TECHNICAL REPORT

ISO/TR 22696

First edition
2020-05

Health informatics — Guidance on the identification and authentication of connectable Personal Healthcare Devices (PHDs)

Informatique de santé — Lignes directrices pour l'identification et l'authentification des dispositifs de soins de santé personnels connectables

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TR 22696:2020
https://standards.iteh.ai/catalog/standards/sist/d4bc39f3-3fe6-4c59-b1c5-2db6edb5a188/iso-tr-22696-2020

Reference number
ISO/TR 22696:2020(E)

© ISO 2020

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/TR 22696:2020
https://standards.iteh.ai/catalog/standards/sist/d4bc39f3-3fe6-4c59-b1c5-2db6edb5a188/iso-tr-22696-2020

COPYRIGHT PROTECTED DOCUMENT

© ISO 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO 2020 – All rights reserved

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TR 22696:2020
https://standards.iteh.ai/catalog/standards/sist/d4bc39f3-3fe6-4c59-b1c5-2db6ad5a188f/iso-tr-22696-2020

© ISO 2020 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TR 22696:2020

This document was prepared by Technical Committee ISO/TC 215, *Health informatics*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO 2020 – All rights reserved

Introduction

An increasing number of Personal Health Devices (PHDs) are designed to exchange information electronically with other health IT systems in the user environment, and such information is frequently exchanged through the internet, which is publicly open to various types of data.

Various PHDs are connected through the network, and the needs for a secure bidirectional connection for the new PHDs are getting more attention. Security threats to PHDs can spread damages to the existing healthcare systems through the networks that are meant to be kept secure for the benefit of the healthcare service users. The threats can cause not only economical damage but also risk to human lives. Currently, there is no proper guidance for identification and authentication of the PHDs in case of the bidirectional connection between the PHDs and the gateway.

Identification and authentication for various connectable personal devices should be consistently applied throughout the lifecycle. This identification and authentication issue should be considered by the manufacturers of the devices and the operators of the healthcare service. The whole identification and authentication process is critical for the successful operation and management of PHDs. Identification and authentication guidance should be set up to secure the healthcare service by providing the interoperability among devices and gateway.

This identification and authentication issue should be both considered by healthcare device manufactures and healthcare delivery organizations. The healthcare device manufacturers and operators should provide users with mutual authentication between the gateway and the connectable devices for a secure bidirectional communication and the integrity of sensitive personal health information.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TR 22696:2020
https://standards.iteh.ai/catalog/standards/sist/d4bc39f3-3fe6-4c59-b1c5-2db6edb5a188/iso-tr-22696-2020

© ISO 2020 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/TR 22696:2020
https://standards.iteh.ai/catalog/standards/sist/d4bc39f3-3fe6-4c59-b1c5-2db6edb5a188/iso-tr-22696-2020

Health informatics — Guidance on the identification and authentication of connectable Personal Healthcare Devices (PHDs)

1 Scope

The document gives guidance for managing healthcare service security using connectable personal health devices. This document considers unidirectional data uploading from the PHD to the gateway (manager device), however, there are many clinical use cases for bidirectional data exchange.

This document is applicable to identification and authentication between the bidirectionally connected PHDs and gateway by providing possible use cases and the associated threats and vulnerabilities. Since some smart devices with mobile healthcare apps and software might connect to the healthcare service network, these devices will be considered connectable PHDs in this document. This document addresses those devices used in a homecare setting, where the knowledge and capabilities regarding the use of PHDs might not be as advanced as in other healthcare settings.

This document excludes specific protocols, methods and technical solutions for identification and authentication.

iTeh STANDARD PREVIEW

2 Normative references

(standards.iteh.ai)

There are no normative references in this document.

ISO/TR 22696:2020
https://standards.iteh.ai/catalog/standards/sist/d4bc39f3-3fe6-4c59-b1c5-2db6edb5a188/iso-tr-22696-2020

3 Terms and definitions

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

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

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

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

3.1
access control
means to ensure that access to assets is authorized and restricted based on business and security requirements

[SOURCE: ISO/IEC 27000:2018, 3.1]

3.2
attack
assault on a system that comes from an intelligent *threat* (3.18) — i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system

Note 1 to entry: There are different commonly recognized classes of attack:

— An "active attack" attempts to alter system resources or affect their operation.

— A "passive attack" attempts to learn or make use of information from the system but does not affect system resources.

