Verfahren zur Verschlüsselung von Textmeldungen

BOSKRYPT

als Ergänzung zur TR BOS

„Geräte für die digitale Funkalarmierung“

Teil 3 – IOP Verfahren

INHALT

Vorwort

Diese Beschreibung regelt das IOP Verfahren mit denen die Hersteller ein- oder gegenseitig die Kompatibilität ihrer Geräte mit der Spezifikation BOYKRYPT überprüfen. Es beschreibt eine Reihe von einfachen Tests um möglichst viele Teile zu überprüfen.

Testprotokoll

Alle Tests müssen in einem Protokoll dokumentiert werden. Dazu kann z.B. die Mustervorlage im Anhang verwendet werden. Falls diese nicht verwendet wird, sind in das eigene Protokoll mindestens die Daten des Musters zu übernehmen. Das Protokoll soll die durchgeführte Prüfung nachvollziehbar dokumentieren, deshalb sind möglichst viele Details aufgeführt. Die Ergebnisse lassen sich in der Regel gut und einfach fotografisch dokumentieren. Der Prüfbericht ist in einem gängigen elektronischen Dateiformat zur Verfügung zu stellen, vorzugsweise als PDF. Die Zusammenfassung am Schluss ermöglicht den Anwendern einen schnellen Überblick über die Leistung der geprüften Komponente ohne den ganzen Bericht lesen zu müssen.

Einstufung der Tests

Die einzelnen Tests haben eine Einteilung in vier Stufen. Eine Komponente muss mindestens alle Tests der mit Stufen A und B klassifizierten Tests bestehen.

A-Test sind dann erfüllt wenn die beschriebene Testbedingung genau wie beschrieben eingehalten wird. B-Tests sind dann erfüllt wenn die beschriebene Testbedingung dem Sinn der Anwendung nach zutrifft. Eine typische B Ausführung ist z.B. wenn die Verwendung eines Logos vorgeschlagen wird, das Logo aber nicht genau beschrieben ist, dem durchschnittlichen Nutzer aber einsichtig ist. Die Art der Erfüllung, z.B. Texte Logos etc. sind zu dokumentieren.
Ergebnisse von C-Tests werden nur zur Dokumentation und Information der Anwender aufgeführt. Sie sind durchzuführen, die Ergebnisse gehen aber nicht in die Gesamtbewertung ein. D-Tests prüfen in der Regel Leistungsmerkmale die einer

starken herstellerspezifischen Auslegung unterliegen bzw. ganz fehlen können. Wenn sie durchgeführt werden sind die Ergebnisse zu dokumentieren, falls nicht die Nichtdurchführung. Werden zusätzliche Leistungsmerkmale geprüft die in dieser Beschreibung nicht aufgeführt sind können diese zwischen den Beteiligten frei festgelegt werden. Eine Aufnahme in das Protokoll ist sinnvoll.

Typografie

Bei Nutzung der Word Datei, wird zur einheitlichen Darstellung darum gebeten, Überschriften und Festtexte in der Schriftart Arial zu belassen und eigene Eintragungen in der `Schriftart Courier` vorzunehmen.

Verhalten im Fehlerfall

Wenn einer der A- oder B-Tests nicht erfüllt wird, ist zuerst die Ursache aufzuklären und zu dokumentieren wenn der Grund für die spätere Verwendung relevant ist. Die Ursache ist dann zu beheben und dieser Test zu wiederholen. Nach der Behebung der Fehlerursache kann die Testreihe zu Ende geführt werden.

Falls dann keine weiteren Fehler gefunden werden, sind nach einer Softwareanpassung alle Tests komplett zu wiederholen, da grundsätzlich nicht ausgeschlossen werden kann dass Änderungen auch Rückwirkungen auf bereits erfolgreich durchgeführte Tests haben.

Prüfgeräte

Zur Durchführung der Test bzw. deren Protokollierung sind neben den Prüflingen weitere Testeinrichtungen erforderlich. Diese sind:

- RPC1 Auswerter mit HF Empfangsteil, z.B. ein weiterer DME
- RPC1 Testsender mit Möglichkeit der Bitmanipulation auf RPC1 Codewortebene
- Digitalkamera

Vor allem der spezielle RPC1 Testsender ist u.U. nicht überall vorhanden. Es ist dann zulässig diese Teiltests extern durchzuführen oder sich entsprechende Prüfmittel zu leihen. Die eingesetzten Komponenten sind zu dokumentieren.

