

	DIN EN 50136-1-7 (VDE 0830-5-1-7)	DIN
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	VDE

ICS 13.320

Einsprüche bis 2010-07-31

Entwurf

**Alarmanlagen –
Alarmübertragungsanlagen und -einrichtungen –
Teil 1-7: Anforderungen an standardisierte Protokolle zur Alarmübertragung in
Paketvermittlungsnetzwerken;
Deutsche Fassung prEN 50136-1-7:2010**

Alarm systems –
Alarm transmission systems and equipment –
Part 1-7: Requirements for common protocol for alarm transmission using packet switched network;
German version prEN 50136-1-7:2010

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2010-05-25 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise als Datei per E-Mail an **dke@vde.com** in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter **www.dke.de/stellungnahme** abgerufen werden
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevante Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 95 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Beginn der Gültigkeit

Diese Norm gilt ab ...

Nationales Vorwort

Die Deutsche Fassung des europäischen Dokuments prEN 50136-1-7:2010 „Alarmanlagen – Alarmübertragungsanlagen und -einrichtungen – Teil 1-7: Anforderungen an standardisierte Protokolle zur Alarmübertragung in Paketvermittlungsnetzwerken“ (Entwurf in der Umfrage) ist unverändert in diesen Norm-Entwurf übernommen worden.

Da die Deutsche Fassung noch nicht endgültig mit der Englischen und der Französischen Fassung abgeglichen ist, ist die englische Originalfassung der prEN 50136-1-7:2010 beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Das europäische Dokument prEN 50136-1-7:2010 „Alarm systems – Alarm transmission systems and equipment – Part 1-7: Requirements for common protocol for alarm transmission using packet switched network“ wurde vom TC 79 „Alarmanlagen“ des Europäischen Komitees für Elektrotechnische Normung (CENELEC) erarbeitet und von CENELEC den Nationalen Komitees zur Stellungnahme vorgelegt.

Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Da der Abstimmungszeitraum für einen späteren „Schluss-Entwurf“ prEN nur 2 Monate beträgt und zum „Schluss-Entwurf“ prEN keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine „JA/NEIN“-Entscheidung möglich ist, wobei eine „NEIN“-Entscheidung fundiert begründet werden muss, wird bereits der „Entwurf“ prEN als Deutscher Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit noch vor der formellen Abstimmung berücksichtigen zu können.

Für diesen Norm-Entwurf ist das nationale Arbeitsgremium UK 713.1 „Gefahrenmelde- und Überwachungsanlagen“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (www.dke.de) zuständig.

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe der Norm.

Eine Information über den Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist in Tabelle NA.1 wiedergegeben.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 50136-1-5	—	DIN EN 50136-1-5 (VDE 0830-5-1-5)	VDE 0830-5-1-5
CLC/TS 50136-7	—	DIN CLC/TS 50136-7 (VDE V 0830-5-7)	VDE V 0830-5-7
ETSI TS 100 900 V7.2.0 (1999-07)	—	—	—
ITU-T Rec. X.509	—	—	—

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 50136-1-5 (VDE 0830-5-1-5), *Alarmanlagen – Alarmübertragungsanlagen und -einrichtungen – Teil 1-5: Anforderungen an ein paketvermittelndes Netz (Packet Switched Network PSN)*

DIN CLC/TS 50136-7 (VDE V 0830-5-7), *Alarmanlagen – Alarmübertragungsanlagen und -einrichtungen – Teil 7: Anwendungsregeln*

— **Entwurf** —

E DIN EN 50136-1-7 (VDE 0830-5-1-7):2010-05

– Leerseite –

**Alarmanlagen –
Alarmübertragungsanlagen und -einrichtungen –
Teil 1-7: Anforderungen an standardisierte Protokolle zur Alarmübertragung in
Paketvermittlungsnetzwerken**

Alarm systems –
Alarm transmission systems and
equipment –
Part 1-7: Requirements for common
protocol for alarm transmission using
packet switched network

Dieser Europäische Norm-Entwurf wird den CENELEC-Mitgliedern zur CENELEC-Umfrage vorgelegt.

CENELEC Termin: 2010-09-03.

Er wurde von CLC/TC 79 erstellt.

Wenn aus diesem Norm-Entwurf eine Europäische Norm wird, sind die CENELEC-Mitglieder gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Dieser Europäische Norm-Entwurf wurde von CENELEC in drei offiziellen Fassungen (Deutsch, Englisch, Französisch) erstellt. Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Zentralsekretariat mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, Ungarn, dem Vereinigten Königreich und Zypern.

Warnvermerk: Dieses Schriftstück hat noch nicht den Status einer Europäischen Norm. Es wird zur Prüfung und Stellungnahme vorgelegt. Es kann sich noch ohne Ankündigung ändern und darf nicht als Europäische Norm in Bezug genommen werden.

CENELEC

Europäisches Komitee für Elektrotechnische Normung
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique

Zentralsekretariat: Avenue Marnix 17, B-1000 Brüssel

© 2010 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Projekt: 22700

Ref. Nr. prEN 50136-1-7:2010 D

— Entwurf —

E DIN EN 50136-1-7 (VDE 0830-5-1-7):2010-05
prEN 50136-1-7:2010

Vorwort

Dieser Entwurf einer Europäischen Norm wurde vom Technischen Komitee CENELEC/TC 79 „Alarmanlagen“ ausgearbeitet. Er wird der formellen Abstimmung unterworfen.

Inhalt

	Seite
1 Anwendungsbereich	5
2 Normative Verweisungen	5
3 Begriffe und Abkürzungen	5
3.1 Begriffe	5
3.2 Abkürzungen	5
4 Zweck	6
5 Meldungsübermittlung	6
5.1 Übersicht über die Meldungsformate	7
5.2 Auffüllen und Länge der Meldung	11
5.3 Hash-Verfahren	12
5.4 Verschlüsselung	12
5.5 Timeouts und Neuanfragen	13
5.6 Versionsnummer	13
5.7 Umkehrbefehle	13
5.8 Anfangswerte	14
6 Meldungstypen	14
6.1 Wegüberwachung	14
6.2 Ereignismeldungen	15
6.3 Konfigurationsmeldungen	19
7 Inbetriebnahme und Verbindungsaufbau	27
7.1 Inbetriebnahme	27
7.2 Einrichten der Verbindung	30
Anhang A (normativ) Ergebniscodes	33
Anhang B (normativ) Protokollbezeichner	34
Anhang C (normativ) Shared Secret	35
C.1 Zeichensatz für Verschlüsselung, Formatierung und Entschlüsselung	35
C.2 Prüfsumme für die Verschlüsselung, Formatierung und Entschlüsselung des Shared Secret	38
C.3 Beispiel für die Verschlüsselung, Formatierung und Entschlüsselung des Secret	38
C.4 Beispiel für die Entschlüsselung	39
Anhang D (informativ) Beispiele von Anwendungsprotokollen	40
D.1 Sia	40
D.2 Ademco Contact ID	40
D.3 Scancom Fast Format	41
Anhang E (informativ) Entwurfsgrundsätze	42
E.1 Informationssicherheit	42
E.2 Anwendung der UDP-Signalgebung	42
Literaturhinweise	43
Tabellen	
Tabelle 1 – Bezeichner	7
Tabelle 2 – Grundformat aller unverschlüsselten Meldungen	8
Tabelle 3 – Grundformat aller verschlüsselten Meldungen	8
Tabelle 4 – Übersicht über die Message ID	10
Tabelle 5 – Flags	11
Tabelle 6 – Kennungen für Hash-Verfahren	12
Tabelle 7 – Verschlüsselungskennungen	12

