Historie und Hinweise zur Anwendung und Implementierung von BOSKRYPT

Ausgabestand : 01.12.2018

INHALT

Vorwort

Dieses Dokument soll dem Anwender und Entwickler die Hintergründe und Überlegungen die bei der Definition des Standards betrachtet wurden erläutern. Ergänzt wurde die historische Entwicklung innerhalb der Bundesrepublik zu diesem Standard.
Es soll ferner Anregungen zur praktischen Ausgestaltung von Endgeräten geben um eine möglichst einheitliche und intuitive Bedienung zu ermöglichen.

Karlsbad, Dezember 2018

Dirk Barthelmes

An der Entwicklung der BOSKRYPT Spezifikation haben mitgewirkt:

[1] Hr. Dipl.-Ing. Florian Fuchs
Grundlegende Arbeiten zum Verfahren, Autor der englischsprachigen Originalversion, Erstellung von Softwarekomponenten für die Entwicklungsunterstützung (PET) und praktische Erprobungen im Bereich der Leitstelle Klagenfurt / Österreich. Vorschlag der XSD Erweiterung zum XML Datenaustausch

[2] Hr. Dipl.-Ing. Michael Pries
Vorschläge für Optimierungen im Bereich der Prüfsummenberechnung und Zeichencodierung, Produktimplementationen in DME und Testsender

[3] Hr. Sylvian Ressigeac (Software Engineer)
Mitautor der englischsprachigen Originalversion, Erstellung einer Windows DLL, Implementierungen in einen DME

[4] Hr. Dipl.-Ing. Dirk Barthelmes
Erstellung der Spezifikation/Beschreibungen, Übersetzung aus dem englischen Original und Anpassungen an die deutschen BOS, IOP und Steuerkommandos, praktische Erprobungen mit DME, DAG und Leitrechnern im Bereich der Leitstelle Karlsruhe

1. Allgemeines

Seit der Einführung der Textverschlüsselung bei der digitalen Alarmierung haben sich zueinander nicht kompatible Systeme entwickelt. Ursache dafür war die nicht erfolgte Normierung durch die Beschlussgremien der BOS Richtlinien. Leider wird anscheinend die Technik nach der Richtlinie „Geräte für die digitale Funkalarmierung“, trotz der beinhalteten Vokabel „digital“, als ein Relikt der „Analogfunkära“ angesehen und erleidet deshalb das Schicksal aller anderen Richtlinien aus diesem Bereich. Im konservativen BOS Umfeld wird die Technik aber noch einige Jahrzehnte im Einsatz bleiben, weshalb eine bedarfsorientierte Aktualisierung sinnvoll wäre.

1.1 Entwicklungsziele

Wesentliche Entwicklungsziele waren, dass das Verfahren keine Lizenzansprüche Dritter berührt und falls doch, die Anwendung frei und ohne Kosten für die BOS Bedarfsträger möglich sein muss. Es sollte die besonderen Anforderungen der einseitigen Funkübertragung in Funkrufsystemen berücksichtigen und einen einfachen Schutz gegen unbefugte Dekodierung ermöglichen. Dieses Schutzziel wurde bewusst einfach gehalten um die Implementierung in tragbare Meldeempfänger ohne große Rechenleistung zu ermöglichen und ist bereits erreicht, wenn das Verfahren mit den im Jahre 2013 vorhandenen technischen Möglichkeiten einem Brute Force Angriff eine kurze Zeit im Wochenbereich standhält.
Hinweis: Der beschriebene BOSKRYPT Algorithmus ist weit sicherer als gefordert, er wurde aus praktischen Erwägungen wegen der weltweiten Verbreitung von AES und entsprechender Tools eingesetzt. Zusätzlich ergeben sich noch Verweise auf die empfohlene Anwendung in der BSI Richtlinie TR-03116-1 für Anwendungen im Gesundheitsbereich.

1.2 BOSKRYPT

Es bleibt ebenfalls möglich, dass Hersteller eigene Standards der Verschlüsselung, parallel oder eigenständig, zur Anwendung bringen, wenn die Anwender und vergaberechtliche Aspekte dies zulassen und wichtige Gründe dafür sprechen. Die Anwendung des Verfahrens kann von allen BOS Anwendern, z.B. im Rahmen von Beschaffungen, in eigener Zuständigkeit gefordert werden, wenn rechtliche Vorgaben, z.B. des Datenschutzes, in der Zukunft eine Verschlüsselung der Texte zwingend erfordern. Es ist frei nutzbar und nicht mit Lizenzkosten

verbunden. Das heißt aber nicht automatisch, dass Komponenten mit Kryptierung zu gleichen Preisen erhältlich sind. Der individuelle Implementierungsaufwand der Hersteller ist dabei ein Zuschlagsfaktor. Bei DME ist aber lediglich ein Aufschlag im einstelligen EUR Bereich wahrscheinlich, da heute schon DME mit Entschlüsselung ohne Aufpreis angeboten werden. Es besteht keine Pflicht der Hersteller von DA Komponenten das Verfahren in Ihre Produkte zu integrieren, folglich ist es auch kein Bestandteil der Prüfung nach TR BOS.

Die Verwendung der Spezifikation durch die Nutzung der darin aufgeführten Verfahren ist allen Herstellern und Anwendern kostenfrei möglich. Die Vertragsgestaltung zwischen Hersteller und Anwender bzw. anderen Herstellern für Produkte oder Dienstleistungen, z.B. die Nachrüstung von DME, Lieferung einer DLL etc. wird im Innenverhältnis zwischen Hersteller / Hersteller und Anwender geregelt. Die Aufwendungen für den in Teil 3 beschriebenen IOP handeln die Beteiligten bei Bedarf untereinander aus.

2. Historie

Die aktuell immer öfters geforderte Sicherung personenbezogener Daten, die auch über die digitale Alarmierung ausgesendet werden, ist historisch gesehen auf die Initiative eines Herstellers zurück zu führen. Es gab also zuerst eine technische Lösung für ein angeblich rechtliches Problem, welches von den meisten Anwendern aber damals als weniger relevant eingestuft wurde. Der Hersteller hat dann versucht über den Bundesdatenschutzbeauftragten eine Stellungnahme einzufordern. Dieser antwortet mit Schreiben vom 18.05.2006 und verweist allgemein auf die Zuständigkeit der Länder, da es sich bei Digitalalarmsystemen der BOS um nichtöffentliche Systeme in Länderzuständigkeit handelt und damit die Landesdatenschutzgesetze greifen. Eine weitere Anfrage z.B. beim ULD des Landes Schleswig-Holstein bejaht dann einen Schutz personengebundener Daten und die Erfordernis technischer Sicherungsmaßnahmen (Antwortschreiben vom 14.08.2006). Durch diese „amtliche Forderung“ stieg dann in der Zukunft die Nutzung / Verkauf entsprechender Systeme und Endgeräte stark an.

Aktuell hat sich die Nutzung der digitalen Alarmierung oft von der reinen Alarmierungsfunktion zu einer datenfunkähnlichen Nutzung gewandelt. Außerdem ist das Bewusstsein für den Schutz personenbezogener Daten weiter ausgeprägt, sodass vor allem die Sicherung der Alarmierungen der Rettungsdienstkräfte in einem anderen Licht erscheint.

2.1 Bisherige Lösungen

Getrieben durch den Markt, haben alle Hersteller in den letzten zehn Jahren zueinander inkompatible Textverschlüsselungssysteme entwickelt. Diese basieren meist auf veröffentlichten und anerkannten kryptografischen Verfahren wie z.B. AES oder IDEA. Auch wenn die Mehrzahl der Hersteller im Kern das neuere AES Verfahren nutzt, sind durch die erforderlichen weiteren Verarbeitungsschritte immer noch inkompatible Systeme gegeben. Die Aussage, dass zwei Systeme AES nutzen, begründet also noch keine funktionale Zusammenarbeit.

2.2 Sitzung an der LFS-BW 2012

Auf Initiative des Verfassers wurde im Juni 2012 zu einem Arbeitskreis „BOS einheitliche Textverschlüsselung“ eingeladen. Die Tagung fand am 27.06.2012 an der Landesfeuerwehrschule Baden-Württemberg in Bruchsal statt. Die LFS ist gleichzeitig auch der Dienstsitz der Prüfstelle für drahtlose BOS Fernmeldeanlagen. Anwesend waren fast alle Hersteller entsprechender Komponenten aus dem europäischen Raum.