Einzeltests

1. Test (Zeichensatzdarstellung)

Klassifizierung: A

Prüfziel: Dieser Test soll, zusammen mit Test 2, überprüfen ob der komplette Zeichensatz dargestellt bzw. ausgelöst werden kann.

Testtext:
`abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ`

Testbedingung erfüllt bei: fehlerfreier Darstellung aller Zeichen

2. Test (Zeichensatzdarstellung)

Klassifizierung: A

Prüfziel: Dieser Test soll, zusammen mit Test 1, überprüfen ob der komplette Zeichensatz dargestellt bzw. ausgelöst werden kann.

Testtext: `!"#$%&'() +,-./:;<=>?§äöüÄÖÜß`

Entsprechend den Hexwerten von 20 bis 2F, 3A bis 3F und 7B bis 7E. Auf die Prüfung der Zeichen 6E, 6F und 7F wird verzichtet.

Testbedingung erfüllt bei: fehlerfreier Darstellung aller Zeichen

3. Test (Steuerzeichen CR und LF, nur DME)

Klassifizierung: B

Prüfziel: Dieser Test soll überprüfen ob eine zeilenweise Formatierung der Darstellung bzw. der Aussendung möglich ist.

Testtext:

```
Zeile 1 (CR + LF)
Zeile 2 (CR + LF)
Zeile 3 (CR + LF)
```

Testbedingung erfüllt bei: einem Endgerät mit mindestens drei Anzeigezeilen und fehlerfreier Anzeige in drei Zeilen

4. Test auf Erkennung gleicher Meldungen

Klassifizierung: A

Prüfziel: Dieser Test soll überprüfen ob textgleiche Meldungen auf der Klartextebene verglichen und entsprechend unterdrückt werden.

Testtext: Dies ist eine doppelte Meldung

Weitere Testbedingungen: Viermalige Auslösung mit einem Abstand von min. 1s und max. 30s. Es muss sichergestellt sein, dass der Alarmgeber durch unterschiedliche Initialisierungsvektoren vier verschiedene Kryptotexte generiert. Die vier Geheimtexte sind über eine Funkauswertung zu protokollieren.

Testbedingung erfüllt bei: einem Endgerät, dass die viermal erfolgte Auslösung nur bei der ersten Auslösung signalisiert.

5. Test auf Erkennung verfristeter Meldungen

Klassifizierung: B

Prüfziel: Dieser Test soll überprüfen ob der Empfänger verfristete Meldungen erkennt und entsprechend den Vorgaben behandelt.

Testtext: Dies ist eine verfristete Meldung +-30

Weitere Testbedingungen:

- Text ergänzt um die jeweils aktuelle Zeitdifferenz (hier +- 30 Minuten).
- Es ist sicherzustellen, dass der Empfänger eine bekannte Zeitinformation hat
- Unterdrückung gleicher Meldungen im Empfänger auf 2 Minuten konfiguriert (Hier handelt es sich nicht um die Zeit verfristeter Meldungen sondern die Zeit in der der Empfänger gleiche Meldungen von sich aus verwirft, siehe auch Test 4).
- Um die Unterdrückung gleicher Meldungen zu umgehen, erfolgt die wiederholte Auslösung frühestens nach 4 Minuten.
- Einen gültigen Alarm auslösen
- Uhrzeit im Alarmgeber um 30 Minuten zurück stellen, erneut auslösen
- Uhrzeit im Alarmgeber um 35 Minuten vor die Empfängerzeit stellen und innerhalb zwei Minuten erneut auslösen

Testbedingung erfüllt bei: einem Endgerät, dass den ersten Alarm richtig und die beiden weiteren Auslösungen entsprechend der Einstellungen jeweils als verfristet kennzeichnet (DME), bzw. bei DSE keine Sirenenansteuerung erfolgt.

6. Test auf minimale Klartextlänge

Klassifizierung: A

Prüfziel: Dieser Test soll überprüfen ob die mindest geforderte Zeichenzahl von 120 Zeichen gesendet, empfangen und dargestellt werden kann.

Testtext: `Dies ist eine Meldung die insgesamt mindestens 120 Klartextzeichen hat um die minimale Klartextlänge über die gesamte Kette zu prüfen`

(Hinweis: Der Text hat 124 Zeichen)

Testbedingung erfüllt bei: einem Endgerät, dass den Text in voller Länge empfangen und dargestellt hat

7. Test Empfängersperrung

Klassifizierung: B

Prüfziel: Dieser Test soll überprüfen ob die Deaktivierung eines Empfängers möglich ist.

