# Zuverlässig und sicher alarmieren

**Dank der Integration von verschiedenen Verschlüsselungssystemen bietet Swissphone seit 2019 ein offenes Verschlüsselungskonzept: Sowohl Swissphone-Netze als auch Swissphone-Melder sind im Stande, adressspezifisch die gewünschten Verschlüsselungsverfahren anzuwenden – jeweils im gleichen Netz und bei Bedarf auch im gleichen Melder. Somit haben Swissphone-Kunden die Wahl, das Verschlüsselungsverfahren frei auf die bestehenden Melder und Gegebenheiten ihrer internen Kunden anpassen. Warum eine Entscheidung gut durchdacht und die Frage nach der Praktikabilität geklärt sein muss, zeigt sich bei der genaueren Betrachtung von Overhead, Rufbeschleunigungsverfahren, sicherem Schlüsselmanagement oder der Zeitauthentifizierung.**


*DiCal-IDEA ist Teil einer integrierten Sicherheitsarchitektur, welche nebst der Verschlüsselung der Meldungen die sichere und zuverlässige Verwaltung der Schlüssel sowie die verschlüsselte Übermittlung der Programmierdaten beinhaltet.* *Fotos und Grafiken: Swissphone*

Die Anforderungen an eine effiziente und zeitgerechte Alarmierung von Einsatzkräften sind vielfältig. Die Einsatzkraft verlangt qualitativ hochwertige Endgeräte, welche Alarme in jeder Situation schnell und zuverlässig übermitteln. Organisationen möchten gezielt und dynamisch alarmieren, um die Einsatzkräfte möglichst schnell selektiv oder auch in Gruppen adressieren zu können. Für den Gesetzgeber ist es wichtig, dass Hilfsfristen eingehalten und schützenswerte Daten verschlüsselt übermittelt werden. Im Rahmen der Einführung der DSGVO hat die Verschlüsselung von Nachrichten mit persönlichen Daten nochmals an Wichtigkeit gewonnen.

Swissphone hat als Hersteller hochwertiger integrierter Alarmierungslösungen mit ideal aufeinander abgestimmten Komponenten bereits vor Jahren mit DiCal-IDEA einen Verschlüsselungsstandard geschaffen. Dieser wird in weit über 100 Alarmierungsnetzen mit mehreren hunderttausend POCSAG-Meldeempfängern erfolgreich verwendet. DiCal-IDEA fügt sich einerseits in die Gegebenheiten von digitalen Funkrufnetzen optimal ein. Andererseits erfüllt er gleichzeitig die oben erwähnten Anforderungen der verschiedensten Anspruchsgruppen. Aufgrund der Erfahrungen und aktueller Kundenwünsche hat Swissphone den DiCal-IDEA-Standard funktional erweitert (siehe Kasten »Neu: Zugleich verschlüsselt und unverschlüsselt«).

## Offenes Verschlüsselungskonzept

Bei den meisten Alarmierungsnetzen besteht bisher keinerlei Notwendigkeit, von der bewährten DiCal-IDEA-Verschlüsselung abzuweichen. Sollten jedoch innerhalb einer Region Funkmeldeempfänger unterschiedlicher Hersteller mit Verschlüsselungswunsch eingesetzt werden, kann sich prinzipiell auch das mittlerweile mehreren Herstellern zugängliche Verfahren BOSKrypt anbieten. In Swissphone-Alarmierungsnetzen können beide Verschlüsselungsverfahren quasi parallel und adressspezifisch genutzt werden, z. B. für die Funkmeldeempfänger DiCal-IDEA von Swissphone und für Funkmelder eines anderen Herstellers BOSKrypt. Ab sofort bietet Swissphone seinen Kunden auch die freie Wahl hinsichtlich Verschlüsselungssystemen im Endgerät an: Sowohl Swissphone-Netze als auch Swissphone-Melder können somit adressspezifisch die verschiedenen Verschlüsselungsverfahren anwenden – jeweils im gleichen Netz und bei Bedarf auch im gleichen Melder. Behörden und Leitstellen haben also die Freiheit, das Verschlüsselungsverfahren auf die bestehenden Melder und/oder auf die Gegebenheiten ihrer Organisationen anzupassen.

