SLOVENSKI STANDARD
oSIST prEN 50090-4-4:2024

01-december-2024

Stanovanjski in stavbni elektronski sistemi (HBES) - 4-4. del: HBES IoT Point API

Home and Building Electronic Systems (HBES) - Part 4-4: HBES IoT Point API

Systèmes électroniques pour les foyers domestiques et les bâtiments (HBES) - Partie 4-4: API de Point IdO HBES

Ta slovenski standard je istoveten z: **prEN 50090-4-4**

ICS:

35.240.67	Uporabniške rešitve IT v gradbeništvu	IT applications in building and construction industry
97.120	Avtomatske krmilne naprave za dom	Automatic controls for household use

oSIST prEN 50090-4-4:2024 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 50090-4-4

November 2024

ICS 35.240.67; 97.120 -

English Version

Home and Building Electronic Systems (HBES) - Part 4-4: HBES IoT Point API

Systèmes électroniques pour les foyers domestiques et les bâtiments (HBES) - Partie 4-4: API de Point IdO HBES

To be completed

This draft European Standard is submitted to CENELEC members for enquiry.
Deadline for CENELEC: 2025-01-24.

It has been drawn up by CLC/TC 205.

If this draft becomes a European Standard, CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

This draft European Standard was established by CENELEC in three official versions (English, French, German).
A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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, Türkiye and the United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

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

Contents

Page

European foreword

This document (prEN 50090-4-4:2024) has been prepared by CLC/TC 205 “Home and Building Electronic Systems (HBES)”.

This document is currently submitted to the Enquiry.

The following dates are proposed:

• latest date by which the existence of this document has to be announced at national level	(doa)	dav + 6 months
• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	dav + 12 months
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	dav + 36 months (to be confirmed or modified when voting)

1 Scope

This document lays down the requirements for the HBES Point API extension to the EN 50090 series, allowing vendor independent communication between smart home and building devices on IPv6 networks.

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 50090-1:2011, *Home and Building Electronic Systems (HBES) — Part 1* Standardization structure

EN 50090-3-3, *Home and Building Electronic Systems (HBES) — Part 3-3: Aspects of application — HBES Interworking model and common HBES data types*

EN 50090-4-1, *Home and Building Electronic Systems (HBES) — Part 4-1: Media independent layers — Application layer for HBES Class 1*

EN 50090-4-2, *Home and Building Electronic Systems (HBES) — Part 4-2: Media independent layers — Transport layer, network layer and general parts of data link layer for HBES Class 1*

EN 50090-7-1, *Home and Building Electronic Systems (HBES) — Part 7-1: System management — Management procedures*

EN ISO 22510, *Open data communication in building automation, controls and building management — Home and building electronic systems — KNXnet/IP communication (ISO 22510)*

RFC 7252, *The Constrained Application Protocol (CoAP)*

RFC 8949, *Concise Binary Object Representation (CBOR)*

RFC 6838, *Media Type Specifications and Registration Procedures*

RFC 6690, *Constrained RESTful Environments (CoRE) Link Fomat*

RFC 1035, *Domain names – Implementation and specification*

RFC 8323, *CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets*

RFC 4291, *IP Version 6 Addressing Architecture*

RFC 6763, *DNS-Based Service Discovery*

RFC 8766, *Discovery Proxy for Multicast DNS-Based Service Discovery*

RFC 6762, *Muticast DNS*

RFC 3596, *DNS Extensions to Support IP Version 6*

RFC 8613, *Object Security for Constrained RESTful Environments (OSCORE)*

RFC 7959, *Block-Wise Transfers in the Constrained Application Protocol (CoAP)*

RFC 9175, *Constrained Application Protocol (CoAP): Echo, Request-Tag, and Token Processing*

RFC 8516, *“Too Many Requests” Response Code for the Constrained Application Protocol*

RFC 3306, *Unicast-Prefix-based IPv6 Multicast Addresses*

RFC 3307, *Allocation Guidelines for IPv6 Multicast Addresses*

RFC 6282, *Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks*

RFC 9148, *EST-coaps: Enrollment over Secure Transport with the Secure Constrained Applicatoin Protocol*