Testtext: `SPERR=abcdefghijklmnop`

Weitere Testbedingungen: Nach der erfolgten Sperrung ist die Wirksamkeit mit einer beliebigen Testalarmierung zu überprüfen.

Testbedingung erfüllt bei: einem Endgerät, dass nach Empfang des Sperrwortes keine weiteren Alarme signalisiert.

8. Test Empfängerfreigabe

Klassifizierung: B

Prüfziel: Dieser Test soll überprüfen ob die Aktivierung eines Empfängers möglich ist.

Testtext: `ENTSPERR=ABCDEFGHIKLMNOP`

Weitere Testbedingungen: Nach der erfolgten Entsperrung ist die Wirksamkeit mit einer beliebigen Testalarmierung zu überprüfen.

Testbedingung erfüllt bei: einem Endgerät, dass nach Empfang des Freigabewortes nachfolgende Alarme wieder normal signalisiert. Bei Empfängern, die bei der Sperrung ihre Schlüsselspeicher löschen, genügt die nicht entschlüsselte Darstellung.

9. Einstellung der Zeit

Klassifizierung: A oder C

(C nur wenn die Zeit auch über ein Menü eingestellt werden kann, sonst A)

Testtexte:

1. #ZEIT=0000010114#ZEIT=0000010114
2. #ZEIT=0102030416#ZEIT=0102030416
3. #ZEIT=0507080916#ZEIT=0507080916
4. #ZEIT=0102030416#ZEIT=0102030416
5. #ZEIT=1234290217#ZEIT=1234290217 (kein Schaltjahr)
6. #ZEIT=1234290216#ZEIT=1234290215 (Jahr unterschiedlich)
7. #ZEIT=1234010716 (keine Wiederholung)

Weitere Testbedingungen: Verschlüsselter Versand an einen RIC mit Unteradresse D.

Testbedingung erfüllt bei:

- einem Endgerät, das nach Empfang des zweiten Zeittelegramms die Zeit richtig korrigiert (auf 02:02 Uhr am 03.04.16) und ggf. den Nutzer auf die Zeitabweichung hinweist, die Anzeige erfolgt in der Regel als Winterzeit (+1h)
- einem Endgerät, das nach Empfang des dritten Zeittelegramms die Uhrzeit richtig korrigiert und ggf. den Nutzer auf die Zeitabweichung hinweist, die Anzeige erfolgt in der Regel als Sommerzeit (+2h)
- einem Endgerät, das nach Empfang des vierten Zeittelegramms die Uhrzeit richtig korrigiert und ggf. den Nutzer auf die Zeitabweichung hinweist, die Anzeige erfolgt in der Regel (wieder) als Winterzeit (+1h)
- einem Endgerät, das nach Empfang des fünften bis siebten und ggf. weiterer syntaktisch falscher Zeittelegramme die Zeit als unlogisch bzw. fehlerhaft verwirft.

10. Unvollständiger Empfang von Alarmtexten

Klassifizierung: A

Prüfziel: Dieser Test soll prüfen was der Empfänger einer verschlüsselten Meldung darstellt wenn der Empfang nicht vollständig ist. Erwartet wird, dass zumindest der Anfang des Alarmtextes fehlerfrei signalisiert wird. Die Anwendung der nachfolgenden Beispiele ist nicht verpflichtend. Sie sollen lediglich dazu dienen den Test auch mit einfachen Alarmgebern, die nicht verschlüsseln können, durchzuführen. Der IOP Tester kann auch eigene Konstellationen berechnen. Da die Testtexte bereits verschlüsselt vorgegeben sind, darf sie der Alarmgeber nicht noch einmal verschlüsseln! Laut Spezifikation muss beim Alarmgeber die Verschlüsselung RIC bezogen ein- und ausgeschaltet werden können. Der Beispiel RIC 3003-B ist also ohne Verschlüsselung im DAG zu konfigurieren.

Testtexte:
1. Testsendung unvollständiger Empfang
2. Testsendung unvollständiger ~~Empfang~~
3. Testsendung unvollst~~ändiger Empfang~~

Weitere Testbedingungen:
Die Zeichen in Klammern werden zwar kodiert, der verschlüsselte Text dann aber vor der Aussendung um 10 bzw. 20 Zeichen gekürzt.

