



BSI Standards Publication

## Alarm systems - Alarm transmission systems and equipment

---

Part 9: Requirements for common protocol for alarm transmission using the Internet Protocol (IP)

## National foreword

This Published Document is the UK implementation of CLC/TS 50136-9:2017. It supersedes PD CLC/TS 50136-9:2013, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee GW/1, Electronic security systems and products.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2017  
Published by BSI Standards Limited 2017

ISBN 978 0 580 91875 9

ICS 13.320; 33.040.40

**Compliance with a British Standard cannot confer immunity from legal obligations.**

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 November 2017.

### Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

---

English Version

**Alarm systems - Alarm transmission systems and equipment -  
 Part 9: Requirements for common protocol for alarm  
 transmission using the Internet Protocol (IP)**

Systèmes d'alarmes - Systèmes et équipements de  
 transmission d'alarme - Partie 9 : Exigences pour le  
 protocole commun de transmission d'alarme utilisant le  
 protocole Internet (IP)

Alarmanlagen - Alarmübertragungsanlagen und -  
 einrichtungen - Teil 9: Anforderungen an standardisierte  
 Protokolle zur Alarmübertragung unter Nutzung des  
 Internetprotokolls (IP)

This Technical Specification was approved by CENELEC on 2017-05-29.

CENELEC members are required to announce the existence of this TS in the same way as for an EN and to make the TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



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

**CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels**

# Contents

Page

<b>European foreword</b> .....	<b>6</b>
<b>1 Scope</b> .....	<b>7</b>
<b>2 Normative references</b> .....	<b>7</b>
<b>3 Terms, definitions and abbreviations</b> .....	<b>7</b>
3.1 Terms and definitions .....	7
3.2 Abbreviations.....	7
<b>4 Objective</b> .....	<b>8</b>
<b>5 Messaging</b> .....	<b>8</b>
5.1 General .....	8
5.2 Message format overview.....	9
5.2.1 General.....	9
5.2.2 Identifiers.....	9
5.2.3 Message format.....	10
5.2.4 Connection handle.....	11
5.2.5 Device ID.....	11
5.2.6 Message ID .....	12
5.2.7 Message Length .....	13
5.2.8 Sequence numbers.....	13
5.2.9 Flags .....	13
5.3 Padding and message length .....	13
5.3.1 General.....	13
5.3.2 Message Length .....	14
5.4 Hashing.....	14
5.4.1 General.....	14
5.4.2 Invalid hash – transmitter response .....	14
5.4.3 Invalid hash - receiver response .....	14
5.5 Encryption .....	14
5.5.1 General.....	14
5.5.2 Key exchange.....	15
5.6 Timeouts and retries.....	15
5.7 Version number .....	16
5.8 Reverse commands .....	16
5.9 Initial values.....	16
<b>6 Message types</b> .....	<b>17</b>
6.1 Path supervision.....	17
6.1.1 General.....	17
6.1.2 Poll message.....	17
6.1.3 Poll response.....	18
6.2 Event message format.....	18
6.2.1 General.....	18
6.2.2 Event field.....	20
6.2.3 Time event field .....	20
6.2.4 Time message field.....	20
6.2.5 Link field – IP Address .....	21
6.2.6 Link field – Port number .....	21
6.2.7 Link field – URL .....	21
6.2.8 Link field - Filename.....	22
6.2.9 Alarm Text.....	22
6.2.10 Site Name.....	22
6.2.11 Building Name .....	22
6.2.12 Location.....	22
6.2.13 Room.....	23

