

STN	Elektronické systémy pre byty a budovy (HBES) Časť 4-4: HBES IoT Point API	STN EN 50090-4-4 36 8051
------------	---	--

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

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 08/25

Obsahuje: EN 50090-4-4:2025

140903



EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 50090-4-4

May 2025

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 IoT HBES

Elektrische Systemtechnik für Heim und Gebäude (ESHG) -
Teil 4-4: ESHG IoT Point API

This European Standard was approved by CENELEC on 2025-04-16. 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.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists 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.



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

EN 50090-4-4:2025 (E)**Contents**

Page

European foreword.....	4
1 Scope	5
2 Normative references	5
3 Terms, definitions and abbreviations.....	6
3.1 Terms and definitions	6
3.2 Abbreviations.....	11
4 HBES IoT Point API	13
4.1 Introduction	13
4.2 System entities	14
4.3 Device Model.....	15
4.4 Conventions used in this document.....	17
5 Point API Standard	17
5.1 Application Protocol.....	17
5.2 Overview	17
5.3 System Design	20
5.4 Device Bootstrapping and Configuration	23
5.5 Resource Model.....	27
5.6 Runtime Interworking.....	75
6 Security.....	100
6.1 Introduction	100
6.2 Device Identity Enrollment.....	100
6.3 Device Identity Certificates.....	105
6.4 Certificate Validation	107
6.5 Device Access Control.....	108
6.6 OSCORE Application Layer Security.....	115
7 Software Update	136
7.1 Introduction	136
7.2 Software Update Client Resource (swu)	137
7.3 Software Update Modes	141
8 Profiles.....	151
8.1 HBES IoT Point API Device.....	151
8.2 CBOR Encoding.....	157
9 Examples	158
9.1 Device point list examples.....	158
9.2 Device configuration example.....	162
9.3 Data encryption/decryption example.....	170
10 HBES IoT Router	173
10.1 Introduction	173
10.2 Conformance.....	174
10.3 Number Format	174
10.4 Uniform Resource Identifiers	174
10.5 Uniform Resource Name.....	174
10.6 HBES IoT Router Specification	174
10.7 Runtime Interworking.....	182
10.8 Profiles.....	184

10.9 Security187
10.10 Examples187
Bibliography190

EN 50090-4-4:2025 (E)**European foreword**

This document (EN 50090-4-4:2025) has been prepared by CLC/TC 205 "Home and Building Electronic Systems (HBES)".

The following dates are fixed:

- latest date by which this document has to be (dop) 2026-05-31
implemented at national level by publication of
an identical national standard or by
endorsement
- latest date by which the national standards (dow) 2028-05-31
conflicting with this document have to be
withdrawn

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.

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

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 22510:2019)*

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 Format*

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, *Multicast 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*

EN 50090-4-4:2025 (E)

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 Application 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 Management 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)*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN