ISO/IEC 15045-3-2

Edition 1.0 2024-10

INTERNATIONAL STANDARD

colour inside

Information technology - Home Electronic System (HES) gateway – Part 3-2: Privacy, security, and safety – Privacy framework

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

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

ISO/IEC 15045-3-2

Edition 1.0 2024-10

INTERNATIONAL STANDARD

colour inside

Information technology - Home Electronic System (HES) gateway – Part 3-2: Privacy, security, and safety – Privacy framework

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 35.200; 35.240.99

ISBN 978-2-8322-9880-0

CONTENTS

INFORMATION TECHNOLOGY – HOME ELECTRONIC SYSTEM (HES) GATEWAY –

Part 3-2: Privacy, security, and safety – Privacy framework

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 15045-3-2 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-SC25/3190/CDV	JTC1-SC25/3261/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 communication, 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 applications 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

The concepts of product interoperability are introduced in ISO/IEC 18012-1. The interworking function (IWF) is specified in ISO/IEC 18012-2. The message content, including applications, interface and service objects will be specified in ISO/IEC 18012-3. The method and format of communication packet exchanges or direct API exchanges within a gateway will be specified in ISO/IEC 18012-4.

0.3 Privacy in HES gateway

The HES gateway is described in ISO/IEC 15045-1. Several structural configurations of the HES gateway are described in ISO/IEC 15045-4-1. All structural classes use the HES interoperability system described above. However, for classes that use physically separated modules, communication among modular elements is provided by a dedicated private serial bus (i.e. Ethernet) and utilizes a set of protocols now known as the common language internal protocol (CLIP), originally called the GL bus in ISO/IEC 15045-2. All HES gateway structural class configurations use the same interworking functions, including lexicon, and event encoding.

Privacy, security and safety requirements for the HES gateway are specified in ISO/IEC 15045-3-1. ISO/IEC 15045-3-2 (this document) provides specifications that fulfil the privacy requirements of ISO/IEC 15045-3-1. These privacy considerations are based upon ISO/IEC 29100.

The privacy aspects in this document are focused on individual premises, and not focused on apartment complexes or multi-family dwellings. Such situations are handled with "interconnected gateways" structural class. A future part of the ISO/IEC 15045-4 series will detail the privacy considerations and enhancements relating to these types of dwellings.

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

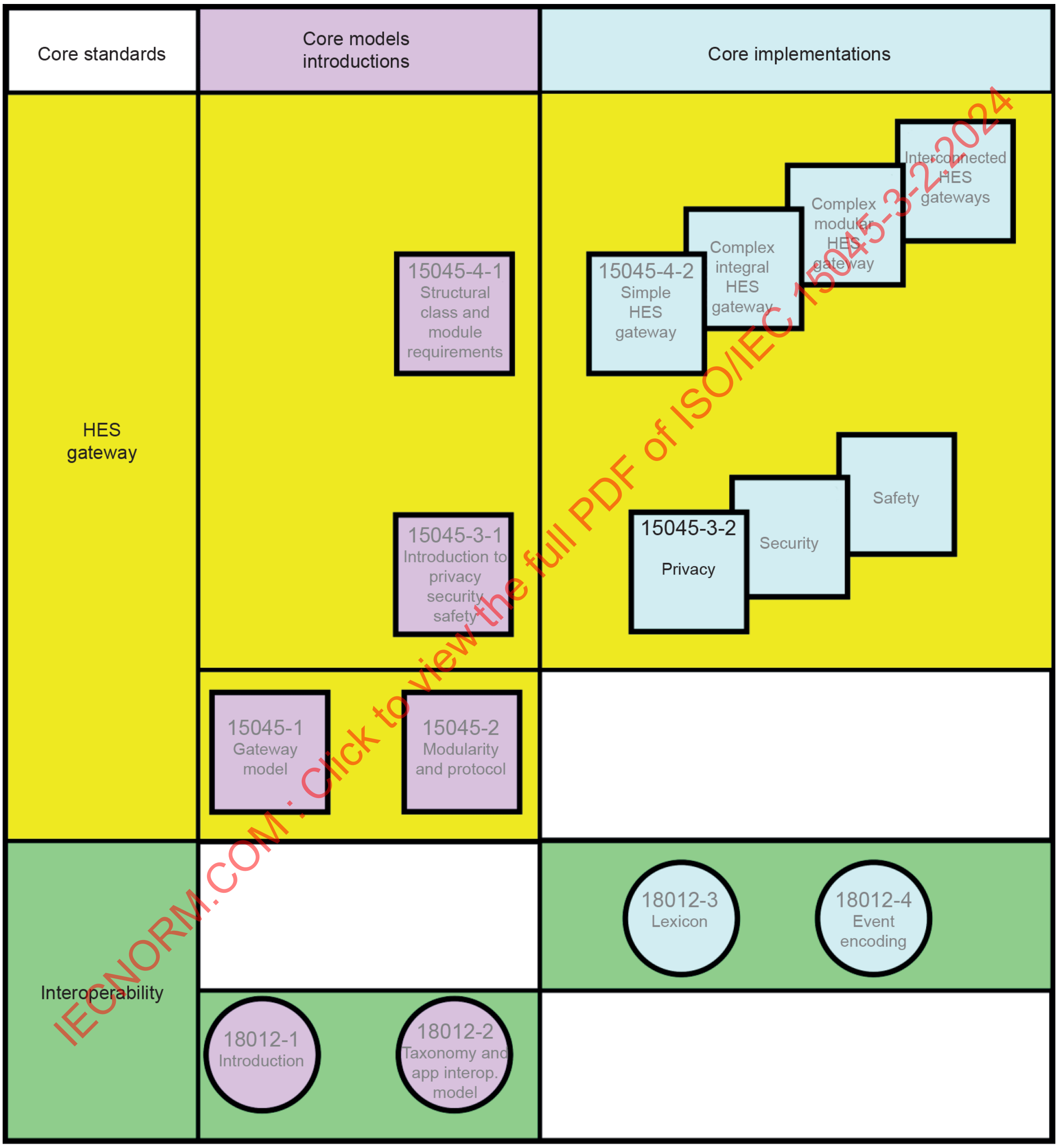
Core standards
Core models introductions
Core implementations
HES gateway
Interoperability
15045-4-1 Structural class and module requirements
15045-3-1 Introduction to privacy security safety
15045-1 Gateway model
15045-2 Modularity and protocol
15045-4-2 Simple HES gateway
Complex integral HES gateway
Complex modular HES gateway
Interconnected HES gateways
15045-3-2 Privacy
Security
Safety
18012-3 Lexicon
18012-4 Event encoding
18012-1 Introduction
18012-2 Taxonomy and app interop. model
IEC

Figure 1 – ISO/IEC 15045-3-2 within the core interoperability and HES gateway standards

0.4 Future features

The HES gateway is structured to provide a foundation upon which features can be added as appropriate while maintaining the privacy, security, safety and interoperability capabilities. The interoperable objects, domains and services defined in the HES Lexicon can be expanded.

