

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

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

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

This Technical Specification was approved by CENELEC on 2012-11-12.

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, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

**CENELEC**

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

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

## Contents

|                                                                |           |
|----------------------------------------------------------------|-----------|
| <b>Foreword</b>                                                | <b>4</b>  |
| <b>1 Scope</b>                                                 | <b>5</b>  |
| <b>2 Normative references</b>                                  | <b>5</b>  |
| <b>3 Terms, definitions and abbreviations</b>                  | <b>5</b>  |
| 3.1 Terms and definitions                                      | 5         |
| 3.2 Abbreviations                                              | 5         |
| <b>4 Objective</b>                                             | <b>6</b>  |
| <b>5 Messaging</b>                                             | <b>6</b>  |
| 5.1 General                                                    | 6         |
| 5.2 Message format overview                                    | 7         |
| 5.3 Padding and message length                                 | 11        |
| 5.4 Hashing                                                    | 12        |
| 5.5 Encryption                                                 | 12        |
| 5.6 Timeouts and retries                                       | 13        |
| 5.7 Version number                                             | 13        |
| 5.8 Reverse commands                                           | 13        |
| 5.9 Initial values                                             | 14        |
| <b>6 Message types</b>                                         | <b>14</b> |
| 6.1 General                                                    | 14        |
| 6.2 Path supervision                                           | 14        |
| 6.3 Event reporting                                            | 15        |
| 6.4 Configuration messages                                     | 19        |
| <b>7 Commissioning and connection setup</b>                    | <b>27</b> |
| 7.1 Commissioning                                              | 27        |
| 7.2 Connection setup                                           | 31        |
| <b>Annex A (normative) Result codes</b>                        | <b>32</b> |
| <b>Annex B (normative) Protocol Identifiers</b>                | <b>33</b> |
| <b>Annex C (normative) Shared secret</b>                       | <b>34</b> |
| C.1 Formatting of the shared secret                            | 34        |
| C.2 Checksum for Shared Secret Formatting                      | 34        |
| C.3 Example of Secret Encoding and Formatting                  | 34        |
| <b>Annex D (informative) Examples of messaging sequences</b>   | <b>35</b> |
| D.1 Commissioning                                              | 35        |
| D.2 Connection setup                                           | 38        |
| <b>Annex E (informative) Examples of application protocols</b> | <b>41</b> |
| E.1 SIA                                                        | 41        |
| E.2 Ademco Contact ID                                          | 41        |
| E.3 Scancom Fast Format                                        | 42        |
| E.4 VdS 2465                                                   | 42        |
| <b>Annex F (informative) Design principles</b>                 | <b>44</b> |
| F.1 General                                                    | 44        |
| F.2 Information Security                                       | 44        |
| F.3 Use of UDP signalling                                      | 44        |
| <b>Bibliography</b>                                            | <b>45</b> |

|                                                                    |    |
|--------------------------------------------------------------------|----|
| Table 1 – Identifiers .....                                        | 7  |
| Table 2– Basic unencrypted format of messages.....                 | 7  |
| Table 3 – Basic encrypted format of messages.....                  | 8  |
| Table 4 – Message ID overview .....                                | 10 |
| Table 5 – Flags.....                                               | 11 |
| Table 6 – Hashing ID's .....                                       | 12 |
| Table 7 – Encryption ID's .....                                    | 12 |
| Table 8 – Reverse commands.....                                    | 14 |
| Table 9 – Initial values.....                                      | 14 |
| Table 10 – Poll message SPT $\leftarrow \rightarrow$ RCT.....      | 15 |
| Table 11 – Poll response RCT $\leftarrow \rightarrow$ SPT.....     | 15 |
| Table 12 – Event message format – SPT $\rightarrow$ RCT .....      | 16 |
| Table 13 – Event message format – Fields .....                     | 16 |
| Table 14 – Event field.....                                        | 16 |
| Table 15 – Time event field .....                                  | 17 |
| Table 16 – Time message field.....                                 | 17 |
| Table 17 – Link field – IP Address .....                           | 17 |
| Table 18 – Link field – IP Port number .....                       | 18 |
| Table 19 – Link field – URL .....                                  | 18 |
| Table 20 – Link field – Filename.....                              | 18 |
| Table 21 – Event response message format.....                      | 18 |
| Table 22 – Connection handle request message format .....          | 19 |
| Table 23 – Connection handle response message format .....         | 20 |
| Table 24 – Device ID request message format.....                   | 20 |
| Table 25 – Device ID request flags.....                            | 20 |
| Table 26 – Device ID response message format.....                  | 21 |
| Table 27 – Encryption selection request message format.....        | 21 |
| Table 28 – ‘Master Encryption Selection request’ flag.....         | 21 |
| Table 29 – Encryption selection response message format .....      | 22 |
| Table 30 – Encryption key exchange request message format .....    | 22 |
| Table 31 – ‘Master Key request’ flag .....                         | 22 |
| Table 32 – Encryption key exchange response message format .....   | 23 |
| Table 33 – Hash selection request message format.....              | 23 |
| Table 34 – Hash selection response message format.....             | 23 |
| Table 35 – Path supervision request message format.....            | 24 |
| Table 36 – Path supervision response message format.....           | 24 |
| Table 37 – Set time command message format.....                    | 24 |
| Table 38 – Set time response message format.....                   | 25 |
| Table 39 – Protocol version request message format .....           | 25 |
| Table 40 – Protocol version response message format.....           | 25 |
| Table 41 – Transparent message format.....                         | 25 |
| Table 42 – Transparent response format .....                       | 26 |
| Table 43 – DTLS completed request message format .....             | 26 |
| Table 44 – DTLS completed response message format.....             | 26 |
| Table 45 – RCT IP parameter request message format.....            | 27 |
| Table 46 – RCT IP parameter response message format .....          | 27 |
| Table 47 – Message flow during the commissioning of a new SPT..... | 28 |
| Table 48 – Message flow during connection setup.....               | 31 |
| Table A.1 – Result codes .....                                     | 32 |
| Table B.1 – Protocol identifiers.....                              | 33 |

## Foreword

This document (CLC/TS 50136-9:2013) has been prepared by CLC/TC 79 "*Alarm systems*".

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

This document is a preview generated by EVS

## 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 shall apply 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                         |
| 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                          |
| NVM   | Non-Volatile Memory                            |
| P-MTU | Path Maximum Transmission Unit                 |