TECHNICAL SPECIFICATION

ISO/TS 17090-3

First edition
2002-10-15

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/TS 17090-3:2002(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Contents

Page

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of normative document:

- an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

- an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years with a view to deciding whether it should be confirmed for a further three years, revised to become an International Standard, or withdrawn. In the case of a confirmed ISO/PAS or ISO/TS, it is reviewed again after six years at which time it has to be either transposed into an International Standard or withdrawn.

Attention is drawn to the possibility that some of the elements of this part of ISO/TS 17090 may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TS 17090-3 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

ISO/TS 17090 consists of the following parts, under the general title *Health informatics — Public key infrastructure*:

- *Part 1: Framework and overview*

- *Part 2: Certificate profile*

- *Part 3: Policy management of certification authority*

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.

PKI is 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, PKI 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 a PKI (including encipherment, information integrity and digital signatures) are able to address many of these security issues. This is especially the case if PKI is used in conjunction with an accredited information security standard. Many individual organizations around the world have started to apply PKI for this purpose.

Interoperability of PKI 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 PKI schemes 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 adopting PKIs 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 PKI standards development activity is restricted to within national boundaries.

PKI technology is still rapidly 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 PKI. This Technical Specification seeks to address the need for guidance of these rapid international developments.

This three-part document is being issued in the Technical Specification series of publications (according to the ISO/IEC Directives, Part 1, 3.1.1.1) as a prospective standard for the use of PKI in the field of healthcare because there is an urgent need for guidance on how standards in this field should be used to meet an identified need. This document is not to be regarded as an International Standard. It is proposed for provisional application so that information and experience of its use in practice may be gathered. ISO/TC 215 intends to revise it into a full International Standard after a three-year period.

This Technical Specification describes the common technical, operational and policy requirements that need to be addressed to enable PKI 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 PKI enabled communication across borders, but could also provide guidance for the establishment of healthcare PKIs nationally or regionally. 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.

This Technical Specification should be approached as a whole, with the three parts all making a contribution to defining how PKIs 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/TS 17090-1 defines the basic concepts of a healthcare public key infrastructure (PKI) and provides a scheme of interoperability requirements to establish a PKI enabled secure communication of health information.

ISO/TS 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 2459 for different types of certificates.

ISO/TS 17090-3 deals with management issues involved in implementing and operating a healthcare PKI. 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 2527 *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 document, as well as comments, suggestions and information on the application of these technical specifications may be forwarded to the ISO/TC 215 secretariat: tsandler@astm.org and the WG4 secretariat w4sec215@medis.or.jp.

TECHNICAL SPECIFICATION **ISO/TS 17090-3:2002(E)**

Health informatics — Public key infrastructure —

Part 3: **Policy management of certification authority**

1 Scope

This part of ISO/TS 17090 gives guidelines for certificate management issues involved in implementing and operating a healthcare public key infrastructure (PKI). It specifies a structure and minimum requirements for certificate policies, as well as a structure for associated certification practice statements.

This part of ISO/TS 17090 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 normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/TS 17090. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO/TS 17090 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/TS 17090-1:2002, *Health informatics — Public key infrastructure — Part 1: Framework and overview*

ISO/TS 17090-2:2002, *Health informatics — Public key infrastructure — Part 2: Certificate profile*

ISO/IEC 17799:2000, *Information technology — Code of practice for information security management*

IETF/RFC 2511, *Internet X.509 Certificate Request Message Format*

IETF/RFC 2527, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*

U.S. government standard FIPS-140-1, level 1 and level 2

3 Terms and definitions

For the purposes of this part of ISO/TS 17090, the terms and definitions given in ISO/TS 17090-1:2002 apply.

4 Abbreviations

AA	attribute authority
CA	certification authority
CP	certificate policy
CPS	certification practice statement
CRL	certificate revocation list
OID	object identifier
PKC	public key certificate
PKI	public key infrastructure
RA	registration authority
TTP	trusted third party

5 Requirements for PKI policy management in a healthcare context

5.1 General

A healthcare PKI shall meet the following objectives in order to be effective in securing the communication of personal health information:

— the reliable and secure binding of unique and distinguished names to individuals, organizations, applications and devices that participate in the electronic exchange of personal health information;

— the reliable and secure binding of professional roles in healthcare to individuals, organizations and applications that participate in the electronic exchange of personal health information, insofar as those roles may used as the basis of role-based access control to such health information;

— (optionally) the reliable and secure binding of attributes to individuals, organizations, applications and devices that participate in the electronic exchange of personal health information, insofar as those attributes may further the secure communication of health information.

The above objectives shall be accomplished in a manner that maintains the trust of all who rely upon the integrity and confidentiality of the personal health information that is securely communicated by means of a healthcare PKI.

To do this, each CA in a healthcare PKI shall operate according to an explicit set of publicly stated policies that promote the above objectives.

5.2 Need for a high level of assurance

Security services required for health applications are specified in clause 6 of ISO/TS 17090-1:2002. For each of these security services (authentication, integrity, confidentiality, digital signature, authorization, access control), a high level of assurance is required.

