BS ISO 17090-5:2017

BSI Standards Publication

Health informatics — Public key infrastructure

Part 5: Authentication using Healthcare PKI credentials

Documents
Document Sharing Hub

Full document details: BS ISO 17090-5:2017

National foreword

This British Standard is the UK implementation of ISO 17090-5:2017.

The UK participation in its preparation was entrusted to Technical Committee IST/35, Health informatics.

A list of organizations represented on this committee can be obtained on request to its secretary.

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

© The British Standards Institution 2017
Published by BSI Standards Limited 2017

ISBN 978 0 580 91040 1

ICS 35.240.80

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2017.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO 17090-5:2017

INTERNATIONAL STANDARD

ISO 17090-5

First edition
2017-07

Health informatics — Public key infrastructure —

Part 5: Authentication using Healthcare PKI credentials

Informatique de santé — Infrastructure de clé publique —
Partie 5: Authentification à l'aide des identifiants ICP de la santé

Reference number
ISO 17090-5:2017(E)

Documents
Document Sharing Hub
© ISO 2017

Full document details: BS ISO 17090-5:2017

COPYRIGHT PROTECTED DOCUMENT

© ISO 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

© ISO 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 17090-5:2017

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **1**
5 Scope of application ... **2**
5.1 General ... 2
5.2 Target systems ... 2
5.3 Phases of method identification ... 3
5.4 Threats and vulnerabilities ... 5
6 Validation procedures for HPKI credentials ... **6**
Annex A (informative) **Examples of authentication technology with available X.509 certification as credentials** ... **9**
Annex B (informative) **Appropriate use of authentication certificates** ... **10**
Bibliography ... **13**

© ISO 2017 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 17090-5:2017

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 on 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 the following URL: www.iso.org/iso/foreword.html.

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

A list of all parts in the ISO 17090 series can be found on the ISO website.

© ISO 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 17090-5:2017

Introduction

The healthcare industry is faced with the challenge of reducing costs by moving from paper-based processes to automated electronic processes. New models of healthcare delivery are emphasizing the need for patient information to be shared among a growing number of specialist healthcare providers and across traditional organizational boundaries.

Healthcare information concerning individual citizens is commonly interchanged by means of electronic mail, remote database access, electronic data interchange and other applications. The Internet provides a highly cost-effective and accessible means of interchanging information, but it is also an insecure vehicle that demands additional measures be taken to maintain the privacy and confidentiality of information. Threats to the security of health information through unauthorized access (either inadvertent or deliberate) are increasing. It is essential to have available to the healthcare system reliable information security services that minimize the risk of unauthorized access.

How does the healthcare industry provide appropriate protection for the data conveyed across the Internet in a practical, cost-effective way? Public key infrastructure (PKI) and digital certificate technology seek to address this challenge.

The proper deployment of digital certificates requires a blend of technology, policy and administrative processes that enable the exchange of sensitive data in an unsecured environment by the use of "public key cryptography" to protect information in transit and "certificates" to confirm the identity of a person or entity. In healthcare environments, this technology uses authentication, encipherment and digital signatures to facilitate confidential access to, and movement of, individual health records to meet both clinical and administrative needs. The services offered by the deployment of digital certificates (including encipherment, information integrity and digital signatures) are able to address many of these security issues. This is especially the case if digital certificates are used in conjunction with an accredited information security standard. Many individual organizations around the world have started to use digital certificates for this purpose.

Interoperability of digital certificate technology and supporting policies, procedures and practices is of fundamental importance if information is to be exchanged between organizations and between jurisdictions in support of healthcare applications (for example, between a hospital and a community physician working with the same patient).

Achieving interoperability between different digital certificate implementations requires the establishment of a framework of trust, under which parties responsible for protecting an individual's information rights may rely on the policies and practices and, by extension, the validity of digital certificates issued by other established authorities.

Many countries are deploying digital certificates to support secure communications within their national boundaries. Inconsistencies will arise in policies and procedures between the certification authorities (CAs) and the registration authorities (RAs) of different countries if standards development activity is restricted to within national boundaries.

Digital certificate technology is still evolving in certain aspects that are not specific to healthcare. Important standardization efforts and, in some cases, supporting legislation are ongoing. On the other hand, healthcare providers in many countries are already using or planning to use digital certificates. This document seeks to address the need for guidance to support these rapid international developments. While underlying security standards address methods for verification, requirements for secure verification processes to support healthcare purposes are not defined.

This document describes the procedural requirements validating an entity credential based on Healthcare PKI defined in ISO 17090 series used in healthcare information systems. Although the cryptographic operations used at the authentication processes and the digital signature processes are the same, authentication and signature have different meanings. Systems and software prevent the users from misuse of the private keys and their certificates especially if both keys are on a secure token. This document describes the requirements to mitigate threats and vulnerabilities within the authentication processes with Healthcare PKI credentials.

Documents
Document Sharing Hub

© ISO 2017 – All rights reserved

Full document details: BS ISO 17090-5:2017