INFORMATION TECHNOLOGY –
HOME ELECTRONIC SYSTEM (HES) GATEWAY –

Part 3-2: Privacy, security, and safety – Privacy framework

1 Scope

This document specifies cybersecurity requirements for protecting the privacy of premises and personally identifiable information through the use of the HES gateway and related HES standards. This document applies a set of principles including those specified in ISO/IEC 29100 that are applicable to the HES gateway such as consent, purpose legitimacy, collection limitation, data minimization, retention, accuracy, openness, and individual access.

2 Normative references

There are no normative references in this document.

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
binding map
table that links inputs to outputs

3.1.2
controller service module
HES gateway service module that performs setup and configuration

Note 1 to entry: This module is similar to the "PII controller" in ISO/IEC 29100.

3.1.3
HES gateway
electronic device that transfers messages among WANs and HANs providing interoperability, privacy, security and safety in accordance with the requirements of the ISO/IEC 15045 series and ISO/IEC 18012 series standards

Note 1 to entry: For an HES gateway, a WAN is a network outside the protected area and a HAN is a network inside the protected area.

[SOURCE: ISO/IEC 15045-3-1:2024, 3.1.3]

3.1.4
HES gateway system
HES gateway use case with specific in-premises networks and devices, and potentially off-premises networks

[SOURCE: ISO/IEC 15045-3-1:2024, 3.1.4]

3.1.5
home electronic system
HES
collection of devices and components operating within the premises and interconnected over one or more networks, in conformance with HES-related ISO/IEC standards

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

[SOURCE: ISO/IEC 15045-3-1:2024, 3.1.2]

3.1.6
home electronic system common language message exchange
HES-CLME
protocol for messaging among HES gateway modules

3.1.7
local
logically situated within the premises

[SOURCE: ISO/IEC 15045-3-1:2024, 3.1.5]

3.1.8
PPII third party
entity or person having access to some premises and personally identifiable information (PPII) intended or not by the other parties

3.1.9
premises and personally identifiable information
PPII
information associated with a premises or an individual that can be identified or linked to the premises or individual

3.1.10
privacy
freedom from being observed or disturbed

[SOURCE: ISO/IEC 15045-3-1:2024, 3.1.6]

3.1.11
processor service module
HES gateway service module that operates real time functions

Note 1 to entry: This module is similar to the "PII processor" in ISO/IEC 29100.

3.1.12
remote
logically situated outside the premises

[SOURCE: ISO/IEC 15045-3-1:2024, 3.1.7]

3.1.13
user
natural person

[SOURCE: ISO/IEC 15045-3-1:2024, 3.1.11]

3.2 Abbreviated terms

HAN	home area network
HES	home electronic system
HES-CLME	HES common language message exchange
IP	Internet Protocol
OSI	Open Systems Interconnection
PII	personally identifiable information
PPII	premises and personally identifiable information
WAN	wide area network

4 Conformance

An HES gateway system conforming to this document shall:

- implement the eight key privacy principles listed in 5.4.1, including supporting the HES gateway lexicon indicated for each principle ("conditioning" in 5.4.2, "privacyAudience" in 5.4.5, etc.), and
- implement those features required for the specific system-application configuration, including protection mechanisms, to cover at least one of the scenarios described in Clause B.1. It shall also declare which of these scenarios it supports.

5 Considerations, architecture and requirements

5.1 Overview

This document outlines the architecture of the HES gateway system as it relates to privacy. This document specifies mechanisms for how the gateway can protect information from entering the premises from unauthorized users or leaving the premises to unauthorized users.

This document also specifies how gateway service modules can aid in privacy protection, both for outgoing communication and for incoming communications, such as spam. It can be used to protect children from accessing sensitive information as determined, for example, by their parents.

Figure 2 shows how the HES gateway system operates within the premises and shows the extent of the HES gateway as covered by the ISO/IEC 15045 and ISO/IEC 18012 series of standards, and the communications between the key modules.

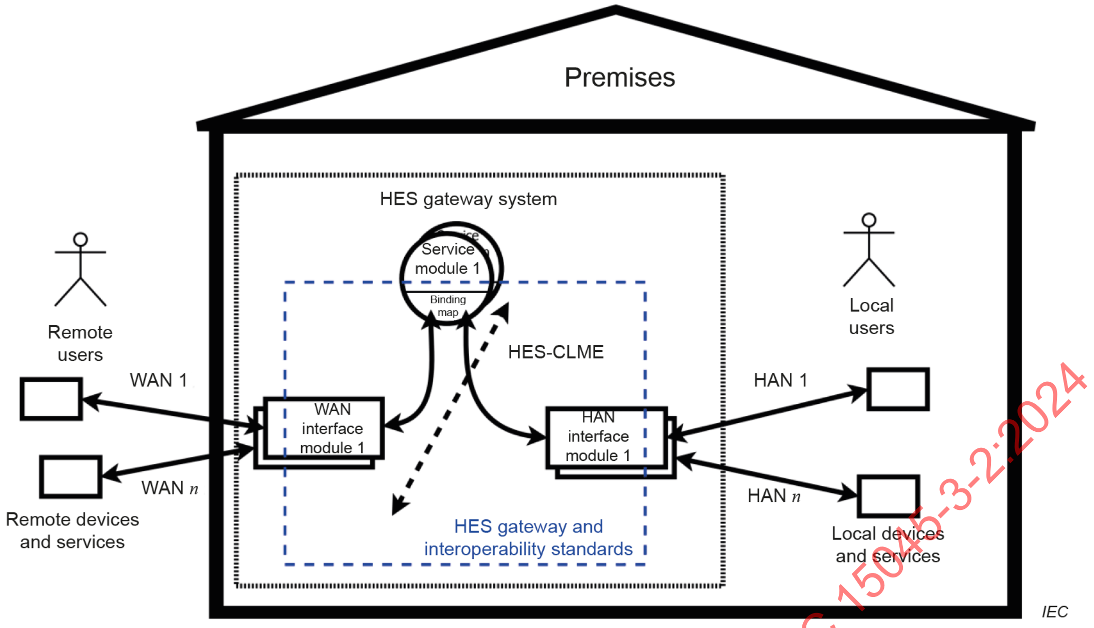

Figure 2 – HES gateway architecture for privacy

HAN and WAN interface modules translate messages from their native HAN or WAN protocol to messages using interoperable objects on the HES gateway internal bus or translate messages from the bus to the native HAN or WAN protocols. This message exchange is called home electronic system common language message exchange (HES-CLME). HAN or WAN interface modules communicate these objects with each other using HES-CLME only via the binding map service, which is part of a service module.