Vor der Wahl eines Verschlüsselungsverfahrens lohnt es sich, die Vor- und Nachteile der jeweiligen Technologien sorgfältig abzuwägen. Dieser Artikel befasst sich deshalb auch mit den Besonderheiten und Unterschieden der verschiedenen Verschlüsselungsverfahren. Aufgrund aktueller Projekte wird dabei insbesondere BOSKrypt diskutiert, ein als herstellerneutral beworbenes Verfahren. Die folgenden Erläuterungen sollen daher helfen, sich in der laufenden Debatte einen Überblick zu verschaffen.

## Tauglichkeit für POCSAG-Funknetze

Das BOSKrypt-Verschlüsselungsverfahren ist hinsichtlich Datensicherheit und Integration gut gelöst:

- Die 256-Bit AES-Verschlüsselung bietet grundsätzlich ein Maximum an Zugriffschutz durch Dritte.
- Der Initialisierungsvektor aus elf Zeichen, der fehlerfrei empfangen werden muss, bietet zusätzlich Datenintegrität.
- Durch Base-64-Encoding des verschlüsselten Produkts lässt sich das Verfahren einfach in Drittsysteme integrieren.

Gleichzeitig haben diese Vorteile im Rahmen eines Funksystems wesentliche Nachteile:

- Die Tatsache, dass sieben POCSAG-Codeworte (11 Zeichen) fehlerfrei empfangen werden müssen, führt bei kleinsten Funkstörungen zum Nichtanzeigen der Meldung. Dies, weil ansonsten die Datenintegrität nicht mehr gewährleistet ist.
- AES 256 und das Base-64-Encoding haben den Nachteil, dass die zu übertragenden Daten um bis zu 40 % größer werden (siehe Kasten »Express-Alarm«). Dieser so genannte Overhead führt zu einer längeren Übertragungsdauer.

DiCal-IDEA arbeitet mit einer Schlüssellänge von 128 Bit. Angesichts der heute verfügbaren enormen Rechenleistungen reicht diese Verschlüsselung gegen einen Brute-Force-Angriff bei weitem aus. Um einen Schlüssel mit $2^{128}$ Zeichen mittels des Bitcoin-Netzwerks mit einer aktuellen Hash-Rate von 60 Mio. TH/s ($2^{65}$) zu knacken, bräuchte ein Angreifer statistisch $2^{63}$ Sekunden, was 13 Mal dem Weltalter entspricht.

Beim Swissphone-IDEA-Verfahren ist der Intitialvektor lediglich zwei Codeworte lang. Dieser muss fehlerfrei empfangen werden, damit die Nachricht korrekt angezeigt werden kann. Um das Verfahren noch robuster zu machen, wurde die automatische Meldungskorrektur im Melder wesentlich verbessert. Dies verringert Fehler und erhöht die Empfangswahrscheinlichkeit der Nachricht zusätzlich.

## Rufbeschleunigungsverfahren

In Deutschland hat sich die selektive Alarmierung mit unterschiedlichen Alarmadressen (RICs) pro Einsatz weitgehend durchgesetzt. Sendet eine Leitstelle für einen Einsatz aber mehrere Alarme bestehend jeweils aus RIC und Einsatztext, wird die Alarmierung aufgrund der großen Anzahl der zu versendenden Nachrichten langsam. Erfolgt noch die Verschlüsselung der Einsatztexte, ist BOSKrypt aufgrund der deutlich größeren Datenmenge im Vergleich zu DiCal-IDEA überproportional langsamer. Zusammen mit der Funktionsweise von Funkrufnetzen ist dieses Verhalten besonders schwerwiegend, da jede Nachricht in mehreren Aussendungen zwischen den Basisstationen weitergesendet werden muss; die Dauer der Aussendungen addiert sich. In beiden Fällen, insbesondere im Fall von BOSKrypt, lohnt es sich deshalb, ein Rufbeschleunigungsverfahren einzusetzen. Swissphone bietet hier das patentierte Express-Alarm-Verfahren an (siehe Kasten). Durch das Zusammenfassen der Nachrichten zu einer Aussendung unterstützt dieses die dynamische Alarmierung optimal. In diesem Zusammenspiel ermöglichen DiCal-IDEA und Express-Alarm eine Alarmierung mit minimalen Alarmierungszeiten und mit zuverlässiger, sicherer Nachrichtenübermittlung.