	Seite
Tabelle 8 – Umkehrbefehle	14
Tabelle 9 – Anfangswerte	14
Tabelle 10 – Abfragemeldung SPT $\leftarrow \rightarrow$ RCT	15
Tabelle 11 – Abfrageantwort RCT $\leftarrow \rightarrow$ SPT	15
Tabelle 12 – Format der Ereignismeldung – SPT $\rightarrow$ RCT	16
Tabelle 13 – Format der Ereignismeldung – Felder	16
Tabelle 14 – Ereignisfeld	17
Tabelle 15 – Zeitereignisfeld	17
Tabelle 16 – Zeitmeldungsfeld	17
Tabelle 17 – Verbindungsfeld – IP-Adresse	18
Tabelle 18 – Verbindungsfeld – IP-Portnummer	18
Tabelle 19 – Verbindungsfeld – URL	18
Tabelle 20 – Verbindungsfeld – Dateiname	18
Tabelle 21 – Format der Ereignisantwortmeldung	19
Tabelle 22 – Format der Anforderungsmeldung für den Verbindungsidentifikator	20
Tabelle 23 – Format der Antwortmeldung für den Verbindungsidentifikator	20
Tabelle 24 – Format der Meldung zur Anforderung einer Geräte-ID	20
Tabelle 25 – Flag ‚Master Device ID request‘	21
Tabelle 26 – Format der Meldung der Antwort der Geräte-ID	21
Tabelle 27 – Format der Meldung zur Anforderung der Verschlüsselungsauswahl	21
Tabelle 28 – Flag ‚Master Encryption Selection request‘	22
Tabelle 29 – Format der Antwortmeldung der Verschlüsselungsauswahl	22
Tabelle 30 – Format der Anforderungsmeldung für den Verschlüsselungscodetausch	22
Tabelle 31 – Flag ‚Master Key Request‘	22
Tabelle 32 – Format der Antwortmeldung des Verschlüsselungscodetausches	23
Tabelle 33 – Format der Anforderungsmeldung zur Hashauswahl	23
Tabelle 34 – Format der Antwortmeldung der Hashauswahl	24
Tabelle 35 – Format der Anforderungsmeldung zur Wegüberwachung	24
Tabelle 36 – Format der Antwortmeldung der Wegüberwachung	24
Tabelle 37 – Format der Befehlsmeldung zur Zeiteinstellung	25
Tabelle 38 – Format der Antwortmeldung der Zeiteinstellung	25
Tabelle 39 – Format der transparente Meldung	25
Tabelle 40 – Format der transparente Antwort	25
Tabelle 41 – Format der Meldung zur Anforderung des Datagram-Verschlüsselungsprotokolls	26
Tabelle 42 – Format der Antwortmeldung des Datagram-Verschlüsselungsprotokolls	26
Tabelle 43 – Format der Anforderungsmeldung zur RCT-Parameter	26
Tabelle 44 – Format der Antwort der RCT-Parameter	27
Tabelle 45 – Ablauf der Meldungen während der Inbetriebnahme einer neuen SPT	28
Tabelle 46 – Fluss der Meldungen während des Einrichtens der Verbindung	31
Tabelle A.1 – Ergebniscode	33
Tabelle B.1 – Protokollbezeichner	34
Tabelle C.1 – Zeichensatz	35

1 Anwendungsbereich

Diese Europäische Norm legt ein Protokoll für die Punkt-zu-Punkt-Übertragung von Alarmen und Störungen sowie die Überwachung der Kommunikation zwischen einer Übertragungseinrichtung und einer Empfangszentrale unter Anwendung des Internet-Protokolls (IP) fest.

Dieses Protokoll soll in jedem Netz angewendet werden, welches die Übertragung von IP-Daten unterstützt. Dazu gehören Ethernet, xDSL, GPRS, WiFi, UMTS und WIMAX.

Die System-Leistungsanforderungen an die Alarmübertragung sind in EN 50136-1 und EN 50136-1-5 festgelegt.

Die Leistungsanforderungen der Einrichtungen im überwachten Objekt müssen die Anforderungen der jeweiligen Alarmanlagen-Norm erfüllen und sie müssen für die Übertragung aller Alarmarten anwendbar sein, einschließlich, jedoch nicht beschränkt auf Brand, Einbruch, Zugangskontrolle und Personen-Hilferufe.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

EN 50136-1:201X ¹⁾, *Alarmanlagen – Alarmübertragungsanlagen – Teil 1: Allgemeine Anforderungen an Alarmübertragungsanlagen*

EN 50136-1-5, *Alarmanlagen – Alarmübertragungsanlagen und –einrichtungen – Teil 1-5: Anforderungen an ein paketvermittelndes Netz (Packet Switched Network PSN)*

NIST SP 800-38A, *Recommendation for Block Cipher Modes of Operation – Methods and Techniques*

NIST Special Publication 800-38A, December 2001

Available from <http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf>

RFC793, *Transmission Control Protocol*

Available from <http://www.faqs.org/ftp/rfc/pdf/rfc793.txt.pdf>

RFC958, *Network Time Protocol (NTP)*

Available from <http://www.faqs.org/ftp/rfc/pdf/rfc958.txt.pdf>

RFC4330, *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI*

Available from <http://www.faqs.org/ftp/rfc/pdf/rfc4330.txt.pdf>

SIA DC-03-1990.01 (R2003.10), *DCS SIA Format Standard*

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach EN 50136-1:201X.

3.2 Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Abkürzungen.

AES	hochentwickelter Verschlüsselungsstandard	(en: advanced encryption standard)
ARC	Alarmempfangsstelle	(en: alarm receiving centre)
ATS	Alarmübertragungsanlage	(en: alarm transmission system)

¹⁾ Im Entwurfsstadium.

CA	X.509-Zertifizierungsstelle	(en: X.509 certificate authority)
CBC	Blockchiffrenkettung	(en: cipher block chaining)
CRC	zyklische Redundanzprüfung	(en: cyclic redundancy check)
DNS	Domänen-Namensystem	(en: domain name system)
DTLS	Datagram-Verschlüsselungsprotokoll	(en: datagram transport layer security)
HL	Kopfdatenlänge	(en: header length)
IP	Internet-Protokoll	(en: internet protocol)
IV	Initialisierungsvektor	(en: initialization vector)
MAC	Medienzugriffskontrolle	(en: media access control)
MTU	Maximale Übertragungseinheit	(en: maximum transmission unit)
NAT	Adressenumsetzung für Netze	(en: network address translation)
NIST	National Institute of Standards and Technology	
NTP	Netzwerk-Zeitsynchronisationsprotokoll	(en: network time protocol)
NVM	nichtflüchtiger Speicher	(en: non-volatile memory)
P-MTU	Pfad-MTU	(en: path maximum transmission unit)
RCT	Empfangszentrale	(en: receiver centre transceiver)
RX	Empfangen	(en: receive)
SCTP	verbindungsorientiertes Transportprotokoll	(en: stream control transmission protocol)
SNTP	vereinfachtes Protokoll zur Synchronisierung von Systemzeiten vernetzter Rechner	(en: simple network time protocol)
SPT	Übertragungseinrichtung	(en: supervised premises transceiver)
TFTP	einfaches Dateiübertragungsprotokoll	(en: trivial file transfer protocol)
TX	Senden	(en: transmit)
UDP	Anwender-Datagrammprotokoll	(en: user datagram protocol)
URI	einheitlicher Bezeichner für Ressourcen	(en: uniform resource identifier)
URL	einheitlicher Quellenanzeiger	(en: uniform resource locator)
UTC	koordinierte Weltzeit	(en: coordinated universal time)
WS	Fenstergröße	(en: window size)

4 Zweck

Der Zweck dieser Europäischen Norm ist die Festlegung von Einzelheiten der Protokolle (Transport- und Anwendungsschicht) für Alarmübertragungsanlagen, die das Internet-Protokoll (IP) nutzen, um damit die Fähigkeit zur Zusammenarbeit der von verschiedenen Herstellern gelieferten SPTs und RCTs sicherzustellen. Weiterhin werden die Mechanismen der Inbetriebnahme von SPT und RCT und der Aufbau eines gegenseitigen Vertrauensverhältnisses zwischen den beteiligten Parteien beschrieben.

Unter der Voraussetzung, dass die in EN 50136-1 enthaltenen Anforderungen erfüllt werden, dürfen auch alle weiteren und nicht in dieser Europäischen Norm behandelten Alarmübertragungsprotokolle oder -einrichtungen zum Einsatz kommen.

Dieses Protokoll ist für die Ausführung von UDP konzipiert und unterstützt IPv4 und IPv6.

5 Meldungsübermittlung

In diesem Abschnitt wird die Schicht der Meldungsübermittlung definiert, auf der die Daten des Alarmereignisses mit den vorhandenen Berichtsformaten, wie z. B. Sia und Contact ID, übertragen werden.

In Abschnitt 7 wird die erste Inbetriebnahme einer SPT sowie die Herstellung der Verbindung zwischen SPTs und der RCT festgelegt.

Die Funktionalität des Alarmübermittlungs- und Abfrageprotokolls umfasst:

- Austausch von Haupt- und Sitzungsparametern;
- (Alarm-)Ereignismeldung (einschließlich Verbindung zu ergänzenden Out-of-band-Daten, die mit den Ereignissen in Beziehung stehen, wie Audio/Video);
- Leitungsüberwachung;
- transparente Meldungsübertragung, z. B. verkäuferspezifische Meldungen, die beispielsweise für Fernsteuerbefehle von der RCT zur SPT benutzt werden können.