2.3 Sitzungsinhalt und Beschlussfassung

Als wesentliche Entwicklungsziele wurden nach eintägiger Diskussion definiert, dass das Verfahren keine Lizenzansprüche Dritter berühren darf und falls doch, die Anwendung frei und ohne Kosten für die BOS Bedarfsträger möglich sein muss. Es soll die besonderen Anforderungen der einseitigen Funkübertragung in Funkrufsystemen berücksichtigen und einen einfachen Schutz gegen unbefugte Dekodierung ermöglichen („Basisverschlüsselung“). Dieses Schutzziel wurde bewusst einfach gehalten um die Implementierung in tragbare Meldeempfänger ohne große Rechenleistung zu ermöglichen. Es wird bereits als erreicht angesehen wenn, das Verfahren mit den im Jahre 2013 vorhandenen technischen Möglichkeiten, einem Brute Force Angriff im Wochenbereich standhält.

Der beschriebene Algorithmus ist weit sicherer als gefordert, er wurde aus praktischen Erwägungen wegen der weltweiten Verbreitung von AES und entsprechender Tools eingesetzt. Zusätzlich ergeben sich noch Verweise auf die empfohlene Anwendung in der BSI Richtlinie TR-03116-1 für Anwendungen im Gesundheitsbereich.

Der Ablauf bis zum fertigen Standard sollte in drei Phasen erfolgen:

- Phase 1 - Definition des Standards
- Phase 2 – Felderprobung, ggf. mit Rückkopplung zu 1.
- Phase 3 – Verabschiedung als BOS Standard

Phase 1 - Definition des Standards

Aufgrund der Beschlusslage zur ersten Phase wurde dann in den Folgemonaten durch die Firmen Oelmann-Elektronik und db Elektronik ein Ansatz weiter verfolgt. Die Arbeiten dazu verliefern aber nur schleppend da die Entwicklung neben dem Tagesgeschäft freiwillig und ohne Kostenträger erbracht werden musste. Durch die Aktivitäten im Rahmen der internationalen Standardisierung eines Verfahrens ergaben sich dann 2014 neue Ansätze. Durch die grundlegenden Arbeiten von [1] konnte damit der BOS Standardisierungsprozess weiter geführt werden. Mit Übersetzung auf Deutsch und Anpassungen und Ergänzungen an die Bedürfnisse der bundesdeutschen BOS durch [1,2 und 4] konnte die Phase 1 im Mai 2015 abgeschlossen werden.

Phase 2 – Felderprobung

Die Phase 2 sieht eine praktische Erprobung der theoretischen Ansätze in „freier Wildbahn“ vor. Dazu sollten möglichst viele Komponenten unter realen Bedingungen getestet werden. Mit Rundschreiben vom 13.05.15 an alle Hersteller wurde zur Mitarbeit aufgerufen. Die praktischen Erprobungen ergaben auch tatsächlich Ansätze für Verbesserungen und zeigten die Erfordernis genauerer Spezifikationen auf.

Phase 3 – Verabschiedung als BOS Standard

Für die Annahme des Standards wurde die Verabschiedung im Umlaufverfahren definiert. Nach Mitteilung vom 11.12.2015 hatten alle Hersteller sechs Wochen Zeit begründete Einsprüche zu erheben. Begründet waren Einsprüche dann, wenn das Verfahren rechtliche Vorgaben verletzt oder wesentliche technische Einschränkungen vorliegen, die dem vorgesehenen Verwendungszweck entgegenstehen.

3. Wettbewerbseinschränkungen bisheriger Lösungen

Wenn ein Landkreis bisher auf die datenschutzrechtlichen Entwicklungen reagiert hat, indem er die vermeintlich einfache und naheliegende Textverschlüsselung eines Herstellers für den Rettungsdienst einführt, war er bereits zur Hälfte in die so genannte „Kryptofalle“ gegangen.

Die negativen Auswirkungen dieser Entwicklung bemerken die Anwender oft viel zu spät, nämlich meist erst dann, wenn sich ein Anwender zu einer Vollverschlüsselung aller DME entschlossen hat und die technische Erneuerung der Infrastrukturkomponenten (DAU, DAG) ansteht. Er stand jetzt meist vor dem Problem entweder alle DME ersetzen zu müssen oder unter Ausschaltung des Wettbewerbs Infrastruktur des gleichen Herstellers erneut zu beschaffen. Dies geschieht dann fast immer unter gravierender Missachtung vergaberechtlicher Grundsätze und zusätzlich zum Nachteil der Haushalte.

4. Leistungsmerkmale und Funktion der Technik

Die Beschreibung ist sehr umfangreich und über weite Teile sehr technisch. Der interessierte Leser wird deshalb auf die Spezifikation verwiesen. Einige Grundzüge werden nachfolgend erläutert.

Bei der Verschlüsselung der Meldetexte kommen grundsätzlich zwei Stellen in Frage. Der digitale Alarmgeber nach TR BOS (DAG) oder das in den meisten Leitstellen eingesetzte Einsatzleitsystem (ELS), näheres siehe Punkt 7.

Als zugrunde liegendes Verfahren wird AES mit einer Schlüssellänge von 256 Bit eingesetzt. Die Aufbereitung der Texte für AES und das Übertragungsmedium RPC1 Funkruf erfordert aber zusätzliche Verarbeitungsschritte, die in der Spezifikation zur einheitlichen Behandlung beschrieben sind.

Es ist möglich verschlüsselt und unverschlüsselt auf einen RIC zu alarmieren. Das Endgerät erkennt dies automatisch an einem Textstring der mit „ENCR“ definiert wurde. Dadurch ergibt sich die Möglichkeit, bei regulärer Nutzung des ELS zur Verschlüsselung, bei Ausfall desselben trotzdem mit voller Textfunktionalität zu alarmieren. Für die Ausfallzeit steht dann lediglich die Verschlüsselungsfunktion nicht zur Verfügung, es wird also Klartext übertragen.
Die Migration zu einer verschlüsselten Aussendung wird dadurch ebenfalls vereinfacht, in der Umstellungsphase eines RIC sind bilinguale DME in der Lage beides anzuzeigen, können dann aber direkt und ohne Neuprogrammierung in den reinen Kryptobetrieb wechseln.

Durch Aufzeichnung einer Aussendung und spätere Wiederaussendung könnte theoretisch eine ungewollte Alarmierung durchgeführt werden, auch wenn die Texte verschlüsselt sind und der Nachrichteninhalt nicht bekannt ist. Um das zu vermeiden wird der Alarmtext durch einen Zeitstempel ergänzt. Ein unbefugter Empfänger kann selbst dann keine Nachrichteninhalte gewinnen, wenn er in der Lage wäre den Zeitstempel zu lesen oder zu erraten (aufgrund des Zeitpunkts des Empfangs).

Bei den BOS werden oft Standardtexte wie „Leitstelle anrufen“, „Brand 1“ oder „Technische Hilfeleistung“ verwendet. Bereits aufgrund der Textlänge könnte durch längere Beobachtung auf den Inhalt geschlossen werden. Das Verfahren verhindert das zuverlässig dadurch, dass Alarme auch mit gleichem Textinhalt, auf der Funkseite unterschiedlich lang sind und unterschiedliche Geheimtexte haben.

5. IOP Prozess

Da eine Überprüfung der Funktionalitäten durch die Zentralprüfstelle an der LFS-BW nicht vorgesehen ist, wird zur Erreichung der Kompatibilität der einzelnen Produkte mit dem so genannten IOP gearbeitet. Dabei testen die Hersteller ihre Produkte gegenseitig auf Funktionalität. Die Ergebnisse werden von den Herstellern an die Prüfstelle schriftlich gemeldet. Diese führt eine Liste mit den festgestellten Kompatibilitäten.

