

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 2020-09-28.

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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, 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: Rue de la Science 23, B-1040 Brussels**

<b>Contents</b>	<b>Page</b>
<b>European foreword</b> .....	<b>5</b>
<b>1 Scope</b> .....	<b>6</b>
<b>2 Normative references</b> .....	<b>6</b>
<b>3 Terms, definitions and abbreviations</b> .....	<b>6</b>
3.1 Terms and definitions .....	6
3.2 Abbreviations .....	6
<b>4 Objective</b> .....	<b>7</b>
<b>5 Messaging</b> .....	<b>7</b>
5.1 General .....	7
5.2 Message format overview .....	8
5.3 Padding and message length .....	12
5.4 Hashing .....	13
5.5 Encryption .....	13
5.6 Timeouts and retries .....	14
5.7 Version number .....	15
5.8 Reverse commands .....	15
5.9 Initial values .....	15
<b>6 Message types</b> .....	<b>16</b>
6.1 General .....	16
6.2 Path supervision .....	16
6.3 Event message format .....	17
6.4 Event response format .....	23
6.5 Configuration messages .....	23
<b>7 Commissioning and connection setup</b> .....	<b>36</b>
7.1 General .....	36
7.2 Commissioning .....	36
7.3 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>
<b>Annex D (informative) Examples of messaging sequences</b> .....	<b>44</b>
<b>Annex E (informative) Examples of application protocols</b> .....	<b>51</b>
<b>Annex F (informative) Design principles</b> .....	<b>53</b>
<b>Bibliography</b> .....	<b>54</b>
 <b>Tables</b>	
Table 1 — Backwards compatibility .....	8
Table 2 — Backwards compatibility result code .....	8

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

Table 43 — Encryption selection response message format.....	26
Table 44 — Encryption selection response - result code.....	26
Table 45 — Encryption key exchange request message format .....	27
Table 46 — 'Master Key request' flag .....	27
Table 47 — Encryption key exchange response message format.....	28
Table 48 — Encryption key - result code .....	28
Table 49 — Hash selection request message format .....	28
Table 50 — Hash selection response message format .....	29
Table 51 — Path supervision request message format .....	29
Table 52 — Path supervision response message format .....	30
Table 53 — Path supervision response - result code .....	30
Table 54 — Set time command message format.....	30
Table 55 — Set time response message format.....	31
Table 56 — Set time response - result code.....	31
Table 57 — Protocol version request message format.....	31
Table 58 — Protocol version response message format .....	32
Table 59 — Protocol version response - result code .....	32
Table 60 — Transparent message format .....	32
Table 61 — Transparent response format .....	33
Table 62 — Transparent response - result code.....	33
Table 63 — DTLS completed request message format.....	33
Table 64 — DTLS completed response message format .....	34
Table 65 — DTLS completed response - result code .....	34
Table 66 — RCT IP parameter request message format .....	34
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 .....	37
Table 70 — Message flow during connection setup .....	40
Table A.1 — Result codes.....	41
Table B.1 — Protocol identifiers.....	42
Table D.1 — Example of the commissioning messaging sequence .....	45
Table D.2 — Example of the connection setup messaging sequence .....	48
Table E.1 — VdS2465 message example .....	52

## European foreword

This document (CLC/TS 50136-9:2020) has been prepared by CLC/TC 79 “Alarm systems”.

This document supersedes CLC/TS 50136-9:2017.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

This document specifies a common IP transport protocol for alarm transmission. The published version (2017, second 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 consists 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 document 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 requirements for the performance of the alarm transmission system, the SPT and the RCT are specified in the relevant parts of the EN 50136 series.

Compliance with this document is voluntary.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. 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.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

### 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