The binding map functions required for privacy protection are specified in this document. The flow of private information in the gateway is managed by one or more binding maps associated with any given application service. The use of multiple binding maps can provide redundancy. A binding map associates inputs with outputs (or sources with destinations), within the gateway. It is up to the application developer (i.e. the software programmer that deals with the desired application service) to use this binding resource properly to control the flow of information within the constraints imposed by 1) the privacy principles, and 2) the particular user and service provider terms of agreement. The default action is to protect the user and the private information.

The HES gateway provides special features to a premises in addition to those of a conventional gateway, including support for interoperability and cybersecurity, protection of data, privacy and safety. Communications involving end-to-end encryption are not able to use these additional services, but in the future limited services can be provided.

To clarify, the premises can have both conventional gateways and HES gateways.

5.2 Premises and personally identifiable information (PPII)

ISO/IEC 29100:2011 specifies several concepts that have been adopted in this document. In particular, it specifies the concept of personally identifiable information (PII)[1]. This document extends the concept of PII by adding information that is or can be directly or indirectly associated with a premises. This premises and personally identifiable information is abbreviated PPII.

[1] See 2.9 in ISO/IEC 29100:2011.

Information like room temperature and power consumption are typical elements of PII premises information that can be misused if seen by unauthorized people.

5.3 PPII parties

A PPII principal is a local device or user that contains or generates information that can be associated with either the building or a resident, and that is not seen by unauthorized users.

A PPII third party is a privacy stakeholder other than 1) the PPII principal, 2) the PPII controller and the PPII processor, and 3) the natural persons who are authorized to process the data. The resident shall instruct the PPII controller for which PPII third parties are authorized to receive the information.

Further provisions are given in Annex B.

5.4 Privacy principles

5.4.1 Privacy principles summary

This HES gateway shall implement the eight key privacy principles summarized in Table 1, which were developed by a number of countries, regions and international organizations. The use of international privacy standards for developing this document is described in Annex C.

NOTE These eight principles are based upon the 11 privacy principles of ISO/IEC 29100:2011, Clause 5.

Table 1 – Summary of HES gateway privacy principles

Section	Privacy principle
5.4.2	Consent and choice
5.4.3	Purpose legitimacy and specification
5.4.4	Collection limitation
5.4.5	Data minimization
5.4.6	Use, retention and disclosure limitation
5.4.7	Accuracy and quality
5.4.8	Openness, transparency and notice
5.4.9	Individual participation and access

In 5.4.2 to 5.4.9, each of the privacy principles is described in detail with reference to how the principle relates to the HES gateway. The mapping of ISO/IEC 29100 to the HES gateway is explained in Annex A.

5.4.2 Consent and choice

NOTE Based upon 5.2 in ISO/IEC 29100:2011.

Most service providers and system implementations do not specify what personal data will be needed until they require the data during enrolment with little or no opportunity for customers to select service options based on data supplied. The HES gateway shall be configurable to block the dissemination of personal data that the user wishes to keep private. This privacy feature in the HES gateway enables users to choose what private data to disclose and what data to keep private. These specifications enable service providers to offer customers a range of services depending on what private data customers are willing to disclose. This is contrasted with the common practice of requiring customers to accept a service provider's privacy policy and requests for personal data in order to use any services.

Adhering to the consent principle means:

- presenting to the local device or user the choice whether or not to allow the processing of their PPII except where the local device or user cannot freely withhold consent or where applicable law specifically allows the processing of PPII without the natural person's consent. The local device or user's choice must be given freely, specific and on a knowledgeable basis;
- informing the local device or user if the default opt-in principle is not possible and, in that case, obtaining the opt-in consent of the local device or user for collecting or otherwise processing sensitive PPII except where applicable law allows the processing of sensitive PPII without the natural person's consent;
- informing the local device or user, before obtaining consent, about their rights under the individual participation and access principle;
- providing the local device or user, before obtaining consent, with the information indicated by the openness, transparency and notice principle; and
- explaining to local device or user the implications of granting or withholding consent.

The local device or user is given the opportunity to choose how their PPII is handled and to allow a local device or user to withdraw consent easily and free of charge. This request is dealt with in accordance with the privacy policy. Even if consent is withdrawn, it is possible that the binding map controller service will retain certain PPII for a period of time in order to comply with legal or contractual obligations (e.g. data retention, accountability). Where the PPII processing is not based on consent but instead on another legal basis, the local device or user should be notified wherever possible. Where the local device or user has the ability to withdraw consent and has chosen to do so, this PPII should be exempted from processing for any purpose not legally mandated.

For a binding map controller service, adhering to the choice principle means:

- providing local device or user with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice and to give consent in relation to the processing of their PPII at the time of collection, first use or as soon as practicable thereafter; and
- implementing the local device or user's preferences as expressed in his or her consent.

Moreover, additional provisions can be specified for processing PPII other than consent (e.g. the performance of a contract, the vital interest of the local device or user, or compliance with the law). Applicable law in some instances provides that the consent of the local device or user does not constitute a sufficient legal basis to process PPII (e.g. the consent of a minor given without a parent or guardian's approval). Moreover, additional requirements on transferring PPII internationally shall be considered. The binding map controller service shall comply with these additional provisions before processing or transferring data.

Not allowing processing of the PPII in the HES gateway is accomplished by setting the "conditioning" (conditioning for input) to "block" in the binding map service. Similarly, allowing processing of the PPII is accomplished by setting the "conditioning" to the appropriate translation value (other than "block"), see Figure 3. The "binding map controller" is used to set up and configure the binding map. The "binding map processor" is used in the real time processing of the messages.

