SLOVENSKI STANDARD
SIST-TS CLC/TS 50136-9:2014

01-junij-2014

Alarmni sistemi - Sistemi in oprema za prenos alarma - 1-7. del: Zahteve za skupni protokol za prenos alarma po paketno komutiranem omrežju

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

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

Systèmes d'alarme - Systèmes et équipements de transmission d'alarme - Partie 1-7: Exigences pour le protocole commun de transmission d'alarme utilisant les réseaux à commutation de paquets

Ta slovenski standard je istoveten z: **CLC/TS 50136-9:2013**

ICS:

13.320	Alarmni in opozorilni sistemi	Alarm and warning systems
33.040.40	Podatkovna komunikacijska omrežja	Data communication networks

SIST-TS CLC/TS 50136-9:2014 **en,de**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CLC/TS 50136-9

January 2013

ICS 13.320; 33.040.40

English version

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

Ref. No. CLC/TS 50136-9:2013 E

Contents

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.

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

RCT	Receiver Centre Tranceiver
RX	Receive
SCTP	Stream Control Transmission Protocol
SNTP	Simple Network Time Protocol
SPT	Supervised Premises Transceiver
TFTP	Trivial File Transfer Protocol
TX	Transmit
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
WS	Window Size

4 Objective

The object of this Technical Specification is to specify the protocol details (transport and application layers) for alarm transmission systems using Internet Protocol (IP), to ensure interoperability between SPTs and RCTs supplied by different manufacturers. Mechanisms to commission SPT and RCT and build mutual trust between the communicating parties are also described.

As compliance with this Technical Specification is voluntary, any other alarm transmission protocol or equipment not covered by this Technical Specification may be used, provided that the requirements of EN 50136-1 are met.

This protocol is designed to run on top of UDP and is designed to support both IPv4 and IPv6.

NOTE For further discussion of IP and UDP in alarm transmission please see F.3.

5 Messaging

5.1 General

This clause defines the messaging layer, on top of which the alarm event data is transmitted using the existing reporting formats like for example Sia and Contact ID. Clause 7 defines the initial commissioning of an SPT, as well as how SPTs connect to the RCT.

The functionality of the alarm messaging and polling protocol includes:

– exchanging master and session parameters;

– (alarm) event reporting (including linking to out-of-band additional data related to events, like audio/video);

– line monitoring;

– transparent message transmission, e.g. vendor specific messages that, for example, can be used for remote commands from RCT to SPT.

It fulfils the following requirements:

– encryption, fulfilling requirements for most demanding category of EN 50136-1;

– authentication, fulfilling requirements for most demanding category of EN 50136-1;

– SPT: allows a broad range of hardware (limited demands on memory footprint as well as CPU power);

– RCT: allows support for at least 10 000 SPTs in compliance with any category in EN 50136-1, using modern general purpose server hardware;

– allow Dynamic IP addresses of the SPTs;

– allow one or more SPTs to be placed behind a NAT firewall.

5.2 Message format overview

5.2.1 General

This subclause describes the basic outline of all messages.

Each message shall be explicitly acknowledged, including line supervision messages.

Backwards compatibility is achieved by the implementation of the RESP_CMD_NOT_SUPPORTED result value, which the receiving party can send as answer to unsupported messages.

Multi-byte values will be transmitted using network byte order (big-endian).

5.2.2 Identifiers

The following identifiers exist:

Table 1 – Identifiers

Description	Purpose	Present in	Encrypted	See
Connection Handle	Look up the current symmetric encryption key	All messages	No	5.2.4
Device ID	Uniquely identify the hardware	Contributing to hashes in all messages	N / A	5.2.5

The Connection Handle is unencrypted. It is a unique number, initialized during the setup of the connection. Its sole purpose is to be able to look up the encryption key. It is valid for the communication session only.

The Device ID uniquely identifies the hardware once the connection has been established. The Device ID is used when computing the hash value for each message. In combination with the encryption of the hash this is used for substitution detection.

NOTE Device ID is not equivalent to any account code or similar ID specified by application protocol

The Device ID shall be stored in non-volatile memory within the SPT.

The IP address is not used for identification purposes, in order to allow for the use of dynamic or translated IP addresses.

5.2.3 Message format

The basic unencrypted format of all messages is as follows. Message in this format is never transmitted. It is described here only to clarify the hash value calculation.

