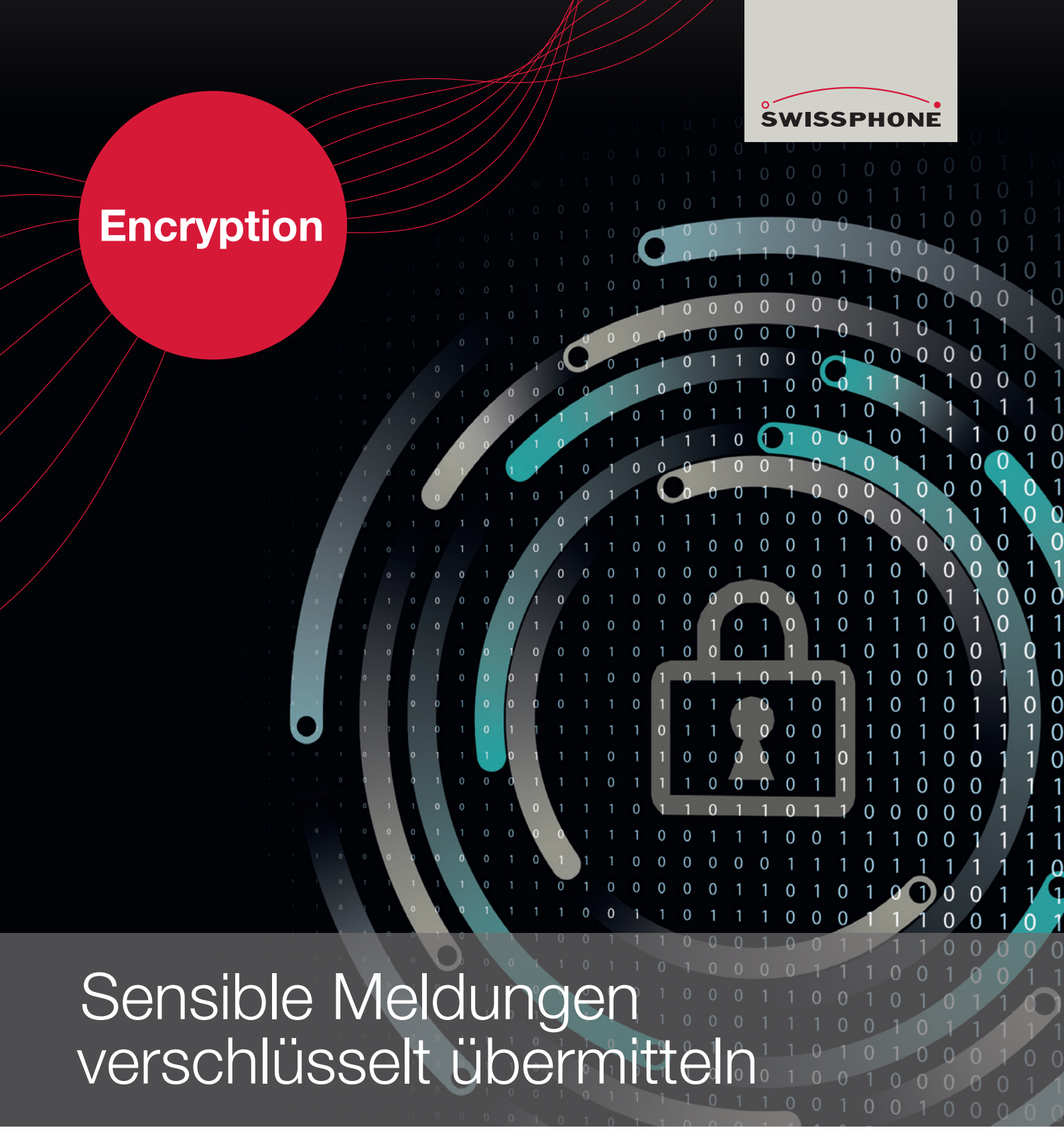
SWISSPHONE

Encryption



Sensible Meldungen verschlüsselt übermitteln

Datenschutzkonformes Versenden von Paging-Nachrichten über das Sicherheitsnetz TELEPAGE®