Die Hersteller können Meldungen auch einseitig abgeben, z.B. ein ELS Hersteller A der im Rahmen eines Kundenauftrages das Verfahren über die Alarmierungsinfrastruktur des Herstellers X ohne dessen Mitwirkung zum DME B positiv evaluiert hat. Nähere Ausführungen zum IOP finden sich in einem getrennten Dokument.

6. Nachrüstung von Bestandskomponenten

Moderne Empfangskomponenten (DME) haben einfach wieder beschreibbare Programmspeicher. Dadurch ist es prinzipiell auch möglich bereits im Einsatz befindliche Komponenten aufzurüsten. Die Entscheidung darüber, ob er für bisherige Produkte eine Nachrüstung anbietet, trifft jeder Hersteller selbst. Für die Anwender kommen aus wirtschaftlichen Gründen nur Nachrüstungen in Frage, die sich auf einen einfachen

Softwareupdate beschränken. Der Anwender muss diesen auch selbst mit eigenem Programmierzubehör durchführen können. Sobald eine Nachrüstung mit Änderungen an der Hardware oder der Einsendung zum Hersteller verbunden ist, kann der Aufwand als zu hoch angesehen werden. Der Update ist in der Regel auch nur wirtschaftlich wenn der DME im ersten Viertel seines Lebenszyklus ist, also ca. im ersten Jahr nach Beschaffung.
Aus wirtschaftlichen Gründen ist es sinnvoll als Ersatz für ausgemusterte DME die langsame Migration durch Neubeschaffung BOSKRYPT-fähiger, Empfänger vorzunehmen. Die Umstellung erfolgt dann RIC basiert. Vor allem bei einer langsamen Migration, muss deshalb für jeden RIC im Alarmgeber gewählt werden können, ob und wie er verschlüsselt.

7. Ort der Verschlüsselung

Bei der Verschlüsselung der Meldetexte kommen grundsätzlich zwei Stellen in Frage. Der digitale Alarmgeber nach TR BOS (DAG) oder das in den meisten Leitstellen eingesetzte Einsatzleitsystem (ELS). Grundsätzlich können auch beide Quellen parallel betrieben werden wenn sichergestellt ist, dass ein durch das ELS verschlüsselter Text nicht noch einmal durch den DAG verschlüsselt wird. Aufgrund dieser Möglichkeiten stellen ELS eine eigene Gattung Sender dar, da sie Texte unabhängig von der verwendeten Infrastruktur verschlüsseln können. Beim Aufbau neuer oder Modernisierung bestehender Systeme ist eine Verschlüsselung im DAG zu bevorzugen. Die Verschlüsselung im ELS ist in den nächsten Jahren vermutlich noch die wirtschaftlichere Ausführung weil dadurch keine Änderungen am DA System erfolgen müssen. Im Zweifelsfall wird der Wettbewerb entscheiden.

8. Anforderungen an Endgeräte

8.1 Schlüsselsicherung

Zur Sicherung des Verfahrens ist es erforderlich, dass Empfänger die verwendeten Schlüssel einem Unbefugten nicht einfach zugänglich machen. Dazu ist es Mindestvoraussetzung, dass die Schlüssel bei den Empfängern über vorhandene externe Schnittstellen nur einprogrammiert aber nicht ausgelesen werden können. Den Herstellern ist es selbst überlassen weitere geeignete Maßnahmen zu ergreifen.

Die Schlüsselsicherung bei den Alarmgebern erfolgt über die üblichen Prozesse bei EDV Anlagen. Die Weitergabe von Schlüsseldateien darf nicht über unsichere Kommunikationswege wie Email oder unverschlüsselte Datenverbindungen erfolgen.

Die Sicherheit des Verfahrens beruht ausschließlich darauf, dass die Schlüssel nicht unbefugt zugänglich gemacht werden. Sobald einer oder mehrere Schlüssel kompromittiert sind, bleibt zur erneuten Sicherung nur ein Schlüsselwechsel. Aufgrund der Struktur von BOSKRYPT ist dies aber meist mit vertretbarem Aufwand zu erreichen. Trotzdem ist die Sicherung der Schlüsseldatei der wichtigste Schritt zur Aufrechterhaltung der Integrität. Es wird empfohlen die Schlüssel nur zentral an einer Stelle zu verwalten und Externen nur die zur Programmierung ihrer eigenen Endgeräte erforderlichen Schlüssel zu übergeben (bei Individualschlüsseln, nicht bei schneller Textalarmierung). Es bietet sich an, dann nur Schlüsseldateien zu erstellen, die höchstens die Werte einer Gemeinde bzw. begrenzte RIC Bereiche enthalten.

Für die Erstellung, Verteilung und den Einsatz der Schlüssel schlägt die Beschreibung entsprechende Verfahren vor. Grundsätzlich ist es möglich Schlüssel bis auf SUB-RIC Ebene (Unteradresse) individuell zu definieren. Dadurch ergeben sich neue Möglichkeiten, da die Schlüssel auch auf Gemeindeebene, Abteilungsebene oder RIC einheitlich definiert werden können. Ein Tausch der Schlüssel auf einer dieser Ebenen erfordert keine Änderungen an den anderen Komponenten eines Landkreises.

8.2 Schlüsselspeicher in den Endgeräten

Durch die individuellen Schlüssel je RIC ergeben sich eine große Anzahl an Schlüsseln. Bei 128 RIC mit je vier Unteradressen und 256 Bit je Schlüssel ergibt sich ein Speicherbedarf von 16 KB. Bei der schnellen Textalarmierung werden für alle 256 Schlüsselindexkombinationen 8kB benötigt. Auch wenn dieser Speicherbedarf für aktuelle Mikrocontroller kein Problem darstellt, könnten aus anderen Gründen nur geringere Ressourcen zur Verfügung stehen.
Eine mögliche Lösung könnte statt einer festen Zuordnung „Schlüssel zu RIC“ darin bestehen alle Schlüssel in einem Pool zu speichern und die Zuordnung zu den RIC über einen Index vorzunehmen. Ein Endgerät kann dadurch Nachrichten an beliebig viele RIC entschlüsseln solange die Zahl unabhängiger Schlüssel die Poolgröße nicht überschreitet. Der Pool könnte sowohl für einzelne RIC als auch für die Auswahl über den Index der schnellen Textalarmierung eingesetzt werden, eigenständige Bereiche sind aber zu bevorzugen, da so ein Mischbetrieb besser unterstützt wird. Wenn der Pool weniger als 256 Einträge hat muss

zusätzlich der Index der schnellen Textalarmierung auf vorhandene Einträge umgeleitet werden. Diese Zuordnung sollte möglichst frei konfigurierbar sein.

Empfehlung:
256 Speicher wenn entweder individuell <u>oder</u> mit schneller Textalarmierung gearbeitet wird, 2 x 256 Speicher wenn beide Varianten in einem Empfänger parallel eingesetzt werden.

Beispiel für eine Eingabemaske zur Zuordnung des Index aus dem IV zu einem Schlüssel. Das Beispiel zeigt lediglich eine Version wie die 255 Möglichkeiten auf 32 Schlüssel verteilt werden können.

	X0	X1	X2	X3	X4	X5	X6	X7	X8	X9	XA	XB	XC	XD	XE	XF
0x	---	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
1x	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
2x	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
3x	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
4x	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
5x	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
6x	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
7x	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
8x	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
9x	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
Ax	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
Bx	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
Cx	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
Dx	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
Ex	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
Fx	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F

Die Eingabe kann 1:1 im Speicher abgelegt werden. Der Schlüsselindex aus dem IV wird dann einfach als Offset im Speicher genutzt um den dort konfigurierten internen Schlüsselindex zu lesen.

8.3 Schlüsselzuordnung beim Empfänger

In der Regel wird die Konfiguration eines Empfängers über eine getrennte Software für das Schlüsselmanagement durchgeführt. Diese Abspaltung ist sinnvoll, da die Geheimhaltung der Schlüssel oberste Priorität haben muss und in der Regel besser gewährleistet werden kann je weniger Stellen damit befasst sind. Falls das Poolverfahren genutzt wird muss die Zuordnung zwischen RIC und Schlüsselindex entweder in der Programmiersoftware oder in der Schlüsselmanagementsoftware erfolgen. Aus obigen Überlegungen sollte die Zuordnung in den Teil Kryptomanagement übernommen werden.

