Verfahren zur Verschlüsselung von Textmeldungen

BOSKRYPT

als Ergänzung zur TR BOS

„Geräte für die digitale Funkalarmierung“

Teil 2 - Schlüsselaustauschverfahren

D. Schlüsselaustauschverfahren

Bei durchschnittlichen DA Systemen kommt es bei Verschlüsselung aller Meldungen zu einer großen Anzahl an Schlüsselwerten. Der manuelle Austausch der Schlüssel zwischen Sender und Empfänger ist mühsam und fehlerträchtig. Die Generierung von sicheren Schlüsseln ist eine weitere Aufgabe, die manuell nur unzureichend durchführbar ist.

Eine einfache Lösung zur Vermeidung vorstehender Probleme ist ein automatischer Schlüsselgenerator. Dieser erstellt eine Datei, die für alle vorkommenden RIC / Unteradressen einen zufälligen Schlüssel enthält. Die Schlüsselgeneratorsoftware ist, da sie nur einmal je DA-Netz benötigt wird, in der Regel eine eigenständige Software. Diese Schlüsseldatei kann von der Programmiersoftware der DA Komponenten eingelesen und im automatischen Verfahren weiter verarbeitet werden. Die Alarmgeber (DAG) lesen die generierten Schlüsselwerte über die in diesem Dokument beschriebene Datei ein.

D1. Aufbau und Nutzung der Datei

Eingesetzt wird zur (herstellerunabhängigen) Schlüsselverteilung eine XML Struktur. Die wesentlichen Daten sind der RIC, die Unteradresse, der zugehörige Schlüssel und ein Kommentar. Für die Daten gelten die unter D2 aufgeführten Randbedingungen:

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.

Die Alarmgeber importieren die relevanten Schlüssel in die eigene Datenbank. Die XML Schlüsseldatei darf nicht unverschlüsselt auf dem Endgerät vorgehalten werden.

D2. Inhalt der XML Datei

- Jede Kombination von RIC / Unteradresse und Cryptoprovider darf nur einmal vorkommen
- Die Werte müssen syntaktisch richtig sein:
    - als Schlüsselzeichen sind nur die Zeichen 0..9, A..F bzw. a..f zulässig
    - als Unteradressen nur A bis D zusätzlich

- E als Kennung für die schnelle Textalarmierung
- N für netzweite Schlüssel anderer Verfahren außerhalb von BOSKRYPT

  - RIC zwischen 1 und 2097152 ohne führende Nullen
    0 bei SubRic N für netzweiten Schlüssel anderer Verfahren
- Die RIC und Unteradressen sollten monoton steigend sein

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 "BOSKRYPT" belegt. Für andere Verfahren können die jeweiligen Hersteller ihre eigene Textkombination definieren. Kombinationen die BOSKRYPT enthalten und ähnliche Schreibweisen sind für herstellereigene Verfahren verboten. Eine abweichende Versionsnummer wird bei späteren Erweiterungen ergänzt um somit eine automatische Unterscheidung zu ermöglichen. Die Versionsnummer ist aufsteigend zu wählen. In herstellereigene Verfahren kann deshalb einfach durch Eintrag einer anderen Zeichenfolge verzweigt werden. Dadurch ist es möglich den Datenaustausch auch in Netzen mit gemischten Kryptierungsverfahren einzusetzen.

Hinweise zum Index bei BOSKRYPT

Bei der Standardalarmierung ist der Schlüsselindex immer auf 0 gesetzt. Es kann für jede Unteradresse eines RIC ein eigener Schlüssel definiert werden. Für die schnelle Textalarmierung stehen die Indexe 0 bis 255 zur Verfügung. Bei der schnellen Textalarmierung werden die Unteradressen zur Zeit nicht benötigt. Um die Verarbeitung zu erleichtern, werden die bis zu 256 Schlüssel der schnellen Textalarmierung mit der Unteradresse „E" codiert.

Beispiel einer Schlüsseldatei aus dem Bereich schnelle Textalarmierung

```
<RicCryptoInfo Address="001008" Cryptoprovider="BOSKRYPT10" Remark="BOSKRYPT Schnelle Textalarmierung">
  <KeyDefinition SubRic="E" Enabled="true" KeyIndex="0"
Key="0A3BADD420C93E845304CA3145D6FC2095AF9E12E8E567BA28CE532A79D33C86" />
  <KeyDefinition SubRic="E" Enabled="true" KeyIndex="1"
Key="15469BC1E1E714E9D0A78836487B8320D20BE26F33F0B5F21EFAFE4D629E55D0" />
  <KeyDefinition SubRic="E" Enabled="true" KeyIndex="2"
Key="21C5722B92FD402CD6790949265C59C9F73958A928523439EFA3A1076C0FB118" />
  <KeyDefinition SubRic="E" Enabled="true" KeyIndex="3"
Key="36883BBB0EE19EB34C2E44503ABC1CACFA22C372FF0B9BAF2E6CD99D3EB0D841" />
  <KeyDefinition SubRic="E" Enabled="true" KeyIndex="4"
Key="40D0E1FF9ADE702C75E062724456D9B4F05577C03D54EEB6E97F99AB3985309D" />
  <KeyDefinition SubRic="E" Enabled="true" KeyIndex="5" Key="5DBE24A33ABC57F8A056D648950C8A46C472E440FD56…..
```

Index, RIC und SubRIC bei anderen (herstellerspezifischen) Verfahren

Bei den herstellerspezifischen Verfahren außerhalb von BOSKRYPT wird der Index als Ordnungszahl der netzweiten Schlüssel verwendet. Als weitere Kennzeichnung wird der RIC auf einen, vom jeweiligen Hersteller definierten, Wert gesetzt. Falls dieser keine Angaben macht wird er auf 0 gesetzt. Als SubRic wird dann „N“ eingetragen.

D.3 Anforderungen an die Schlüssel

Alphanumerische RIC

Die eingesetzte Schlüsseldatei muss für jeden RIC (mit Ausnahme des Text RIC) einen netzweit individuellen Schlüssel haben. Anzustreben ist auch jeder Unteradresse einen eigenen individuellen Schlüssel zuzuweisen.

Schnelle Textalarmierung

Die 256 Schlüssel der schnellen Textalarmierung müssen netzweit verschieden sein. Die Alarmgeber prüfen die Einmaligkeit beim Import der Schlüsseldatei.

Anhang

Beispieldateien: BOSKRYPT_KEY.xml , BOSKRYPT_KEY.xsd