Sie erfüllen die folgenden Anforderungen:

- Verschlüsselung, erfüllt die Anforderungen der höchsten Sicherheitsklasse nach EN 50136-1;
- Authentifikation, erfüllt die Anforderungen der höchsten Sicherheitsklasse nach EN 50136-1;
- SPT: lässt ein breites Spektrum an Hardware zu (begrenzte Forderungen an Speicherplatzbedarf und CPU-Leistung);
- RCT: unterstützt gleichzeitig bis zu 10 000 SPTs nach EN 50136-1, Klasse D3, unter Anwendung moderner universeller Server-Hardware;
- erlaubt dynamische IP-Adressen der SPTs;
- lässt die Anordnung von einem oder mehr SPTs hinter einer NAT-Firewall zu.

5.1 Übersicht über die Meldungsformate

In diesem Unterabschnitt wird die grundsätzliche Gliederung aller Meldungen beschrieben.

Jede Meldung muss explizit bestätigt werden, einschließlich der Leitungsüberwachungsmeldungen.

Die Abwärtskompatibilität wird durch Implementierung des Ergebniswertes `RESP_CMD_NOT_SUPPORTED` erreicht, den die empfangende Seite als Antwort auf nicht unterstützte Meldungen senden kann.

Mehrbyte-Werte werden in der Netz-Bytereihenfolge übertragen (Big-Endian).

5.1.1 Bezeichner

Die folgenden Bezeichner existieren:

Tabelle 1 – Bezeichner

Beschreibung	Zweck	Vorhanden in	Verschlüsselt	Siehe
Verbindungsidentifikator (Connection Handle)	Suche des aktuellen symmetrischen Verschlüsselungsschlüssels	Alle Meldungen	Nein	5.1.3
Geräte-ID (Device ID)	Eindeutige Identifikation der Hardware	Trägt zu den Hashwerten in allen Meldungen bei	N/A	5.1.4

Der Verbindungsidentifikator ist unverschlüsselt. Es ist eine zufällig gewählte Zahl, die während der Einrichtung der Verbindung initialisiert wird. Ihr alleiniger Zweck besteht darin, nach dem Verschlüsselungscode suchen zu können. Sie ist nur für die Kommunikationssitzung gültig.

Sobald die Verbindung hergestellt ist, identifiziert die Geräte-ID eindeutig die Hardware (dies ist kein Konto-Code). Die RCT muss die Geräte-ID als Index für ihre SPT-Datenbank verwenden. Die Geräte-ID wird bei der Berechnung des Hashwertes für jede Meldung verwendet. In Kombination mit der Verschlüsselung des Hashwertes wird dies für die Substitutionserkennung verwendet.

Die Geräte-ID muss in einem nichtflüchtigen Speicher abgelegt werden.

Die IP-Adresse wird nicht für Identifikationszwecke verwendet, um damit dynamische oder umgesetzte IP-Adressen zuzulassen.

5.1.2 Meldungsformat

Im Folgenden wird das unverschlüsselte Grundformat aller Meldungen beschrieben. In diesem Format wird keine Meldung übertragen. Die Beschreibung in diesem Unterabschnitt dient nur dazu, die Berechnung des Hashwertes zu erklären.

Tabelle 2 – Grundformat aller unverschlüsselten Meldungen

Byte-Index	Bytes	Beschreibung	Siehe	Gruppe
0	4	Verbindungsidentifikator	5.1.3	Kopfdaten
4	16	Geräte-ID	5.1.4	
20	2	Tx Folgenummer	5.1.7	
22	2	Rx Folgenummer	5.1.7	
24	2	Flags	5.1.8	
26	1	Protokollversionsnummer		Meldung
27	1	Meldung-ID	5.1.5	
28	2	Länge der Meldung	5.1.6	
30	n	Daten der Meldung	Abschnitt 6	

Im Folgenden wird das verschlüsselte übertragene Grundformat aller Meldungen beschrieben. Es ist zu beachten, dass das Feld Geräte-ID nicht in der verschlüsselten Meldung enthalten ist, dessen Wert jedoch zur Berechnung des Hashwertes verwendet wird, d. h. der Hashwert wird aus der unverschlüsselten Version der vorstehend beschriebenen Meldung berechnet.

Tabelle 3 – Grundformat aller verschlüsselten Meldungen

Byte-Index	Bytes	Beschreibung	Siehe	Verschlüsselt	Gruppe
0	4	Verbindungsidentifikator	5.1.3	Nein	Kopfdaten
4	2	Tx Folgenummer	5.1.7	Ja	
6	2	Rx Folgenummer	5.1.7	Ja	
8	2	Flags	5.1.8	Ja	
10	1	Protokollversionsnummer		Ja	
11	1	Meldung-ID	5.1.5	Ja	Meldung
12	2	Länge der Meldung	5.1.6	Ja	
14	n	Daten der Meldung	Abschnitt 6	Ja	
14 + n		Füllbytes	5.2.1	Ja	
	32 32	Hash – SHA-256 oder Hash – RIPEMD-256	5.3	Ja	Abschlussdaten

Der Verbindungsidentifikator ist unverschlüsselt; das Übrige der Meldung ist nach dem Verschlüsselungsverfahren verschlüsselt, welches während der Inbetriebnahmephase vereinbart worden ist.

Die Meldung-IDs werden paarweise definiert; jede Meldung hat ihre passende Quittung. Für die Quittungen enthält das erste Datenbyte der Meldung einen „Ergebniscode“, der in Anhang A definiert ist.

In den folgenden Unterabschnitten werden alle Felder ausführlich beschrieben.

5.1.3 Verbindungsidentifikator

Der Verbindungsidentifikator wird (eindeutig für die RCT, an die eine SPT berichtet) mit dem Inbetriebnahmeprotokoll zugewiesen. Die RCT erzeugt einen eindeutigen Verbindungsidentifikator und verbindet ihn in ihrer internen Datenbank mit der Geräte-ID der SPT. Diese Umsetzung ergibt einen kompakten Verbindungsidentifikator mit fester Länge.

Der Zweck des Verbindungsidentifikators besteht darin, den Verschlüsselungscode bestimmen zu können, der – unabhängig von der IP-Adresse der Meldung – für die Entschlüsselung der empfangenen Meldung anzuwenden ist.

Der Verbindungsidentifikator ist kein (vom Errichter/Bediener) konfigurierbarer Parameter, und wird auch nicht an der Nutzerschnittstelle sichtbar gemacht. Sie wird erzeugt und intern nur von den SPT/RCT-Einrichtungen benutzt.

5.1.4 Geräte-ID

Die Geräte-ID dient der eindeutigen Kennzeichnung von SPT und RCT. Sie wird (in Kombination mit der Verschlüsselung) für die Substitutionserkennung verwendet. SPT und RCT können mit diesem Feld die Kennung des verbundenen Beteiligten überprüfen und in dem Fall, das sie verändert ist, einen Substitutionsalarm erzeugen.

Die Geräte-ID selbst wird niemals in den Kopfdaten der Meldung übertragen. Jedoch trägt die Geräte-ID zur Hashberechnung der Meldung bei.

Die Geräte-ID hat eine Länge von 16 Byte.

5.1.4.1 Geräte-ID der SPT

Die Geräte-ID der SPT ist eine ID, die für die SPT zufallsbedingt, jedoch über die Lebensdauer der SPT unveränderlich und schreibgeschützt ist, d. h. eine Hardware-Seriennummer. Sie kommt in der SPT-Datenbank in der RCT nur einmal vor.

Die Geräte-ID wird bei der Herstellung des Gerätes erzeugt; sie wird bei der Meldungsübermittlung nie selbst im Klartext übertragen, muss der ARC aber im Klartext bekannt sein, um die RCT entsprechend zu konfigurieren.

Sie wird folglich nur während der ersten Inbetriebnahmephase an die RCT übertragen.

Die Eindeutigkeit wird durch die folgenden Prinzipien gesichert:

- Jeder Hersteller muss seine aus 24 Bit bestehende „Eindeutige Herstellerkennung“ verwenden, die ihm von der IEEE für die Generierung der MAC-Adresse zugewiesen worden ist.
- Jeder SPT-Hersteller, der keinen derartigen Code besitzt, muss sich an die IEEE zur Bereitstellung eines derartigen Codes wenden.
- Wenn eine Schnittstelle in der SPT eine MAC-Adresse verwendet, müssen die nächsten 24 Bit in der Geräte-ID die gleichen wie der Rest der vom Hersteller festgelegten MAC-Adresse sein. Ist eine derartige Schnittstelle nicht vorhanden, muss der Hersteller ein anderes dokumentiertes Benummerungsschema verwenden.
- Für den Rest des Feldes der Geräte-ID muss der Hersteller nicht aufeinander folgende, zufallsverteilte Zahlen verwenden und für alle von ihm gelieferten SPT-Geräte die Eindeutigkeit zusichern.