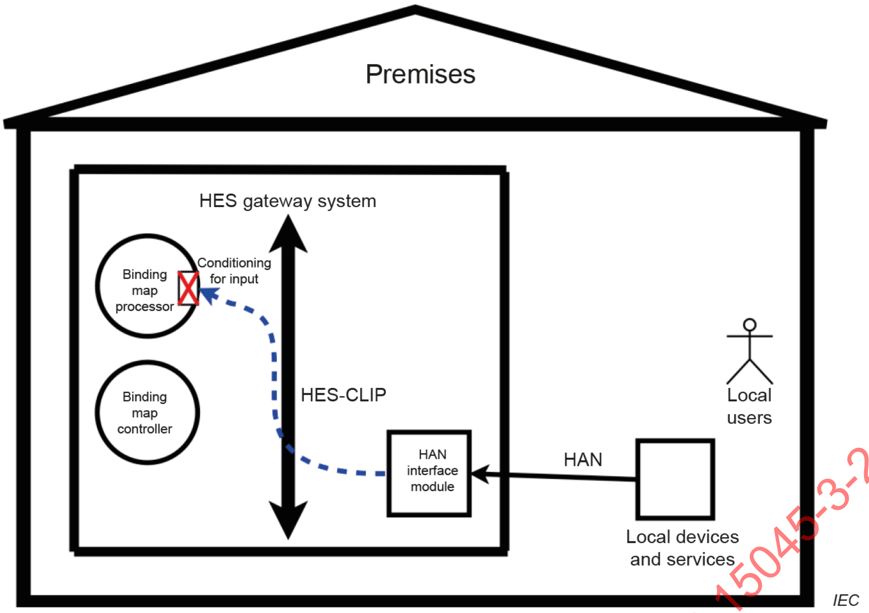

Figure 3 – Conditioning for input of binding map allows blocking of PPII processing

5.4.3 Purpose legitimacy and specification

NOTE Based upon 5.3 in ISO/IEC 29100:2011.

Adhering to the purpose legitimacy and specification principle means:

- ensuring that the purpose or purposes complies with applicable law and relies on a permissible legal basis;
- communicating the purpose or purposes to the local device or user before information is collected or used for the first time for a new purpose;
- using language for this specification that is both clear and appropriately adapted to the circumstances; and
- if applicable, giving sufficient explanations for the need to process sensitive PPII.

With regard to sensitive PPII, stricter rules can apply for the purpose of processing. A purpose can require a legal basis or a specific authorization by a data protection authority or a government authority.

5.4.4 Collection limitation

NOTE Based upon 5.4 in ISO/IEC 29100:2011.

Adhering to the collection limitation principle means:

- limiting the collection of PPII to that which is within the bounds of applicable law and strictly necessary for the specified purpose or purposes.

Organizations should not collect PPII indiscriminately. Both the amount and the type of PPII collected should be limited to that which is necessary to fulfil the legitimate purpose or purposes specified by the binding map controller service. Organizations should carefully consider what PPII will be needed to realize a particular purpose before proceeding with the collection of PPII. Organizations should document the type of PPII collected, as well as their justification for doing so as part of their information-handling policies and practices.

Some binding map controller services wish to collect additional PPII for purposes other than the provision of a particular service requested by the local device or user (e.g. for direct marketing purposes). Depending on the jurisdiction, such additional information is possibly only collected with the consent of the local device or user. It is also possible that the collection of certain information is mandated by applicable law. Whenever possible, the local device or user should be given the ability to choose whether or not to provide such information. The local device or user should also be clearly informed of the fact that his or her response to such requests for additional information can be optional.

5.4.5 Data minimization

NOTE Based upon 5.5 in ISO/IEC 29100:2011.

Data minimization is closely linked to the principle of "collection limitation" but goes further than that. Whereas "collection limitation" refers to limited data being collected in relation to the specified purpose, "data minimization" strictly minimizes the processing of PPII.

Adhering to the data minimization principle means designing and implementing data processing procedures and ICT systems in such a way as to:

- minimize the PPII that is processed and the number of privacy stakeholders and people to whom PPII is disclosed or who have access to it. The intended audience of data is placed in the standardized "privacyAudience" characteristic of the currentValue property. This feature provides filtering for outgoing traffic so that it does not reveal premises secrets to unauthorized persons. In addition, one should filter the incoming traffic to ensure privacy of external services is preserved;
- ensure adoption of a "need-to-know" principle, i.e. one should be given access only to the PPII necessary for the conduct of his or her official duties in the framework of the legitimate purpose of the PPII processing;
- use or offer as default options, wherever possible, interactions and transactions that do not involve the identification of local device or user, reduce the observability of their behaviour and limit the linkability of the PPII collected; and
- delete and dispose of (make impossible to recover) PPII whenever the purpose for PPII processing has expired, there are no legal requirements to keep the PPII or whenever it is practical to do so.

As described in ISO/IEC 15045-3-1, risk is a combination of adverse impact and the likelihood. All three levels – adverse impact, likelihood and risk – are placed in the standardized "adverseImpactLevel", "likelihoodLevel" and "riskLevel" characteristics of the HAN interface module object.

5.4.6 Use, retention and disclosure limitation

NOTE Based upon 5.6 in ISO/IEC 29100:2011.

Adhering to the use, retention and disclosure limitation principle means:

- limiting the use, retention and disclosure (including transfer) of PPII to that which is necessary in order to fulfil specific, explicit and legitimate purposes. The intended purpose of data is placed in the standardized "privacyPurpose" characteristic of the currentValue property;
- limiting the use of PPII to the purposes specified by the binding map controller service prior to collection, unless a different purpose is explicitly required by applicable law;
- retaining PPII only as long as necessary to fulfil the stated purposes, and thereafter securely destroying or anonymizing it (how data is collected and retained is placed in the standardized "collectedDataType" and "collectedDataParameter" characteristics of the currentValue Property; and

- locking (i.e. archiving, securing and exempting the PPII from further processing) any PPII when and for as long as the stated purposes have expired, but where retention is required by applicable laws.

When PPII data are transferred internationally, the binding map controller service shall be programmed to block transfers of PPII data that violate national or local laws on cross-border transfers.

5.4.7 Accuracy and quality

NOTE Based upon 5.7 in ISO/IEC 29100:2011.

Adhering to the accuracy and quality principle means:

- ensuring that the PPII processed is accurate, complete, up-to-date (unless there is a legitimate basis for keeping outdated data), adequate and relevant for the purpose of use;
- ensuring the reliability of PPII collected from a source other than from the local device or user before it is processed;
- verifying, through appropriate means, the validity and correctness of the claims made by the local device or user prior to making any changes to the PPII (in order to ensure that the changes are properly authorized), where it is appropriate to do so;
- establishing PPII collection procedures to help ensure accuracy and quality; and
- establishing control mechanisms to periodically check the accuracy and quality of collected and stored PPII.