8.4 Schlüsselspeicher in den Alarmgebern

Die Schlüssellänge je RIC / Unteradresse beträgt 256 Bit. Alarmgeber müssen in der Lage sein für jeden RIC / Unteradresse einen Schlüssel mit maximaler Länge zu speichern. Dies stellt im Gegensatz zu Empfängern kein Problem dar, da selbst einfachste PCs für alle bundesweit vorkommenden RIC die Schlüssel speichern könnten. Die Herausforderung ist hier nicht die Speicherausnutzung, sondern die Sicherung dieser zentralen Schlüsseldatei.

9. Behandlung von Zeitfehlern

Einige Funktionen des Verfahrens erfordern eine zeitliche Synchronität zwischen Sender und Empfänger. Die aktuelle Ortszeit ist dabei nicht erforderlich solange Sender und Empfänger über die gleiche Zeit verfügen. Aus praktischen Gründen bietet es sich an UTC zu nutzen. So sind bei der Sommer / Winterzeit keine Zeitsprünge zu beachten. Die richtige Anzeige von Datum/Uhrzeit bleibt dann dem Endgerät vorbehalten. Der Algorithmus nutzt 32 Bits des IV für den Zeitstempel. Er ist in Sekunden ab dem 1. Januar 2014 00.00.00 in UTC codiert. Der Zeitstempel hat damit eine Laufzeit bis zum 7. Februar 2150 06:28:15 Uhr.

Das Verhalten des Empfängers bei Abweichungen des Zeitstempels ist von den Wünschen der Anwender abhängig. Deshalb ist es sinnvoll das Verhalten bei DME konfigurierbar zu gestalten. Während der Träger eines DME ggf. falsche Alarme am Textinhalt erkennen kann, ist dies bei Sirenensteuerempfängern nicht möglich. Deshalb müssen bei DSE verfristete Alarme ignoriert werden.

Für DME ergeben sich folgende Optionen

- A. mit einer Warnung versehen und normal signalisieren
- B. nur optisch signalisieren und anzeigen
- C. nur eine Warnung anzeigen
- D. komplett verwerfen

Die Zeit, nach der ein Empfänger eine Alarmierung als zeitlich verfristet ansieht, kann im Endgerät konfigurierbar gestaltet werden. Die Programmiersoftware soll dann 30 Minuten als Standardwert vorgeben. Sie darf nicht unter 10 Minuten einstellbar sein um Uhrenfehler abzufangen. Die Funktion muss abschaltbar sein. Die Empfänger prüfen das Zeitintervall in beide Richtungen, d.h im Falle des Standardwertes auf +- 30 Minuten.

Falls ein Empfänger die Option D nutzt ergibt sich ein Manipulationsrisiko durch die Änderung der Empfängerzeit über Funk (siehe auch 20).

10. Behandlung von Prüfsummenfehlern

Das BOSKRYPT Verfahren hat drei Kryptovariablen anhand derer Zustände und Fehler erkannt werden können.
Die drei ergeben insgesamt acht Möglichkeiten, die in der Tabelle weiter unten aufgeführt sind. Wie die acht Kombinationen gewertet werden, kann zwischen den Anwendern durchaus unterschiedlich sein. Als Beispiel sei hier der Fall 5 genannt. Hier könnte es Anwender geben denen es lieber ist wenigstens einen Teil zu sehen, andere sagen eine Teilinformation ist zu unsicher, weil in ihrem Bereich z.B. Alarmierungen ohne Rückfrage mit der Leistelle ausgeführt werden.
Zwei der üblichen Kombinationen wurden in der Tabelle aufgenommen und als Profil „nur Krypto“ bzw. „Mischbetrieb“ bezeichnet. Für den Anwender sollte eines dieser Profile wählbar sein. Die Auswahl sollte für jeden RIC individuell wählbar sein. Ohne Auswahlmöglichkeit ist Mischbetrieb vorzusehen. Reiner Kryptobetrieb ist nur empfehlenswert wenn der DAG die Verschlüsselung durchführt.
Der Idealfall wäre es wenn der Anwender für jeden RIC, z.B. über die Fallzahl, ein Profil festlegen kann. Dadurch können über eine Einstellmöglichkeit alle Kombinationen abgebildet werden.

Fall	SHA1 gültig?	CRC-8 gültig?	ENCR erkannt?	nur Krypto	Mischbetrieb
1	J	J	J	entschlüsselt anzeigen	entschlüsselt anzeigen (1)

2	J	J	N	nicht anzeigen	direkt anzeigen
3	J	N	J	nicht anzeigen	direkt anzeigen
4	J	N	N	nicht anzeigen	direkt anzeigen
5	N	J	J	nicht anzeigen	entschlüsselt anzeigen (2)
6	N	J	N	nicht anzeigen	direkt anzeigen
7	N	N	J	nicht anzeigen	direkt anzeigen
8	N	N	N	nicht anzeigen	direkt anzeigen

(1) Dies ist der Idealfall der fehlerfreien Übertragung
(2) Dieser Fall kann auftreten wenn ein Empfang fehlerfrei beginnt und dann vor dem Ende abbricht. Die Wahl „entschlüsselt anzeigen“ sichert dann die Darstellung des Textes soweit er empfangen werden konnte.

11. Vermeidung von Manipulationen durch wiederholte Aussendung

Durch Aufzeichnung einer Aussendung und spätere Wiederaussendung könnte eine ungewollte Alarmierung durchgeführt werden, auch wenn die Texte verschlüsselt sind und der Nachrichteninhalt nicht bekannt ist. Um das zu vermeiden wird der Initialisierungsvektor (IV) durch einen Zeitstempel ergänzt. Ein unbefugter Empfänger kann selbst dann keine Nachrichteninhalte gewinnen, wenn er in der Lage wäre den Zeitstempel zu lesen. Eine Manipulation des Zeitstempels und erneute Übertragung scheitert daran, dass der Zeitstempel ein Teil des IV ist und eine Änderung dazu führt das der Text nicht entschlüsselt werden kann.

Ein Empfänger darf einen (erneuten) Empfang einer Alarmierung mit falscher Zeitinformation nicht grundsätzlich ignorieren. Durch Konfiguration am Endgerät soll festgelegt werden können, ob er unterdrückt oder dem Anwender signalisiert wird. Falls er angezeigt wird ist der Anwender über eine geeignete Darstellung am Endgerät auf die Zeitabweichung hinzuweisen. Es ist dann Aufgabe des Nutzers anhand des Textes über die Relevanz zu entscheiden.
Als Anzeige sollen bevorzugt der Text „ZEIT“, ggf. durch Attribute wie Blinken oder Inversdarstellung unterstützt, oder ein leicht verständliches Symbol wie eine Uhr oder Sanduhr eingesetzt werden.

Bei DSE macht eine Anzeige über die Zeitabweichung wenig Sinn, sie kann aber für Servicezwecke vorhanden sein. DSE sollten aber dahingehend konfigurierbar sein ob sie die Funktion nutzen.

12. Initialisierungsvektor

Der Initialisierungsvektor ist 64 Bit lang und besteht aus einem 32-Bit-Zeitstempel und einem weiteren 32-Bit-Wert der sich aus den drei Teilen Schlüsselindex, Zufallsbits und CRC-8 zusammensetzt. Der Zeitstempel ist ähnlich wie der von Unix/Linux Systemen und zählt in Sekundenschritten. Im 32 Bit Wert sind Datum und Uhrzeit codiert. Abweichend zu Linux Systemen, die am 01.01.1970 mit der Sekundenzählung beginnen, startet der Timestamp bei BOSKRYPT ab 1. Januar 2014 00.00.00 UTC und hat eine entsprechend längere Restlaufzeit. Beispiel: Der 1. Dezember 2014 14:29:11 wird als B720B901 codiert.

Für eine erfolgreiche Entschlüsselung benötigt der Empfänger einen fehlerfreien Empfang der Kryptovariablen (IV + SHA1). Bereits ein einziges falsches Bit verhindert die korrekte Entschlüsselung. Der IV + SHA1 wird in den ersten Zeichen einer Aussendung übertragen. Ein DA Netz mit möglichst geringer Bitfehlerrate in der Fläche ist erforderlich, ggf. ist die Versorgung durch zusätzliche DAU zu verbessern. Kürzere IV erhöhen die Chance auf eine fehlerfreie Übertragung. Daher sollte die Größe des IV so kurz, wie im Hinblick auf die Sicherheit annehmbar, gehalten werden.

Die CRC-8-Prüfsumme soll die Integrität der Verfahrensvariablen des IV gewährleisten. Ein Empfänger erkennt an einem falschen CRC einen Fehler, bei den zur erfolgreichen Entschlüsselung erforderlichen Werten. Er hat keine wesentliche kryptografische Relevanz, hilft aber fehlerhafte Darstellungen („Zeichensalat“) zu vermeiden. Eingesetzt wird das international für Telekommunikationsanwendungen bekannte CRC-8. Es ist für die hier vorgesehene Anwendung ausreichend sicher und entsprechend kurz.

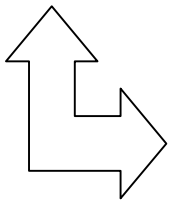
13. Schlüsselindex

Bei der Anwendung von Verfahren zur zeitlichen Optimierung von gleichen Textmeldungen an verschiedene, dynamisch gebildete Empfängergruppen wird die Textinformation über einen speziell definierten, immer gleichen Text RIC übertragen. Der Text kann wie jede andere Alarmierung über das hier beschriebene Verfahren gesichert werden. Dafür würden

dann nur die vier Schlüssel der Unteradressen A..D zur Verfügung stehen. Um den Schlüsselraum zu erweitern wird im IV ein 8 Bit Index übertragen über den der zugehörige Schlüssel zur Dekodierung ausgewählt wird. Da dieser Index bei jedem Alarm individuell übertragen wird, entfällt die Notwendigkeit einer manuellen oder automatisch getrennt durchgeführten Schlüsselumschaltung. Damit besteht auch nicht die Gefahr, dass Empfänger die ausgeschaltet oder außerhalb des Empfangsbereiches waren, Kommandos zur Schlüsselumschaltung verpassen. Empfänger wenden diesen Index nur auf den Text RIC der schnellen Textalarmierung an. Außerhalb der schnellen Textalarmierung wird er mit 00 belegt. Der Schlüsselindex ist 8 Bit lang, das MSB wird zuerst übertragen.

Textübertragung der Leitstelle

Zeit	Index	Sonst.	CRC	Kennung	Alarmtext
0005A378	**01**	1234	AB	ENCR	Brandeinsatz A-Dorf



Index	256 Bit Schlüssel
00	a897c8a234566de4977e…
01	**82837498723424562355….**
02	8972347823c234e234f2…
…..	
254	89134759128734852323….
255	8923754f2e233a23d223c….

Schlüsselspeicher im Empfänger

14. Sicherheitshinweis zum IV, Belegung der Zufallsbits

Durch konstruktive Maßnahmen innerhalb der Verschlüsselungssoftware ist sicherzustellen, dass ein IV nur einmal genutzt wird. Da sich der IV mit dem Zeitstempel automatisch jede Sekunde ändert und zur Zeit 16 Zufallsbits möglich sind, ist dies einfach zu erreichen. Eine Verletzung dieser Vorgabe behindert nicht die Alarmierung, eröffnet aber eine Sicherheitslücke.

Die zur Zeit 16 Bits, die innerhalb des IV zufällig belegt werden sollen, können durch die Verschlüsselungssoftware nach einem beliebigen Verfahren ermittelt werden. Das Verfahren muss nicht offen gelegt werden, da es für die Dekodierung nicht erforderlich ist.

15. Trennung von Nutzergruppen

Ausgangssituation

Bei den bisherigen BOS Systemen der digitalen Alarmierung im 2m Bereich nach Standard RPC1 waren bisher ausschließlich herstellerspezifische Verschlüsselungsverfahren im Einsatz. In der Regel arbeiten die Systeme mit einem Schlüssel, der aus einer Menge von n Schlüsseln ausgewählt wird. Die Umschaltung der Schlüssel kann oft über einen speziellen Funkbefehl erfolgen. Die Schlüssel an sich werden dabei nicht übertragen, sondern lediglich ein Verweis auf im Empfänger vorprogrammierte Schlüssel. Praktisch wird dieses aber fast nie durchgeführt, da die Umschaltung auch das Risiko birgt, dass einzelne Empfänger den Umschaltbefehl nicht erhalten und dann ab der Umschaltung keine (sinnvolle) Textdarstellung mehr haben.
Ein weiteres Problem besteht darin, dass jeder, der Zugriff auf einen mit Schlüssel versehenen Empfänger erlangt, die Möglichkeit hat zusätzliche RIC zu programmieren. Moderne DME mit bis zu 128 RIC oder Tischanzeigen mit großen RIC Bereichen ermöglichen dabei schon die Überwachung aller Nutzer eines ganzen Netzes / Landkreises oder Landes. Dadurch können auch Meldungen mitgelesen werden, die für diesen Empfänger nicht vorgesehen waren. Bei Landeslösungen mit bis zu 30.000 identisch verschlüsselten DME, ist es wahrscheinlich dass DME auch für diese Zwecke genutzt werden.
Die DA Netze werden fast immer BOS Dienst übergreifend genutzt. Der Teil Rettungsdienst, der öfters mit personenbezogenen sensiblen Daten arbeitet, will ggf. verhindern dass DME aus anderen BOS Diensten mitlesen können. Führungskräfte wollen verhindern, dass nachrangige Empfänger Ihre vertraulichen Mitteilungen mitlesen usw. Besonders wichtig wird diese Forderung wenn verschlüsselte DME an Externe, z.B. Vertreter der Presse ausgegeben werden.

Hinweis:

Nachfolgende Beschreibung stellt nur einen Vorschlag dar, wie Anwender organisatorisch eine Trennung der Nutzergruppen durchführen können. Die Angaben bedeuten weder, dass Hersteller dies implementieren müssen, noch dass es auf Seiten der Anwender

erforderlich ist eine Trennung durchzuführen. Die Beschreibung dient lediglich dazu eine mögliche Lösung aufzuzeigen wenn der Bedarf in Zukunft besteht.

Mögliche Lösungen mit BOSKRYPT

Das Verschlüsselungsverfahren BOSKRYPT bietet hier Möglichkeiten diese Trennung sehr einfach durchzuführen. Da grundsätzlich jeder RIC/Unteradresse einen eigenen Schlüssel haben kann, werden auf den Empfängern nur die für die gewünschten RIC verwendeten Schlüssel vorgehalten. Es können zwar nach wie vor zusätzlich RIC programmiert werden, wegen der fehlenden Schlüssel erfolgt dann aber keine lesbare Textdarstellung mehr.
Eine besondere Situation ergibt sich bei Einsatz von Verfahren die Textalarmierungen an dynamische Gruppen beschleunigen sollen. Dabei werden die Texte für alle DME auf einen netzweit einheitlichen Text RIC übertragen. Hier würde die Lösung einen Schlüssel je RIC zu verwenden erstmal nicht greifen. Die Unterscheidung anhand der Unteradresse würde eine Nutzungseinschränkung bedeuten und zudem auch nur vier Möglichkeiten bieten. Der Einsatz von unterschiedlichen Text RIC je BOS Dienst schränkt die Bildung von dynamischen Gruppen zunehmend ein und schmälert dadurch den gewünschten Beschleunigungseffekt deutlich.
BOSKRYPT bietet durch den im Initialisierungsvektor übertragenen Schlüsselindex eine elegante Möglichkeit diese Trennung auf einem einzigen Text RIC durchzuführen. Der mit acht Bit Länge ausgeführte Index verweist auf einen von 256 möglichen Schlüsseln. Der Schlüsselindex wird bei jedem Alarm mit übertragen, kann also auch bei jedem Alarm individuell gesetzt werden. Der vorhandene Schlüsselraum kann jetzt für die Gruppen aufgeteilt werden. Diese Zuteilung kann entweder streng isolierend oder auch mit gemeinsamen Schnittmengen ausgeführt werden. Eine individuelle Meldung an den Leiter der Feuerwehr wird dadurch anders indiziert als eine kombinierte Alarmierung Feuerwehr / Rettungsdienst. Für jeden DME kann dabei die individuelle Gruppenzugehörigkeit durch Konfiguration des Gruppenschlüssels hergestellt werden.