Table 2– Basic unencrypted format of messages

Byte Index	Bytes	Description	See	Group
0	4	Connection Handle	5.2.4	Header
4	16	Device ID	5.2.5	
20	2	Tx Sequence number	5.2.8	
22	2	Rx Sequence number	5.2.8	
24	2	Flags	5.2.9	
26	1	Protocol version number	5.7	

Byte Index	Bytes	Description	See	Group
27	1	Message ID	5.2.6	Message
28	2	Message Length	5.2.7	
30	n	Message Data	Clause 6	

The basic encrypted, transmitted format of all messages is as follows. Note that the Device ID field is not included in the encrypted message, but its value is used to compute the message hash value i.e. the hash is calculated from the unencrypted version of the message described above.

Table 3 – Basic encrypted format of messages

Byte Index	Bytes	Description	See	Encrypted	Group
0	4	Connection Handle	5.2.4	No	Header
4	2	Tx Sequence number	5.2.8	Yes	
6	2	Rx Sequence number	5.2.8	Yes	
8	2	Flags	5.2.9	Yes	
10	1	Protocol version number	5.7	Yes	
11	1	Message ID	5.2.6	Yes	Message
12	2	Message Length	5.2.7	Yes	
14	n	Message Data	Clause 6	Yes	
14 + n		Padding	5.3.1	Yes	Tail
	32 32	Hash – SHA-256, or Hash – RIPEMD-256	5.4	Yes	

The Connection Handle is unencrypted, the remainder of the message is encrypted using the encryption method as negotiated during the commissioning stage.

Message ID's are defined in pairs: each message has its matching response. For responses the first byte of the Message Data always holds a 'Result code' as defined in Annex A.

All fields are described in detail in the following subclauses.

5.2.4 Connection Handle

The Connection Handle is assigned (uniquely for the RCT to which a SPT reports) using the commissioning protocol. The RCT creates a unique Connection Handle and links this to the Device ID of the SPT in its internal database. This translation results in a compact, fixed length Connection Handle.

The purpose of the Connection Handle is to be able to determine the encryption key to be used to decrypt the received message, independent of the IP address of the message.

The Connection Handle is not a (by the installer/operator) configurable parameter, nor made visible on user interfaces. It is generated and used internally by the SPT/RCT equipment only.

5.2.5 Device ID

5.2.5.1 General

The Device ID uniquely identifies the SPT and RCT. It is used (in combination with the encryption) for substitution detection. Both SPT and RCT can verify the identity of the connected party using this field, and create a substitution alarm in case it has changed.

Within the message header, the Device ID itself is never transmitted. However Device ID is used to contribute to the message hash calculation

Device ID is 16 bytes long.

5.2.5.2 SPT Device ID

The Device ID of the SPT is an ID that is random to the SPT, but fixed and read-only over the lifetime of the SPT, i.e. A hardware serial number. It is unique within the SPT database in the RCT.

The Device ID is created during manufacturing time of the device; in messaging, it is never transmitted itself in cleartext, but is needed to be known in cleartext for the ARC to configure the RCT accordingly.

Thus, it is only transmitted during initial commissioning phase to the RCT.

Uniqueness is assured by the following principles:

– Each SPT manufacturer shall use his 24 bits “Organizationally Unique Identifier” as assigned to him by the IEEE for MAC-address generation

– Each SPT manufacturer not having such a code shall attend for such a code from IEEE.

– If an interface in the SPT makes use of a MAC address, the next 24 bits in the device ID shall be the same as the rest of MAC address specified by the manufacturer. If such interface does not exist, the manufacturer shall use another numbering scheme documented by the manufacturer.

– The manufacturer shall use non-consecutive, randomly distributed numbers for the rest of the device ID field and guarantee uniqueness for all his delivered SPT devices.

5.2.5.3 RCT Device ID

The Device ID of the RCT is an ID that is unique within the receiver and never changed within the lifetime of a receiver. It represents the unique identity of the RCT.

The RCT device ID is made available to the SPT during the commissioning phase.