5.1.4.2 Geräte-ID der RCT

Die Geräte-ID der RCT ist eine ID, die innerhalb des Empfängers nur einmal vorkommt und sich während der Lebensdauer eines Empfängers niemals verändert. Sie stellt eine Seriennummer des RCT dar, nur dass sie zu Beginn von der ARC eingerichtet werden kann.

Die Geräte-ID der RCT wird der SPT während der Inbetriebnahmephase zur Verfügung gestellt.

5.1.5 Meldung-ID

Die Meldung-IDs, wie sie zum Einsatz kommen, sind in der folgenden Tabelle aufgeführt.

Tabelle 4 – Übersicht über die Message ID

Name der Meldung	Beschreibung	Richtung SPT ← → RCT	Version	Meldung-ID
POLL_MSG	Abfragemeldung	→	1	0x11
EVENT_MSG	Ereignismeldung	→	1	0x30
CONN_HANDLE_REQ	Anforderung des Verbindungsidentifikators	→	1	0x40
DEVICE_ID_REQ	Anforderung der Geräte-ID	→	1	0x41
ENCRYPT_SELECT_REQ	Anforderung der Verschlüsselungsauswahl	→	1	0x42
ENCRYPT_KEY_REQ	Austausch des Verschlüsselungscodes	← →	1	0x43
HASH_SELECT_REQ	Anforderung der Hashauswahl	→	1	0x44
PATH_SUPERVISION_REQ	Anforderung der Wegüberwachung	→	1	0x45
SET_TIME_CMD	Befehl zur Zeiteinstellung	←	1	0x47
PMTU_REQ	Anforderung der P-MTU	→	1	0x60
PMTU_PROBE	Pfad-MTU-Probe	→	1	0x61
DTLS_COMPLETE_REQ	Anforderung des Datagram-Verschlüsselungs-protokolls	→	1	0x62
TRANSPARENT_MSG	Transparente Meldung	← →	1	0x70
POLL_RESP	Abfrageantwort	←	1	0x91
EVENT_RESP	Ereignisantwort	←	1	0xB0
CONN_HANDLE_RESP	Antwort des Verbindungsidentifikators	←	1	0xC0
DEVICE_ID_RESP	Antwort der Geräte-ID	←	1	0xC1
ENCRYPT_SELECT_RESP	Antwort der Verschlüsselungsauswahl	←	1	0xC2
ENCRYPT_KEY_RESP	Antwort des Verschlüsselungscodes	← →	1	0xC3
HASH_SELECT_RESP	Antwort der Hashauswahl	←	1	0xC4
PATH_SUPERVISION_RESP	Antwort der Wegüberwachung	←	1	0xC5
SET_TIME_RESP	Antwort der Zeiteinstellung	→	1	0xC7
PMTU_RESP	Antwort der Pfad-MTU	←	1	0xE0
PMTU_PROBE_RESP	Antwort der Pfad-MTU-Probe	←	1	0xE1
DTLS_COMPLETE_RESP	Antwort des Datagram-Verschlüsselungs-protokolls	←	1	0xE2
TRANSPARENT_RESP	Transparente Antwort	← →	1	0xF0

Die Meldung-ID jeder Antwort ist die gleiche Meldung-ID des entsprechenden Befehls, jedoch mit gesetztem Bit 7.

5.1.6 Länge der Meldung

Dies ist die Länge der Daten der Meldung (außer Meldung-ID und Länge der Meldung). Dieses Feld wird verwendet:

- bei variabler Länge der Meldung (siehe z. B. 6.2.1 und 6.3.15) zur Prüfung des Endes der Daten;
- und um den Anfang eines eingebetteten Umkehrbefehls bestimmen zu können (siehe 5.7).

Bei der Berechnung des Wertes des Feldes Länge der Meldung wird ein mögliches Auffüllen niemals in Betracht gezogen.

5.1.7 Folgenummern

Die Folgenummer wird zur Bestimmung einer fehlenden oder doppelten Meldung verwendet. Beide Enden haben eine Sende-Folgenummer und eine Empfangs-Folgenummer.

Diese beiden Zähler sind an beiden Enden vorhanden (d. h., wir sprechen insgesamt von 4 Zählern), während die RX_Folgenummern für die Realisierung einer „state-full machine“-Implementierung verwendet werden.

Diese Zähler werden für die gleichzeitige Erfüllung von drei Funktionen eingesetzt:

- am Anfang wählen SPT und RCT ihre TX-seqs (Sende-Folgenummer) als eine Zufallszahl und verwenden sie anschließend als ein Datagramm-Zähler, der für jedes gesendete Datagramm um eins inkrementiert wird. Die RX_seqs (Empfangs-Folgenummer) sind die erwarteten nächsten TX_seqs vom anderen Kommunikationsendpunkt. Das heißt: Wenn einer eine „42“ als die letzte TX-seq „sieht“, die von einem Kommunikationspartner kommt, würde er selbst eine „43“ als nächste RX-seq senden. Da das andere Ende dies in der gleichen Weise ausführt, funktionieren TX-seq und RX-seq als ein gegenseitiger Folgesteuermechanismus;
- als Zweites können sie gleichzeitig als ein Rücksendemechanismus funktionieren: wenn einer feststellt, dass einem ein Datagramm fehlt (z. B. weil die ankommende TX-seq den Wert „44“ hat, obwohl eine TX-seq = 43 erwartet wird) oder das eine empfangene Datagramm beschädigt ist (durch Überprüfen des Hashwertes), dann wird das eigene alte und vorher gesendete letzte Datagramm zurückgesendet und die andere Seite wird anhand der alten TX-seq erkennen, dass eine nochmalige Übertragung gewünscht wird;
- dadurch, dass sie zufällig ausgewählt wurden und Teil des verschlüsselten Datenblocks sind, schließen sie alle Replay-Angriffe aus.

Bei jeder Verbindung ist jede Meldung zu bestätigen, bevor die nächste neue (keine nochmalige Übertragung) Meldung übertragen werden kann.

5.1.8 Flags

Die folgenden Flags sind definiert:

Tabelle 5 – Flags

Byte	Bit	Definition
0	0	Umkehrbefehl vorhanden: – Wert 0 = kein Umkehrbefehl enthalten – Wert 1 = Umkehrbefehl enthalten
0	1 ... 7	Reserviert
1	0 ... 7	Reserviert

5.2 Auffüllen und Länge der Meldung

5.2.1 Auffüllen

Das Auffüllen ist aus den beiden folgenden Gründen erforderlich:

- Erzeugen einer Meldungslänge, die ein Vielfaches der Blocklänge des verwendeten Verschlüsselungsalgorithmus ist;
- Erzeugung von Abfrage- und Alarmmeldungen, die ähnlich sind.

Das Auffüllen erfolgt mit Zusatzdaten. Die Füllbytes werden den eigentlichen Daten der Meldung angehängt bis die Gesamtlänge der Meldung eine derjenigen ist, die im nächsten Unterabschnitt festgelegt sind.

5.2.2 Länge der Meldung

Die Längen der Meldungen, die zur Erfüllung der in 5.2.1 angeführten Anforderungen (bei Anwendung einer Blocklänge von 16 Byte oder 32 Byte) verwendet werden, sind ein Kompromiss zwischen der Entstellung von Alarmereignissen und Bandbreitennutzung.

Dies führt zu Längen der Meldungen, die ein Vielfaches von 128 + 4 Byte für den Verbindungsidentifikator sind:

- 132 Bytes (4 Byte Verbindungsidentifikator + 8 × 16 Byte);
- 260 Bytes (4 Byte Verbindungsidentifikator + 16 × 16 Byte);
- usw.

5.3 Hash-Verfahren

Für die Validierung der Meldung werden die folgenden Verfahren unterstützt:

Tabelle 6 – Kennungen für Hash-Verfahren

Hash-Kennung	Beschreibung	Hashgröße in Byte
0	SHA-256	32
1	RIPEMD-256	32

Die RCTs müssen alle Verfahren ausführen können. Es ist jedoch auch möglich, eine RCT so zu konfigurieren, dass sie nicht alle Hash-Verfahren akzeptiert.

Die SPTs müssen mindestens das voreingestellte Verfahren realisieren können, dürfen jedoch auch alle Verfahren ausführen.

Das voreingestellte Verfahren ist 0 (SHA-256), solange bis es ausdrücklich mit den Meldungen aktualisiert wird, die in 6.3.9 und 6.3.10 definiert sind.

Das anzuwendende Hash-Verfahren wird während der Initialisierung der Sitzung mit den in 6.3.9 und 6.3.10 definierten Meldungen vereinbart.

Das wählbare Hash-Verfahren lässt unter Beibehaltung der Abwärtskompatibilität die zukünftige qualitätsmäßige Verbesserung der Sicherheit zu.

