INTERNATIONAL STANDARD

ISO 17090-2

Second edition
2015-11-15

Health informatics — Public key infrastructure —

Part 2: Certificate profile

Informatique de santé — Infrastructure de clé publique —

Partie 2: Profil de certificat

Reference number
ISO 17090-2:2015(E)

© ISO 2015



COPYRIGHT PROTECTED DOCUMENT

© ISO 2015, 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

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Abbreviated terms **1**

5 Healthcare CPs **2**
5.1 Certificate types required for healthcare 2
5.2 CA certificates 2
5.2.1 Root CA certificates 2
5.2.2 Subordinate CA certificates 2
5.3 Cross/Bridge certificates 3
5.4 End entity certificates 3
5.4.1 Individual identity certificates 3
5.4.2 Organization identity certificate 4
5.4.3 Device identity certificate 4
5.4.4 Application certificate 4
5.4.5 AC 4
5.4.6 Role certificates 5

6 General certificate requirements **6**
6.1 Certificate compliance 6
6.2 Common fields for each certificate type 6
6.3 Specifications for common fields 7
6.3.1 General 7
6.3.2 Signature 8
6.3.3 Validity 8
6.3.4 Subject public key information 8
6.3.5 Issuer name field 9
6.3.6 The subject name field 10
6.4 Requirements for each healthcare certificate type 11
6.4.1 Issuer fields 11
6.4.2 Subject fields 11

7 Use of certificate extensions **14**
7.1 General 14
7.2 General extensions 14
7.2.1 authorityKeyIdentifier 14
7.2.2 subjectKeyIdentifier 14
7.2.3 keyUsage 14
7.2.4 privateKeyUsagePeriod 14
7.2.5 certificatePolicies 14
7.2.6 subjectAltName 14
7.2.7 basicConstraints 15
7.2.8 CRLDistributionPoints 15
7.2.9 ExtKeyUsage 15
7.2.10 Authority information access 15
7.2.11 Subject information access 15
7.3 Special subject directory attributes 15
7.3.1 hcRole attribute 15
7.3.2 subjectDirectoryAttributes 17
7.4 Qualified certificate statements extension 17
7.5 Requirements for each health industry certificate type 17
7.5.1 Extension fields 17

© ISO 2015 – All rights reserved

Annex A (informative) **Certificate profile examples** **19**
Bibliography **31**

 © ISO 2015 – 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 on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

The committee responsible for this document is ISO/TC 215, *Health informatics*.

This second edition cancels and replaces the first edition (ISO 17090-2:2008), which has been technically revised.

ISO 17090 consists of the following parts, under the general title *Health informatics — Public Key Infrastructure*:

— *Part 1: Overview of digital certificate services*

— *Part 2: Certificate profile*

— *Part 3: Policy management of certification authority*

— *Part 4: Digital Signatures for healthcare documents*

The following document is under preparation:

— *Part 5: Authentication using Healthcare PKI credentials*

Annex A of this part of ISO 17090 is for information only.

© ISO 2015 – All rights reserved

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 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) technology seeks 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 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 International Standard seeks to address the need for guidance of these rapid international developments.

This International Standard describes the common technical, operational and policy requirements that need to be addressed to enable digital certificates to be used in protecting the exchange of healthcare information within a single domain, between domains and across jurisdictional boundaries. Its purpose is to create a platform for global interoperability. It specifically supports digital certificate enabled communication across borders, but could also provide guidance for national or regional deployment of digital certificates in healthcare. The Internet is increasingly used as the vehicle of choice to support the movement of healthcare data between healthcare organizations and is the only realistic choice for cross-border communication in this sector.

 © ISO 2015 – All rights reserved

This International Standard should be approached as a whole, with the three parts all making a contribution to defining how digital certificates can be used to provide security services in the health industry, including authentication, confidentiality, data integrity and the technical capacity to support the quality of digital signature.

ISO 17090-1 defines the basic concepts underlying the use of digital certificates in healthcare and provides a scheme of interoperability requirements to establish digital certificate enabled secure communication of health information.

ISO 17090-2 provides healthcare specific profiles of digital certificates based on the International Standard X.509 and the profile of this specified in IETF/RFC 5280 for different types of certificates.

ISO 17090-3 deals with management issues involved in implementing and using digital certificates in healthcare. It defines a structure and minimum requirements for certificate policies (CPs) and a structure for associated certification practice statements. This part is based on the recommendations of the IETF/RFC 3647 *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* and identifies the principles needed in a healthcare security policy for cross border communication. It also defines the minimum levels of security required, concentrating on the aspects unique to healthcare.

Comments on the content of this International Standard, as well as comments, suggestions and information on the application of these standards may be forwarded to the ISO/TC 215 Secretariat: Lisa.Spellman@ahima.org or WG4 PKI project leader Ross Fraser at RossFraser@SextantSoftware.com.

© ISO 2015 – All rights reserved

Health informatics — Public key infrastructure —

Part 2: Certificate profile

1 Scope

This part of ISO 17090 specifies the certificate profiles required to interchange healthcare information within a single organization, between different organizations and across jurisdictional boundaries. It details the use made of digital certificates in the health industry and focuses, in particular, on specific healthcare issues relating to certificate profiles.

2 Normative references

The following referenced documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 17090-1, *Health informatics — Public key infrastructure — Part 1: Overview of digital certificate services*

ISO 17090-3:2008, *Health informatics — Public key infrastructure — Part 3: Policy management of certification authority*

IETF/RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 17090-1 apply.

4 Abbreviated terms

AA attribute authority

AC attribute certificate

CA certification authority

CP certificate policy

CPS certification practice statement

CRL certificate revocation list

PKC public key certificate

PKI public key infrastructure

RA registration authority

TTP trusted third party

© ISO 2015 – All rights reserved