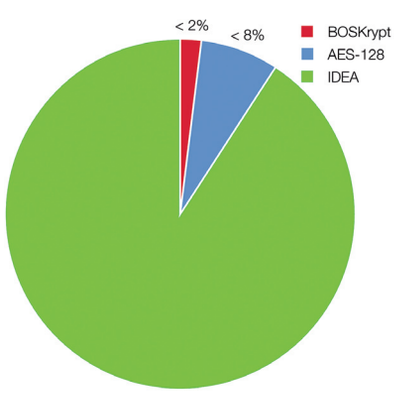
## End-zu-End-Verschlüsselung

Es gibt symmetrische und asymmetrische Verschlüsselungsverfahren. Bei Systemen, welche wie Funkrufnetze nur in eine Richtung kommunizieren, werden symmetrische Verfahren angewendet. Diese bedingen, dass der Sender und der Empfänger einen gemeinsamen Schlüssel für die zu übertragende Nachricht haben. Bei einer Vielzahl von Empfängern respektive Adressen haben Organisationen heute folgende zwei Optionen, Schlüssel einzusetzen.

• Alle Empfänger verfügen über einen gemeinsamen Schlüsselsatz, wovon jeweils einer den einzelnen Organisationen als aktiver Schlüssel zugeteilt ist. Hierbei kann weiterhin die Alarmierung von Gruppen durchgeführt werden. Dies vereinfacht das Handling der Schlüssel wesentlich, bedingt aber, dass der jeweils aktive Schlüssel in allen Endgeräten gewechselt werden müsste, wenn dieser bekannt würde. Dieser wird dann mit einem neuen Schlüssel aus dem gemeinsamen Schlüsselsatz ersetzt. Der Tausch geschieht über einen OAP-Befehl (On-Air-Programming) über das Funknetz. Die Funk-Melder müssen also nicht von Hand neu konfiguriert werden. Bei Bedarf können auch diese Schlüsselsätze ausgetauscht werden, was aber eine neue manuelle Programmierung oder eine Fern-

**Verbreitung der Verschlüsselungsverfahren**

Für die Verschlüsselung stehen drei verschiedene Verfahren zur Verfügung: AES-128 (Advanced Encryption Standard), DiCal-IDEA (International Data Encryption Algorithm) und BOSKrypt. Alle drei Verfahren sind lizenzfrei nutzbar und gewährleisten als Ende-zu-Ende-Verschlüsselung einen hohen Sicherheitsstandard. Allein in Deutschland nutzen mehr als hundert Alarmierungsfunknetze mit mehreren hunderttausend Endgeräten die DiCal-IDEA-Verschlüsselung mit 128 Bit. Damit ist dieses Verfahren das bei Weitem verbreitetste. Bei AES-128 liegt der Marktanteil im einstelligen Prozentbereich, und bei BOSKrypt gibt es nach Schätzungen von Swissphone bislang wenige tausend Endgeräte, die mit dieser Verschlüsselung arbeiten. Somit kann DiCal-IDEA als De-facto-Standard bei den deutschen BOS gelten. Swissphone bietet auf Wunsch die Integration verschiedener Verschlüsselungssysteme sowohl netz- wie auch endgeräteseitig.




