



NSAI
Standards

Irish Standard
I.S. EN 50090-3-4:2017

Home and Building Electronic Systems (HBES) - Part 3-4: Secure Application Layer, Secure Service, Secure configuration and security Resources

I.S. EN 50090-3-4:2017

Incorporating amendments/corrigenda/National Annexes issued since publication:

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard — national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation — recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

This document replaces/revises/consolidates the NSAI adoption of the document(s) indicated on the CEN/CENELEC cover/Foreword and the following National document(s):

NOTE: The date of any NSAI previous adoption may not match the date of its original CEN/CENELEC document.

This document is based on:

EN 50090-3-4:2017

Published:

2017-08-25

*This document was published
under the authority of the NSAI
and comes into effect on:*

2017-09-12

ICS number:

97.120

NOTE: If blank see CEN/CENELEC cover page

NSAI
1 Swift Square,
Northwood, Santry
Dublin 9

T +353 1 807 3800
F +353 1 807 3838
E standards@nsai.ie
W NSAI.ie

Sales:
T +353 1 857 6730
F +353 1 857 6729
W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

National Foreword

I.S. EN 50090-3-4:2017 is the adopted Irish version of the European Document EN 50090-3-4:2017, Home and Building Electronic Systems (HBES) - Part 3-4: Secure Application Layer, Secure Service, Secure configuration and security Resources

This document does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

For relationships with other publications refer to the NSAI web store.

Compliance with this document does not of itself confer immunity from legal obligations.

In line with international standards practice the decimal point is shown as a comma (,) throughout this document.

This page is intentionally left blank

EUROPEAN STANDARD

EN 50090-3-4

NORME EUROPÉENNE

EUROPÄISCHE NORM

August 2017

ICS 97.120

English Version

Home and Building Electronic Systems (HBES) - Part 3-4: Secure Application Layer, Secure Service, Secure configuration and security Resources

Systèmes électroniques pour les foyers domestiques et les
bâtiments (HBES) - Partie 3-4 : Spécification des KNX S
AL, Service sécurisé, configuration sécurisée et Ressources
en matière de sécurité

Elektrische Systemtechnik für Heim und Gebäude (ESHG) -
Teil 3-4: Informationssicherheit auf Anwendungsschicht,
Dienste, Konfiguration und Ressourcen

This European Standard was approved by CENELEC on 2017-06-12. 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, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, 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: Avenue Marnix 17, B-1000 Brussels

Contents

Page

European foreword	3
Introduction	4
1 Scope	5
2 Normative references	5
3 Terms, definitions and abbreviations	5
3.1 Terms and definitions	5
3.2 Abbreviations	7
4 General Introduction (informative)	7
4.1 General	7
4.2 General Overview	11
5 Specification	12
5.1 Stack and communication	12
5.2 Resource definition or used Resources	50
Annex A (informative) Use of CCM	52
A.1 Goal	52
A.2 Definitions	52
A.3 CCM operation	52
Annex B (informative) Examples — Full encoding of a HBES Secure APDU	57
B.1 General	57
B.2 S-A_Data-PDU	57
B.3 S-A_Data-PDU	58
B.4 S-A_Sync.req	59
B.5 S-A_Sync.res	60
Bibliography	62

European foreword

This document (EN 50090-3-4:2017) 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) 2018-06-12
implemented at national level by publication of an
identical national standard or by endorsement
- latest date by which the national standards conflicting (dow) 2020-06-12
with this document have to be withdrawn

EN 50090-3 is composed with the following parts:

- EN 50090-3-1, *Home and Building Electronic Systems (HBES) — Part 3-1: Aspects of application — Introduction to the application structure*;
- EN 50090-3-2, *Home and Building Electronic Systems (HBES) — Part 3-2: Aspects of application — User process for HBES Class 1*;
- 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 50090-3-4, *Home and Building Electronic Systems (HBES) — Part 3-4: Secure Application Layer, Secure Service, Secure configuration and security Resources*.

Introduction

KNX Association as Cooperating Partner to CENELEC confirms that to the extent that the standard contains patents and like rights, the KNX Association's members are willing to negotiate licenses thereof with applicants throughout the world on fair, reasonable and non-discriminatory terms and conditions.

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

CEN and CENELEC maintain online lists of patents relevant to their standards. Users are encouraged to consult the lists for the most up to date information concerning patents (<ftp://ftp.cenelec.eu/EN/IPR/Patents/IPRdeclaration.pdf>).

1 Scope

This European Standard defines security for Home and Building HBES Open Communication System. It is based on ISO/IEC 24767-2, Home network security / Secure Communication Protocol Middleware (SCPM).

Having a secure HBES solution has several advantages.

- It makes the HBES RF Communication Medium more secure:

HBES RF Radio Frames in plain communication can easily be traced (by sniffer for example).

- It allows for secure applications.

Secure communication is interesting in shutter – and door control and anti-intrusion security, in order to prevent intrusive commands (burglars...).

It is also interesting in metering to protect for example electrical consumption data.

This document does not define any type of application.

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

EN 50090-3-2, *Home and Building Electronic Systems (HBES) - Part 3-2: Aspects of application - User process for HBES Class 1*

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*

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.

3.1.1

Access Control

definition and evaluation of which communication partner has the right to access which data or call which services, which is solved by collecting communication partners with the same rights for all data and services in Roles and defining for each Role and for each piece of data or service the Permissions that this Role has

3.1.2

Security Black List

standard list of services or DPs that shall exclusively be accepted using HBES Secure communication using confidentiality

This is a free preview. Purchase the entire publication at the link below:

[Product Page](#)

-
- Looking for additional Standards? Visit Intertek Inform Infostore
 - Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation
-