Die acht Bit des Indexes werden acht verschiedenen Gruppen zugeteilt. Der zu verwendete Schlüsselindex ergibt sich einfach durch die Addition der Wertigkeiten (wie bei der Umrechnung vom Binär in das Dezimalsystem)

8	7	6	5	4	3	2	1
RD	Führung RD	FW	Führung FW	HIOG	THW + Werk FW	Frei	Presse + Sonstige
128	64	32	16	8	4	2	1

Beispiele:

- Eine Alarmierung die nur an Presse + Sonstige geht erhält den Schlüsselindex 1
- Eine Alarmierung die FW + RD betrifft enthält den Index 128+32=160
- Der wöchentliche Probealarm für alle außer Presse geht an den Index 128+64+32+16+8+4+2=254

16. SHA1-Prüfsumme

Die SHA1-Prüfsumme soll die Nachrichtenintegrität gewährleisten. Da sie mit verschlüsselt wird, ist ein Angreifer nicht in der Lage sie bei Bedarf auf einen bestimmten Wert zu ändern, außer er ist in der Lage die Verschlüsselung zu brechen. Der SHA1 Hashwert ist 160 Bit lang. Es werden jedoch, um Übertragungskapazität zu sparen und die Wahrscheinlichkeit eines fehlerfreien Empfangs zu erhöhen, nur die ersten 40 Bits (MSB) verwendet.

17. Meldungsvergleich

Die Eigenschaft innerhalb einer (programmierbaren) Frist eingegangene identische Textmeldungen nur einmal zu signalisieren muss auch bei Anwendung der Verschlüsselung erhalten bleiben. Der Vergleich erfolgt grundsätzlich mit den entschlüsselten Texten (Klartextvergleich). Diese Vorgabe war erforderlich, da sich im Feldtest bei einer Konstellation ein Fehler bemerkbar gemacht hat. Zur Erhöhung der Anrufsicherheit wurden im Testsystem „echte“ Alarmierungen gedoppelt. Dies erfolgte dadurch, dass beim Meldungseingang des ELS zwei eigenständige Aufträge angelegt wurden, die nachfolgend getrennt weiter verarbeitet wurden. Dadurch ergaben sich durch zeitlichen Versatz und die Zufallswerte im IV aber zwei verschiedene Kryptotexte. Der DME hat sich vereinfacht aber nicht die entschlüsselten Texte gemerkt, sondern hat bereits auf RPC1 Codewortebene verglichen. Trotz gleichen Klartextinhalt sind aber diese immer unterschiedlich, sodass der DME einen neuen Alarm erkannt und signalisiert hat. Aus diesem Grund wurde die Forderung nach Vergleich auf Klartextebene in die Spezifikation aufgenommen.

18. Länge verschlüsselter Texte

Die Länge einer Übertragung wird durch verfahrensabhängige Faktoren gegenüber dem

Klartext erhöht. Zur Sicherung der Kompatibilität der Komponenten unterschiedlicher Hersteller musste deshalb eine Mindest- und Maximaltextlänge, die alle Geräte beherrschen können müssen, festgelegt. Daraus resultiert eine kürzere maximale Klartextlänge bei verschlüsselter Übertragung. Der Wert von 180 Zeichen stellt aber keine praktische Einschränkung dar, da die durchschnittliche Zeichenzahl bei Alarmen bei 130 Zeichen liegt.

19. Füllzeichen

POCSAG-Meldungen sind im Vergleich zu PC Anwendungen sehr kurz. Außerdem werden oft Standardtexte wie „Bitte Rückruf“ oder „Brand 1“ übertragen. Insbesondere bei der Verwendung von CTR kann durch längere Beobachtung der Aussendungen und einfacher Kenntnis des BOS Dienstes, bereits durch die Auswertung der Länge des verschlüsselten Textes auf den Inhalt einer Nachricht geschlossen werden. Daher ermöglicht es der Algorithmus durch mengenmäßig zufällig gewählte Füllzeichen die Länge zu variieren obwohl immer die gleiche Nutzdatenlänge übertragen wird. Bei Nutzung dieser Funktion wird durch den Algorithmus eine zufällige Zahl von (binären, 8 Bit) Nullbyte Werten (hex 00) an das Ende des Klartextes angehängt.

Da sich durch diese Option die Aussendezeiten verlängern, sollten durch den Sender folgende Optimierungen möglich sein:

- Abschalten der Funktion durch Konfiguration des Anwenders
- Füllzeichen nur bei Texten unter 30 Zeichen
- Begrenzung der (Zufalls)Zahl auf einen Wert zwischen 5 bis 30

20. Steuerfunktion Zeit / Datum

Die Empfänger sollen eine automatische Einstellung des Datums/Zeit über Funk durch spezielle Textinhalte ermöglichen. Dafür können die bereits eingeführten Verfahren der einzelnen Hersteller oder dass nachfolgend beschriebene Verfahren zum Einsatz kommen.

Auf einen, netzweit einheitlichen RIC, wird ein Text gesendet wie er nachfolgend beschrieben ist:

#ZEIT=HHmmddMMyy#ZEIT=HHmmddMMyy

Beispiel für 17:23 Uhr am 03.11.2015 #ZEIT=1723031115#ZEIT=1723031115

Hinweis:
Nachfolgend wird nur noch von Zeit gesprochen, es ist aber immer die Kombination aus Datum und Uhrzeit (UTC) gemeint.

Ein einheitlicher RIC ist erforderlich um die Netzlast bei der Verteilung möglichst gering zu halten. Die Netzinfrastruktur muss diesen RIC regelmäßig aussenden, empfohlen werden einmal pro Stunde. Im Fall einer unverschlüsselten Aussendung wird die Unteradresse A genutzt, für eine verschlüsselte Aussendung die Unteradresse D.

Verhalten der Empfänger

1. Ein Empfänger prüft den RIC auf die obige Zeichenkombination. Zur Sicherung wird die Information gedoppelt, beide Zeitstempel müssen gleich sein, sonst muss der Empfänger die Meldung verwerfen.

2. Eine nach 1. korrekte, über Unteradresse= D verschlüsselt übertragene Zeitinformation wird dazu genutzt die interne Uhr zu stellen. Beträgt die Abweichung mehr als 30 Minuten soll der DME Träger die Umstellung bestätigen. Auf die erforderliche Bestätigung ist der Anwender entsprechend der Einstellungen akustisch und optisch hinzuweisen. Die Bestätigung entfällt bei Sirenensteuerempfängern (DSE).

Falls die Übertragung unverschlüsselt erfolgt (UA=A) besteht eine erhöhte Gefahr der externen Einflussnahme auf die Empfängerzeit. Aber auch ein vielen bekannter Schlüssel birgt die Gefahr des Missbrauchs. Besonders wenn Alarme bei falschem Zeitstempel unterdrückt werden, müssen die Schlüssel besonders sorgfältig geheim gehalten werden und es darf dann keine unverschlüsselte Übertragung der Zeitinformation erfolgen.

Es wird empfohlen bei DME nur dann die Zeit automatisch anzupassen wenn die Abweichung kleiner drei Minuten (Uhrenfehler) ist. In diesem Fall wird der Alarm mit dem Zeitkommando weder akustisch / optisch signalisiert noch in den Meldungsspeicher geschrieben. Wenn eine derart durchgeführte Zeitkorrektur die bisherige Zeit um mehr als drei Minuten verstellt, dürfen für 60 Minuten keine Korrekturen über Funk mehr angenommen werden.

Hinweis:

Bei der Implementierung in Empfängern ist darauf zu achten, dass bisherige herstellereigene Verfahren der Zeiteinstellung, vor allem wenn sie unverschlüsselt arbeiten, deaktiviert sein müssen.