www.swissphone.com

Datenschutz: eine sensible Thematik

Schützenswerte Personen- oder Kundendaten werden von diversen Institutionen übermittelt: etwa bei der Alarmierung von Blaulichtorganisationen, bei der Datenübermittlung von Banken, Versicherungen oder Behörden wie auch im Gesundheitswesen. Um die Datenschutzrichtlinien einzuhalten, gilt es sicherzustellen, dass Unbefugte sensible und schützenswerte Daten nicht einsehen oder weiterverbreiten können.

Gesetzliche Rahmenbedingungen

Fernmeldedienstgesetz
Swissphone als Betreiberin des TELEPAGE-Funkrufnetzes ist gemäss Fernmeldedienstgesetz Kapitel 7, Art. 43 zur Geheimhaltung der Nachrichten verpflichtet: «Wer mit fernmeldedienstlichen Aufgaben betraut ist oder betraut war, darf Dritten keine Angaben über den Fernmeldeverkehr von Teilnehmerinnen und Teilnehmern machen und niemandem Gelegenheit geben, solche Angaben weiterzugeben.»

Damit ist die Weitergabe, Analyse oder die reine Betrachtung Ihrer Daten durch den Netzbetreiber geregelt – er darf die Daten nicht verwerten oder gar Dritten zugänglich machen.

Im Kapitel 9, Artikel 50 ist der Missbrauch der Fernmeldedaten durch Dritte geregelt und unter Strafe gestellt: «Wer mit einer Fernmeldeanlage nichtöffentliche Informationen empfängt, die nicht für sie oder ihn bestimmt sind und sie unbefugt verwendet oder Dritten bekannt gibt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft».

Somit ist das Abhören, Aufzeichnen oder gar die Weiterverbreitung von Fernmeldedaten klar illegal und verboten.

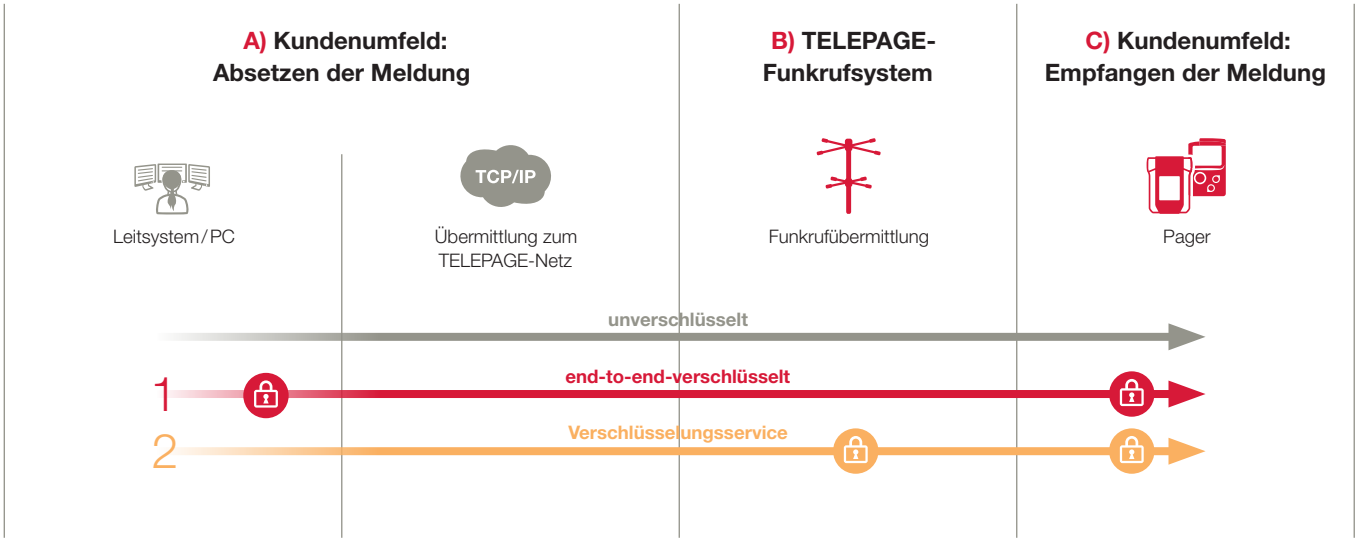
Verantwortung des Nutzers von Telekomanwendungen
Der jeweilige Nutzer der Telekomanwendungen muss sich selbst darüber hinaus jedoch die Frage stellen, inwieweit er mit (besonders) schützenswerten Daten zu tun hat und muss eigene, zusätzliche Massnahmen ergreifen. Das Bundesgesetz über den Datenschutz gibt Auskunft darüber, welche Daten besonders zu schützen sind.