***Marktanteile (Schätzung) der drei Verschlüsselungsverfahren für digitale Alarmierungsnetze in Deutschland.***

**Neu: Zugleich verschlüsselt und unverschlüsselt**

Es kann erforderlich sein, dass ein Alarmsystem Meldungen abwechselnd verschlüsselt und unverschlüsselt versenden kann. Einerseits um eine einfachere Migration von alten zu neuen Funkmelderausstattungen zu ermöglichen, andererseits um einen Notbetrieb sicherzustellen, falls z. B. ein Verschlüsselungsserver ausfallen sollte. Ebenso wie BOSKrypt unterstützt die neueste Version von DiCal-IDEA deshalb das Empfangen unverschlüsselter Nachrichten auf Adressen, welche normalerweise eine verschlüsselte Nachricht empfangen. Dies muss allerdings durch ein entsprechendes Schlüsselwort geschehen, was die Datenintegrität erhöht. Alle Swissphone-Melder mit DiCal-IDEA-Verschlüsselung, welche über einen Firmwarestand verfügen, lassen diese Möglichkeit bei entsprechender Implementierung im Netz zu. In der neuesten Version von DiCal-IDEA wurde außerdem die automatische Meldungskorrektur im Melder wesentlich verbessert, was die Empfangswahrscheinlichkeit der Nachricht zusätzlich erhöht (siehe Abschnitt »Tauglichkeit für POCSAG-Funknetze«).

**Express-Alarm**

Angesichts der knappen Ressourcen der heutigen Freiwilligenarbeit ist es immer wichtiger, ihre Zeit und Verfügbarkeit zu respektieren und nur die aktuell verfügbaren Ressourcen zu alarmieren. Das patentierte Express-Alarm-Verfahren von Swissphone ermöglicht es Einsatzkräfte einzeln zu alarmieren, ohne die Alarmdauer zu erhöhen.
Anstelle jeder RIC-Adresse (A1, A2, A3, ...., An) einzeln die Nachricht mit dem gesamten Meldungstext zuzustellen,

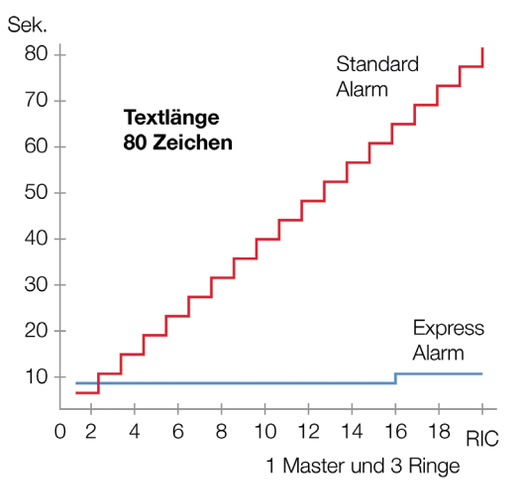
| A1 | Alarmtext | | A2 | Alarmtext | | A3 | Alarmtext | .... | An | Alarmtext |
|---|---|---|---|---|---|---|---|---|---|---|

werden zu Beginn einer Übertragung nur die Einzeltonrufe (RICs der Empfänger: A1, A2, A3, ...., An) übermittelt. Anschließend wird eine gemeinsame alphanumerische Adresse Aα mit anschließendem Alarmtext gleichzeitig an alle erforderlichen Benutzer gesendet.

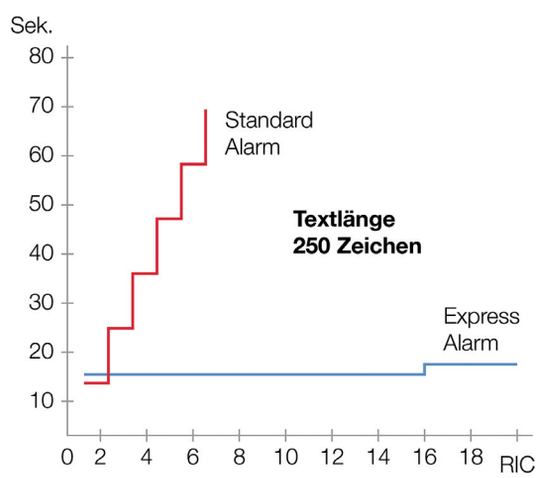
| A1 | A2 | A3 | .... | An | Aα | Alarmtext |
|---|---|---|---|---|---|---|

Abhängig von seinem RIC zeigt das Terminal die Meldung an (oder nicht). Dieses Verfahren reduziert das Volumen der zu sendenden Daten, was die Zeit der Alarmübertragung erheblich verkürzt. Beispielsweise können bis zu 32 Alarmadressen in einer Sekunde gesendet werden (POCSAG bei 1200 Bit/s).