RFC 8995, *Bootstrapping Remote Secure Key Infrastructure (BRSKI)*

RFC 5967, *The application/pkcs10 Media Type*

RFC 5273, *Certificate Management over CMS (CMC): Transport Protocols*

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

RFC 2818, *HTTP Over TLS*

RFC 7251, *AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for TLS*

RFC 8392, *CBOR Web Token (CWT)*

RFC 3986, *Uniform Resource Identifier (URI): Generic Syntax*

RFC 8747, *Proof-of-Possession Key Semantics for CBOR Web Tokens (CWTs)*

RFC 8152, *CBOR Object Signing and Encryption (COSE)*

RFC 3339, *Date and Time on the Internet: Timestamps*

RFC 6335, *Internet Assigned Numbers Authority (IANA) Procedures for the Managmenet of the Service Name and Transport Protocol Port Number Registry*

RFC 4492, *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)*

RFC 5869, *HMAC-based Extract-and-Expand Key Derivation Function (HKDF)*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 50090-1:2011 and the following apply.

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

— IEC Electropedia: available at https://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

3.1.1
Actuator
Point performing an actuation in HBES IoT (executed by a specific procedure, with an expected result) that changes an Installation state during Runtime

3.1.2
Advanced Message Queuing Protocol
open standard application layer protocol for message-oriented middleware with defining features such as message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security

3.1.3
Application Function
set of Functions used to achieve the desired behavior of a technical system, typically using a combination of devices exchanging information via their input and output Datapoints

Note 1 to entry: An Application Function may be split into several Functional Blocks (located in one or more devices) with their input and output Datapoints that are logically connected to each other.

EXAMPLE “direct electrical heating”, “electrical heating with accumulators”, “warm water heating”, “fan coil air-conditioning” …

3.1.4
Authorization and Group Manager
entity service that supports an authorized access so that a device can join to a specific communication channel

3.1.5
Channel
collection of Datapoints of a device that are logically related to each other typically by association with a hardware feature or a specific function of that device

Note 1 to entry: These Datapoints may be derived from one or more defined Functional Blocks (as defined by KNXA) or may be an expansion above and beyond defined Functional Blocks or may be independent of a NX Functional Block if none is defined for the function associated with the channel.

3.1.6
Datapoint
representation of a logical input entity of a device acting as recipient of Installation state data, whereas a logical output of a device acts as source of Installation state data

3.1.7
Device
physical element that is part of the network and an object a customer can buy

3.1.8
Domain CA
entity that issues operational certificates for the domain

3.1.9
Endpoint
interface to a service, a process, or a queue or topic destination in service-oriented architecture

3.1.10
Function
part of the intended behavior of a Functional Block in a building context

3.1.11
Functional Block
one or more Functions that belong together, that cannot be separated across two devices but is big enough that a device with only one such entity could be marketed and that has a well-defined black box behavior

3.1.12
Function Point
runtime system state information of a specific Application Function shared by at least two datapoints and having a unique identifier that addresses a group of controlled objects called a Group Address

EXAMPLE < Light Switch > in room living on/off, whereas the < … > is the Function Point name

3.1.13
Group Address
numerical identifier of a Function Point

3.1.14
Group Communication
communication model in which one sender communicates information to one and typically more receivers

Note 1 to entry: In HBES IoT, this can be realized by simple UDP communication or by using a message broker system or other.

Note 2 to entry: In non-IoT HBES this is referred to as multicast or P2P based Group Communication, either with Group Addresses or Interface Objects (Points) exchanging state data

3.1.15
Group Message
message exchanged between Group Objects using a specific group identifier, not necessarily expressing any type of IP unicast or IP multicast communication pattern

3.1.16
Group Object
preferably foreseen for Group Communication using Group Address(es) - becoming a member of a Function Point represented by the assigned Group Address – or accessible via P2P communication, if no Group Address is assigned

3.1.17
HBES Installation ID

ID used to separate HBES Installations from each other, specified as a random, unique ID

3.1.18
HBES IoT
protocol suite/framework for transport of HBES data on the Internet of Things with IPv6

3.1.19
HBES IoT 3rd Party API
the set of requirements and regulations through which partial access to an Installation can be gained by offering a collection of Endpoints

Note 1 to entry: It offers an access at the level of the Installation and supports more sophisticated queries to (history) values of installation state data or specific elements of the Installation, such as location, Application Function and Datapoints.

