

# DiCaI-IDEA

## Verschlüsselte Alarmierung





## DiCal-IDEA - Verschlüsselte Alarmierung

DiCal-IDEA macht die digitale Alarmierung zu einem in sich geschlossenen System und verhindert das Abhören und Mitlesen von Alarmmeldungen. Somit bietet die digitale Alarmierung einen entscheidenden Vorteil: Sie ist nicht nur schnell sondern auch sicher.

### Sicheres Paging

Die Swissphone DiCal-IDEA Verschlüsselung ist eine Option für digitale Pagingssysteme, welche absolute Diskretion gewährleistet. Sämtliche Meldungen sind von der Eingabe bis zum Pager verschlüsselt und somit für Unberechtigte nicht lesbar.

DiCal-IDEA hat im Vergleich zum standardisierten AES, bei gleicher Sicherheit, kürzere Übertragungszeiten

sowie ein kleinerer Speicherbedarf der einzelnen Meldungen.

### Übermittlung von sensiblen Informationen

Einsatzbefehle von Sicherheitsdiensten oder anderen «Blaulicht»-Organisationen erhalten oft vertrauliche Daten. Wenn solche sensiblen Informationen übermittelt werden, müssen sie bestmöglich gegen jegliche Einflüsse von aussen geschützt werden. Das Versenden von unverschlüsselten Nachrichten birgt demnach vielerlei Gefahren. Auf der nächsten Seite erläutern wir vier mögliche Szenarien näher.



### DiCal-IDEA Facts:

- Verhindert das Mithören oder Mitlesen von sensiblen Daten
- Schutz vor Wiedereinspielung eines Alarmes zu einem späteren Zeitpunkt (Zeit-Authentifizierung)
- Meldungen sind von der Eingabe bis zum Pager verschlüsselt (End to End)
- Integration in bestehende Umgebungen
- Durchdachtes Konzept der Schlüsselverwaltung

**1** **Angriff durch Einspeisung von Falschnachrichten**

Gelingt es dem Angreifer, sich Zugang zur Verbindung zwischen Einsatzzentrale und Alarmzentrale (oder Sendestation) zu verschaffen, kann er eigene Falschnachrichten einspeisen. Die Einsatzkräfte würden ausrücken, da die Alarmierung auf einem Vertrauensverhältnis zwischen Sender und Empfänger basiert.