© ISO 2020 – All rights reserved

— An "inside attack" is an attack initiated by an entity inside the security perimeter (an "insider") – i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization.

— An "outside attack" is initiated from outside the perimeter by an unauthorized or illegitimate user of the system (including an insider attacking from outside the security perimeter). Potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

[SOURCE: IEC/TS 62443-1-1:2009, 3.2.9]

3.3
authenticate
verify the identity of a *user* (3.20), user device, or other entity, or the *integrity* (3.11) of data stored, transmitted, or otherwise exposed to unauthorized modification in an information system, or to establish the validity of a transmission

[SOURCE: IEC/TS 62443-1-1:2009, 3.2.12]

3.4
authentication
provision of assurance that a claimed characteristic of an entity is correct

[SOURCE: ISO/IEC 27000:2018, 3.5]

3.5
authorization
right or permission that is granted to a system entity to access a system resource

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SOURCE: IEC/TS 62443:2009, 3.2.14]

3.6
availability
property of being accessible and usable on demand by an authorized entity

ISO/TR 22696:2020
https://standards.iteh.ai/catalog/standards/sist/1dbc2083-26c4-c59-b1c5-2db6edb5a188/iso-tr-22696-2020

[SOURCE: ISO/IEC 27000:2018, 3.7]

3.7
bidirectional connection
two-way communication connection between a *personal health device* (3.16) and a *gateway* (3.9) for data exchange

3.8
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO/IEC 27000:2018, 3.10]

3.9
gateway
relay mechanism that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables host computers on one network to communicate with hosts on the other

Note 1 to entry: Also described as an intermediate system that is the translation interface between two computer networks.

[SOURCE: IEC/TS 62443-1-1:2009, 3.2.53]

3.10
identification
process of identifying and recognizing a *user* (3.20), *personal health device* (3.16), or home *gateway* (3.9) as a unique entity that establishes connections

© ISO 2020 – All rights reserved

3.11
integrity
quality of a system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data

Note 1 to entry: In a formal security mode, integrity is often interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

[SOURCE: IEC/TS 62443-1-1:2009, 3.2.60]

3.12
interface
logical entry or exit point that provides access to the module for logical information flows

[SOURCE: IEC/TS 62443-1-1:2009, 3.2.62]

3.13
malicious code
programs or code written for the purpose of gathering information about systems or *users* (3.20), destroying system data, providing a foothold for further intrusion into a system, falsifying system data and reports, or providing time-consuming irritation to system operations and maintenance personnel

Note 1 to entry: Malicious code attacks can take the form of viruses, worms, Trojan horses, or other automated exploits.

Note 2 to entry: Malicious code is also often referred to as "malware".

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SOURCE: IEC/TS 62443-1-1:2009, 3.2.70]

3.14
manufacturer
ISO/TR 22696:2020
https://standards.iteh.ai/catalog/standards/sist/d4bc39f3-3fe6-4c59-b1c5-2db6edb5a188/iso-tr-22696-2020
natural or legal person with responsibility for designing, manufacturing, packaging or labelling a *medical device* (3.15), assembling a system, or adapting a medical device before it is placed on the market or put into service, regardless of whether these operations are carried out by that person or on that person's behalf by a third party

3.15
medical device
instrument, apparatus, implement, machine, appliance, implant, in vitro reagent or calibrator, software, material or other similar or related article

a) intended by the *manufacturer* (3.14) to be used, alone or in combination, for human beings for one or more of the specific purpose(s) of:

   — diagnosis, prevention, monitoring, treatment or alleviation of disease,

   — diagnosis, monitoring, treatment, alleviation of or compensation for an injury,

   — investigation, replacement, modification, or support of the anatomy or of a physiological process,

   — supporting or sustaining life,

   — control of conception,

   — disinfection of medical devices,

   — providing information for medical or diagnostic purposes by means of in vitro examination of specimens derived from the human body; and

b) which does not achieve its primary intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its intended function by such means

© ISO 2020 – All rights reserved

Note 1 to entry: The definition of a device for in vitro examination includes, for example, reagents, calibrators, sample collection and storage devices, control materials, and related instruments or apparatus. The information provided by such an in vitro diagnostic device may be for diagnostic, monitoring or compatibility purposes. In some jurisdictions, some in vitro diagnostic devices, including reagents and the like, might be covered by separate regulations.