21. Steuerfunktion Empfänger sperren

21.1 - Teil Empfänger

Durch die Nutzung dieser Funktion können verloren gegangene Empfänger über Funk gesperrt werden (sofern sie noch erreichbar sind). 16 alphanumerische Zeichen bieten genügend Kombinationen um alle Empfänger eines Landkreises mit einem individuellen Sperrcode zu versehen. Die Programmiersoftware sollte eine Möglichkeit haben einen Empfänger auch direkt zu sperren ohne den Umweg über den HF Empfang zu gehen. Bezüglich des Verhaltens eines gesperrten Empfängers besteht eine weitgehende Gestaltungsfreiheit der Hersteller. Es ist ebenso möglich mehrere 16 Zeichen Sequenzen zu speichern um unterschiedlich umfangreiche Maßnahmen anzuregen. Die Maximalmaßnahme ist die Löschung aller Parameter, insbesondere der Kryptoschlüssel, und die nachfolgende Abschaltung. Eine Aktivierung kann dann nur noch durch Neuprogrammierung, verschärfend nur beim Hersteller, erfolgen. Eine Implementierung im Sinne von BOSKRYPT, insbesondere unter Beachtung von Kapitel 22, ist z.B. die Deaktivierung aller Tasten, die Ausgabe eines Hinweistextes sowie die Sperrung aller Alarmsignalisierungen bei ansonsten weiter bestehender Empfangsbereitschaft für den Freigabecode.

21.2 - Teil Sender

Für die Aussendung sind keine besonderen Maßnahmen erforderlich. Jeder DAG, der in der Lage ist verschlüsselte Aussendungen nach dieser Spezifikation durchzuführen, kann für die Steuerkommandos nach Teil C der Beschreibung eingesetzt werden. Für eine effektive Durchführung der Sperranweisung sollte der DAG die Aussendung über längere Zeiträume in unregelmäßigen Abständen wiederholen.

22. Steuerfunktion Empfänger freigeben

22.1 - Teil Empfänger

Durch Empfang einer vordefinierten Zeichenfolge (Entsperrwort) soll ein Empfänger wieder aktiviert werden können. Durch die Nutzung dieser Funktion können wieder gefundene

Empfänger über Funk auch wieder aktiviert werden. Eine zweite Möglichkeit ist das ein DME vor dem Versand zum Empfänger gesperrt wird und erst dann freigegeben wird, wenn dieser den Erhalt bestätigt.

22.2 - Teil Sender

Für die Aussendung gilt das unter C2.2 angeführte. Auf die automatische Wiederholung kann verzichtet werden.

23. Schlüsselaustauschverfahren

In den ersten Entwürfen waren einfache textbasierte Dateien vorgesehen. Diese haben den Vorteil dass sie mit Software der üblichen Betriebssysteme einfach eingesehen und bearbeitet werden können. Auf mehrfachen Vorschlag hin wurde aber eine XML Struktur aufgenommen. Für die Bearbeitung und Nutzung von XML Dateien gibt es fertige Softwareroutinen, die sich einfach in eigene Softwareprodukte integrieren lassen. Der Vorteil einfach lesbarer Dateien geht dabei trotzdem nicht verloren.

23.1 Aufbau der Datei

Die wesentlichen Daten sind der RIC, die Unteradresse, der zugehörige Schlüssel und ein Kommentar. Für die Daten gelten folgende Randbedingungen:

- Jede Kombination von RIC / Unteradresse darf nur einmal vorkommen
- Die Werte müssen syntaktisch richtig sein:
    - als Schlüsselzeichen sind nur die Zeichen 0..9, A..F bzw. a..f zulässig
    - Unteradressen nur A bis D
    - RIC zwischen 1 und 2097152 ohne führende Nullen
- Die RIC und Unteradressen müssen monoton steigend sein

Die ebenfalls beispielhaft aufgeführte XSD Datei kann dabei helfen Werte auf Plausibilität zu prüfen. Manuelle Änderungen, z.B. die Einsetzung eines gleichen Schlüssels für alle Unteradressen eines RIC können auch mit einfachen Texteditoren durchgeführt werden.

Der Parameter „Cryptoprovider" setzt sich zusammen aus dem Namen des Verfahrens oder Herstellers ergänzt um eine fortlaufende Versionsnummer und wird bei Anwendung dieses Verfahrens mit "BOSKRYPT10" belegt. Die Versionsnummer wird ggf. bei späteren Erweiterungen hoch gezählt. In herstellereigene Verfahren kann durch Eintrag einer anderen Zeichenfolge verzweigt werden. Dadurch ist es möglich den Datenaustausch auch in Netzen mit gemischten Kryptierungsverfahren einzusetzen. Diese Möglichkeit unterstützt damit die sanfte Migration von einem oder mehreren herstellereigenen Verfahren zu BOSKRYPT.

23.2 Schlüsselgenerator

Die Generierung der XML Datei und vor allem der großen Zahl an Schlüsseln ist per Hand mühsam. Hier besteht die Gefahr dass die Anwender den Schlüsselraum nicht ausnutzen, zu viele ähnliche oder gar gleiche Schlüssel einsetzen oder eine fremde Datei übernehmen.

Die Austauschdatei ist sinnvoll da Schlüssel immer beim Sender und Empfänger benötigt werden. Selbst wenn einer von beiden die Funktion der Schlüsselgenerierung implementiert hat, müsste er die xml Datei exportieren können damit die Gegenseite die Schlüssel automatisiert übernehmen kann.

Eine eigene Schlüsselgeneratorsoftware kann innerhalb einiger Sekunden, zumindest ein Grundgerüst generieren, welches dann an die lokalen Verhältnisse angepasst werden muss und als Quelle sowohl für die Sender als auch Empfänger dient. Da diese Software pro Alarmierungsnetz nur einmalig eine Datei erzeugen muss, würde es ausreichen wenn ein einziger Anbieter diese anbietet.

23.3 Anweisungen zur Schlüsselverwaltung

1. Die Datei mit allen in einem Netz verwendeten Schlüsseln muss als Verschlusssache angesehen und entsprechend behandelt werden. Sie darf den Bereich der Leitstelle in dieser Gesamtform nicht verlassen (Ausnahme: Eine Sicherung auf Datenträger im Verschlusssachenraum der Behörde).
2. Die Verwaltung und Sicherung dieser (Gesamt)Datei ist möglichst nur einer Person, ggf. mit einem Stellvertreter zu übertragen.
3. Wenn Dritte Schlüssel zur Programmierung der Endgeräte benötigen sind diese aus der Gesamtdatei zu extrahieren und nur auf den tatsächlichen Bedarf zu beschränken.

4. Die Dateien aus 3. dürfen nicht per Email oder unsichere Datenverbindungen versendet oder auf Speichern im Internet vorgehalten werden. Dritte sind besonders darauf hinzuweisen.

24. Sirenensteuerempfänger (DSE)

Bei der Auslösung von Sirenensteuerempfängern (DSE) kann BOSKRYPT mit zwei verschiedenen Leistungsmerkmalen unterstützen:

1. Der eigentlichen Textverschlüsselung zur Übertragung eines Passwortes, hier vor allem mit den Füllzeichen zur Verschleierung,
2. Mit der Zeitüberprüfung

Beide Funktionen müssen mit Konfiguration durch den Anwender auch abschaltbar sein (Rückfall auf Standardverhalten nach TR BOS).