Bundesgesetz über den Datenschutz
Das Bundesgesetz schreibt in Artikel 3, Absatz c vor, dass besonders schützenswerte Personendaten nicht veröffentlicht werden dürfen – also zu schützen sind. Dies gilt unter anderem für Daten über

- die Gesundheit,
- die Intimsphäre,
- religiöse Ansichten oder
- Massnahmen der sozialen Hilfe.

Mit der Verschlüsselung der Paging-Nachrichten sind Sie auf der sicheren Seite, den Anforderungen an die Datensicherheit zu genügen.

Lösungen zur Sicherstellung des Datenschutzes



A) Die Datenverschlüsselung kann direkt bei der alarmauslösenden Stelle (Leitsystem, Alarmserver) über vor Ort eingebundene Verschlüsselungslösungen (Hard-/Software) erfolgen.

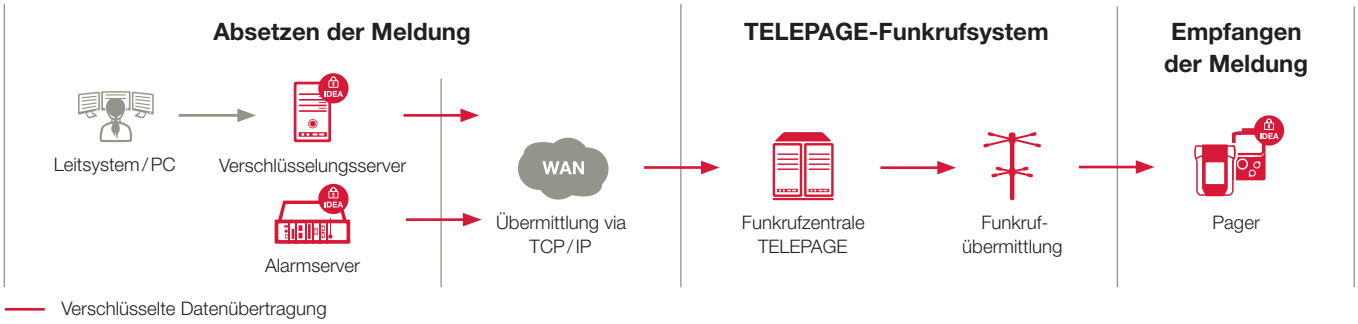
B) Das TELEPAGE-Funkrufsystem kann als offener Standard verschlüsselte Nachrichten entgegennehmen und diese versenden: Der Kunde ist bei der Wahl des jeweiligen Verschlüsselungsverfahrens frei.

C) Nach Empfang der Nachricht im Pager müssen verschlüsselt übermittelte Daten entschlüsselt werden. Nur so sind sie für den Empfänger lesbar.