This principle is particularly important in cases where the data can be used to grant or deny a significant benefit to the natural person or in which inaccurate data can otherwise result in significant harm to the natural person.

5.4.8 Openness, transparency and notice

NOTE Based upon 5.8 in ISO/IEC 29100:2011.

Adhering to the openness, transparency and notice principle means:

- providing local devices or users with clear and easily accessible information about the service policies, procedures and practices with respect to the handling of PPII by the binding map controller service;
- including in notices the fact that PPII is being processed, the purpose for which this is done, the types of privacy stakeholders to whom the PPII is disclosed, and the identity of the binding map controller service including information on how to contact the binding map controller service;
- disclosing the choices and means offered by the binding map controller service to local devices or users for the purposes of limiting the processing of, and for accessing, correcting and removing their information; and
- giving notice to the local devices or users when major changes in the PPII handling procedures occur.

Transparency, including general information on the logic underlying the PPII processing, can be required, particularly, if the processing involves a decision impacting the local device or user. Privacy stakeholders that process PPII should make specific information about their policies and practices relating to the management of PPII readily available to the public. All contractual obligations that impact PPII processing should be documented and communicated internally as appropriate. They should also be communicated externally to the extent those obligations are not confidential.

In addition, the purpose of the processing of PPII should be sufficiently detailed in order to allow the local device or user to understand:

- the specified PPII required for the specified purpose;
- the specified purpose for PPII collection;
- the specified processing (including collection, communication and storage mechanisms);
- the types of authorized natural persons who can access the PPII and to whom the PPII can be transferred; and
- the specified PPII data retention and disposal requirements.

5.4.9 Individual participation and access

NOTE Based upon 5.9 in ISO/IEC 29100:2011.

Adhering to the individual participation and access principle means:

- giving local devices or users the ability to access and review their PPII, provided their identity is first authenticated with an appropriate level of assurance and such access is not prohibited by applicable law;
- allowing local devices or users to challenge the accuracy and completeness of the PPII and have it amended, corrected or removed as appropriate and possible in the specific context;
- providing any amendment, correction or removal to local devices or users and remote devices or users to whom personal data had been disclosed, where they are known; and
- establishing procedures to enable local devices or users to exercise these rights in a simple, fast and efficient way, which does not entail undue delay or cost.

The binding map controller service should apply appropriate controls to ensure that local devices or users access strictly their own PPII and not that of other local devices or users, unless the natural person accessing is acting under authority on behalf of a local device or user who is unable to exercise his or her right of access. Applicable law can provide the natural person with the right to access, review and object to the processing of PPII under certain circumstances. When a challenge is not resolved to the satisfaction of the natural person, the substance of the unresolved challenge should be recorded by the organization. When appropriate, the existence of the unresolved challenge should be transmitted to binding map processor services and other third parties having access to the information in question.

Annex A
(informative)

Mapping ISO/IEC 29100 to the HES gateway

As described in ISO/IEC 29100:2011, 4.2, there are four types of actors in PII situations.

- PII principals: "… give consent and determine their privacy preferences for how their PII should be processed." [ISO/IEC 29100:2011, 4.2.1].
- PII controllers: "… determines why (purpose) and how (means) the processing of PII takes place." [ISO/IEC 29100:2011, 4.2.2].
- PII processors: "… carries out the processing of PII on behalf of a PII controller, acts on behalf of, or in accordance with the instructions of the PII controller, …" [ISO/IEC 29100:2011, 4.2.3].
- Third parties: "… receive PII from a PII controller or a PII processor." [ISO/IEC 29100:2011, 4.2.4].

From the General System Diagram for the HES gateway in Figure 2, the corresponding PII actors of ISO/IEC 29100:2011, 4.2 are shown in Table A.1.

Table A.1 – ISO/IEC 29100 and HES gateway terms

ISO/IEC 29100	HES gateway
PII principal	Local device or user
PII controller	Controller service module
PII processor	Processor service module
Third party	Remote device or user

This results in the system layout shown in Figure A.1 for applying ISO/IEC 29100 within the HES gateway specification.

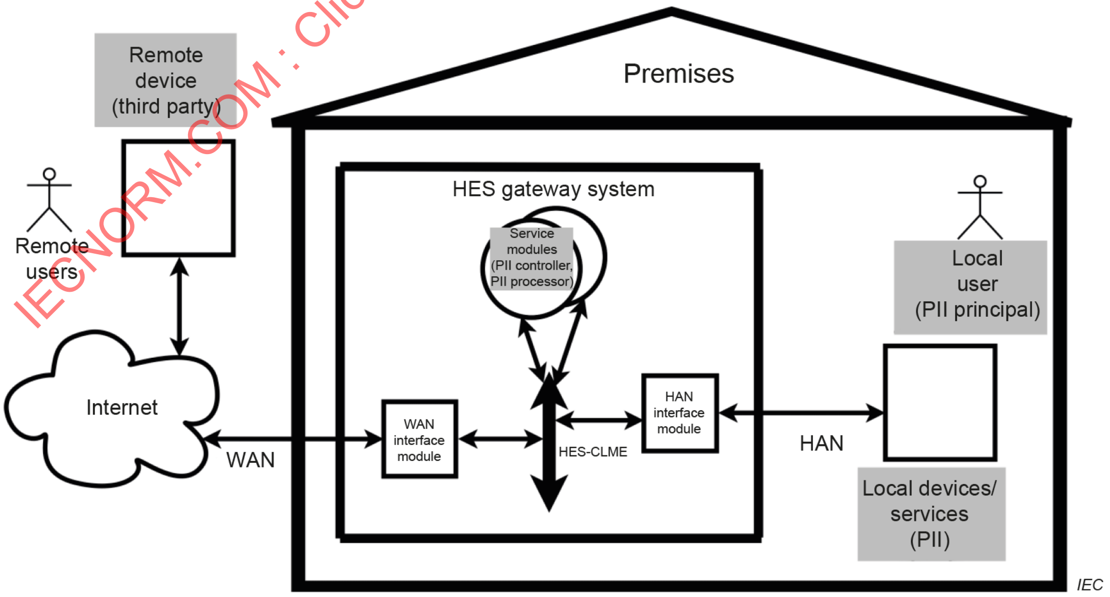
Remote device (third party)
Premises
HES gateway system
Service modules (PII controller, PII processor)
Remote users
Local user (PII principal)
Internet
WAN
WAN interface module
HES-CLME
HAN interface module
HAN
Local devices/ services (PII)
IEC

Figure A.1 – System layout for ISO/IEC 29100

Annex B
(normative)

Permitted PPII flows

B.1 General

PII originated by the local user is extended to include content from the local device and local services (PPII) and is called privacy-protected local information. This content is provided by the local device or user, which consists of the local device and associated local services and the related local user.

