Cryptage

SWISSPHONE

Transmettre des messages sensibles de manière cryptée

Envoi de messages de radiomessagerie conforme à la protection des données via TELEPAGE®

La protection des données : sujet sensible

Les données personnelles ou les données des clients qui méritent d'être protégées sont transmises par diverses institutions : par exemple lors de l'alerte des organisations d'urgence, lors de la transmission de données par les banques, les assurances ou les autorités, ainsi que dans le secteur de la santé. Pour respecter les directives de protection des données, il faut s'assurer que des personnes non autorisées ne puissent pas consulter ou transmettre des données sensibles et dignes de protection.

Cadre juridique

Loi sur les services de télécommunication
En tant qu'exploitant du réseau de radiomessagerie TELEPAGE®, Swissphone est tenu de respecter le secret des communications conformément à la loi sur les services de télécommunication, chapitre 7, art. 43 : « Quiconque est ou était chargé de tâches relevant des services de télécommunication ne doit pas fournir à des tiers des indications sur le trafic de télécommunication des abonnés et ne doit donner à personne la possibilité de transmettre de telles indications ».

Ainsi, la transmission, l'analyse ou la simple observation de vos données par l'opérateur de réseau est réglementée – il ne peut pas exploiter les données ni même les rendre accessibles à des tiers.

Au chapitre 7, article 43, l'utilisation abusive des données de télécommunication par des tiers est réglementée et punie : « Quiconque reçoit, au moyen d'une installation de télécommunication, des informations non publiques qui ne lui sont pas destinées et les utilise ou les communique à des tiers sans autorisation est puni d'une peine privative de liberté d'un an au plus ou d'une peine pécuniaire ».

Par conséquent, l'écoute, l'enregistrement ou même la retransmission de données de télécommunication sont clairement illégaux et interdits.

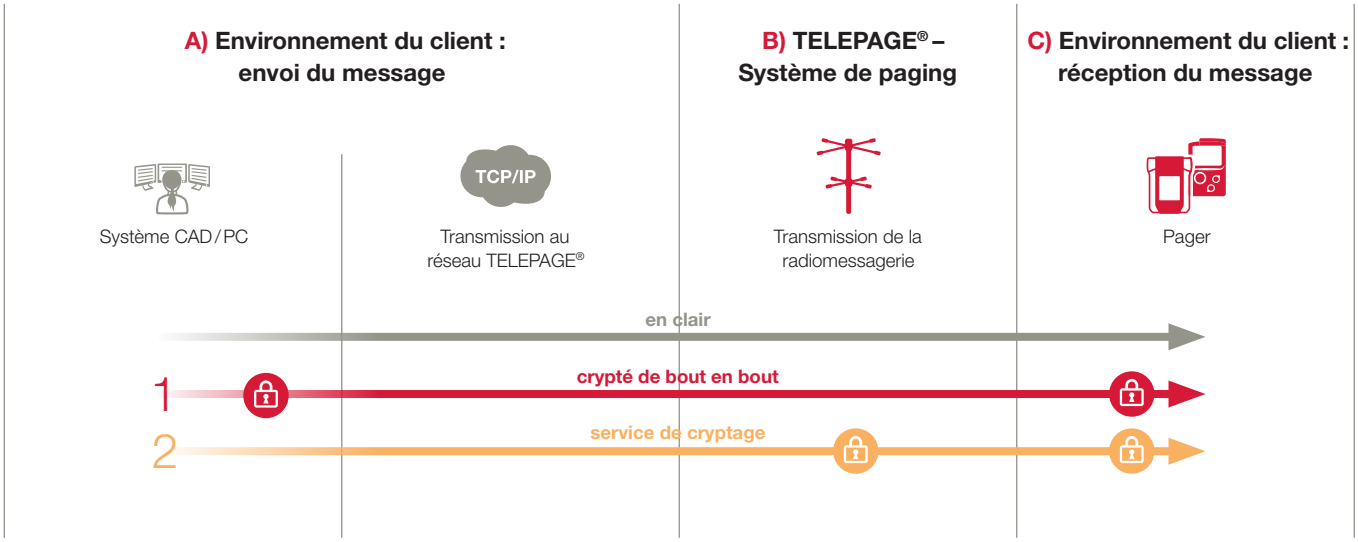
Responsabilité de l'utilisateur d'applications de télécommunications
L'utilisateur des applications de télécommunication doit toutefois se demander dans quelle mesure il a affaire à des données (particulièrement) sensibles et doit prendre des mesures supplémentaires. La loi fédérale sur la protection des données indique quelles données doivent faire l'objet d'une protection particulière.

Loi fédérale sur la protection des données
La loi fédérale stipule à l'article 3, alinéa c, que les données personnelles sensibles ne doivent pas être publiées – et doivent donc être protégées. Cela vaut notamment pour les données concernant

- à la santé,
- la sphère intime,
- les opinions religieuses ou
- les mesures d'aide sociale.