Swissphone-Verschlüsselungslösungen

1 Ende-zu-Ende-Verschlüsselung

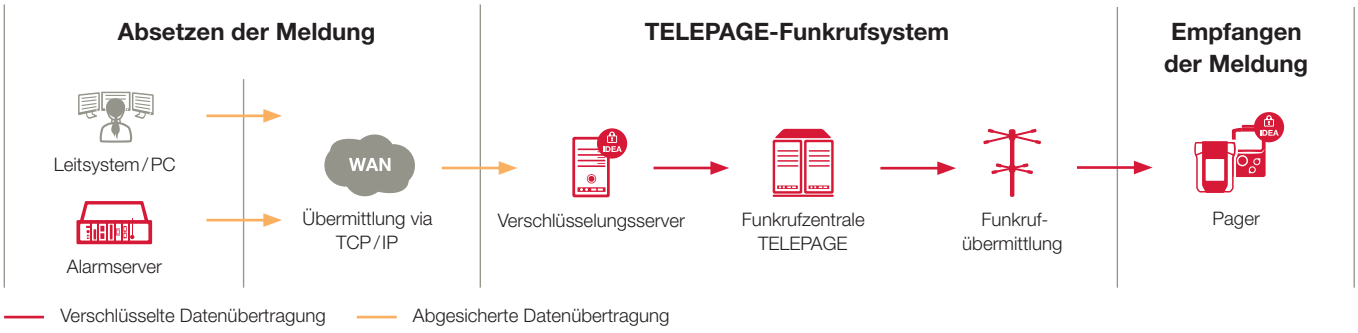
Die grösstmögliche Sicherheit bietet eine Gesamtlösung aus einer Hand.



- Der **«On-Site-Verschlüsselungs-Server»** ist geeignet für Leitstellen oder Callcenter. Das höhere Meldungsaufkommen, die vielen betroffenen Rufnummern oder die gewünschte Autonomie rechtfertigen eine umfassende Sicherheitslösung. Dabei wird der Verschlüsselungsserver beim Kunden installiert. Um die Systemverfügbarkeit zu gewährleisten, kann dieser redundant betrieben werden. Der Server sendet die verschlüsselten Meldungen über öffentliche Netze an die Funkrufzentrale TELEPAGE. Swissphone bietet auf Wunsch Gesamtlösungen, Verschlüsselungs-Software und Wartungsverträge an.
- Die **I.SEARCH-Option IDEA-Encryption** ist für Unternehmen mit firmenspezifischen Alarmserver-Anwendungen die optimale Lösung. Die Meldungen werden direkt im Alarmserver I.SEARCH verschlüsselt, lokal im Firmenareal oder national über TELEPAGE ausgesendet. Bestehende I.SEARCH-Alarmserver können mit der IDEA-Option erweitert werden.

2 Verschlüsselungsservice

Die Datenschutzrichtlinien dank neuer TELEPAGE-Serviceleistungen einhalten



- Die alarmauslösende Stelle nutzt optional bereits bei der Übermittlung an TELEPAGE **TLS-Zertifikate** (ehemals SSL-Zertifikate), welche wie beim E-Banking den Datentransfer absichern. Die Übermittlung an die TELEPAGE-Funkrufzentrale erfolgt mittels UCP TELEPAGE-Protokoll.
- Der **TELEPAGE-Verschlüsselungsservice** verschlüsselt die Meldung nach dem DiCal-IDEA-Verfahren. Der Kunde abonniert einen Zusatzservice für diejenigen Rufnummern, die Meldungen verschlüsselt erhalten sollen.
- Diese Lösung ist geeignet für Organisationen, die Meldungen mit schützenswerten Daten erhalten, das Absetzen von Meldungen aber nicht selbst vornehmen oder wenig beeinflussen können. Diese Lösung erfordert keine spezifischen Anpassungen oder Investitionen bei der alarmauslösenden Stelle.

Unterstützte Pager-Endgeräte

Das eingesetzte Verschlüsselungsverfahren muss von den verwendeten Pagern unterstützt werden. Das von Swissphone eingesetzte DiCAL-IDEA-Verschlüsselungsverfahren ist kompatibel mit Swissphone-Pagern ab der Modelpalette DE925, RES.Q und s.QUAD. Dazu braucht der Kunde eine IDEA-Verschlüsselungs-Lizenz pro Pager.

Verschlüsselung als Gesamtaufgabe mit diversen Schnittstellen

Eine Verschlüsselungslösung sollte ganzheitlich betrachtet, geplant und realisiert werden. Nicht die Wahl eines bestimmten Verfahrens macht die Qualität der Verschlüsselungslösung aus, sondern der sinnvolle Einbezug aller Aspekte.

