ISO/IEC 15045-3-1

Edition 1.0 2024-12

INTERNATIONAL STANDARD

colour inside

Information technology – Home Electronic System (HES) gateway – Part 3-1: Privacy, security, and safety – Introduction



ISO/IEC 15045-3-1:2024-12(en)

THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2024 ISO/IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about ISO/IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

ISO/IEC 15045-3-1

Edition 1.0 2024-12

INTERNATIONAL STANDARD

colour inside

Information technology – Home Electronic System (HES) gateway – Part 3-1: Privacy, security, and safety – Introduction

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 35.200; 35.240.99

ISBN 978-2-8327-0002-0

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD 4
INTRODUCTION 6
0.1 Overview 6
0.2 Relation to existing work 6
0.3 Relevant affected stakeholder categories 7
1 Scope 9
2 Normative references 9
3 Terms, definitions and abbreviated terms 9
3.1 Terms and definitions 9
3.2 Abbreviated terms 11
4 Conformance 11
5 Protection of privacy, security, and safety 11
5.1 Privacy, security and safety concepts and principles in the HES gateway 11
5.2 Structural protections provided by the HES gateway system 11
5.3 Interface and application services protections 12
5.3.1 Key concepts, principles and practices 12
5.3.2 HES concept 12
5.3.3 HES gateway concept 12
5.3.4 Interface module concept 13
5.3.5 Service module concept 13
5.3.6 Application platform concept 13
5.3.7 Internal communication bus concept 13
5.3.8 DSS principle and practice 13
5.4 Operational protections 14
5.5 Risk management 14
5.5.1 Overview 14
5.5.2 Risk assessment 14
5.5.3 Risk treatment 27
5.6 Privacy, security, and safety guidelines and requirements 28
5.6.1 Privacy-by-design approach 28
5.6.2 External services non-reliance principle and practice 28
5.6.3 Use of wireless or shared media principle and practice 28
5.6.4 Privacy best practice 29
5.6.5 Privacy next best practice 29
5.6.6 Online update vulnerability principle 29
5.6.7 Online OS update vulnerability principle 29
5.6.8 "Social engineering" vulnerability principle 29
5.6.9 Privacy-by-design principle and practice 29
5.6.10 User priority principle 29
5.6.11 Fail-safe principle 30
5.6.12 Precautionary principle 30
5.6.13 Normal accident principle 30
5.6.14 Privacy principles 30
5.6.15 Watchdog practice 30
5.6.16 Redundancy principle 30
6 Common services 30

6.1 Common services 30
6.2 Binding map 31
6.3 HES gateway unique ID service module 31
6.4 Cryptographic services 31
6.5 Authorization and authentication service 31
6.6 Time service 32
Annex A (informative) Privacy protection principles and sources 33
A.1 Privacy protection principles 33
A.2 Sources 33
Annex B (informative) Guidance to developers 35
B.1 General protection 35
B.2 Privacy protection 35
B.3 Security protection 36
B.4 Safety protection 36
Bibliography 38

Figure 1 – ISO/IEC 15045-3-1 within the core interoperability and HES gateway standards 8
Figure 2 – HES gateway generalized architecture 12
Figure 3 – Risk assessment diagram 15
Figure 4 – HAN masquerade and replay 16
Figure 5 – WAN masquerade and replay 17
Figure 6 – HAN interception: eavesdropping and modification 18
Figure 7 – WAN interception: eavesdropping and modification 20
Figure 8 – HAN denial-of-service and resource-exhaustion attack 21
Figure 9 – WAN denial-of-service and resource-exhaustion attack 22
Figure 10 – Worm, virus or Trojan horse 23
Figure 11 – Risk level for HAN: example 26
Figure 12 – Risk level of data inside user objects: example 27
Figure 13 – Risk treatment and risk assessment flow 28
Figure A.1 – Primary sources for privacy protection principles 34

INFORMATION TECHNOLOGY – HOME ELECTRONIC SYSTEM (HES) GATEWAY –

Part 3-1: Privacy, security, and safety – Introduction

FOREWORD

1) ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.
2) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC and ISO National bodies.
3) IEC and ISO documents have the form of recommendations for international use and are accepted by IEC and ISO National bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC and ISO documents is accurate, IEC and ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC and ISO National bodies undertake to apply IEC and ISO documents transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC and ISO document and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC and ISO do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC and ISO marks of conformity. IEC and ISO are not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this document.
7) No liability shall attach to IEC and ISO or their directors, employees, servants or agents including individual experts and members of its technical committees and IEC and ISO National bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this ISO/IEC document or any other IEC and ISO documents.
8) Attention is drawn to the Normative references cited in this document. Use of the referenced publications is indispensable for the correct application of this document.
9) IEC and ISO draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC and ISO take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC and ISO had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch and www.iso.org/patents. IEC and ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 15045-3-1 has been prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology. It is an International Standard.