Der Hash ist im verschlüsselten Teil der Meldung enthalten.

5.4 Verschlüsselung

5.4.1 Verschlüsselungsverfahren

Mit Ausnahme des Verbindungsidentifikators ist die gesamte Meldung verschlüsselt. Das anzuwendende Verschlüsselungsverfahren ist bei der Inbetriebnahme zu vereinbaren. Die folgenden Verfahren werden unterstützt:

Tabelle 7 – Verschlüsselungskennungen

Verschlüsselungskennungen	Beschreibung
0	Unverschlüsselt Darf nur für Zwecke der Fehlersuche oder in Testumgebungen verwendet werden.
1	AES-128
2	AES-256

Die RCTs müssen alle Verfahren ausführen können. Die SPTs müssen mindestens das voreingestellte Verfahren realisieren können, dürfen jedoch auch alle Verfahren ausführen. Das voreingestellte Verfahren ist 1 (AES-128), solange bis es ausdrücklich mit den Meldungen aktualisiert wird, die in 6.3.5 und 6.3.6 definiert sind.

Der Verschlüsselungscode ist nur für eine Verbindung zwischen SPT und RCT gültig, z. B. muss die RCT die Übersicht über alle unterschiedlichen Schlüssel behalten, die von den angeschlossenen SPTs benutzt werden.

Die bei AES anzuwendende Betriebsart ist CBC (Blockchiffrenkettung), wie sie in der NIST-Sonderpublikation 800-38A (Ausgabe 2001) festgelegt ist. Der IV (Initialisierungsvektor) besteht nur aus Nullen.

Das wählbare Verschlüsselungsverfahren lässt unter Beibehaltung der Abwärtskompatibilität die zukünftige qualitätsmäßige Verbesserung der Sicherheit zu.

Der alleinige Zweck der unverschlüsselten Betriebsart ist die Vereinfachung der Realisierung (die Schicht der Meldungsübermittlung kann ohne vorhandene Verschlüsselung realisiert werden, und wenn diese erst einmal hergestellt ist, kann die Verschlüsselung mit hinzugenommen werden).

5.4.2 Austausch des Schlüssels

Die Lebensdauer eines Schlüssels wird durch die Anzahl der übertragenen Pakete bestimmt. Für die Sicherstellung der Sicherheit werden Aktualisierungen des Schlüssels regelmäßig von der RCT nach jeweils N erfolgreich übermittelten Paketen ausgelöst (als Bezugswert wird der Folgezähler der RCT verwendet), dabei ist N ein Wert, der von der RCT während der ersten Inbetriebnahmephase an die SPT gesendet wird.

Zur Durchsetzung der Sicherheit ist ein Austausch des Schlüssels von der RCT mindestens einmal wöchentlich auszulösen oder nach mindestens $2^{16} = 65\,536$ erfolgreichen Paketen (der zuerst auftretende Wert gilt).

Zusätzlich zu diesem regelmäßigen Muster können RCT und SPT zusätzliche Austausche des Schlüssels in Anspruch nehmen.

Um zu vermeiden, dass die Synchronisation zwischen RCT und SPT verloren geht, wenn eine Alarmmeldung exakt während einer laufenden Sitzung des Schlüsselaustausches ausgelöst wird, muss die RCT den alten Sitzungsschlüssel behalten, bis die erste erfolgreiche Übertragung eines Paketes mit dem neuen Sitzungsschlüssel bestätigt worden ist.

5.5 Timeouts und Neuanfragen

Die Timeouts (Zeitsperren) (nach denen eine Meldung neu angefragt wird) werden sich mit jeder Neuanfrage vergrößern, wie es in RFC793 festgelegt ist.

Zusätzlich zu RFC793 ist der sich ergebende Wert der Zeitsperre begrenzt durch einen absoluten Maximalwert von 100 s plus/minus eines gleichmäßig zufällig verteilten Zeitversatzes von 10 %.

ANMERKUNG RFC793 definiert einen Lernalgorithmus, der sich an die verfügbare Kapazität des Netzes anzupassen versucht. Dazu versucht er einen besten Schätzwert der Rundreiseverzögerungszeit zu berechnen, die aus 90 % des vorigen verwendeten Timeout-Wertes plus 10 % der Rundreiseverzögerungszeit des letzten Paketes besteht.

Es wird die Absicht verfolgt, sich an den Überlastzustand des Netzes anzunähern: je mehr das Netz überlastet wird, desto stärker steigt der Timeout-Wert an, und es wird versucht ein Überschwemmen des RCT im Falle der Netzüberlastung zu vermeiden.

Zur Vermeidung einer zu langen Verzögerung einer Neuanfrage ist dieses Prinzip nach unten durch einen maximalen Timeout-Wert begrenzt.

Besonders im Fall einer Erfindung, die noch an allen SPT dazu führen würde, ein paralleles wiederholtes Senden an ihre RCT zu versuchen, wird die obere Grenze von 100 s durch eine gleichmäßig verteilte Zufallskomponente verändert.

Die Zufallszahlenkomponente muss auf einem Zufallszahlengenerator beruhen, der zufällig verteilte Ausgangsgrößen von allen SPT sichert, selbst wenn sie den Wert zum selben Zeitpunkt generieren, z. B. durch Aufnahme der Geräte-ID der SPT in die Berechnung der Zufallszahl.

5.6 Versionsnummer

Die Versionsnummer in den Kopfdaten der Meldung ist ein vorzeichenloser numerischer Bytewert, der die Version des gegenwärtig benutzten Protokolls angibt.

Sie wird standardmäßig auf „1“ gesetzt und stellt die erste Version dieser Protokollimplementation dar. SPT und RCT müssen sich während der Inbetriebnahmephase gegenseitig auf das anzuwendende Protokoll einigen. Die RCT kann so konfiguriert sein, dass sie eine festgelegte Reihe von Protokollversionen fordert und die Kommunikation mit anderen Versionen verweigert.

5.7 Umkehrbefehle

Um es einer RCT zu ermöglichen, Befehle an eine SPT zu senden, ohne von den Eigenschaften der dazwischen liegenden Netzwerkumgebung abhängig zu sein (z. B. alle umlenkenden oder übernommenen Firewall-Regeln, besonders auf der Seite der Netzwerkumgebung der SPT), wird ein Mechanismus für das Einpacken von Umkehrbefehlen in Antwortmeldungen realisiert.

Der gewählte Ansatz besteht darin, einen eingebetteten Umkehrbefehl der Antwortmeldung zusätzlich aufzuladen („Huckepack“). Dies wird durch ein Flag in den Kopfdaten der Antwortmeldung angegeben (siehe 5.1.8).

Die Meldungs-ID und die Daten der Meldung werden der Meldung wie folgt hinzugefügt:

Tabelle 8 – Umkehrbefehle

Byte-Index	Byte	Beschreibung	Was
0	HL	Kopfdaten, „Umkehrbefehl“-Flag auf 1 gesetzt	Kopfdaten
HL	1	Meldung-ID	Antwortmeldung
HL + 1	2	Meldung Länge der Antwortdaten	
HL + 3	n	Daten der Antwortmeldung	
HL + 3 + n	1	Meldung-ID	Eingebettete Umkehrbefehl-Meldung
HL + 4 + n	2	Meldung Länge des Umkehrbefehls	
HL + 6 + n	m	Daten des Umkehrbefehls	
HL + 6 + n + m		Auffüllen	Abschlussdaten
		Hash	

Die Länge der Meldung muss innerhalb der Antwortmeldung liegen, die zur Bestimmung der Anfangsposition der Meldung des eingebetteten Umkehrbefehls verwendet wird.

Es ist für eine RCT immer noch möglich, Befehle asynchron (ohne warten auf eine zyklische Abfrage) zu senden, jedoch wird der Befehl die SPT in Abhängigkeit von der Netzwerkumgebung möglicherweise nicht erreichen.

5.8 Anfangswerte

für das Protokoll werden die folgenden Werte verwendet, bis die Variablen durch die entsprechenden Konfigurationsmeldungen ausdrücklich gesetzt werden.

Tabelle 9 – Anfangswerte

Was	Wert	Beschreibung
Verbindungsidentifikator	0	Noch nicht gesetzt
Hash	0	SHA-256
Verschlüsselungs-ID	1	AES-128
Heartbeat-Intervallzeit	0	Keine zyklische Abfrage
Sendefolgezähler	Zufällig	
Empfangsfolgezähler	0	Bisher kein Paket empfangen

6 Meldungstypen

In diesem Abschnitt werden die Meldungen definiert, wie sie in diesem Protokoll verwendet werden. Es ist zu beachten, dass die Beispiele nur die Daten der Meldungen aufzeigen; Kopfdaten, Meldung-ID und Länge der Meldung werden in den Übersichten über Meldungen nicht dargestellt.