24.1 Passwort bei DSE

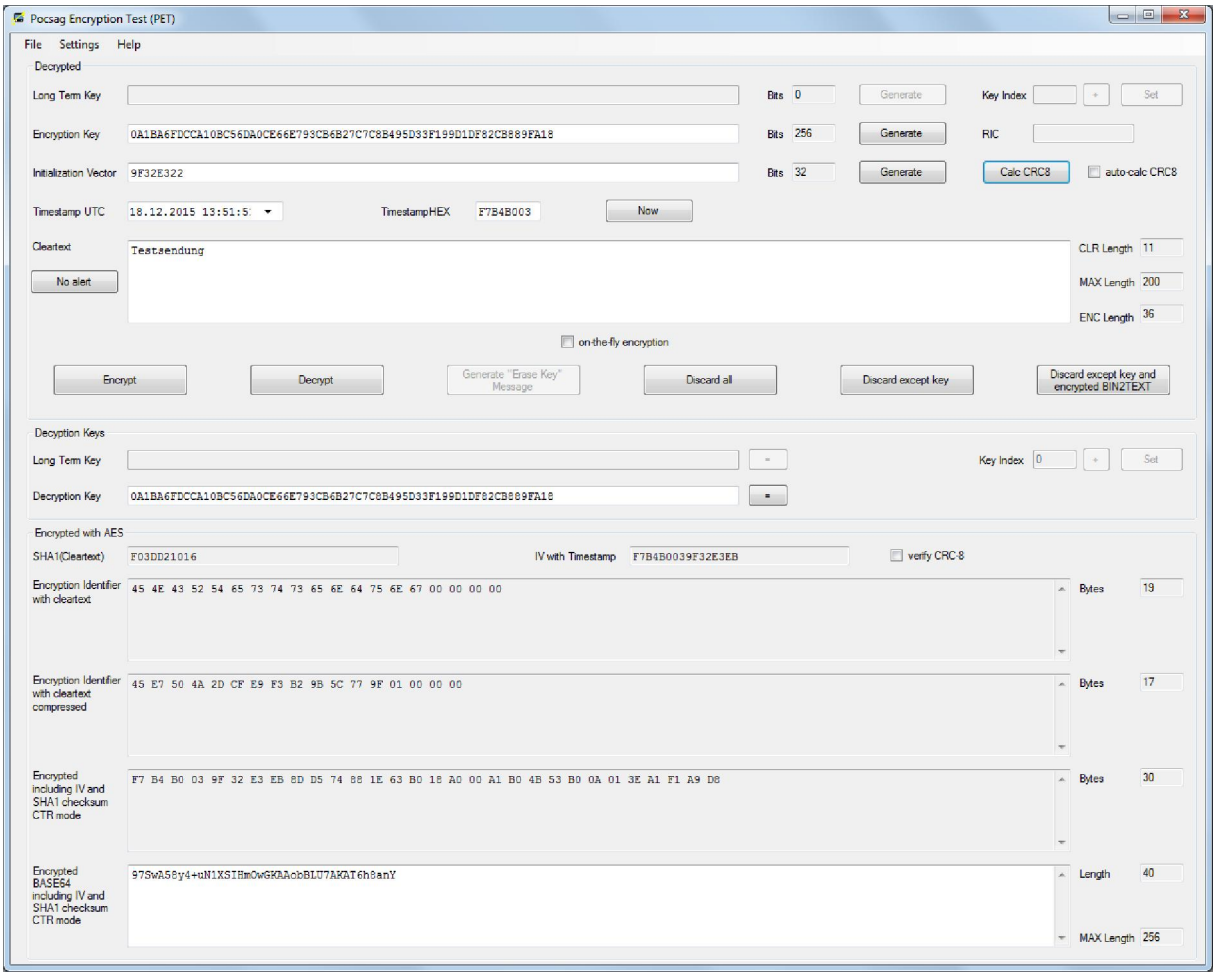
Für die Passwortfunktion sind in den Alarmgebern und DSE Speicher für mindestens 20 und maximal 40 Zeichen vorzusehen. Die obere Grenze ergibt sich theoretisch zwar durch die Spezifikation mit 180 Zeichen, zur Optimierung der Auslösezeiten sollten aber keine Passwörter über 40 Zeichen gewählt werden. Für Passwörter sind alle druckbaren Zeichen des POCSAG Zeichensatzes zugelassen.

25. Tools zur Entwicklungsunterstützung

25.1 PET Software

Für die Entwicklung von Komponenten mit BOSKRYPT Funktionalität steht als eine Möglichkeit ein sehr leistungsfähiges Tool zur Verfügung. Eingangsvariablen lassen sich frei einstellen. Als Ausgabe steht der berechnete Kryptotext sowie alle Zwischenschritte zur Verfügung. Damit lassen sich die Ergebnisse der eigenen Softwareentwicklung Stück für Stück nachvollziehen und so eine wesentliche Beschleunigung erzielen.

Die Software wurde von Hr. Dipl.-Ing. Florian Fuchs entwickelt. Die Urheberechte liegen beim Österreichischen Roten Kreuz, Landesverband Kärnten, bei Bedarf wenden sie sich bitte direkt an technik@rls.k.roteskreuz.at
Die Abgabe erfolgt grundsätzlich, ggf. gegen NDA, nur an Personen, die sich nachweislich mit der Entwicklung von nach TR-BOS geprüften Endgeräten befassen.

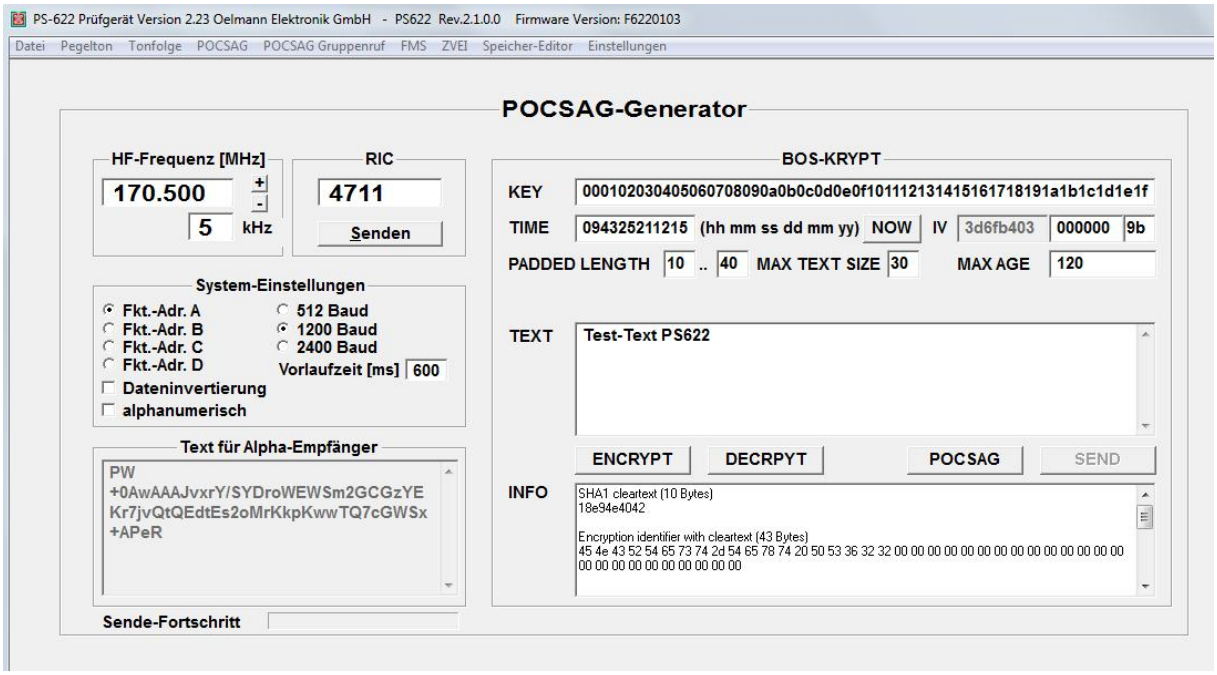


25.2 PS622 Testsender

Der PS622 der Firma Oelmann Elektronik ist ein Testsender der direkt im 4m, 2m und 70cm Bereich modulierte Signale mit verschiedensten Signalisierungen zur Verfügung stellt. Er kann auch mittels einer Windows Software angesteuert werden, die für die BOSKRYPT Anwendung erweitert wurde. Auch hier werden in der Entwicklerversion alle Zwischenschritte angezeigt. Zusätzlich kann aber ein Empfänger durch den integrierten HF Generator gleich über Funk getestet werden. Insgesamt also ein Gerät, welches über die Entwicklung hinaus eingesetzt werden kann und auch für Anwender die Prüfung einer DME Programmierung incl. Entschlüsselung erlaubt.

Mobiles Prüfgerät für Meldeempfänger

Tri-Band-Gerät 70cm, 2m und 4m



Maske der Laborversion, aktuelle Versionen können abweichen

Versionshistorie

31.05.16	Ergänzungen im Bereich der Empfängersperrung (Kapitel 21)
01.05.18	BOSKRYPT Schreibweise angepasst, Hinweis bei Zeitkommando ergänzt
01.12.18	Kleine sprachliche Änderungen