The text of this International Standard is based on the following documents:

Draft	Report on voting
JTC1-SC25/3189/CDV	JTC1-SC25/3260/RVC

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1, and the ISO/IEC Directives, JTC 1 Supplement available at www.iec.ch/members_experts/refdocs and www.iso.org/directives.

A list of all parts in the ISO/IEC 15045 series, published under the general title *Information technology – Home Electronic System (HES) gateway*, can be found on the IEC and ISO websites.

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

0.1 Overview

The Home Electronic System (HES) is a set of standards that supports communications, control, and monitoring applications for homes and buildings. However, homes and buildings present a heterogeneous and evolving networked environment, where many of these networks and applications (including some that are based on HES standards) are not directly interoperable with each other. HES standards achieve interoperability through the ISO/IEC 15045 series, which relies on the ISO/IEC 18012 series to support functional interworking among the dissimilar home devices, applications, protocols, and networks found in this environment. The ISO/IEC 15045 series and ISO/IEC 18012 series were created to render all protocols interoperable.

The HES gateway enables an open and adaptable market for incompatible products by specifying a standardized modular system intended to provide interoperability among the diversity of networks found in homes and buildings. The HES interoperability process does not require modification of the various networks, applications, or protocols that use it. Appropriate interworking functions translate network messages through interface modules to a common lexicon expression that is then exchanged using a private internal network bus protocol. A protected application platform using a bus protocol supports an expanding array of services for both the application and the network.

In summary, the ISO/IEC 15045 series specifies a standardized modular dedicated private internal network system that includes:

– interfaces (i.e. interface modules) for communication and semantic translation among dissimilar home area networks (HANs), and between a HAN and external wide area networks (WANs),

– a platform for supporting a variety of application services (i.e. service modules), and

– a secure communication path among these modular elements with access restricted to the appropriate elements in order to protect data, safety and privacy.

0.2 Relation to existing work

ISO/IEC 15045-1 identifies a range of threats relating to privacy, security, and safety in general terms. ISO/IEC 15045-2 specifies the underlying architecture for the HES gateway. However, neither part provides specific privacy, security and safety requirements for HES gateway conformance. ISO/IEC 15045-3-1 (this document) introduces the privacy, security, and safety standards and requirements that are applicable to the HES gateway in order to protect the interest of consumers within the home and small office environments. This document also describes the inter-relationships among the overlapping topics of privacy, security, and safety.

This document anticipates and introduces the series of additional Part 3 subparts dealing with specific aspects of privacy (ISO/IEC 15045-3-2), security (ISO/IEC 15045-3-3), and safety (ISO/IEC 15045-3-4).

The purpose of the ISO/IEC 15045-3 series requirements is to specify methods for protecting home and building systems from both internal and external threats, intrusions, or unintended observation of data and unsafe conditions that can result from network functions. The ISO/IEC 15045-3 series specifies a set of basic and advanced requirements for gateway monitoring and control of both inbound and outbound traffic, including switching, routing, addressing, encryption, intrusion detection and prevention, and other "firewall" functions.

The ISO/IEC 15045-3 series requirements specify the following functions:

a) prevention of active inbound attacks and unsafe commands;

b) discovery and classification of outbound traffic;

c) management of privacy and security mechanisms;

d) blocking unauthorized HAN and WAN services and devices from communicating with internal networks and with each other;

e) enabling and managing authorized HAN and WAN services and devices including certification and other similar processes;

f) provision for a management and reporting dashboard for use by a non-technical end-user.

Devices or other entities communicating with each other but not on the same HAN use the HES gateway.

0.3 Relevant affected stakeholder categories

Manufacturers and vendors of smart home devices and other electrical or electronic products and appliances in the home and building systems market will be able to make and offer interoperable products with the benefit of a private, secure, and safe HES environment. Conformity with HES gateway interoperability, privacy, security, and safety requirements can create significant market synergy, expand the available range of applications, and serve the interests of consumers, manufacturers, vendors, and society as a whole. Specifically, this document, together with other parts in the ISO/IEC 15045-3 series, will ensure the privacy, security, and safety of personal and premises information in the emerging economy of devices connected to online services.

Figure 1 shows the core interoperability and HES gateway series of standards and where this document fits into the HES gateway series.