6.1 Wegüberwachung

In diesem Unterabschnitt wird das Format der Abfragemeldung und ihrer Antwort beschrieben. Die Vereinbarung der Abfragerate erfolgt während der Inbetriebnahme mit einer Konfigurationsmeldung. Diese Konfigurationsmeldung ist in 6.3.11 beschrieben. Die zyklische Abfragemeldung selbst enthält nicht das Heartbeat-Zeitintervall (Kontrollsignal-Zeitintervall).

Die Wegüberwachung arbeitet auf dem Heartbeat-Verkehr von der SPT zur RCT.

Jede weitere Meldung kann bedingungslos als Abfragemeldung arbeiten, z. B. kann das abfragende Gerät seinen Zeitgeber „Abfrageintervall“ bei Aussendung einer Meldung zurücksetzen und das Abfrageüberwachungsgerät kann seinen Zeitgeber „Timeout“ bei Empfang einer gültigen Meldung vom anderen Ende zurücksetzen.

6.1.1 Abfragemeldung

Die Abfragemeldung hat das folgende Format:

SPT ← → RCT

Tabelle 10 – Abfragemeldung SPT ← → RCT

Byte-Index	Bytes	Beschreibung
0	HL	Kopfdaten, Meldung-ID und Länge der Meldung
HL		Auffüllen
		Hash

Diese Meldung wird vom abfragenden Gerät in dem Fall gesendet, wenn keine Meldungen für die Heartbeat-Intervallzeit gesendet wurden, wie es mit den Anforderungs-/Antwortmeldungen der Wegüberwachung (6.3.11/6.3.12) während des Einrichtens der Verbindung vereinbart worden ist.

6.1.2 Abfrageantwort

Die Abfrageantwort-Meldung hat das folgende Format:

RCT ← → SPT

Tabelle 11 – Abfrageantwort RCT ← → SPT

Byte-Index	Bytes	Beschreibung
0	HL	Kopfdaten, Meldung-ID und Länge der Meldung
HL	1	Ergebniscode ^{a)}
		Auffüllen
		Hash
^{a)} Der Ergebniscode kann sein: RESP_ACKNOWLEDGE RESP_POLL_REESTABLISH_CONNECTION		

6.2 Ereignismeldungen

6.2.1 Format der Ereignismeldung

Die (Alarm-)Ereignismeldung muss stets die eigentlichen Ereignisdaten enthalten. Neben dieser vorgeschriebenen Information enthält das Protokoll die Möglichkeit, zusätzliche Informationen zu übertragen. Damit der Zusammenhang zwischen den Ereignis- und Zusatzdaten erhalten bleibt, werden die Daten gemeinsam in einer Meldung übertragen.

Zu diesem Zweck wird die Ereignismeldung in fünf Felder aufgeteilt, zu denen jeweils die eigene Längenkennung gehört.

Begründung:

- Felder, wie „Verbindung“ sind von variabler Länge, deshalb die „Längen“-Bytes;
- für die Beibehaltung eines einheitlichen Formates wird keine Unterscheidung zwischen variablen und festen Längengeldern vorgenommen.

Die Alarmereignismeldung hat das folgende Format:

SPT → RCT

Tabelle 12 – Format der Ereignismeldung – SPT → RCT

Byte-Index	Bytes	Beschreibung
0	HL	Kopfdaten, Meldung-ID und Länge der Meldung
HL	1	Bezeichner des Feldes
HL + 1	2	Länge des Feldes (L1)
HL + 3	L1	Daten des Feldes
HL + 3 + L1	1	2. Bezeichner des Feldes (freigestellt)
HL + 4 + L1	2	2. Länge des Feldes (L2) (freigestellt)
HL + 6 + L1	L2	2. Daten des Feldes (freigestellt) ... usw.
HL + 6 + L1 + L2		Auffüllen
		Hash

Die Länge des Feldes (L1, L2 ...) ist die Länge der Daten des Feldes (außer den Bytes für Bezeichner des Feldes und Länge des Feldes).

Die folgenden Felder sind definiert:

Tabelle 13 – Format der Ereignismeldung – Felder

Feldnummer	Beschreibung
0x00	Ereignisfeld
0x01	Zeitereignisfeld
0x02	Zeitmeldungsfeld
0x80	Verbindungsfeld: IP-Adresse
0x81	Verbindungsfeld: IP-Port
0x82	Verbindungsfeld: URL
0x83	Verbindungsfeld: Dateiname

Feldnummern über 0x80 stellen eine Verbindung zu ergänzenden Out-of-band-Informationen bereit, wie beispielsweise

- Bilder, die das Ereignis begleiten (IP-Adresse und -Portnummer, Dateiname);
- Audio- oder Videodatenstrom,

die über einen Sekundärkanal übertragen werden. Es ist zu beachten, dass die Zeitfelder auch dazu benutzt werden können, um den Ereignissen die begleitenden Daten zuzuordnen.

Diese Felder werden in den nächsten Unterabschnitten erläutert.

6.2.1.1 Ereignisfeld

SPT: Vorgeschrieben

RCT: Vorgeschrieben

Tabelle 14 – Ereignisfeld

Relativer Byte-Index	Bytes	Beschreibung
0	1	Protokollbezeichner (siehe Anhang B zur Festlegung und Aufbau der Meldung)
1	L	Ereignisdaten, z. B.: <SIA Account Block><SIA Event Block><SIA ASCII Block>

6.2.1.2 Zeitereignisfeld

SPT: Freigestellt

RCT: Vorgeschrieben

Tabelle 15 – Zeitereignisfeld

Relativer Byte-Index	Bytes	Beschreibung
0	8	Zeitformat nach RFC958 (NTP) / RFC4330 (SNTP V4)

Dieses Feld enthält den Zeitstempel, an dem das Ereignis aufgetreten ist.

Das Zeitformat ist eine 64-Bit-Zahl, wie sie in RFC958 (NTP) / RFC4330 (SNTP V4) beschrieben wird, die eine einfache lokale Synchronisation zulässt. Es ist zu beachten, dass NTP grundsätzlich einen 32-Bit-Zähler für Sekunden seit dem 1. Januar 1900 verwendet, so dass ein Zählerumlauf im Jahr 2036 auftreten wird. Aufgrund der „136-Jahre-Präzision“ genügt für die Abschätzung das korrekte Datum (entweder 1900, 2036, 2172 usw.) für die Wiedersynchronisierung für die nächsten 136 Jahre. Dies sollte mit den Geräten leicht auszuführen sein, muss jedoch bei der Übereinstimmungsprüfung mit einer besonderen Prüfung berücksichtigt werden.

Dieser Ansatz ist unabhängig von Gebieten mit Sommerzeitregelungen und unabhängig von den Zeitzonen, weil NTP die auf UTC beruhende Zeit angibt, so dass länderübergreifende Berechnungen einfacher werden. Derartige lokale Zeitanpassungen in Bezug auf die UTC (z. B. Zeitanzeige/Zeiteingabe in einem vom Menschen lesbaren Format) werden damit den Endgeräten überlassen.

6.2.1.3 Zeitmeldungsfeld

SPT: Freigestellt

RCT: Vorgeschrieben

Tabelle 16 – Zeitmeldungsfeld

Relativer Byte-Index	Bytes	Beschreibung
0	8	Zeitformat nach RFC958 (NTP) / RFC4330 (SNTP V4)

Dieses Feld enthält den Zeitstempel, an dem die Ereignismeldung von der SPT übertragen wird.

Dieser Wert ist für die Lebensdauerprüfung der Datagramme zu verwenden, z. B. Stärken des Protokolls gegen Angreifer in dem Sinne, das ein Datagramm nur dann als gültig akzeptiert wird, wenn es innerhalb einer angemessenen Dauer (z. B. 51 h) am Ende des Kommunikationspartners eintrifft.

Weiterhin gibt die Differenz der Werte von Zeitereignis und Zeitmeldung Anlass zur Überprüfung, ob die Alarmanlage die maximalen Rundreiseverzögerungszeiten erfüllt.

6.2.1.4 Verbindungsfeld – IP-Adresse

SPT: Freigestellt

RCT: Freigestellt

Tabelle 17 – Verbindungsfeld – IP-Adresse

Relativer Byte-Index	Bytes	Beschreibung
0	L	IP-Adresse: L = 4 → IPv4-Adresse L = 32 → IPv6-Adresse

Dieses Feld definiert die IP-Adresse, an die die ergänzende Information gesendet wird.