Gemäss Auguste Kerckhoffs (niederländischer Kryptologe 1835-1903) beruht die Sicherheit eines Verschlüsselungsverfahrens auf der Geheimhaltung des Schlüssels und nicht auf der Geheimhaltung des Verschlüsselungsalgorithmus.

Das bedeutet, dass nebst den technischen Lösungen vor allem auch der Schlüsselverwaltung, den Zugriffsrechten und betrieblichen Aspekten im Zusammenhang mit der Schlüsselerzeugung, der Endgerätprogrammierung und der Schlüsselverwaltung eine sehr grosse Bedeutung zukommt. Hier bietet Swissphone mit s.ONE Fleet einen umfassenden Service an: s.ONE Fleet ermöglicht ein schnelles Update und eine zentralisierte Verwaltung von Melderdaten wie zum Beispiel RIC-Adressen oder Schlüssel. Die Programmierung der Melder erfolgt dezentral per Fernkonfiguration. Dies vermeidet Fehler, reduziert den Programmieraufwand und erhöht zusätzlich die Datensicherheit.

Bewährt und erprobt: Das von Swissphone eingesetzte DiCal-IDEA-Verschlüsselungsverfahren

Die von Swissphone eingesetzten Verschlüsselungslösungen basieren auf dem DiCal-IDEA-Verfahren. Das Schlüssel-Handling ist beispielsweise so organisiert, dass die entsprechenden Files selbst auch verschlüsselt werden. Nur die Systemkomponenten können diese Files einlesen und entschlüsseln. Dabei werden die Schlüssel nie im Klartext dargestellt, um sicherzustellen, dass Schlüssel nicht lesbar werden, wenn sie in falsche Hände kommen. Dies funktioniert unabhängig davon, ob ein Schlüssel pro Organisation oder einer pro Rufnummer vergeben wird, mit entsprechenden Konsequenzen für die Verschlüsselungskonzepte.

Der von der ETH Zürich entwickelte IDEA-Algorithmus bietet seit Jahrzehnten höchste Sicherheit. Allein in Deutschland hat Swissphone über 200'000 IDEA-verschlüsselte Pager im Einsatz. Nach erfolgreichen früheren Projekten setzt Swissphone gegenwärtig in der Schweiz verschiedene kundenspezifische Verschlüsselungsprojekte um, die den höheren Anforderungen an den Datenschutz gerecht werden.

Informationen zu den Verschlüsselungsverfahren anderer Hersteller und unterstützte Endgeräte erhalten Sie direkt bei deren Vertriebspartnern.

Zusatzleistungen von Swissphone

Management-/Verwaltungs-Services

s.ONE erlaubt die sichere und feingliedrige Zuordnung und Vergabe von Rechten und Rollen an die einzelnen Benutzer. Sensible Daten – wie zum Beispiel Schlüssel – werden dabei vom System vor unautorisiertem Zugriff geschützt. Das Definieren von RIC und die Zuweisung an Einsatzkräfte kann durch verschiedene Benutzer erfolgen. Dabei sieht die Person welche RIC an Einsatzkräfte zuweist den RIC nicht, sondern nur eine taktische Bezeichnung. Und beim Verlust eines Endgerätes wird schnell und ortsunabhängig ein über s.ONE Fleet individuell konfigurierter Ersatzpager bereitgestellt.
Die RIC und Schlüssel werden direkt über https an die Melder übermittelt. Melder müssen nicht an zentraler Stelle mit Schlüssel programmiert werden.

Die für s.ONE Fleet benötigte Infrastruktur ist äusserst schlank: Ein Fernkonfigurationsclient kann überall installiert werden, wo Internet vorhanden ist.

Beratung/Projektunterstützung

Swissphone unterstützt Sie auf Wunsch in den verschiedenen Projektphasen von der Planung bis zur Realisierung oder für den Betrieb der Lösung.

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

DE 06/2019 0342408 V1 WEC