1. Vollständiger verschlüsselter Text:

Text verschlüsselt `am 01.04.18 um 00:00 Uhr`
Entsprechend einem IV: `80C6FC07 5D4892AA` sowie mit dem Schlüssel: `4b220ba82db70c7065a2a9dbfa2388869e5f8f7fee56b35bd9920a31c8366621`
(RIC 3003-B der Musterschlüsseldatei)

Ciphertext:

AOjTBwAAAEeD8aWW8tKICHNn3Qxbqk94D9klgM4eQNmAbtvPl/PgDTUFCifpbYx+JQ==

Anzeige: **1. Testsendung unvollständiger Empfang**

2. Gekürzter verschlüsselter Text:

Text verschlüsselt am 01.04.18 um 00:00 Uhr
Entsprechend einem IV: 80C6FC07 00847C8A sowie mit dem Schlüssel: 4b220ba82db70c7065a2a9dbfa2388869e5f8f7fee56b35bd9920a31c8366621

Ciphertext:

gMb8BwCEfIqGXabMbsAZwQuGXLH0RYL6PtgdDUg3PeN/2G3QpqmqsZIv1K~~Hkwn5nEWM=~~

Anzeige: 2. Testsendung unvollständiger

3. Gekürzter verschlüsselter Text:

Text verschlüsselt am 01.04.18 um 00:00 Uhr
Entsprechend einem IV: 80C6FC07 BF6D5314 sowie mit dem Schlüssel: 4b220ba82db70c7065a2a9dbfa2388869e5f8f7fee56b35bd9920a31c8366621

Ciphertext:

gMb8B79tUxQ4nM1hukiL44HMH0np/Ali0JVwoKl6w8WDhLHE~~g6JrEUNub87SKJo7VPU=~~

Anzeige: 3. Testsendung unvolls

Weitere Testbedingungen:

Die drei Testtexte sind zu senden und die Ergebnisse zu protokollieren. Um die Unterdrückung gleicher Alarme zu vermeiden wird das erste Zeichen hoch gezählt. Dadurch ergeben sich gesichert unterschiedliche Kryptotexte.

Testbedingung erfüllt bei:

Bei einem Empfänger der alle drei Aussendungen mindestens entsprechend den Erwartungswerten darstellt. Da das Ende des Ciphertextes willkürlich gewählt ist, sind bei den gekürzten Texten zusätzliche Zeichen zulässig, solange mindestens die obigen Erwartungswerte richtig dargestellt werden.

11. Übermittlung mehrerer kurzer Alarmtexte (Füllzeichen)

Klassifizierung: B

Prüfziel: Dieser Test soll beim Sender die Ergänzung von einer zufälligen Zahl an Füllzeichen sowie deren richtige Verarbeitung im Empfänger überprüfen.

Testtext: `Test`

Hinweis: Der Text soll mindestens fünfmal gesendet werden

Weitere Testbedingungen:

Es muss sichergestellt sein, dass der Sender durch Füllzeichen fünf verschieden lange Kryptotexte produziert.

Testbedingung erfüllt bei:

Bei einem Empfänger der den Text beim ersten Empfang fehlerfrei darstellt und innerhalb der Unterdrückungszeit gleicher Meldungen nicht erneut signalisiert. Beim Sender muss der Geheimtext unterschiedliche Zeichen und Längen aufweisen. Die Vorgabe ist durch parallelen Empfang und Aufzeichnung der verschlüsselten Textdarstellung zu prüfen.

12. Schnelle Textalarmierung mit Index

Klassifizierung: D

Prüfziel: Dieser Test soll die Verarbeitung des Index bei der schnellen Textalarmierung überprüfen. Die richtige Zuordnung von Index zu Schlüssel ist besonders bei verkürztem Schlüsselraum wichtig.

Testtexte:

`1. Schnelle Textalarmierung`	(mit Index 0 = hex 00)
`2. Schnelle Textalarmierung`	(mit Index 77 = hex 4D)
`3. Schnelle Textalarmierung`	(mit Index 255 = hex FF)

Weitere Testbedingungen:

Es muss dokumentiert werden ob das Verfahren vollständig, d.h. mit 256 Schlüsseln, implementiert wurde. Insbesondere sind die Anzahl der Schlüssel, sowie die Art der Zuordnung bei verkürztem Schlüsselraum zu vermerken. Bei einem verkürztem Schlüsselraum ist der Index beim zweiten Testtext ist so zu wählen dass er außerhalb des eigentlichen Schlüsselbereiches liegt und in diesen projiziert wird. Der Beispielindex 77 würde bei einem 128 Schlüssel großen Speicher innerhalb liegen, bei einem 64 großen außerhalb. Im ersten Fall müsste er deshalb z.B. auf 145 angepasst werden.