Avec le cryptage des messages de radiomessagerie, vous êtes sûr de satisfaire aux exigences en matière de sécurité des données.

Solutions pour assurer la protection des données



A) Le cryptage des données peut être effectué directement au niveau de l'organisme déclenchant l'alarme (système de contrôle, serveur d'alarme) par le biais de solutions de cryptage intégrées sur place (matériel / logiciel).

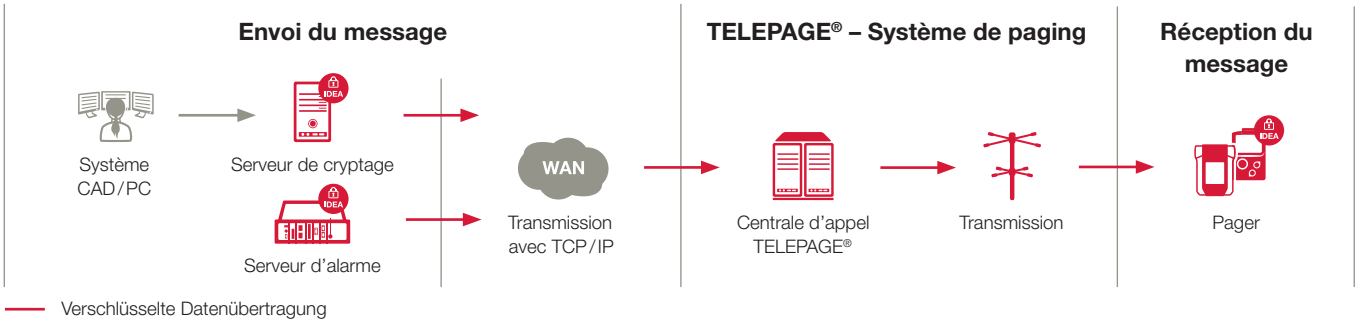
B) Le système de paging TELEPAGE®, en tant que standard ouvert, peut recevoir des messages codés et les transmettre à des tiers envoyer : Le client est libre de choisir la méthode de cryptage correspondante.

C) Après réception du message dans le pager, les données transmises sous forme cryptée doivent être décryptées. Ce n'est qu'ainsi qu'elles peuvent être lues par le destinataire.

Solutions de cryptage Swissphone

1 Cryptage de bout en bout

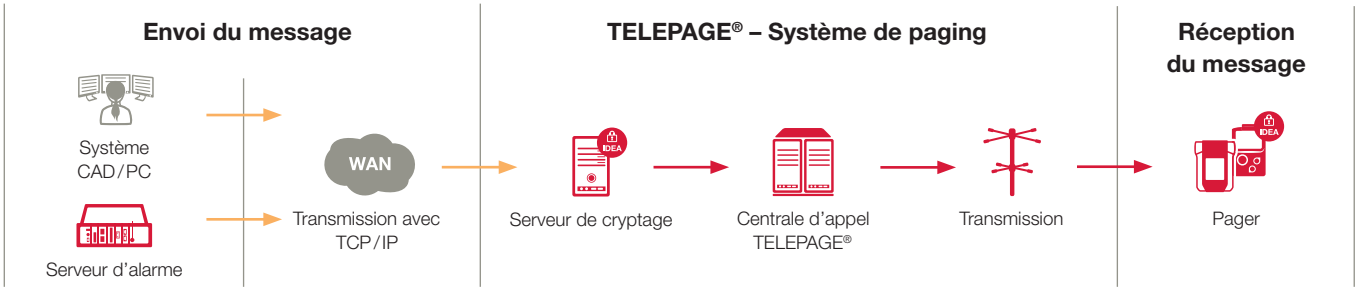
Une solution globale d'un seul tenant offre la plus grande sécurité possible.



- Le **« serveur de cryptage sur site »** convient aux centres de contrôle ou aux centres d'appels. Le volume plus élevé de messages, les nombreux numéros d'appel concernés ou l'autonomie souhaitée justifient une solution de sécurité complète. Dans ce cas, le serveur de cryptage est installé chez le client. Afin de garantir la disponibilité du système, celui-ci peut être exploité de manière redondante. Le serveur envoie les messages cryptés via les réseaux publics à la centrale d'appel TELEPAGE®. Nous proposons sur demande des solutions globales, des logiciels de cryptage et des contrats de maintenance.
- L'option **I.SEARCH IDEA-Cryptage** est la solution optimale pour les entreprises disposant d'applications de serveur d'alarme spécifiques à l'entreprise. Les messages sont cryptés directement dans le serveur d'alarme I.SEARCH, envoyés localement sur le site de l'entreprise ou au reseau national de TELEPAGE®. Les serveurs d'alarme I.SEARCH existants peuvent être étendus avec l'option IDEA.