The HES gateway shall screen data flows to protect privacy. PPII in the HES gateway shall flow from one provider of PPII to one recipient authorized to receive the PPII. There is a limited number of suitable scenarios[2]; no other scenarios are permitted. For example, the local device or user shall not send PPII directly to a remote user.

In each permitted scenario, there is one provider of the PPII and one recipient authorized to receive the PPII (duplicate). Table B.1 lists all of the permitted PPII flows between parties using the HES gateway system.

Table B.1 – Permitted PPII flow

Scenario[a]	Local device or user	Controller service module	Processor service module	Remote device or user
Scenario A)	PPII provider	PPII recipient		
Scenario B)		PPII provider	PPII recipient	
Scenario C)		PPII recipient	PPII provider	
Scenario D)	PPII recipient	PPII provider		
Scenario E)	PPII provider		PPII recipient	
Scenario F)	PPII recipient		PPII provider	
Scenario G)		PPII provider		PPII recipient
Scenario H)			PPII provider	PPII recipient

[a] Based upon 4.3 of ISO/IEC 29100:2011; some scenario letters have been changed.

For clarification, each of the scenarios is described in Clauses B.2 to B.10, including an example diagram and example description. All scenario examples are combined into one overarching example, describing the data flows of PPII.

In this overarching example, a person on a smart phone outside the premises wishes to read temperatures from a device placed within the premises.

To accomplish such remote readings, the device is registered by the HES gateway. A datalogging service application within the HES gateway platform is set up so that the temperature values are stored within the HES gateway. The remote person with appropriate permission from the HES gateway platform is able to retrieve the temperatures from the HES gateway.

These scenarios describe processes that shall be aligned with appropriate permissions and authorizations. Permission and authorization are addressed in other documents.

[2] Based upon 4.3 of ISO/IEC 29100:2011; some scenario letters have been changed.

B.2 Local device or user to controller service module (Scenario A)

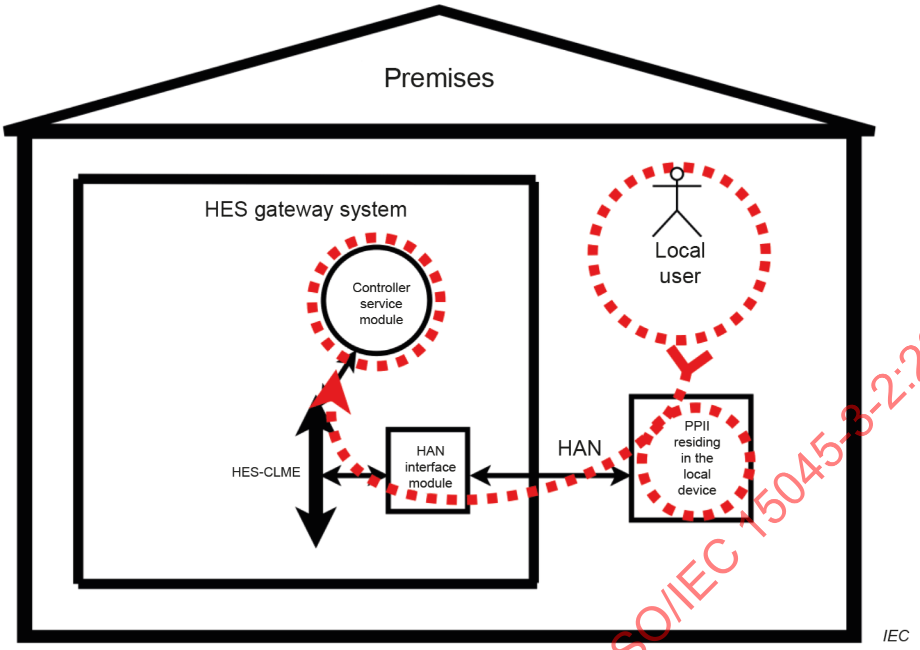

Figure B.1 – Local device or user to controller service module

Scenario A)[3] consists of a local device or user providing PPII (privacy-protected local information) to a controller service module and is shown in Figure B.1.

EXAMPLE Register device: initial setup of an application such as when a smart home system installer registers a new HAN device with the HES gateway.

[3] Based on ISO/IEC 29100:2011, 4.3 a).

B.3 Controller service module to processor service module (Scenario B)

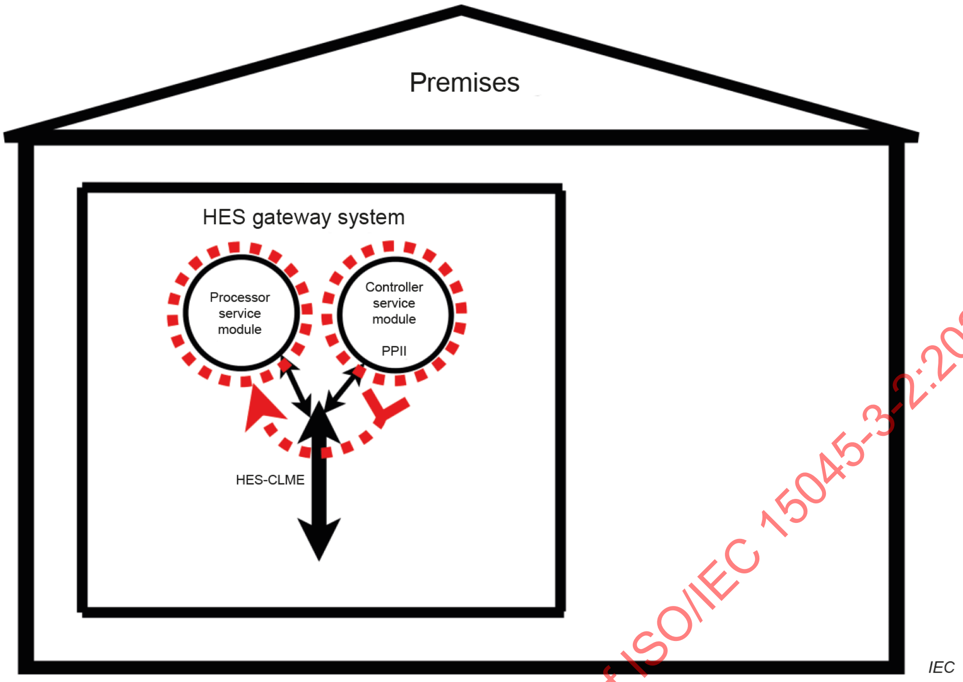

Figure B.2 – Example of controller service module to processor service module

Scenario B)[4] consists of a controller service module providing PPII to a processor service module and is shown in Figure B.2.

