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

Reference number
ISO/TR 22696:2020(E)

© ISO 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

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **5**
5 Information security objectives in healthcare and PHDs ... **5**
6 Security vulnerabilities and threats of PHDs ... **5**
6.1 Security vulnerabilities of PHDs ... 5
6.2 Security threats of PHDs ... 6
7 Identification and authentication for connectable PHDs ... **7**
7.1 General ... 7
7.2 Person or entity identification and authentication ... 7
7.2.1 Objectives ... 7
7.2.2 User or entity registration procedure ... 7
7.2.3 Device identification and authentication ... 8
7.2.4 Human user identification and authentication ... 8
7.2.5 Authentication information management ... 8
7.3 Application, identification and authentication ... 9
7.3.1 Objectives ... 9
7.3.2 Unique Identification and Authentication ... 9
7.3.3 Application, firmware and information integrity ... 9
7.3.4 Secure upgrade ... 9
7.3.5 Input validation ... 10
7.3.6 Information confidentiality ... 10
7.4 Access control ... 10
7.4.1 Objectives ... 10
7.4.2 Secure log-on procedures ... 10
7.4.3 Emergency account ... 11
7.4.4 Automatic log-off ... 11
7.4.5 Device lock ... 12
Annex A (informative) **Mapping to other standards** ... **13**
Bibliography ... **15**

© 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.

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.

© ISO 2020 – All rights reserved

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.

2 Normative references

There are no normative references in this document.

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