2 Service de cryptage

Respecter les directives de protection des données grâce aux services de TELEPAGE®



- Le service qui déclenche l'alarme utilise en option, dès la transmission à TELEPAGE®, des certificats **TLS** (anciennement certificats SSL) qui sécurisent le transfert de données comme pour l'e-banking. La transmission à la centrale d'appel TELEPAGE® s'effectue au moyen du protocole UCP TELEPAGE®.
- Le service de **cryptage de TELEPAGE®** crypte le message selon le procédé DiCal-IDEA. Le client s'abonne à un service supplémentaire pour les numéros d'appel, qui doivent recevoir des messages codés.
- Cette solution convient aux organisations qui reçoivent des messages contenant des données sensibles, mais qui ne peuvent pas ou peu influencer l'envoi des messages. Cette solution ne nécessite pas d'adaptations ou d'investissements spécifiques de la part de l'organisme qui déclenche l'alerte.

Terminaux de radiomessagerie pris en charge

La méthode de cryptage utilisée doit être supporté par les pagers utilisés. La méthode de cryptage DiCAL-IDEA utilisée par Swissphone est compatible avec les pagers Swissphone à partir de la gamme DE925, RES.Q et s.QUAD. Pour cela, le client a besoin d'une licence de cryptage IDEA par pager.

Le cryptage comme tâche globale avec diverses interfaces

Une solution de cryptage doit être considérée, planifiée et réalisée de manière globale. Ce n'est pas le choix d'un procédé particulier qui fait la qualité de la solution de chiffrement, mais la prise en compte judicieuse de tous les aspects.

Selon Auguste Kerckhoffs (cryptologue néerlandais 1835-1903), la sécurité d'un procédé de cryptage repose sur le secret de la clé et non sur le secret de l'algorithme de cryptage.

Cela signifie qu'en plus des solutions techniques, la gestion des clés, les droits d'accès et les aspects opérationnels liés à la génération des clés, à la programmation des terminaux et à la gestion des clés revêtent une très grande importance. Dans ce domaine, Swissphone propose un service complet avec s.ONE Fleet : s.ONE Fleet permet une mise à jour rapide et une gestion centralisée des données de pager, comme par exemple les adresses RIC, les clés, etc. La programmation des pagers s'effectue de manière décentralisée par configuration à distance. Cela évite les erreurs, réduit le travail de programmation et augmente en outre la sécurité des données.

Éprouvé et testé : Le procédé de cryptage DiCal-IDEA utilisé par Swissphone

Les solutions de cryptage utilisées par Swissphone sont basées sur le procédé DiCal-IDEA. La gestion des clés est par exemple organisée de manière à ce que les fichiers correspondants soient également cryptés. Seuls les éléments du système peuvent lire et décrypter ces fichiers. Les clés ne sont jamais représentées en texte clair, afin de garantir que les clés ne soient pas lisibles si elles tombent entre de mauvaises mains. Cela fonctionne indépendamment du fait qu'une clé soit attribuée par organisation ou une par numéro d'appel, avec les conséquences correspondantes pour les concepts de cryptage.

L'algorithme IDEA développé par l'EPF de Zurich offre depuis des décennies une sécurité maximale. Rien qu'en Allemagne, Swissphone a mis en service plus de 200'000 pagers cryptés par IDEA. Après le succès de projets antérieurs, Swissphone met actuellement en œuvre en Suisse divers projets de cryptage spécifiques aux clients, qui répondent à des exigences plus élevées. Ces projets répondent aux exigences de la protection des données.

Vous pouvez obtenir des informations sur les méthodes de cryptage des autres fabricants et les terminaux pris en charge directement auprès de leurs partenaires commerciaux.

Prestations supplémentaires de Swissphone

Services de gestion / administration

s.ONE permet d'attribuer des droits et des rôles à chaque utilisateur de manière sûre et précise. Les données sensibles – comme les clés – sont ainsi protégées par le système contre tout accès non autorisé. La définition des RIC et leur attribution aux forces d'intervention peuvent être effectuées par différents utilisateurs. La personne qui attribue le RIC aux forces d'intervention ne voit pas le RIC, mais seulement une désignation tactique. Et en cas de perte d'un terminal, un pager de remplacement configuré individuellement via s.ONE Fleet est mis à disposition rapidement et indépendamment du lieu. Les RIC et les clés sont transmis directement aux pagers via https. Les pagers ne doivent pas être programmés à un endroit central avec une clé.

L'infrastructure nécessaire à s.ONE Fleet est extrêmement légère : un client de configuration à distance peut être installé partout où il y a Internet.

Conseil / soutien de projet

Swissphone vous soutient sur demande dans les différentes phases du projet, de la planification à la réalisation ou pour l'exploitation de la solution.

SWISSPHONE

Swissphone Wireless AG
Fälmisstrasse 21
CH-8833 Samstagern
Tel. +41 44 786 77 70
Fax +41 44 786 77 71
E-Mail info@swissphone.com