6.2.1.5 Verbindungsfeld – IP-Portnummer

SPT: Freigestellt

RCT: Freigestellt

Tabelle 18 – Verbindungsfeld – IP-Portnummer

Relativer Byte-Index	Bytes	Beschreibung
0	2	Portnummer

Dieses Feld definiert die Portnummer, an die die ergänzende Information gesendet wird.

6.2.1.6 Verbindungsfeld – URL

SPT: Freigestellt

RCT: Freigestellt

Tabelle 19 – Verbindungsfeld – URL

Relativer Byte-Index	Bytes	Beschreibung
0	L	URL

Dieses Feld definiert die URL, an die die ergänzende Information gesendet wird.

6.2.1.7 Verbindungsfeld – Dateiname

SPT: Freigestellt

RCT: Freigestellt

Tabelle 20 – Verbindungsfeld – Dateiname

Relativer Byte-Index	Bytes	Beschreibung
0	L	Dateiname

Der Dateiname kann beispielsweise dazu verwendet werden, um die Dateien anzugeben, die auf einen TFTP-Server hochgeladen werden können.

6.2.2 Format der Ereignisantwort

Die Ereignisantwortmeldung hat das folgenden Format:

RCT → SPT

Tabelle 21 – Format der Ereignisantwortmeldung

Byte-Index	Bytes	Beschreibung
0	HL	Kopfdaten, Meldung-ID und Länge der Meldung
HL	1	Ergebniscode ^{a)}
HL + 1		Auffüllen
		Hash
^{a)} Der Ergebniscode kann sein: RESP_ACKNOWLEDGE RESP_NEGATIVE_ACKNOWLEDGE RESP_EVENT_RCT_COULD_NOT_PROCESS_MESSAGE RESP_EVENT_PROTOCOL_ID_NOT_SUPPORTED RESP_EVENT_ACKNOWLEDGE_UNKNOWN_FIELD		

Für den Fall, dass die SPT freigestellte Felder in der Ereignismeldung enthält, die nicht von der RCT unterstützt werden, wird das Ereignis noch quittiert, jedoch mit einem RESP_ACKNOWLEDGE_UNKNOWN_FIELD. Dies ist eine gültige Bestätigung und es ist nicht notwendig, das Ereignis noch einmal zu senden.

6.3 Konfigurationsmeldungen

In diesem Unterabschnitt werden die Inhalte der Konfigurationsmeldungen beschrieben. Hinsichtlich des Meldungsflusses und weiterer Erläuterungen siehe Abschnitt 7.

Die Konfigurationsmeldungen werden für die beiden Inbetriebnahmeverfahren (DLTS und Out-of-band) verwendet, weil die Meldungsprotokolle die gleichen Parameter benötigen, unabhängig davon, wie die Verbindung hergestellt worden ist.

Die meisten konfigurierbaren Parameter kommen in der SPT für jede RCT, an die sie meldet, nur einmal vor, z. B.:

- Verbindungsidentifikator;
- Geräte-ID;
- Verschlüsselungsauswahl;
- Sitzungsschlüssel;
- Hash;
- Wegüberwachung.

Für den Fall, dass die SPT an zwei RCT meldet, gibt es für jeden Parameter zwei Instanzen, und zwar eine für jede verbundene RCT.

Wenn sich in der SPT die Parameter der RCT verändern (z. B. Wechsel zu einer anderen RCT), mit der sie zu verbinden ist, muss die SPT neue Parameter anfordern.

Weitere Parameter (z. B. Zeit) sind nur ein Wert, der von der SPT für alle RCT verwendet wird, an die sie meldet.

6.3.1 Anforderung des Verbindungsidentifikators

Die Anforderungsmeldung für den Verbindungsidentifikator hat das folgende Format:

SPT → RCT

Tabelle 22 – Format der Anforderungsmeldung für den Verbindungsidentifikator

Byte-Index	Bytes	Beschreibung
0	HL	Kopfdaten, Meldung-ID und Länge der Meldung
HL		Auffüllen
		Hash

Diese Meldung wird von der SPT zur Anforderung eines Verbindungsidentifikators ausgegeben, der eine Zufallszahl ist. Die Verbindungskennung wird anstelle von der SPT von der RCT erzeugt, weil sie bei der RCT nur einmal vorkommen darf und der Zufallsgenerator der RCT üblicherweise eine bessere Qualität als einer der SPTs besitzt. SPT und RCT verwenden denselben Verbindungsidentifikator.

Für den Fall, dass die Verbindung unterbrochen ist, wird die nächste Sitzung einen neu erzeugten (anderen) Verbindungsidentifikator haben.

6.3.2 Antwort des Verbindungsidentifikators

Die Antwortmeldung für den Verbindungsidentifikator hat das folgende Format:

RCT → SPT

Tabelle 23 – Format der Antwortmeldung für den Verbindungsidentifikator

Byte-Index	Bytes	Beschreibung
0	HL	Kopfdaten, Meldung-ID und Länge der Meldung
HL	1	Ergebniscode
HL + 1	2	Verbindungsidentifikator
HL + 2		Auffüllen
		Hash

Diese Meldung selbst und die vorigen Meldungen haben einen Verbindungsidentifikator mit dem Wert 0. Die nächste Meldung wird die erste mit einem gültigen Verbindungsidentifikator-Feld sein.

6.3.3 Anforderung der Geräte-ID

Die Meldung zur Anforderung einer Geräte-ID hat das folgende Format:

SPT → RCT

Tabelle 24 – Format der Meldung zur Anforderung einer Geräte-ID

Byte-Index	Bytes	Beschreibung
0	HL	Kopfdaten, Meldung-ID und Länge der Meldung
HL	1	Flags
HL + 1	16	Geräte-ID
HL + 17		Auffüllen
		Hash

Diese Meldung wird von der SPT ausgegeben, um eine Geräte-ID anzufordern, die eine Zufallszahl ist. Die Geräte-ID wird von der RCT anstelle der SPT erzeugt, weil sie an der RCT nur einmal vorkommen darf und weil der Zufallszahlengenerator der RCT üblicherweise eine bessere Qualität als der einer SPT besitzt. SPT und RCT verwenden die gleiche Geräte-ID.

Das Folgende gilt, um die Inbetriebnahme des 2. Kanals zu ermöglichen:

- wenn das Flag Master Device ID request gesetzt ist, fordert die SPT nur einmal eine neue Geräte_ID an und speichert diese neue Geräte-ID, wie sie sie empfangen hat, in der Antwortmeldung im NVM. Diese Geräte-ID wird auch von der RCT gespeichert;
- wenn das Flag Master Device ID request gelöscht wird und das Feld Geräte-ID nicht den Wert 0 hat, dann hat die SPT bereits eine Master Device ID und informiert die RCT darüber. Die RCT wird in ihrer Antwort die gleiche Geräte-ID zurückgeben.

Anderenfalls wird das Flag Master Device ID request gelöscht und das Feld Geräte-ID hat den Wert 0.

Flags:

Tabelle 25 – Flag ‚Master Device ID request‘

Bit	Beschreibung
0	Master Device ID request
1	0: SPT-Geräte-ID 1: RCT-Geräte-ID
2 ... 7	Nicht verwendet

6.3.4 Antwort der Geräte-ID

Die Meldung der Antwort der Geräte-ID hat das folgende Format:

RCT → SPT

Tabelle 26 – Format der Meldung der Antwort der Geräte-ID

Byte-Index	Bytes	Beschreibung
0	HL	Kopfdaten, Meldung-ID und Länge der Meldung
HL	1	Ergebniscode
HL + 1	1	Flags
HL + 2	16	Geräte-ID
HL + 18		Auffüllen
		Hash

Die nächste Meldung wird die erste sein, die in den Kopfdaten der Meldung ein gültiges Feld Geräte-ID hat.

Die Geräte-ID in den Kopfdaten dieser Meldung selbst und den vorhergehenden Meldungen sind:

- 0 im Falls von DTLS;
- die ID des „One-Time-Pad“ / Einrichten des 2. Kanals.

Die Flag-Felder behalten den Wert 0.

6.3.5 Anforderung der Verschlüsselungsauswahl

Die Meldung zur Anforderung der Verschlüsselungsauswahl hat das folgende Format:

SPT → RCT

Tabelle 27 – Format der Meldung zur Anforderung der Verschlüsselungsauswahl

Byte-Index	Bytes	Beschreibung
0	HL	Kopfdaten, Meldung-ID und Länge der Meldung
HL	1	Flags
HL + 1	1	Verschlüsselung 1
HL + 2	1	Verschlüsselung 2 (freigestellt) ... usw.
		Auffüllen
		Hash

Diese Meldung wird während der Inbetriebnahme von der SPT ausgegeben, um die von ihr unterstützten Verschlüsselungsverfahren anzugeben. Zu möglichen Verschlüsselungsverfahren siehe 5.4.