Folgender Vergleich illustriert die Alarmzeiten beider Verfahren unter Berücksichtigung unterschiedlicher Zeichenlängen (Berechnung auf Basis von POCSAG 1200 Bit/s):




***Ein Alarm mit bis zu 15 Adressen und ca. 80 Zeichen Text in einem Netzwerk bestehend aus einem Master und drei Ringen dauert nur acht Sekunden. Ohne Express-Alarm endet die Übertragung erst nach 60 sec.***




***Alarmmeldungen mit einer Länge von 250 Zeichen, eine durchaus übliche Länge, benötigen auch bei 15 Alarmadressen nur 16 sec.***

Das patentierte Rufbeschleunigungsverfahren Express-Alarm ist insbesondere nützlich, wenn diese selektive Alarmierung mit einer Verschlüsselung kombiniert wird, welche die Nachricht zusätzlich verlängert (siehe Kasten »Verschlüsselungs-Overhead«).

programmierung der betroffenen Melder erfordert. Somit bleibt die Sicherheit jederzeit gewährleistet.

- Jede Adresse im Melder besitzt einen eigenen Schlüssel. Dies bedingt, dass jeder Melder den für seine Adresse gültigen Schlüssel gespeichert haben muss. Der Vorteil dieser Handhabung ist, dass beim Verlust eines Pagers bzw. beim Diebstahl des Schlüssels nur eine Adresse kompromittiert ist. Ein neuer Schlüssel muss zu dieser Adresse generiert werden, der Verschlüsselungsserver muss aufdatiert und der Melder neu programmiert werden. Falls Gruppenrufe oder Expressalarme eingesetzt werden, entfällt dieser Vorteil jedoch, da dann dennoch auf allen betroffenen Pagern dieselbe Adresse programmiert ist. Ein Nachteil dieser Lösung ist, dass das Schüsselmanagement deutlich aufwendiger ist, um sicherzustellen, welcher Adresse welchem Schlüssel zugeordnet wird.

Um den jeweiligen Kundenanforderungen gerecht zu werden, bietet Swissphone mit DiCal-IDEA beide Optionen für die Schlüsseladressierung an. Sowohl DiCal-IDEA als auch BOSKrypt lassen zu, dass jeder Adresse ein eigener Schlüssel zugewiesen werden kann. Hier bleibt es dem Anwender überlassen, wie er die großen logistischen Hürden meistert, die Sicherheit der Schlüssel zu gewährleisten.

## Sicheres Schlüsselmanagement

Das Schüsselmanagement an sich ist eine der größten Herausforderungen, wenn es um sichere Datenübertragung bei der Alarmierung geht. Es birgt einerseits das Risiko von Fehlern, andererseits von Sicherheitslücken. Swissphone bietet mit seiner Gesamtlösung aufeinander abgestimmte Produkte, welche ein sicheres und zuverlässiges Verwalten der Schlüssel ermöglichen. Die Fernprogrammierungslösung ist ein Teil dieser Gesamtlösung, die sowohl das Schlüsselmanagement als auch die Fernkonfiguration der Melder fehlerfrei und sicher ermöglicht. Durch die Zuordnung von Rechten und Rollen der Funkwarte gewährleistet die Leitstelle jederzeit, dass die Adressen mit den zugehörigen Schlüsseln programmiert und auch entsprechend im DAG hinterlegt werden. Zudem sind die Adressen und Schlüssel für niemanden ersichtlich. Die Übermittlung der Programmierdaten geschieht End-zu-End-verschlüsselt von der Plattform bis zum Melder. Der Melder selbst ist durch ein Passwort geschützt, das nur das Fernprogrammiersystem kennt.