3.1.20
HBES IoT Router
gateway between HBES IoT and non-IoT HBES

3.1.21
HBES IoT Point API
set of requirements and regulations through which devices directly exchange information with each other based on HBES IoT

3.1.22
HBES System
system which ncompasses HBES standards and definitions, allowing the creation of an Installation, and including aspects such as topology constraints for devices, device configuration procedures and runtime interworking principles, Functional Blocks, with Application behavior specified in FBs and more

3.1.23
Installation
assembly of materials and components (devices) placed in position to provide a service, a deployed system consisting of equipment and Functions that are used for a particular purpose

EXAMPLE A deployed Installation may be a HVAC system or a fire protection system.

3.1.24
Management Client
means to configure and commission Devices, as well as to plan, design and diagnose an entire Installation

Note 1 to entry: Is also responsible to write specific configuration data such as Device parameters or group tables to the Devices.

3.1.25
MaC Project
Project created by a Management Client documenting the Configuration of an Installation

3.1.26
Message Broker
entity that is receiving messages from publishers and providing it to interested subscribers, the defining characteristic is that the broker itself is a discrete service

3.1.27
MQTT
Message Queuing Telemetry Transport publish-subscribe-based messaging Protocol, standardized as ISO/IEC 20922

3.1.28
Non-IoT HBES
HBES TP, RF, PL and KNXnet/IP protocol for transport of HBES data, in this standard colloquially also used as synonym for an HBES System without any HBES IoT Devices

3.1.29
Ontology
conceptual descriptions of things that have a real-world commonality sharing the knowledge of a domain, mainly expressed with OWL

Note 1 to entry: Are a structured way to describe the meaning of data in ontology classes and should not be mixed up with common data model structures.

3.1.30
OWL
Web Ontology Language, informally OWL 2, specified by the World Wide Web Consortium (W3C), mainly serialized with XML syntax for RDF (RDF/XML)

Note 1 to entry: In this specification the abbreviation OWL is always an explicit reference to OWL 2.

3.1.31
Point
represents an interface to data in the system

Note 1 to entry: In this standard the term Point is used as an umbrella for data that can be accessed from outside the Device, for instance to interact with other Points from other Devices, hence the term is a generic superset of the term Datapoint (describing more precisely the technics how the “data” in the system are structured and/or coded).

3.1.32
Point API
simple RESTful (CoAP or HTTP) application programming interface designed for, but not limited to, constrained class 2 devices [RFC 7228] supporting device individualization, device linking and accessing device runtime data (e.g., Functional Block or Channel Datapoints)

3.1.33
Publisher
entity that is sending messages to a Message Broker

3.1.34
Recipient
entity that is receiving messages from a Publisher

Note 1 to entry: If the Recipient is not Subscriber at the same time, then the Recipient endpoint needs to be a fixed configuration in the Publisher group table.

3.1.35
RDF
framework to represent information in the web by using triples, which can be serialized and stored in many formats

Note 1 to entry: Fomats such as the TURTLE or JSON(-LD) are described under https://www.w3.org/TR/rdf11-concepts/

3.1.36
Registrar
entity that is a service representative of a certain domain, configured to decide whether a new device is allowed to join the domain

3.1.37
Runtime
process-to-process communication of data between Devices, opposing to Configuration

Note 1 to entry: Concerns mainly the communication of Datapoint values (control and status information).

3.1.38
Security Zone
group of devices that all make use of the same Trust Anchor

3.1.39
Sensor
Point in HBES IoT, performing an observation (executed by a specific procedure, triggered by a stimulus), responding a result as an Installation state during Runtime

3.1.40
Subscriber
HBES IoT device receiving messages from a Message Broker

3.1.41
Tag
kind of annotation term used to extend available data with (in most cases) well known standardized information from a dictionary (in contrast to user defined, arbitrary term)

3.1.42
Thing Description
semantic metadata model to describe (abstract or physical) things, as specified by the thing description https://www.w3.org/TR/wot-thing-description/ and thing Ontology https://www.w3.org/2019/wot/td