6.2.14	Alarm Trigger.....	23
6.2.15	Longitude.....	23
6.2.16	Latitude.....	23
6.2.17	Altitude .....	24
6.3	Event response format .....	24
6.4	Configuration messages.....	25
6.4.1	General.....	25
6.4.2	Connection handle request.....	25
6.4.3	Connection handle response .....	25
6.4.4	Device ID request.....	26
6.4.5	Device ID response .....	27
6.4.6	Encryption selection request.....	27
6.4.7	Encryption selection response .....	27
6.4.8	Encryption key exchange request.....	28
6.4.9	Encryption key exchange response .....	29
6.4.10	Hash selection request .....	29
6.4.11	Hash selection response .....	30
6.4.12	Path supervision request .....	30
6.4.13	Path supervision response.....	31
6.4.14	Set time command.....	31
6.4.15	Set time response.....	31
6.4.16	Protocol version request.....	32
6.4.17	Protocol version response .....	32
6.4.18	Transparent message.....	33
6.4.19	Transparent response.....	33
6.4.20	DTLS completed request .....	34
6.4.21	DTLS completed response .....	34
6.4.22	RCT IP parameter request.....	35
6.4.23	RCT IP parameter response.....	35
<b>7</b>	<b>Commissioning and connection setup .....</b>	<b>36</b>
7.1	Commissioning.....	36
7.1.1	General.....	36
7.1.2	Procedures.....	36
7.1.3	Commissioning message sequence .....	36
7.1.4	Commissioning using Shared Secret.....	37
7.1.5	Commissioning using X.509 Certificates and DTLS .....	38
7.2	Connection setup.....	39
	<b>Annex A (normative) Result codes .....</b>	<b>41</b>
	<b>Annex B (normative) Protocol Identifiers .....</b>	<b>42</b>
	<b>Annex C (normative) Shared secret .....</b>	<b>43</b>
C.1	Formatting of the shared secret.....	43
C.2	Checksum for Shared Secret Formatting.....	43
C.3	Example of Secret Encoding and Formatting.....	43
	<b>Annex D (informative) Examples of messaging sequences .....</b>	<b>44</b>
D.1	Commissioning .....	44
D.2	Connection setup.....	48
	<b>Annex E (informative) Examples of application protocols .....</b>	<b>51</b>
E.1	SIA.....	51
E.2	Ademco Contact ID.....	51
E.3	Scancom Fast Format .....	52
E.4	VdS 2465 .....	52
	<b>Annex F (informative) Design principles .....</b>	<b>54</b>
F.1	General.....	54

F.2 Information security .....54  
 F.3 Use of UDP signalling .....54  
 Bibliography.....55

Tables

Table 1 — Backwards compatibility .....9  
 Table 2 — Backwards compatibility result code .....9  
 Table 3 — Identifiers .....9  
 Table 4 — Basic unencrypted format of messages .....10  
 Table 5 — Basic encrypted format of messages .....10  
 Table 6 — Message ID overview .....11  
 Table 7 — Flags .....13  
 Table 8 — Hashing ID's .....14  
 Table 9 — Encryption ID's .....15  
 Table 10 — Reverse commands .....16  
 Table 11 — Initial values .....17  
 Table 12 — Poll message SPT ← → RCT .....17  
 Table 13 — Poll response RCT ← → SPT .....18  
 Table 14 — Poll response - result code .....18  
 Table 15 — Event message format – SPT → RCT .....19  
 Table 16 — Event message format – Fields .....19  
 Table 17 — Event field .....20  
 Table 18 — Time event field .....20  
 Table 19 — Time message field .....21  
 Table 20 — Link field – IP Address .....21  
 Table 21 — Link field – Port number .....21  
 Table 22 — Link field – URL .....21  
 Table 23 — Link field – Filename .....22  
 Table 24 — Alarm Text .....22  
 Table 25 — Site Name .....22  
 Table 26 — Building Name .....22  
 Table 27 — Location .....23  
 Table 28 — Room .....23  
 Table 29 — Alarm Trigger .....23  
 Table 30 — Longitude .....23  
 Table 31 — Latitude .....24  
 Table 32 — Altitude .....24  
 Table 33 — Event response message format .....24  
 Table 34 — Event response - result code .....24  
 Table 35 — Connection handle request message format .....25  
 Table 36 — Connection handle response message format .....26  
 Table 37 — Connection handle response - result code .....26  
 Table 38 — Device ID request message format .....26  
 Table 39 — Device ID request flags .....27  
 Table 40 — Device ID response message format .....27  
 Table 41 — Encryption selection request message format .....27  
 Table 42 — 'Master Encryption Selection request' flag .....28

