CH-8833 Samstagern
www.swissphone.com

Demandes de renseignements techniques

Centre d'exploitation Telepage
opc@swissphone.com

Hotline pour nos clients et partenaires

Téléphone: 0848 88 99 99
Courriel : cc@swissphone.com