INTERNATIONAL STANDARD

ISO 17090-3

First edition
2008-02-15

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 17090-3:2008(E)

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.org
Web www.iso.org

Published 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 2.

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.

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.

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

This first edition cancels and replaces the Technical Specification (ISO/TS 17090-3:2002), which has been revised and brought to the status of International Standard.

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*

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. ISO 17090 seeks to address the need for guidance of these rapid international developments.

ISO 17090 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 17090 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 3280 for different types of certificates.

This part of ISO 17909 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 of ISO 17090 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.

Comments on the content of this document, as well as comments, suggestions and information on the application of these standards, may be forwarded to the ISO/TC 215 secretariat at adickerson@himss.org or WG4 convenor, Ross Fraser, and WG4 secretariat at w4consec@medis.or.jp.

Health informatics — Public key infrastructure —

Part 3:
Policy management of certification authority

1 Scope

This part of ISO 17090 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 part of ISO 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 referenced documents are indispensable for the application 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 17090-1:2008, *Health informatics — Public key infrastructure — Part 1: Overview of digital certificate services*

ISO 17090-2:2008, *Health informatics — Public key infrastructure — Part 2: Certificate profile*

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

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.

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 digital certificate policy management in a healthcare context

5.1 General

Deployment of digital certificates in healthcare 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 be 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 personal health information that is securely communicated by use of digital certificates.

To do this, each CA issuing digital certificates for use in healthcare 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 17090-1:2008. 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 deployment of digital certificates 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 part of ISO 17090 is to define the essential elements of a healthcare digital certificate deployment to support the secure transmission of healthcare information across national or regional 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 digital certificates to facilitate the secure exchange of health information across national boundaries are discussed in 9.2 of ISO 17090-1:2008. These approaches (such as cross-recognition and cross-certification) are greatly facilitated if healthcare 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 the 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 17090, the entire process of accreditation of healthcare CAs is expedited by the consistency of format and the minimum standards which this part of ISO 17090 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.

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 issuing digital certificates for healthcare use shall have policies and procedures available for the services they provide. These policies and procedures shall cover:

— registering potential certificate holders prior to certificate issuance, including, where applicable, the certificate holder's role in accordance with Clause 6 of ISO 17090-2:2008;

— authenticating the identity of potential certificate holders prior to certificate issuance;

— maintaining the privacy of any personal information held about the people to whom certificates are given;

— distributing certificates to certificate holders and to directories;

— accepting information about possible private key compromise;

— distributing CRLs (frequency of issue, and how and where to publish them);

— other key management issues, including key size, key generation process, certificate lifespan, re-keying, etc.;

— 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 in the CP.

Digital certificates contain one or more registered CP OIDs, which identify 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 OIDs 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 17090.

a) Each digital certificate issued in accordance with this part of ISO 17090 shall contain at least one 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 3647.

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

While CP and CPS documents are essential for describing and governing CPs and practices, many digital 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 17090.

a) CPSs shall be in accordance with IETF/RFC 3647.

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 or may choose to make portions of its CPS available.

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 17090 applies to CPs and CPSs that are used for the purpose of issuing healthcare certificates as specified in Clause 5 of ISO 17090-2:2008.

7 Minimum requirements for a healthcare CP

7.1 General requirements

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

The numbers in parentheses beneath the headings in this clause indicate the corresponding section in IETF/RFC 3647.

7.2 Publication and repository responsibilities

7.2.1 Repositories

(2.1)

Information maintained about certificate holders in RA or CA repositories shall:

— be kept current and up to date (within one day of changes being verified and earlier, depending on circumstances);

— be managed in accordance with ISO/IEC 27002 (or its equivalent) or approved accreditation or licensing criteria.

7.2.2 Publication of certification information

(2.2)

All CAs issuing digital certificates for use in healthcare shall make available to their certificate holders and relying parties:

— the URL of an available web site maintained by, or on behalf of, the CA, containing its certificate policies;

— each certificate issued or renewed under this policy;

— the current status of each certificate issued under this policy;

— the accreditation or licensing criteria under which the CA operates, where such accreditation or licensing is applicable in the jurisdiction in which the CA operates.

An electronic copy of the CP document, digitally signed by an authorized representative of the CA, is to be made available:

— on a web site available to all relying parties or

— via an electronic mail request.

As the CPS precisely details the implementation of a CA service as well as the procedures for key life-cycle management and is more detailed than the CP, it contains information that may therefore need to remain confidential to ensure the CA's security.

7.2.3 Frequency of publication

(2.3)

CAs shall publish information, whenever such information has been modified.

7.2.4 Access controls on repositories

(2.4)

Published information such as policies, practices, certificates and the current status of such certificates shall be read-only.

7.3 Identification and authentication

7.3.1 Initial registration

7.3.1.1 Types of name

(3.1.1)

The subject names used for certificates issued under this policy shall be in accordance with ISO 17090-2.

7.3.1.2 Need for names to be meaningful

(3.1.2)

The effective use of certificates requires that the relative distinguished names that appear on the certificate can be understood and used by a relying party. Names used in these certificates shall identify the certificate holder to which they are assigned in a meaningful way. See also 7.3.1.3.

In the case of certificate holders who are regulated health professionals, non-regulated health professionals, sponsored healthcare providers, supporting organization employees or patients/consumers, the name should match the name authenticated in 7.3.2.

7.3.1.3 Anonymity or pseudonymity

(3.1.3)

The need for names to be meaningful (see 7.3.1.2 above) does not preclude the use of pseudonyms in certificates issued to patients/consumers.

7.3.1.4 Rules for interpreting various name forms

(3.1.4)

A CP shall have a name claim dispute resolution procedure to apply and a convention to be used in interpreting name forms used in those situations where name claim disputes arise.

7.3.1.5 Uniqueness of names

(3.1.5)

The subject distinguished name listed in a certificate shall be unambiguous and unique to distinct certificate holders of a CA.

Where necessary, the inclusion of the distinguished name attribute type “serial number” in the distinguished entity (as described in IETF/RFC 3280) may be used to guarantee uniqueness. Where possible, it is recommended that the serial number be meaningful (e.g. the license number of a regulated health professional). See 7.3.1.2.

7.3.1.6 Recognition, authentication and role of trademarks

(3.1.6)

A CA shall not knowingly issue certificates containing trademarks that do not belong to the subject of the certificate.

7.3.2 Initial identity validation

7.3.2.1 Method to prove possession of private key

(3.2.1)

In those cases where the CA does not generate the key pair, key holders shall be required to prove possession of their private key [e.g. by the key holder submitting a Certificate Signing Request (CSR)]. Key holders may also be periodically required to sign a challenge from the CA.

7.3.2.2 Authentication of identity of organizations

(3.2.2)

Healthcare organizations, supporting organizations, or persons acting on behalf of organizations or devices shall present to the RA evidence of their existence and healthcare role by presenting documentation appropriate to their country, state or provincial government. The CA, the RA and, where applicable, the AA shall verify this information, as well as the authenticity of the requesting representative and the representative’s authorization to act in the name of the organization.

7.3.2.3 Authentication of identity of individuals

(3.2.3)

Individuals, including regulated health professionals, non-regulated health professionals, sponsored healthcare providers, supporting organization employees and patients/consumers shall authenticate their identity to an RA prior to certificate issuance. This part of ISO 17090 recommends the same proof of identity that would be necessary for such individuals to be issued a passport, or a procedure of equivalent rigour.

Regulated health professionals, in order that they authenticate their healthcare license, role and medical speciality (if any), shall present to the RA proof of their professional credentials established by the professional regulatory or accrediting body in their jurisdiction.