**2** **Angriff durch Wiedereinspielen von Nachrichten**

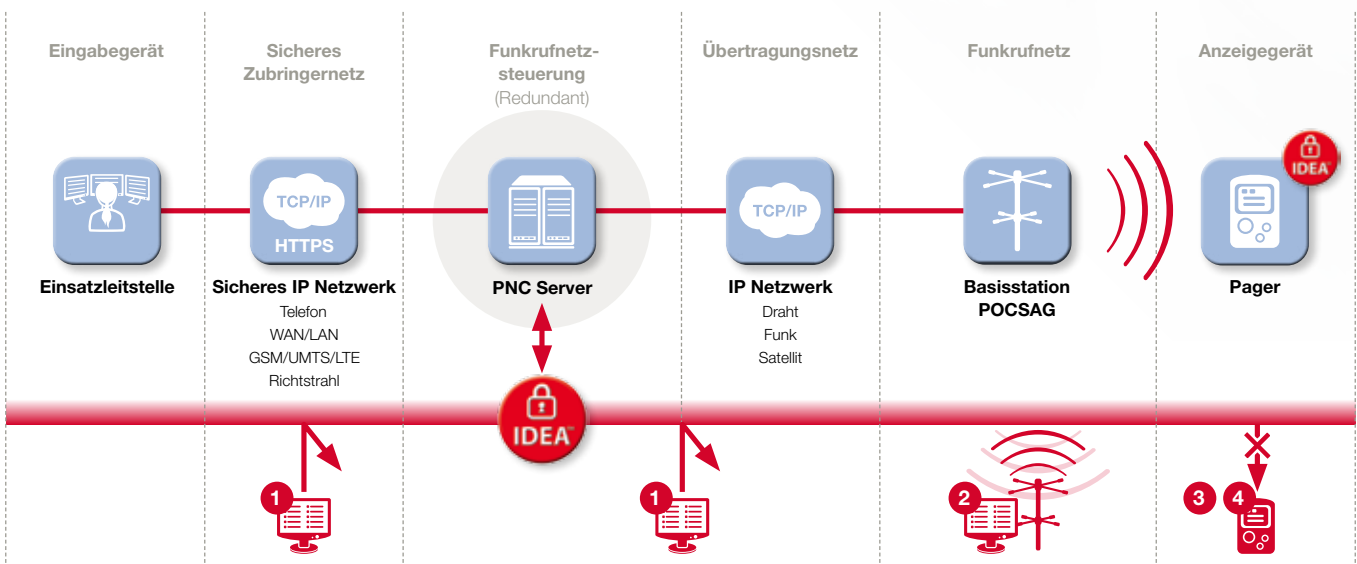
Eine mögliche Gefahr stellt auch das Wiedereinspielen von Nachrichten respektive das Versenden von Falschnachrichten dar. So können zum Beispiel Nachrichten von einer Drittperson aufgezeichnet und zu einem späteren Zeitpunkt über einen Fremdsender erneut übermittelt werden. Wie in Szenario 1 würden auch in diesem Fall die Einsatzkräfte der Alarmierung Folge leisten.

**3** **Lauschangriff durch Mitlesen von Nachrichten**

Nachrichten können von technisch versierten Personen empfangen und gelesen werden. Diesen Umstand können sich interessierte Kreise zu Nutze machen, indem sie Alarme abhören und analysieren. Insbesondere Rettungskräfte und Polizei haben aber ein grosses Interesse, dass ihre Aktivitäten und Nachrichten vertraulich bleiben.

**4** **Ausspionierung von Kommandostrukturen**

Sind die Sendefrequenz und Adressen der Meldungen für eine Organisation einmal bekannt, kann über die empfangenen Mitteilungen auf die Kommandostruktur einer Organisation geschlossen werden. Mit diesem Wissen können Meldungen sogar den verschiedenen Funktionsträgern der Organisation zugeordnet werden und die Mitteilungen werden für die «Mitleser» leichter interpretierbar.



**Ausgeklügeltes Schlüsselmanagement**

Sicherheit kann allerdings nicht alleine durch ein sicheres Schloss erreicht werden, man muss auch dafür sorgen, dass nur berechtigte Personen Zugang zum Schlüssel haben und diese entsprechend gesichert sind. Die eingesetzten Schlüssel sollten zudem periodisch gewechselt werden, um die Sicherheit aufrecht zu erhalten. Swisphone hat hierfür ein ausgeklügeltes Schlüsselmanagement entwickelt,

das sichere Schlüsselwechsel über die Luftschnittstelle ermöglicht. Das Einsammeln der Pager ist für den Schlüsselwechsel nicht nötig. Und selbst wenn ein Pager verloren geht, können die Schlüssel nicht gelesen werden.

Die Schlüssel können «unsichtbar» in die Endgeräte programmiert werden. Somit kennt der Programmierer

die Schlüssel auch nicht und diese Sicherheitslücke entfällt ebenfalls.

**Einfache Integration**

Das DiCal-IDEA-Sicherheitspaging von Swisphone kann einfach in bestehende Umgebungen integriert werden. Swisphone unterstützt Sie gerne bei der Integration von DiCal-IDEA-Sicherheitspaging.



Swissphone  
Telecommunications GmbH  
Industriestr. 51  
D-79194 Gundelfingen  
Tel: +49 761 59 05 0  
Fax: +49 761 59 05 100  
[www.swissphone.de](http://www.swissphone.de)