Note 2 to entry: Products which can be considered to be medical devices in some jurisdictions but for which there is not yet a harmonized approach, are:

— aids for disabled/handicapped people;

— devices for the treatment/diagnosis of diseases and injuries in animals;

— accessories for medical devices (see Note 3 to entry);

— disinfection substances;

— devices incorporating animal and human tissues which might meet the requirements of the above definition but are subject to different controls.

Note 3 to entry: Accessories intended specifically by manufacturers to be used together with a 'parent' medical device to enable that medical device to achieve its intended purpose should be subject to the same GHTF procedures as apply to the medical device itself. For example, an accessory will be classified as though it is a medical device in its own right. This may result in the accessory having a different classification than the 'parent' device.

Note 4 to entry: Components to medical devices are generally controlled through the manufacturer's quality management system and the conformity assessment procedures for the device. In some jurisdictions, components are included in the definition of a 'medical device'.

[SOURCE: IEC 80001-1:2010, 2.14]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.16
personal health device
PHD
connectable *medical device* (3.15) used in the home healthcare environment

ISO/TR 22696:2020
https://standards.iteh.ai/catalog/standards/sist/d4bc39f3-3fe6-4c59-b1c5-2ab6edb9a1a6/iso-tr-22696-2020

3.17
public key infrastructure
PKI
complex security system environment for providing encryption and electronic signature using a public key algorithm

Note 1 to entry: Here, it means the basic technology of the equipment certificate used in the smart health care device.

3.18
threat
potential cause of an unwanted incident, which can result in harm to a system or organization

[SOURCE: ISO/IEC 27000:2018, 3.74]

3.19
unidirectional connection
one-way communication connection between a *personal health device* (3.16) and a *gateway* (3.9)

Note 1 to entry: This standard does not provide any method to ensure security of data exchange. It assumes that data exchange is secured by other means, for example, a secure transport channel.

3.20
user
entities using *personal health devices* (3.16) to transfer information

© ISO 2020 – All rights reserved

4 Abbreviated terms

I&A Identification and Authentication

ICS Industrial Control System

ICU Intensive Care Unit

PHI Personal Health Information

5 Information security objectives in healthcare and PHDs

Information security has been addressed in three security objectives: confidentiality, integrity, and availability. Although in most information technology domains confidentiality has been considered more important than integrity and availability, there is room for debate, depending on the needs of each situation.

For example, when it comes to the ICS, availability is deemed more significant than integrity or confidentiality. Its importance is clear when considering the large amount of loss and high level of impact that the stoppage of national power plants or burning furnaces have.

In the healthcare domain, it is crucial to prioritize confidentiality, integrity and availability according to specific requirements of the domain. Practical guidelines for emergency situations prompt healthcare providers to consider human life above any other requirements, i.e. privacy rules.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

When it comes to integrity and availability, it is difficult to definitively prioritize one over the other. For example, it is clear that availability would be the priority for a patient in an ICU since a system-off would be fatal and cause death. For a patient who is supported by a pacemaker, the availability of the pacemaker is also critical.

ISO/TR 22696:2020
https://standards.iteh.ai/catalog/standards/sist/44bc30f2-3fe6-4c59-b1e5-2db6eab5a188/iso-tr-22696-2020

However, if the data that is connected to a patient's critical equipment in ICU or to a pacemaker is manipulated or falsely reported, the patient faces the same risks that those associated with unavailability. Hence, integrity should also be prioritized in the healthcare sector when it comes to the PHD's security and accurate functionality, since contaminated data can pose a threat to human life.

6 Security vulnerabilities and threats of PHDs

6.1 Security vulnerabilities of PHDs

PHDs are defined by the ISO/IEEE 11073 series as a health device that is normally used for measurement by a chronic patient, especially seniors, for telemedicine at home or in other buildings. Currently, the number of medical services and health management programs supported by Medical IoT devices is growing dramatically, which requires the security vulnerabilities of the devices to be sufficiently scrutinized.

Security vulnerabilities of PHDs are related to their projected benefits; usability, real-time interaction, remote access, etc. The common vulnerabilities concerned are as follows:

— unsecure end-point;

— wireless real-time services;

— bidirectional connection.

Data collected from PHDs go to web/app services or medical centres through gateways, which can be divided into dedicated gateways and non-dedicated gateways, such as smart-phones, tablet PCs, or desk-top computers. In many cases, PHDs are operated in private places with unsecure endpoints by a person who manages various networked equipment without deep knowledge of IT.

© ISO 2020 – All rights reserved