5.3 Need for a high level of infrastructure availability

Emergency healthcare is a round-the-clock endeavour and the ability to obtain certificates, revoke certificates and check revocation status is in no way bound by the normal working hours of most businesses. Unlike e-commerce, healthcare imposes high availability requirements on any PKI that will be relied upon to secure the communication of personal health information.

5.4 Need for a high level of trust

Unlike electronic commerce (where a vendor and a customer are often the only parties to an electronic transaction and are reliant upon its security and integrity), healthcare applications that store or transmit personal health information may implicitly require the trust of the patients whose information is being exchanged, as well as that of the general public. It is unlikely that either healthcare providers or patients will cooperate in the electronic exchange of personal health information if such exchanges are believed to be insecure.

5.5 Need for Internet compatibility

As the purpose of this Technical Specification is to define the essential elements of a healthcare PKI to support the secure transmission of healthcare information across national boundaries, it is based as much as possible upon Internet standards so as to effectively span those boundaries.

5.6 Need to facilitate evaluation and comparison of CPs

Approaches for using PKI to facilitate the secure exchange of health information across national boundaries are discussed in 9.2 of ISO/TS 17090-1:2002. These approaches (such as cross-recognition and cross-certification) are greatly facilitated if healthcare PKI CPs follow a consistent format so that comparisons may be readily drawn between the provisions of one CP and another.

Healthcare CPs also constitute a basis for accreditation of CAs (a CA being accredited to support one or more CPs which it proposes to implement). While accreditation criteria are beyond the scope of this part of ISO/TS 17090, the entire process of accreditation of healthcare CAs is expedited by the consistency of format and the minimum standards which this Technical Specification promotes.

6 Structure of healthcare CPs and healthcare CPSs

6.1 General requirements for CPs

When a CA issues a certificate, it provides a statement to a relying party that a particular public key is bound to a particular certificate holder. Different certificates are issued following different practices and procedures, and may be suitable for different applications and/or purposes.

PKI certificates contain a registered CP OID, which identifies the CP under which the certificate was issued, and may be used to decide whether or not a certificate is trusted for a particular purpose. The registration process follows the procedures specified in ISO/IEC and ITU standards. The party that registers the OID also publishes the CP for examination by certificate holders and relying parties.

Because of the importance of a CP in establishing trust in a PKC, it is fundamental that the CP be understood and consulted not only by certificate holders but by any relying party. Certificate holders and relying parties shall therefore have ready and reliable access to the CP under which a certificate was issued.

The following requirements apply to all CPs specified in accordance with this part of ISO/TS 17090.

a) Each PKI certificate issued in accordance with this part of ISO/TS 17090 shall contain a registered CP OID, which identifies the CP under which the certificate was issued.

b) The structure of CPs shall be in accordance with IETF/RFC 2527.

c) CPs shall be accessible to certificate holders and relying parties.

While CP documents are essential for describing and governing CPs and practices, many PKI certificate holders, especially consumers, find these detailed documents difficult to understand. These certificate holders and other relying parties may benefit from access to a concise statement of the elements of a CP that require emphasis and disclosure and a model PKI disclosure statement is given in clause 8 for this purpose.

6.2 General requirements for CPSs

A CPS is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of certificate life-cycle management and will generally be more detailed than the associated CP.

The following requirements apply to all CPSs specified in accordance with this part of ISO/TS 17090.

a) CPSs shall be in accordance with IETF/RFC 2527.

b) A CA with a single CPS may support multiple CPs (used for different application purposes and/or by different groups of relying parties).

c) A number of CAs with non-identical CPSs may support the same CP.

d) A CA may choose not to make its CPS accessible to certificate holders or relying parties.

6.3 Relationship between a CP and a CPS

A CP states what assurance can be placed in a certificate (including restrictions on certificate use and limitations on liability). A CPS states how a CA establishes that assurance. A CP may apply more broadly than to just a single organization, whereas a CPS applies only to a single CA. CPs best serve as the vehicle on which to base common interoperability standards and common assurance criteria industry-wide (or possibly more global). A detailed CPS alone does not form a suitable basis for interoperability between CAs operated by different organizations.

6.4 Applicability

This part of ISO/TS 17090 applies to CPs and CPSs that are used for the purpose of issuing healthcare certificates as specified in clause 4 of ISO/TS 17090-2:2002.

7 Minimum requirements for a healthcare PKI CP

7.1 General requirements

A CP shall meet all the following requirements in order to comply with this part of ISO/TS 17090.

The numbers in brackets beneath the headings in clause 7 indicate the corresponding section in IETF/RFC 2527.

7.2 CA-RA requirements

7.2.1 Obligations

(2.1)

7.2.1.1 CA obligations

(2.1.1)

7.2.1.1.1 General

The CA is responsible for all aspects of the issuance and management of a certificate, including control over the registration process, verification of information contained in a certificate, the certificate manufacture, publication, revocation, suspension and renewal. The CA is responsible for ensuring that all aspects of the CA services and operations are performed in accordance with the requirements, representations and warrantees of this CP and with the CA's CPS.