Table 43 — Encryption selection response message format .....	28
Table 44 — Encryption selection response - result code .....	28
Table 45 — Encryption key exchange request message format .....	28
Table 46 — 'Master Key request' flag .....	29
Table 47 — Encryption key exchange response message format .....	29
Table 48 — Encryption key - result code .....	29
Table 49 — Hash selection request message format .....	30
Table 50 — Hash selection response message format .....	30
Table 51 — Path supervision request message format .....	30
Table 52 — Path supervision response message format .....	31
Table 53 — Path supervision response - result code .....	31
Table 54 — Set time command message format .....	31
Table 55 — Set time response message format .....	32
Table 56 — Set time response - result code .....	32
Table 57 — Protocol version request message format .....	32
Table 58 — Protocol version response message format .....	33
Table 59 — Protocol version response - result code .....	33
Table 60 — Transparent message format .....	33
Table 61 — Transparent response format .....	33
Table 62 — Transparent response - result code .....	34
Table 63 — DTLS completed request message format .....	34
Table 64 — DTLS completed response message format .....	34
Table 65 — DTLS completed response - result code .....	34
Table 66 — RCT IP parameter request message format .....	35
Table 67 — RCT IP parameter response message format .....	35
Table 68 — RCT IP parameter response - result code .....	35
Table 69 — Message flow during the commissioning of a new SPT .....	36
Table 70 — Message flow during connection setup .....	40
Table A.1 — Result codes .....	41
Table B.1 — Protocol identifiers .....	42
Table D1 — Example of the commissioning messaging sequence .....	45
Table D.2 — Example of the connection setup messaging sequence .....	48
Table E.1 — VdS2401 message example .....	53

## European foreword

This document (CLC/TS 50136-9:2017) has been prepared by CLC/TC 79 “Alarm systems”.

This document supersedes CLC/TS 50136-9:2013.

This technical specification specifies a common IP transport protocol for alarm transmission. The published version (2013, first version) required solving both technical and security issues identified during the first actual implementations of the protocol. The working group was working closely with the early adopters of the protocol and has a very clear and complete list of issues and solutions. This revision supersedes the previous version.

EN 50136 will consist of the following parts, under the general title “Alarm systems – Alarm transmission systems and equipment”:

- Part 1            General requirements for alarm transmission systems
- Part 2            General requirements for Supervised Premises Transceiver (SPT)
- Part 3            Requirements for Receiving Centre Transceiver (RCT)
- Part 4            Annunciation equipment used in alarm receiving centres
- Part 5            (Free)
- Part 6            (Free)
- Part 7            Application guidelines
- Part 8            (Free)
- Part 9            Requirements for a common protocol for alarm transmission using the Internet Protocol (IP)

## 1 Scope

This Technical Specification specifies a protocol for point-to-point transmission of alarms and faults, as well as communications monitoring, between a Supervised Premises Transceiver and a Receiving Centre Transceiver using the Internet Protocol (IP).

The protocol is intended for use over any network that supports the transmission of IP data. These include Ethernet, xDSL, GPRS, WiFi, UMTS and WIMAX.

The system performance characteristics for alarm transmission are specified in EN 50136-1.

The performance characteristics of the supervised premises equipment should comply with the requirements of its associated alarm system standard and applies for transmission of all types of alarms including, but not limited to, fire, intrusion, access control and social alarms.

Compliance with this Technical Specification is voluntary.

## 2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 50136-1:2012, *Alarm systems - Alarm transmission systems and equipment - Part 1: General requirements for alarm transmission systems*

## 3 Terms, definitions and abbreviations

### 3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 50136-1:2012 apply.

### 3.2 Abbreviations

For the purposes of this document, the following abbreviations apply.

AES	Advanced Encryption Standard
ARC	Alarm Receiving Centre
ATP	Alarm Transmission Path
ATS	Alarm Transmission System
CA	X.509 Certificate Authority
CBC	Cipher Block Chaining
CRC	Cyclic redundancy check
DNS	Domain Name System
DTLS	Datagram Transport Layer Security
HL	Header Length
IP	Internet Protocol
IV	Initialization Vector
MAC	Media Access Control
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol