INTERNATIONAL STANDARD

ISO 17090-3

Second edition
2021-03

Health informatics — Public key infrastructure —

Part 3: Policy management of certification authority

Informatique de santé — Infrastructure de clé publique —
Partie 3: Gestion politique d'autorité de certification

Reference number
ISO 17090-3:2021(E)

© ISO 2021



COPYRIGHT PROTECTED DOCUMENT

© ISO 2021

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
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviations **1**
5 Requirements for digital certificate policy management in a healthcare context **2**
5.1 General 2
5.2 Need for a high level of assurance 2
5.3 Need for a high level of infrastructure availability 2
5.4 Need for a high level of trust 2
5.5 Need for Internet compatibility 3
5.6 Need to facilitate evaluation and comparison of CPs 3
6 Structure of healthcare CPs and healthcare CPSs **3**
6.1 General requirements for CPs 3
6.2 General requirements for CPSs 4
6.3 Relationship between a CP and a CPS 4
6.4 Applicability 4
7 Minimum requirements for a healthcare CP **5**
7.1 General requirements 5
7.2 Publication and repository responsibilities 5
7.2.1 Repositories 5
7.2.2 Publication of certification information 5
7.2.3 Frequency of publication 5
7.2.4 Access controls on repositories 5
7.3 Identification and authentication 6
7.3.1 Initial registration 6
7.3.2 Initial identity validation 7
7.3.3 Identification and authentication for re-keying requests 8
7.3.4 Identification and authentication for revocation request 8
7.4 Certificate life-cycle operational requirements 9
7.4.1 Certificate application 9
7.4.2 Certificate application processing 10
7.4.3 Certificate issuance 10
7.4.4 Certificate acceptance 11
7.4.5 Key pair and certificate usage 11
7.4.6 Certificate renewal 12
7.4.7 Certificate re-key 13
7.4.8 Certificate modification 13
7.4.9 Certificate revocation and suspension 14
7.4.10 Certificate status services 17
7.4.11 End of subscription 18
7.4.12 Private key escrow 18
7.5 Physical controls 18
7.5.1 General 18
7.5.2 Physical controls 18
7.5.3 Procedural controls 18
7.5.4 Personnel controls 18
7.5.5 Security audit logging procedures 18
7.5.6 Record archive 18
7.5.7 Key changeover 19
7.5.8 Compromise and disaster recovery 19

© ISO 2021 – All rights reserved

7.5.9 CA termination 19
7.6 Technical security controls 19
7.6.1 Key pair generation and installation 19
7.6.2 Private key protection 20
7.6.3 Other aspects of key management 22
7.6.4 Activation data 23
7.6.5 Computer security controls 23
7.6.6 Life-cycle technical controls 23
7.6.7 Network security controls 23
7.6.8 Time stamping 24
7.7 Certificate, CRL and OCSP profiles 24
7.8 Compliance audit 24
7.8.1 General 24
7.8.2 Frequency of CA compliance audit 24
7.8.3 Identity/qualifications of auditor 24
7.8.4 Auditor's relationship to audited party 24
7.8.5 Topics covered by audit 24
7.8.6 Actions taken as a result of deficiency 25
7.8.7 Communication of audit results 26
7.9 Other business and legal matters 26
7.9.1 Fees 26
7.9.2 Financial responsibility 26
7.9.3 Confidentiality of business information 26
7.9.4 Privacy of personal information 26
7.9.5 Intellectual property rights 27
7.9.6 Representations and warranties 27
7.9.7 Disclaimers of warranties 29
7.9.8 Limitations of liability 29
7.9.9 Indemnities 30
7.9.10 Term and termination 30
7.9.11 Individual notices and communication with participants 30
7.9.12 Amendments 30
7.9.13 Dispute resolution procedures 30
7.9.14 Governing law 31
7.9.15 Compliance with applicable law 31
7.9.16 Miscellaneous provisions 31
8 Model PKI disclosure statement 31
8.1 Introduction 31
8.2 Structure of PKI disclosure statement 32
Bibliography 33

 © ISO 2021 – 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*.

This second edition cancels and replaces the first edition (ISO 17090-3:2008), of which it constitutes a minor revision. The changes compared to the previous edition are as follows:

— update to references;

— editorial update.

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

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 2021 – 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 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. The ISO 17090 series seeks to address the need for guidance of these rapid international developments.

The ISO 17090 series 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 the 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 2021 – All rights reserved

The ISO 17090 series should be approached as a whole, with the five 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[9] and the profile of this, specified in IETF/RFC 5280 for different types of certificates.

This document 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 document is based on the recommendations of the informational IETF/RFC 3647, 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.

ISO 17090-4 supports interchangeability of digital signatures and the prevention of incorrect or illegal digital signatures by providing minimum requirements and formats for generating and verifying digital signatures and related certificates.

ISO 17090-5 defines the procedural requirements for validating an entity credential based on PKI defined in the ISO 17090 series, used in healthcare information systems including accessing remote systems.

© ISO 2021 – All rights reserved

Health informatics — Public key infrastructure —

Part 3: Policy management of certification authority

1 Scope

This document gives guidelines for certificate management issues involved in deploying digital certificates in healthcare. It specifies a structure and minimum requirements for certificate policies, as well as a structure for associated certification practice statements.

This document also identifies the principles needed in a healthcare security policy for cross-border communication and defines the minimum levels of security required, concentrating on aspects unique to healthcare.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 17090-1:2021, *Health informatics — Public key infrastructure — Part 1: Overview of digital certificate services*

ISO 17090-2:2015, *Health informatics — Public key infrastructure — Part 2: Certificate profile*

ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

IETF/RFC 3647, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*

IETF/RFC 4211, *Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)*

3 Terms and definitions

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

4 Abbreviations

AA attribute authority

CA certification authority

CP certificate policy

© ISO 2021 – All rights reserved