A CA within a healthcare PKI shall have policies and procedures available for the services they provide. They shall cover:

- procedures for registering potential certificate holders prior to certificate issuance, including, where applicable, the certificate holder's role in accordance with clause 6 of ISO/TS 17090-2:2002;
- procedures for authenticating the identity of potential certificate holders prior to certificate issuance;
- procedures to maintain the privacy of any personal information held about the people to whom certificates are given;
- procedures for distribution of certificates to certificate holders and to directories;
- procedures for accepting information about possible private key compromise;
- procedures for distribution of certificate revocation lists (frequency of issue, and how and where to publish them);
- other key management issues, including key size, key generation process, certificate lifespan, rekeying, etc.;
- procedures for cross-certifying with other CAs;
- security controls and auditing.

In order to perform these functions, each CA within the infrastructure will need to provide some basic services to its certificate holders and relying parties. These CA services are listed below.

7.2.1.1.2 Notification of certificate issuance, suspension and revocation

An issuing CA shall notify each certificate holder when a certificate bearing the certificate holder's distinguished name is issued.

An issuing CA shall notify any certificate holder when a certificate bearing the certificate holder's distinguished name is revoked or suspended (notification shall be made to the responsible individual or organization in the case of device or application certificates).

An issuing CA shall make CRLs available to relying parties in accordance with 7.4 of this part of ISO/TS 17090.

7.2.1.1.3 Accuracy of CA representations

When an issuing CA publishes a certificate, it certifies that it has issued a certificate to a certificate holder and that the information stated in the certificate was verified in accordance with the CA's CP. Publication of the certificate in a repository to which the certificate holder has access shall constitute notice of such verification.

A CA shall provide to each certificate holder notice of the certificate holder's rights and obligations under this CP. Such notice may be in the form of a certificate holder agreement and shall include a description of the permitted uses of certificates issued under this CP; the certificate holder's obligations concerning key protection and procedures for communication between the certificate holder and the CA or LRA, including communication of changes in service delivery or changes to this policy. A CA shall notify certificate holders as to procedures for dealing with suspected key compromise, certificate or key renewal, service cancellation and dispute resolution.

7.2.1.1.4 Time between certificate request and issuance

It is recommended that the CA state a maximum period of time that a certificate holder has to complete the key activation process after the generation of the key activation material.

7.2.1.1.5 Certificate revocation and renewal

The issuing CA shall ensure that any procedures for the expiration, revocation and renewal of a certificate shall conform to the relevant provisions of this CP. It is recommended that the address of the CRL distribution points be defined in the certificate in accordance with 7.2.8 of ISO/TS 17090-2:2002.

7.2.1.1.6 Protection of private keys

A CA shall ensure that the private keys and activation data that it holds or stores are protected in accordance with 7.6.2, 7.6.3 and 7.6.4 of this part of ISO/TS 17090.

A CA shall ensure that any private decipherment keys of a certificate holder that it has backed up or archived are protected in accordance with 7.6.2 of this part of ISO/TS 17090. The CA shall not disclose private decipherment keys to any other party without the prior consent of the certificate holder, unless required to do so by law. Despite the foregoing, CA's may offer a private key backup service for the purposes of data recovery of encrypted data. In such a case, because a non-regulated health professional or a supporting organization employee receives a certificate in order to conduct the business of his/her employer, the CA may, for the purposes of data recovery, disclose private decipherment keys to the employer of a non-regulated health professional or a supporting organization employee, where such arrangements have been agreed to prior to certificate issuance.

7.2.1.1.7 Restrictions on CA's private key use

The CA shall ensure that its certificate signing private key is used only to sign certificates and certificate revocation lists. The CA shall ensure that private keys issued to its personnel to access and operate CA applications are used only for such purposes.

7.2.1.2 RA obligations

(2.1.2)

7.2.1.2.1 General

The CA may delegate identification and authentication functions, for which it is responsible, to an RA. The prime function that a healthcare organization RA performs is verification of a certificate holder's identity and healthcare role during initial registration. The RA shall follow the same set of rules and methods of authentication as the CA uses itself. RAs may be separately accredited, independently of a particular CA.

In order to be assured of the authenticity and integrity of a certificate and public keys contained within it, the certificate holders shall have their certificates created by a trusted source. As RAs perform authentication functions for CAs, they shall be trusted to follow the CA's certificate holder authentication policies and to pass the correct certificate holder information to the CA. Similarly, the RAs shall be trusted to pass certificate revocation requests to a CA in an accurate and timely fashion.

It is recommended that RAs be individually accountable for actions performed on behalf of the CA. The RA shall:

- ensure that its signing private key is used only to sign certificate requests, if the RA is performing its duties on-line;
- certify to the CA that it has authenticated the identity of the certificate holder;
- securely transmit and store certificate application information and records of registration;
- initiate a revocation request (where applicable) according to 7.3.4.2 of this part of ISO/TS 17090.