## Zeitauthentifizierung

Auch wenn damit die Verschlüsselung möglichst sicher ist, muss immer noch sichergestellt werden, dass Sicherheitsmaßnahmen nicht übergangen werden können. So zum Beispiel durch das Aufnehmen und Wiedereinspielen von verschlüsselten Nachrichten zu einem späteren Zeitpunkt, das zur Auslösung von Falschalarmen führt. Eine Vermeidung des Wiedereinspielens von Nachrichten bietet die Zeitauthentifizierung. Mit jeder verschlüsselten Nachricht wird gleichzeitig ein Zeitstempel mitgeschickt; die Nachricht wird nur dann dargestellt, wenn der Zeitstempel mit der Zeit auf dem Funkempfänger übereinstimmt. So wird ein Wiedereinspielen verhindert.

Damit die Zeitauthentifizierung funktioniert, muss dem Melder regelmäßig über einen Over-the-air-Befehl (OAP) ein Zeitstempel übermittelt werden. BOSKrypt sieht keine Spezifizierung des Setzens der Uhrzeit vor und überlässt dies stattdessen einfach den Herstellern. Dabei ist es entscheidend, dass die Zeitsetzung verschlüsselt geschieht, weil sonst der Zeitstempel abgefangen und damit die Zeit auf allen Pagern falsch gestellt werden kann. In diesem Fall würde bei der Aktivierung der Zeitauthentifizierung gar kein Melder Nachrichten empfangen, das Netz wäre komplett sabotiert.

## Klare Verantwortlichkeit

Diese voneinander abhängigen Elemente einer Verschlüsselung wirken sich auf die Zuverlässigkeit, Schnelligkeit und Sicherheit der Alarmierung aus. Sie sollten von Organisationen bei der Wahl einer Verschlüsselungsoption berücksichtigt werden. Bis heute gibt es in Alarmierungsnetzen keinen Mischbetrieb der beiden Verfahren. BOSKrypt wird seit Kurzem nur in wenigen Netzen eingesetzt und daher fehlt jegliche Langzeiterfahrung. Als Systemanbieter übernimmt Swissphone die Verantwortung für die einwandfreie Funktionalität seiner Lösungen und im Markt erprobter Technologien und Verfahren.

Institutionen, die die Einführung einer Verschlüsselung planen, sollten ihre Alarmierungslösung ganzheitlich betrachten. Nicht die Wahl eines bestimmten Verfahrens entscheidet über ein sorgloses Verschlüsselungssystem, sondern vielmehr der sinnvolle Einbezug aller Komponenten der Alarmierungskette. Aus Sicht von Swissphone empfiehlt sich deshalb die Wahl eines Generalunternehmers, der das gesamte System, das heißt Alarmierungsrechner (DAG), Funknetz (DAU) und Endgeräte (DME) sowie Verwaltungssoftware, aus einer Hand liefert.

Damit kann einerseits die Kompatibilität aller Netzkomponenten im Hinblick auf eine reibungslose Umsetzung vorausgesetzt und sichergestellt werden. Andererseits steht dem Betreiber ein alleiniger Ansprechpartner zur Verfügung, sollte es tatsächlich einmal zu Fehlern oder Nichtalarmierungen kommen.

