FAKTENBLATT VERSCHLÜSSELTER PAGING-VERSAND

F: Bietet der POCSAG Standard eine Verschlüsselungsmöglichkeit?
A: Nein. Der POCSAG Standard sieht keine Verschlüsselung von Daten im Protokoll selbst vor.

F: Kann eine Paging-Meldung verschlüsselt werden?
A: Ja. Dazu muss der Meldungstext vor der Übermittlung an die Funkrufzentrale TELEPAGE verschlüsselt oder der Verschlüsselungs-Dienst TELEPAGE für Swissphone Pager verwendet werden.

F: Verschlüsselt die Funkrufzentrale TELEPAGE die Paging-Meldungen direkt?
A: Nein und Ja. Da der POCSAG Standard keine Verschlüsselung vorsieht, dürfen wir nicht alle Meldungen standardmässig verschlüsseln. Jedoch ist es im möglich, kundenseitig verschlüsselte Funkrufmeldungen im sogenannten Transparent-Modus (Meldungstyp 4, Siehe UCP TELEPAGE Protokoll-Spezifikation) zu versenden. Das verwendete Verschlüsselungsverfahren ist für die Funkrufzentrale unerheblich. Zusätzlich bieten wir einen Verschlüsselungs-Service an, den der Kunde spezifisch bestellen muss. Dabei kommt das Swissphone IDEA Verschlüsselungsverfahren zur Anwendung, das nur mit Swissphone Pagern kompatibel ist.

F: Bietet die Swissphone Verschlüsselungsmöglichkeiten an?
A: Ja. Die Swissphone bietet einen eigenen Verschlüsselungsservice und für Grosskunden Verschlüsselungsserver an. Die aktuellen Pager der Swissphone können (auch nachträglich) mit der Verschlüsselungsfunktion ausgestattet werden.

F: Kann jeder Swissphone Pager verschlüsselte Meldungen decodieren?
A: Nein. Sie benötigen einen Pager des Typen DE910, DE915, DE925, RES.Q, TRIO, alle s.QUAD Modelle. Bitte beachten Sie, dass die Verschlüsselungsfunktion im Pager freizuschalten ist. Zusätzlich muss die zur Verschlüsselung verwendete Schlüsseldatei auch in den Pager programmiert werden.

F: Können auch Nicht-Swissphone Pager verschlüsselte Meldungen empfangen und decodieren?
A: Ja. Allerdings können Nicht-Swissphone Pager Meldungen, die über unsere Verschlüsselungsdienste versendet werden, nicht decodieren. Die Hersteller implementieren jeweils ein proprietäres Protokoll, da der POCSAG Standard keine Verschlüsselung vorsieht.

F: Muss ich die Pager speziell programmieren?
A: Ja. Sie müssen die Verschlüsselungsfunktion freischalten lassen und die verwendete Schlüsseldatei in den Pager programmieren. Nur so kann der Pager die erhaltenen Meldungen entschlüsseln und darstellen.

F: Können verschlüsselte Paging-Meldungen illegaler Weise gefischt und aufgezeichnet werden?
A: Ja. Allerdings ist die Meldung mit den bekannten Tools nicht mehr lesbar, da Ihre Meldung durch die Verschlüsselung nicht mehr im Klartext lesbar ist. Die Textmeldung «Hallo Welt» sieht dann z.B. so aus: «2 *6 26530557*650-49] 797---76», wobei der von uns genutzte Algorithmus die gleiche Meldung immer wieder unterschiedlich chiffriert, was die unbefugte Entschlüsselung zusätzlich erschwert.

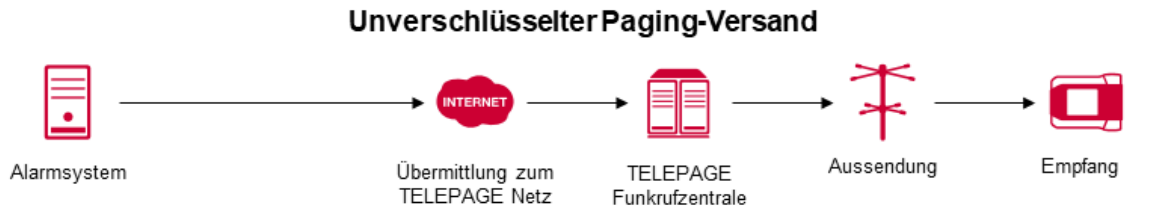
F: Welches Verschlüsselungsverfahren bietet die Swissphone an?
A: Die Swissphone bietet ein proprietäres Verfahren an. Dieses basiert auf dem IDEA 128 Bit Algorithmus