Flags:

Tabelle 28 – Flag ‚Master Encryption Selection request‘

Bit	Beschreibung
0	Master Encryption Selection request
1 ... 7	Nicht verwendet

6.3.6 Antwort der Verschlüsselungsauswahl

Die Antwortmeldung der Verschlüsselungsauswahl hat das folgende Format:

RCT → SPT

Tabelle 29 – Format der Antwortmeldung der Verschlüsselungsauswahl

Byte-Index	Bytes	Beschreibung
0	HL	Kopfdaten, Meldung-ID und Länge der Meldung
HL	1	Flags
HL + 1	1	Ergebniscode
HL + 2	1	Anzuwendendes Verschlüsselungsverfahren
HL + 3		Auffüllen
		Hash

Die Flag-Felder behalten den Wert 0.

6.3.7 Anforderung des Verschlüsselungscodetausches

Die Anforderungsmeldung für den Verschlüsselungscodetausch hat das folgende Format:

SPT ← → RCT

Tabelle 30 – Format der Anforderungsmeldung für den Verschlüsselungscodetausch

Byte-Index	Bytes	Beschreibung
0	HL	Kopfdaten, Meldung-ID und Länge der Meldung
HL	1	Flags
HL + 1	L	Verschlüsselungscode (üblicherweise 256 Bit → 32 Byte)
HL + 1 + L		Auffüllen
		Hash

Flags:

Tabelle 31 – Flag ‚Master Key Request‘

Bit	Beschreibung
0	Key Request (SPT) / Key Push (RCT)
1	Master Key Request
2 ... 7	Nicht verwendet

Diese Meldung wird ausgegeben, um eine Aktualisierung des Verschlüsselungscodes anzufordern. SPT und RCT können beide eine Aktualisierung der Verschlüsselungscodes anfordern, wobei in diesem Fall das Flag Master Key Request gesetzt wird. Wenn dieses Flag gesetzt ist, behält der Verschlüsselungscode den gegenwärtig benutzten Schlüssel.

Die SPT fordert einen neuen Schlüssel von der RCT an. Der neue Schlüssel muss von der RCT anstelle der SPT erzeugt werden, weil er von einem kryptografisch exakten Zufallszahlengenerator erzeugt werden muss, und der Zufallszahlengenerator der RCT besitzt üblicherweise eine bessere Qualität als der von einer der SPTs.

Die RCT kann einen neuen Sitzungsschlüssel durch Setzen des Flags Key Request bei der SPT einspeichern. Der neue Schlüssel ist das Feld Encryption key. Die SPT wird anschließend diesen Schlüssel bestätigen, indem sie diesen Schlüssel in der Antwortmeldung des Verschlüsselungscodetausches zurückgibt.

6.3.8 Antwort des Verschlüsselungscodetausches

Die Antwortmeldung des Verschlüsselungscodetausches hat das folgende Format:

SPT ← → RCT

Tabelle 32 – Format der Antwortmeldung des Verschlüsselungscodetausches

Byte-Index	Bytes	Beschreibung
0	HL	Kopfdaten, Meldung-ID und Länge der Meldung
HL	1	Ergebniscode
HL + 1	1	Flags
HL + 2	L	Verschlüsselungscode (üblicherweise 256 Bit → 32 Byte)
HL + 2 + L		Auffüllen
		Hash

Der neue Schlüssel wird unmittelbar wirksam, so wird z. B. die nächste Meldung mit dem neuen Schlüssel verschlüsselt (für den Fall, dass der Wert von Verschlüsselungsauswahl > 0 ist). Zur Überwindung von Übermittlungsfehlern muss die RCT den vorigen Schlüssel noch als Reserve behalten, bis eine nächste Meldung erfolgreich empfangen worden ist.

6.3.9 Anforderung zur Hashauswahl

Die Anforderungsmeldung zur Hashauswahl hat das folgende Format:

SPT → RCT

Tabelle 33 – Format der Anforderungsmeldung zur Hashauswahl

Byte-Index	Bytes	Beschreibung
0	HL	Kopfdaten, Meldung-ID und Länge der Meldung
HL	1	Hash 1
HL + 1	1	Hash 2 (freigestellt) ... usw.
		Auffüllen
		Hash

Diese Meldung wird während der Inbetriebnahme von der SPT ausgegeben, um die von ihr unterstützten Hashes anzugeben. Zu möglichen Hashfunktionen siehe 5.3.

6.3.10 Antwort der Hashauswahl

Die Antwortmeldung der Hashauswahl hat das folgende Format:

RCT → SPT

Tabelle 34 – Format der Antwortmeldung der Hashauswahl

Byte-Index	Bytes	Beschreibung
0	HL	Kopfdaten, Meldung-ID und Länge der Meldung
HL	1	Ergebniscode
HL + 1	1	Anzuwendender Hash
HL + 2		Auffüllen
		Hash

Dies ist die erste Meldung, die einen neu gesetzten Hash verwendet. Standardmäßig (nach dem Neustart) wird die Internet-Prüfsumme (Wert 1) als Hash verwendet.

6.3.11 Anforderung zur Wegüberwachung

Die Anforderungsmeldung zur Wegüberwachung hat das folgende Format:

SPT → RCT

Tabelle 35 – Format der Anforderungsmeldung zur Wegüberwachung

Byte-Index	Bytes	Beschreibung
0	HL	Kopfdaten, Meldung-ID und Länge der Meldung
HL	4	Heartbeat-Intervallzeit (Sekunden)
HL + 4	1	Push (0) oder Pull (1)
HL + 5		Auffüllen
		Hash

Die Heartbeat-Intervallzeit legt die Dauer fest, bis die SPT den nächsten Heartbeat senden wird.

Die Push-Pull-Möglichkeit bestimmt das Abfragegerät:

- 0: Push: die SPT sendet die Abfrage an die RCT;
- 1: Pull: die RCT sendet die Abfrage an die SPT, die die Lastverteilung zulässt.

6.3.12 Antwort der Wegüberwachung

Die Antwortmeldung der Wegüberwachung hat das folgende Format:

RCT → SPT

Tabelle 36 – Format der Antwortmeldung der Wegüberwachung

Byte-Index	Bytes	Beschreibung
0	HL	Kopfdaten, Meldung-ID und Länge der Meldung
HL	1	Ergebniscode ^a
HL + 1	4	Heartbeat-Intervallzeit (s)
HL + 5	1	Push (0) oder Pull (1)
HL + 6		Auffüllen
		Hash
^a Der Ergebniscode kann sein: RESP_ACKNOWLEDGE RESP_POLL_TOO_SLOW		

6.3.13 Befehl zur Zeiteinstellung

Die Befehlsmeldung zur Zeiteinstellung hat das folgende Format:

RCT → SPT

Tabelle 37 – Format der Befehlsmeldung zur Zeiteinstellung

Byte-Index	Bytes	Beschreibung
0	HL	Kopfdaten, Meldung-ID und Länge der Meldung
HL	8	Zeitformat nach RFC958 (NTP) / RFC4330 (SNTP V4)
HL + 8		Auffüllen
		Hash

Dieser Befehl ist freigestellt. Für den Fall, dass Ereignisse mit Zeitstempel übertragen werden, kann dieser Befehl zur Synchronisierung von der RCT gesendet werden.

6.3.14 Antwort der Zeiteinstellung

Die Antwortmeldung der Zeiteinstellung hat das folgende Format:

SPT → RCT

Tabelle 38 – Format der Antwortmeldung der Zeiteinstellung

Byte-Index	Bytes	Beschreibung
0	HL	Kopfdaten, Meldung-ID und Länge der Meldung
HL	1	Ergebniscode
HL + 1		Auffüllen
		Hash

6.3.15 Transparente Meldung

Die transparente Meldung hat das folgende Format:

Tabelle 39 – Format der transparenten Meldung

Byte-Index	Bytes	Beschreibung
0	HL	Kopfdaten, Meldung-ID und Länge der Meldung
HL	L	Transparente Daten
HL + L		Auffüllen
		Hash

Diese Meldung lässt (verkäuferspezifische) Daten zu, die zwischen SPT und RCT zu übertragen sind. Sie kann beispielsweise zur Konfiguration von Daten oder zum Hochladen von Firmware benutzt werden.

6.3.16 Transparente Antwort

Die transparente Antwort hat das folgende Format:

Tabelle 40 – Format der transparenten Antwort

Byte-Index	Bytes	Beschreibung
0	HL	Kopfdaten, Meldung-ID und Länge der Meldung
HL	1	Ergebniscode
HL + 1	L	Transparente Daten
HL + 1 + L		Auffüllen
		Hash