**Verschlüsselungs-Overhead**

Der Overhead bezeichnet die durch die Verschlüsselung entstehende zusätzliche Nachrichtenlänge. DiCal-IDEA verwendet den numerischen Zeichensatz gemäß POCSAG-Standard, welcher aus 16 druckbaren Zeichen besteht. Damit kann die verschlüsselte Nachricht in derselben Länge wie die Klartextmeldung angezeigt werden. Der verschlüsselten Nachricht werden bloß 40 Bit vorangestellt, beispielsweise mit Informationen zur Zeitauthentifizierung (siehe Abschnitt »Zeitauthentifizierung«). Dadurch ist der DiCal-IDEA-Verschlüsselungs-Overhead vernachlässigbar gegenüber einer Klartextmeldung (siehe Illustration 3). Bei BOSKrypt ist diese vorangestellte Information länger als bei DiCal-IDEA. Außerdem verwendet das Verfahren einen anderen Zeichensatz für die Kodierung der verschlüsselten Meldung (Base64). Dieser hat den Vorteil, dass mit BOSKrypt verschlüsselte Nachrichten herstellerübergreifend gelesen werden können, allerdings verlängert sich die Nachricht dadurch um 40 % gegenüber dem Klartext. Dadurch wird die Übertragungszeit länger und die Netz-Performance sinkt, was sich besonders bei selektiven Alarmierungsverfahren negativ auswirkt. Die Übertragungszeit kann durch das patentierte Express-Alarm-Rufbeschleunigungsverfahren verkürzt werden (siehe Kasten »Express-Alarm«).

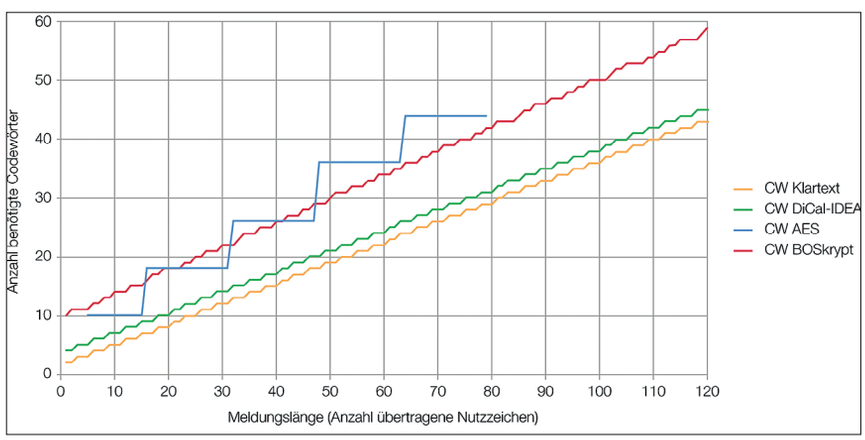



*Illustration 3: Vergleich des Overheads der erhältlichen Verschlüsselungsverfahren.*

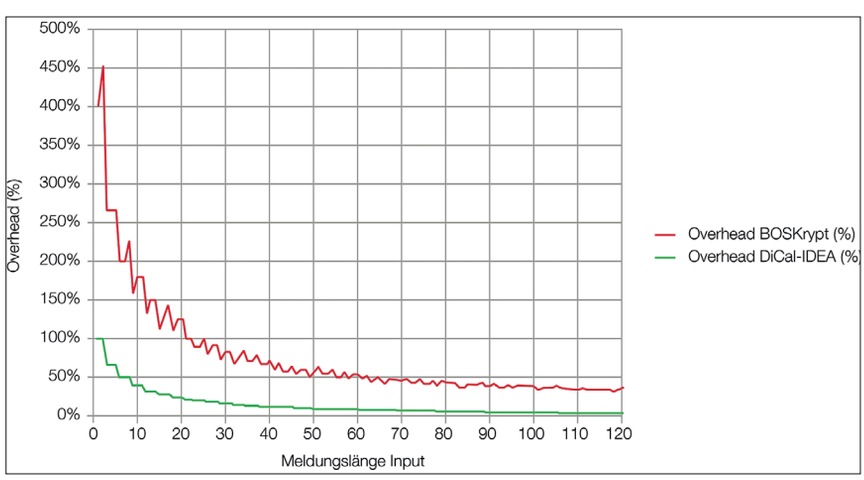



*Illustration 4: Overhead in Prozent der Meldungslänge: DiCal-IDEA/BOSKrypt.*

Philipp Zimmermann
Swissphone Wireless AG