5.2.6 Message ID

The Message ID's as used are listed in the following table:

Table 4 – Message ID overview

Message name	Description	Direction SPT ←·→ RCT	Version	Message ID
POLL_MSG	Poll message	→	1	0x11
EVENT_MSG	Event message	→	1	0x30
CONN_HANDLE_REQ	Connection handle request	→	1	0x40
DEVICE_ID_REQ	Device ID request	→	1	0x41
ENCRYPT_SELECT_REQ	Encryption selection request	→	1	0x42
ENCRYPT_KEY_REQ	Encryption key exchange	← →	1	0x43
HASH_SELECT_REQ	Hash selection request	→	1	0x44
PATH_SUPERVISION_REQ	Path supervision request	← →	1	0x45
SET_TIME_CMD	Set time command	←	1	0x47
VERSION_REQ	Protocol version request	→	1	0x48
PMTU_REQ	P-MTU	→	1	0x60
PMTU_PROBE	P-MTU probe	→	1	0x61
DTLS_COMPLETE_REQ	DTLS completed request	→	1	0x62
TRANSPARENT_MSG	Transparent message	← →	1	0x70
POLL_RESP	Poll Response	←	1	0x91
EVENT_RESP	Event response	←	1	0xB0
CONN_HANDLE_RESP	Connection handle response	←	1	0xC0
DEVICE_ID_RESP	Device ID response	←	1	0xC1
ENCRYPT_SELECT_RESP	Encryption selection response	←	1	0xC2
ENCRYPT_KEY_RESP	Encryption key exchange response	← →	1	0xC3
HASH_SELECT_RESP	Hash selection response	←	1	0xC4
PATH_SUPERVISION_RESP	Path supervision response	← →	1	0xC5
SET_TIME_RESP	Set time response	→	1	0xC7
VERSION_RESP	Protocol version response	←	1	0xC8
PMTU_RESP	P-MTU response	←	1	0xE0
PMTU_PROBE_RESP	P-MTU probe response	←	1	0xE1
DTLS_COMPLETE_RESP	DTLS completed response	←	1	0xE2
TRANSPARENT_RESP	Transparent response	← →	1	0xF0

The Message ID of any Response is the same as the Message ID of the corresponding Command, but with bit 7 set.

5.2.7 Message length

This is the length of the Message Data (excluding Message ID and Message length). This field is used:

– in variable length messages (see for example 6.3.1 and 6.4.18) to check for the end of data;

– to be able to determine the start of an embedded reverse command (see 5.8).

Possible padding is never considered when calculating the value of message length field.

5.2.8 Sequence numbers

The sequence number is used to determine if a message is missing or duplicated. Both ends have a transmit sequence number and a receive sequence number.

These two counters exist at both ends (e.g. we are speaking about 4 counters in total), whereas the RX_Sequence counters are used to realize a “state-full machine” implementation.

These counters are used to fulfil three simultaneous functions:

a) Initially, both the SPT and RCT choose their TX_seqs to be a random number, then they use it as a datagram counter, incrementing them for each sent datagram by one. The RX_seqs are the expected next TX_seqs from the other communication end-point. That is: If one did see “42” as the last TX_seq coming in from the communication partner, oneself would send out “43” as next RX_seq. As the other end does this in the same style, the TX_seq and RX_seq function as a mutual sequence control mechanism.

b) Second, they can simultaneously function as a resend-mechanism: If one detected that one missed a datagram (because for example, the incoming TX_seq is “44”, but one expected TX_seq=43) or the one got is corrupt (by checking the hash), one just resends the own old previously sent last datagram and the other side will see by the old TX_seq that one wants to get a re-transmission.

c) Being chosen randomly and being part of the encrypted data block, they rule out replay attacks.

For each connection, every message has to be acknowledged before the next new (not retransmission) message may be transmitted.

5.2.9 Flags

The following flags are defined:

Table 5 – Flags

Byte	Bit	Definition
0	0	Reverse command included in response: – value 0 = no reverse command included, – value 1 = reverse command included
0	1…7	Reserved
1	0…7	Reserved

5.3 Padding and message length

5.3.1 Padding

Padding is required for the following two reasons:

– create a message length which is a multiple of the block length of the encryption algorithm as used;

– make poll and alarm messages look alike.

Padding is done using random or pseudo-random data. Random bytes are appended to the actual messages data until the total message length is one of those as specified in the next clause.

5.3.2 Message length

The message lengths as used fulfil the requirements as mentioned in 5.3.1 (using a 16 or 32 byte block length), and are a compromise between obfuscation of alarm events and bandwidth usage.

This results message lengths that are a multiple of 128 + 4 bytes for the Connection Handle:

– 132 bytes (4 bytes Connection Handle + 8 × 16 bytes);