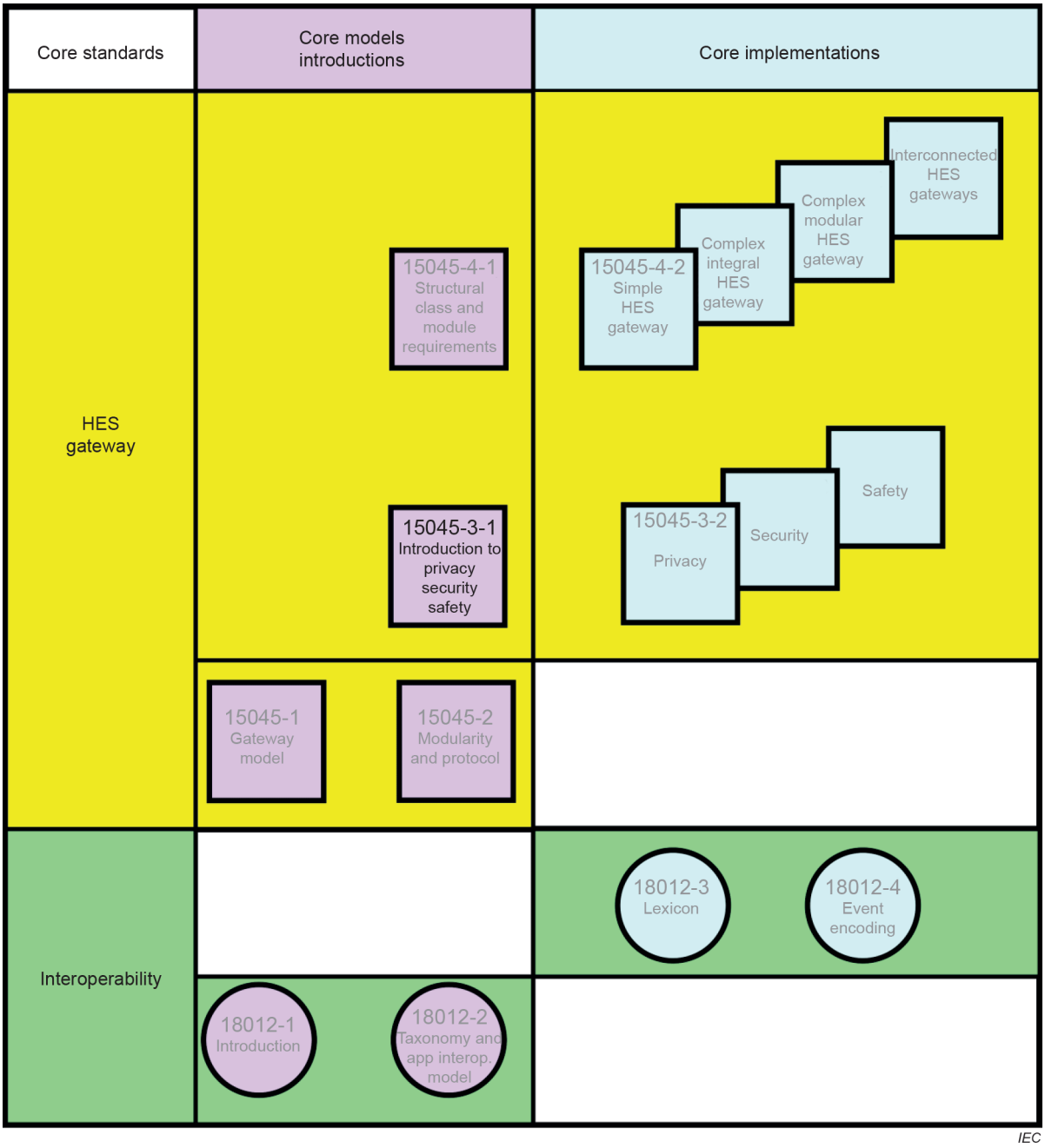


Figure 1 – ISO/IEC 15045-3-1 within the core interoperability and HES gateway standards

INFORMATION TECHNOLOGY – HOME ELECTRONIC SYSTEM (HES) GATEWAY –

Part 3-1: Privacy, security, and safety – Introduction

1 Scope

This document specifies the architectures for the HES gateway related to protection of privacy, security and safety of communications between different networks. It also offers guidelines for HES gateway implementations, interfaces, and application services regarding privacy, security and safety. Such HES gateway guidelines include suggested approaches, choices, or recommended practices. Further, it identifies some areas of vulnerability to be addressed and offers relevant categories or use cases.

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.

ISO/IEC 15944-8:2012, *Information technology – Business Operational View – Identification of privacy protection requirements as external constraints on business transactions*

ISO/IEC 29100, *Information technology – Security techniques – Privacy framework*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology 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
home area network
HAN
network serving nodes, devices, components and functions within a premises protected area

3.1.2
home electronic system
HES
control and sensing system for homes and buildings based on home electronic system (HES) ISO/IEC standards

Note 1 to entry: The referenced ISO/IEC standards normally include HES in the title of each standard.