EXAMPLE Enable datalogging: the HES gateway enables ambient temperature readings from a local device to be datalogged inside the HES gateway.

[4] Based on ISO/IEC 29100:2011, 4.3 b).

B.4 Processor service module to controller service module (Scenario C)

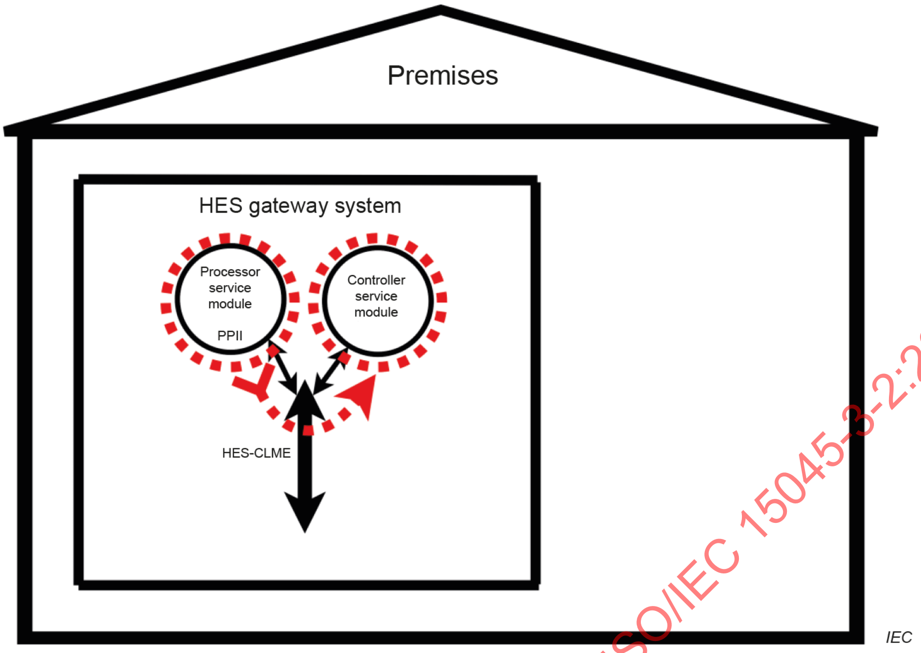

Figure B.3 – Processor service module to controller service module

Scenario C)[5] consists of a processor service module providing PPII to a controller service module and is shown in Figure B.3.

EXAMPLE Confirm datalogging: the processor service module confirms to the controller service module that it has enabled the temperature data logging service.

[5] Based on ISO/IEC 29100:2011, 4.3 f).

B.5 Controller service module to local device or user (Scenario D)

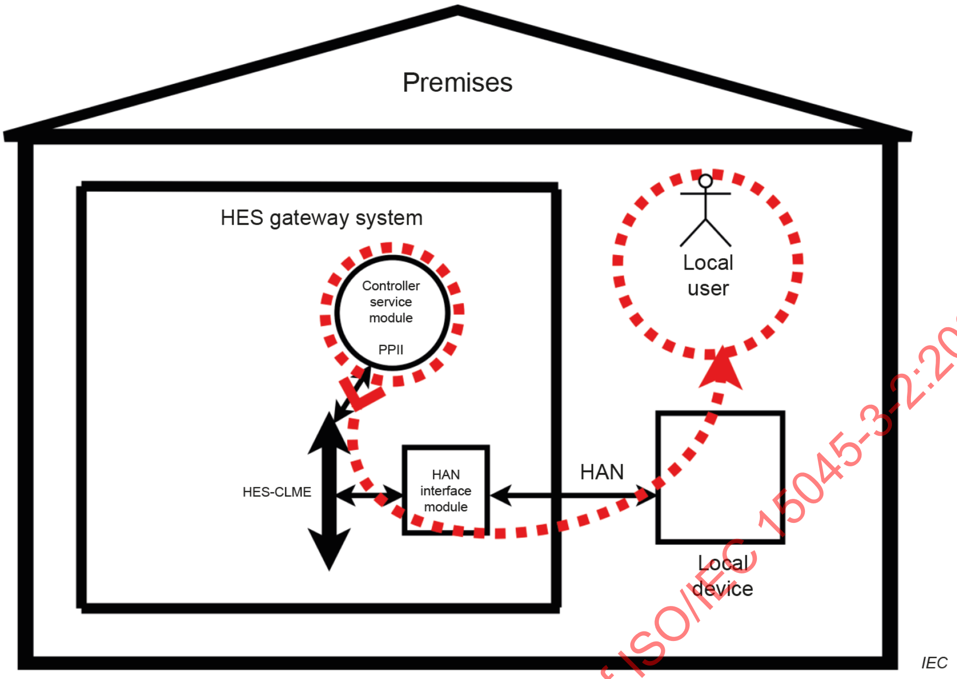

Figure B.4 – Controller service module to local device or user

Scenario D)[6] consists of a controller service module providing PPII to a local device or user and is shown in Figure B.4.

EXAMPLE Confirm service: the HES gateway (i.e. controller service module) sends confirmation to the local user that this attempt to register the local device has been successful and that datalogging is enabled.

[6] Based on ISO/IEC 29100:2011, 4.3 d).