3.1.43
Trust Anchor
authoritative entity for which trust is assumed and not derived (e.g. an X.509 root certificate)

3.1.44
X.509
certificate format

3.2 Abbreviations

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

AEAD	Authenticated Encryption with Additional Data
AL	Application Layer
AMQP	Advanced Message Queuing Protocol
AP	Access Point
API	Application Programming Interface
BLE	Bluetooth Low Energy
BRSKI	Bootstrapping Remote Secure Key Infrastructure
C	Conditional
CBOR	Concise Binary Object Representation
CoRE	Constraint RESTful Environments
COSE	CBOR Object Signing and Encryption
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CWT	CBOR Web Token
DAD	Duplicate Address Detection
DNS	Domain Name System
DNS-SD	Domain Name System Service Discovery
DB	Database
DER	Distinguished Encoding Rules
DTLS	Datagram Transport Layer Security
EST	Enrollment over Secure Transport
FQDN	Fully Qualified Domain Name
GA	Group Address
GO	Group Object
FB	Functional Block
FP	Function Point
HBES	Home and Building Electronic Systems
HKDF	Hash-based Key Derivation Function

HMAC	Hash-Based Message Authentication Code
IANA	Internet Assigned Numbers Authority
IOO	Info On off
IO	Input Output
IP	Internet Protocol
IoT	Internet of Things
JSON	JavaScript Object Notation
KDC	Key Distribution Center
KDF	Key Derivation Function
KNXA	KNX Association
KDC	Key Distribution Center
LLA	Link Local Address
LRI	Logical Resource Identifier
LSM	Load State Machine
LTE	Logical Tag Extended
M	Mandatory
MaC	Management Client
MAC	media access control address
MQTT	Message Queuing Telemetry Transport
NB	Narrow Band
NFC	Near Field Communication
O	Optional
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OSCORE	Object Security for Constrained RESTful Environments
OSV	Out of Service
OT	Operational Technology
PAKE	Password Authenticated Key Exchange
PASE	Password Authenticated Session Establishment
PBKDF	Password-based Key Derivation Function
PSK	Pre-shared Key
PTR	Pointer
QR	Quick Response
RD	Resource Directory
RDF	Resource Description Framework
RT	Resource Type
SAN	Subject Alternative Name
S-Mode	System Mode
SP	Sleep Period

SRP	Service Registration Protocol
SSM	Source-Specific Multicast
TCP	Transport Control Protocol
TD	Thing Description
TOFU	Trust on First Use
UDP	User Datagram Protocol
ULA	Unique Local Address
URN	Uniform Resource Name
URI	Uniform Resource Identifier
REST	Representational State Transfer
W3C	World Wide Web Consortium
WoT	Web of Things
WPAN	Wireless Personal Area Network

4 HBES IoT Point API

4.1 Introduction

HBES IoT uses Internet Protocol (IP) suite standards for the transmission of HBES IoT application layer data across IP networks.

Physical media like Ethernet (IEEE 802.3), Wi-Fi (802.11), or WPAN (802.15.4) carry HBES IoT packets. These may contain unicast TCP or UDP frames or multicast UDP frame transmission of HBES IoT application data. HBES IoT application data is agnostic to the underlying communication layers. Hence, it is possible to send HBES IoT messages over non-IP transport bindings such as NB IoT, or BLE. However, this is out-of-scope of this standard.

A typical (IP-based) interworking infrastructure allows heterogeneous data link media to work seamlessly with each other. The Point API maps HBES AL data to a RESTful resource model, and CBOR/JSON-based data representation is used to communicate over IP. Using this API, a client can read/write values or subscribe to Point events (e.g., switch on/off). The HBES IoT Point API is based on the following building blocks:

- **Discovery**

Discovery (of resources, including devices) can be made with unicast or multicast. Resource discovery in CoAP (CoRE) is accomplished using a "/.well-known/core" resource URI that returns a list of links about resources (e.g., *Functional Block* Properties) hosted by that server that matches filter attributes.

- **S-Mode Messaging**

The S-Mode messaging uses a secure message-oriented communication pattern for group communication where a producer sends a message to notify consumers of a change in the domain. A tool, or rather a Management Client (MaC), configures group communication events via group tables.

- **Point Read, Write, and Publish/Subscribe**

Parameter and diagnostic Properties are used for sensor, actuator, parameter, and diagnostic values, such as getting the current sensor value or setting a setpoint. They are addressed by URIs, can be directly accessed with the corresponding standard CoAP access method GET (read values), and can be manipulated with PUT/POST (write values). Additionally, also subscribing to Property values is possible.

- **Security**