Testbedingung erfüllt bei:

Bei einem Empfänger der alle drei Texte fehlerfrei darstellt.

Muster IOP Protokoll Nr.

Prüfzeitraum : 00.00.2015 bis 00.00.2016

Prüfort : Testhausen, Fa. Digitalalarm

Prüfer/Prüferin : Frau Testingenieur

: Herr Testmitarbeiter

: Herr Mitarbeiter

Kontaktdaten des verantwortlichen Prüfers (Anschrift / Telefon / Email)

Digitalalarm GmbH, Pocsagstr. 1, 12345 Testhausen

Telefon: 089-123456, testingenieur@digitalalarm.net

Sender / Ort der Verschlüsselung

Einsatzleitsystem Typ x , DAG3 Typ y, Testsender z

Hard- und Softwarestände des Senders (ELS oder DAG)

Server Typ : xy, 4 GB RAM, Windows 7 Ultimate SP1, DotNet V.4.5.2 usw.

Seriennummer Server PC :

Softwarestände des ELS :

Verschlüsselung mit : über Windows DLL V1.0.0….

Hard- und Softwarestände des Übertragungssystems (DAU)

DAU Typ : 4711

Software : V x.y

Hardwarestand : V xx

Seriennummer : 123456

Hard- und Softwarestände des Empfängers

Produktname : Supipager 4711

BOS Prüfnummer : DME II 00/70

Seriennummer :

Softwarestand :

Hardwarestand :

Hard- und Softwarestände zusätzlicher Prüfmittel

Produktname : Testsender 4711

Seriennummer :

Softwarestand :

Produktname : RPC1 Empfänger 4711

Seriennummer :

Softwarestand :

Betriebsmodus

Bei der Empfangseinrichtung handelt es sich um ein Gerät welches nur verschlüsselt / im Mischbetrieb (unzutreffendes streichen). arbeit (Seite 12 BOSKRYPT – Teil 1) .

Allgemeine Testparameter

Da die Empfangsfrequenz keinen Einfluss auf das Prüfergebnis haben darf, kann sie frei gewählt werden. Der HF Sendepegel ist zur Vermeidung von empfangsbedingten Bitfehlern so hoch zu wählen, dass die Mindestempfindlichkeit für DME nach TR BOS von 10 uV/m deutlich überschritten wird (min. Faktor 3). Es muss also sichergestellt sein, dass mit hoher Wahrscheinlichkeit nur die gewollten Fehler auftreten.

Solange nichts anderes angegeben ist, kann als Testschlüssel

0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF

und als RIC `1234568` verwendet werden. Anzeigedarstellungen sind fotografisch zu dokumentieren und in den Ergebnisbericht einzufügen.

Testfrequenz : `173.140 MHz`

Test RIC : `1234568-A`

Zusammenfassung

In allen weißen Feldern muss ein Kreuz sein, in grauen Feldern kann zusätzlich ein Kreuz sein wenn es nicht durch ein „=“ Querstrich gesperrt ist.

	A	B	C	D
Test 1 Zeichensatz		=	=	=
Test 2 Zeichensatz		=	=	=
Test 3 Steuerzeichen CR und LF		=	=	=
Test 4 Erkennung gleicher Meldungen		=	=	=
Test 5 Erkennung verfristeter Alarmierungen			=	=
Test 6 Test auf minimale Klartextlänge		=	=	=
Test 7 Empfängersperrung				=
Test 8 Empfängerfreigabe				=
Test 9 Einstellung der Zeit		=		=
Test 10 Unvollständiger Empfang von Alarmtexten		=	=	=
Test 11 Übermittlung mehrerer kurzer Alarmtexte (mit Füllzeichen)		=	=	=
Test 12 Schnelle Textalarmierung mit Index	=		=	=

Versionshistorie

01.05.18

Beim Test 10 (Unvollständiger Empfang) wurden die Beispiele aktualisiert, die Beschreibung präzisiert sowie weitere Parameter wie Schlüssel ergänzt.

Beim Test 9 wurde der fünfte Test angepasst von 30.02.16 auf 29.02.17

Die Teile Empfängersperrung und Empfängerfreigabe wurden von B auf C herabgestuft.