B.6 Local device or user to processor service module (Scenario E)

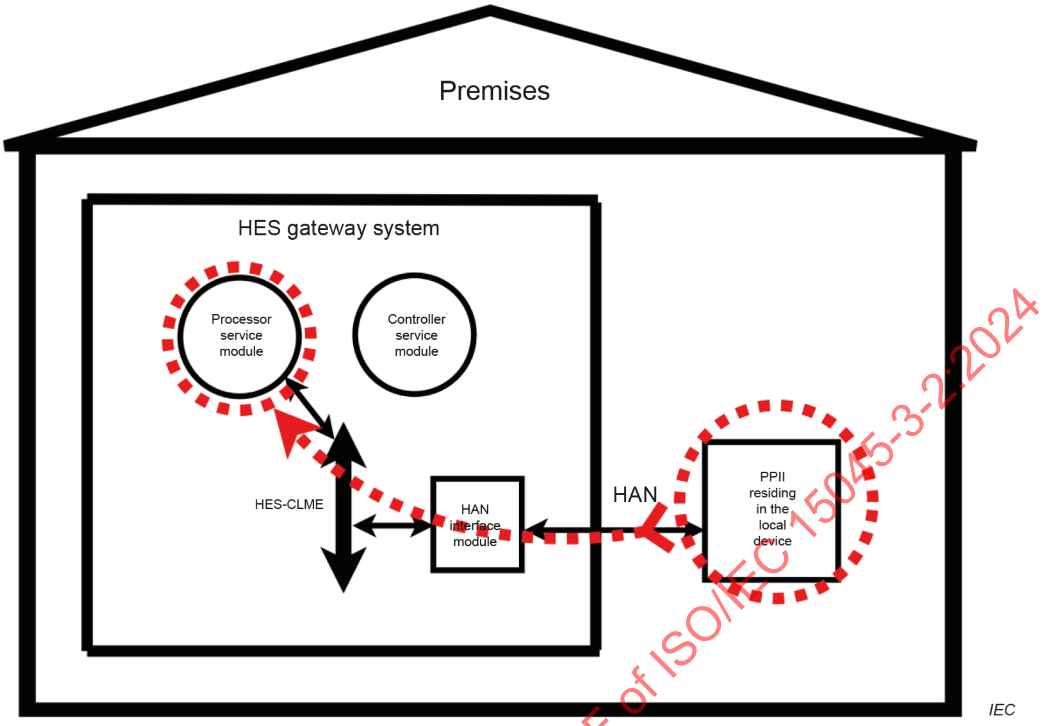

Figure B.5 – Local device or user to processor service module

Scenario E)[7] consists of a local device or user providing PPII to a processor service module and is shown in Figure B.5.

EXAMPLE Live datalogging: periodic ambient temperature readings from a local device are logged within the HES gateway (i.e. processor service module) in real time.

[7] Based on ISO/IEC 29100:2011, 4.3 c).

B.7 Processor service module to local device or user (Scenario F)

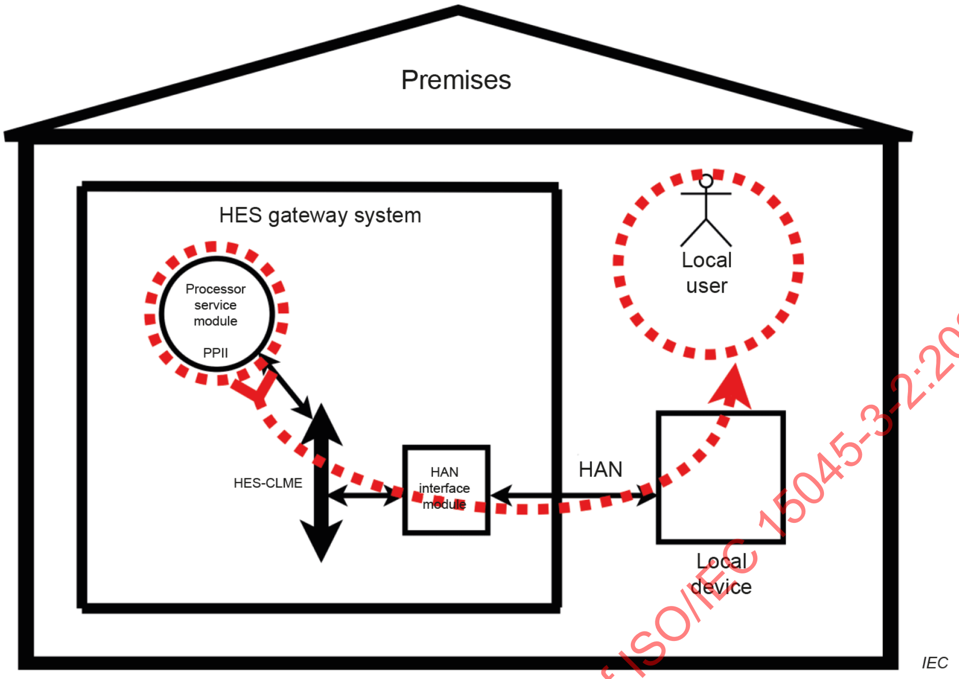

Figure B.6 – Processor service module to local device or user

Scenario F)[8] consists of a processor service module providing PPII to a local device or user and is shown in Figure B.6.

EXAMPLE Recall last temperature: the local user retrieves the last ambient temperature stored in the HES gateway (i.e. processor service module).

B.8 Controller service module to remote device or user (Scenario G)

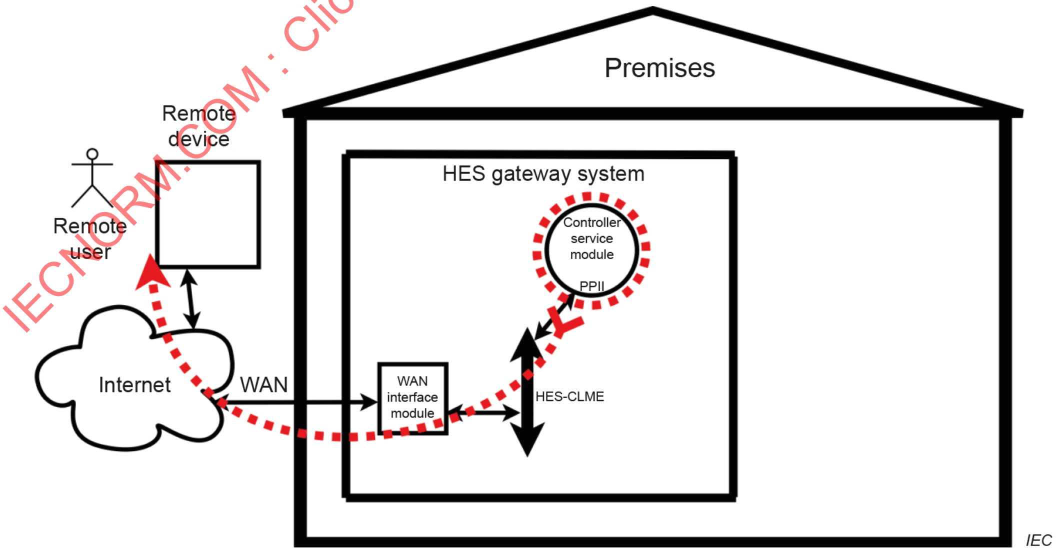

Figure B.7 – Controller service module to remote device or user

[8] Based on ISO/IEC 29100:2011, 4.3 e).