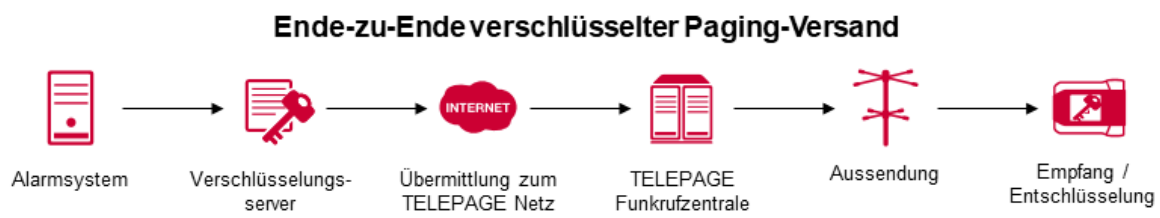
F: Ist das IDEA 128 Bit Verschlüsselungsverfahren sicher?
A: Uns ist bis zum jetzigen Zeitpunkt nicht bekannt, dass das IDEA 128 Bit Verfahren durch Hacker geknackt wurde. Das IDEA 128 Bit Verschlüsslungsverfahren wurde von Kryptographie-Spezialisten an der ETH Zürich entwickelt und durch die Swissphone lizenziert.

F: Wie kann ich meine Meldungen verschlüsseln?
A: Wir bieten drei Möglichkeiten an:

1. Sie nutzen den Verschlüsselungsservice von Swissphone. Dabei senden Sie die Meldungen an die Funkrufzentrale TELEPAGE. Je nach Bedarf kann diese Übermittlung auch TLS gesichert erfolgen. Die Funkrufzentrale verschlüsselt dann auf Basis der Rufnummer die Paging-Meldungen. Das ist das einfachste und von uns empfohlene Verfahren, da keine zusätzlichen Schnittstellen zu entwickeln oder Server aufzubauen sind.
2. Die Verschlüsselung mittels PNC Verschlüsselungsserver. Der PNC wird beim Kunden installiert und ist auch redundant zu betreiben. Nach der Meldungsverschlüsselung sendet der PNC die Paging-Meldung selbstständig an die Funkrufzentrale TELEPAGE. Dies entspricht einer End-to-End Verschlüsselung.
3. Wenn Sie einen Alarmserver vom Typ I.SERACH verwenden, können Sie die Paging-Meldungen bereits im I.SEARCH verschlüsseln und an die Funkrufzentrale TELEPAGE übermitteln. Somit verfügen Sie ebenfalls über die Möglichkeit der End-to-End Verschlüsselung.

F: Was ist eine End-to-End Verschlüsselung?
A: Bei der End-to-End Verschlüsselung wird die Meldung vor dem Aussenden im Kundenumfeld verschlüsselt. Die Meldung bleibt auf allen Übermittlungswegen verschlüsselt und wird erst auf dem Pager entschlüsselt und lesbar dargestellt.





F: Wie sicher ist der Verschlüsselungsservice von Swissphone?
A: Wenn Sie den Verschlüsselungsservice der Swissphone nutzen müssen Sie sicherstellen, dass die Meldungen von Ihrer Auslösestelle zum Verschlüsselungsserver anderweitig gesichert ist. Das kann zum Beispiel durch die Verwendung von TLS-Zertifikaten (ehemals SSL-Zertifikate) geschehen. Auch Anbindungen über Virtuelle, Private Netzwerke (VPN) sind denkbar.

F: Ich nutze das IMASYS Messaging Gateway. Kann das Paging-Meldungen verschlüsseln?
A: IMASYS wird die Paging-Meldungen nicht verschlüsseln. Jedoch kann der Verschlüsselungsdienst vom TELEPAGE Funkrufnetz die Meldung anschliessend verschlüsseln.

F: Ab wann kann ich die Verschlüsselungsfunktionen nutzen?
A: Die Verschlüsselungsdienste sind im Markt eingeführt und können jederzeit bestellt werden.

F: Wie kann ich eine Verschlüsselung einführen?
A: Am besten kontaktieren Sie den für Sie zuständigen Vertriebspartner oder unseren Kundendienst. Gerne vereinbaren wir einen Termin um Ihre Bedürfnisse zu klären und ein auf Sie zugeschnittenes Angebot zu unterbreiten.

Unsere Kontaktmöglichkeiten:

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

Technische Anfragen
Telepage Operation Center
opc@swissphone.com

Hotline für unsere Kunden und Partner
Tel.: 0848 88 99 99
E-Mail: cc@swissphone.com

V 2.0 21.02.2023 SUD