INTERNATIONAL STANDARD

ISO 17090-2

First edition
2008-02-15

Health informatics — Public key infrastructure —

Part 2: Certificate profile

Informatique de santé — Infrastructure de clé publique —

Partie 2: Profil de certificat

Reference number
ISO 17090-2:2008(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 17090-2 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

This first edition cancels and replaces the Technical Specification (ISO/TS 17090-2:2002), 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.

This part of ISO 17090 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.

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. ISO 17090-3 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 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 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, *Health informatics — Public key infrastructure — Part 1: Overview of digital certificate services*

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

IETF/RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

IETF/RFC 3281, *An Internet Attribute Certificate Profile for Authorization*

IETF/RFC 3739, *Internet X.509 Public Key Infrastructure Qualified Certificates Profile*

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
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

5 Healthcare CPs

5.1 Certificate types required for healthcare

Identity certificates shall be issued to:

- individuals (regulated health professionals, non-regulated health professionals, sponsored healthcare providers, supporting organization employees and patients/consumers);
- organizations (healthcare organizations and supporting organizations);
- devices;
- applications.

The roles of individuals and organizations are to be captured; either in the identity certificate itself (in a certificate extension) or in an associated AC. The different kinds of certificate and the way they interrelate are shown in Figure 1.

5.2 CA certificates

5.2.1 Root CA certificates

Root CA certificates are used when the subject of the certificate is itself a CA, they are self-signed and are used to issue certificates to relying parties, including subordinate CAs. The basic constraints field indicates whether the certificate is a CA.

5.2.2 Subordinate CA certificates

Subordinate CA certificates are issued for a CA that is itself certified by another CA higher up in the hierarchy to be able to issue certificates either for other CAs lower down the hierarchy or for end entities.

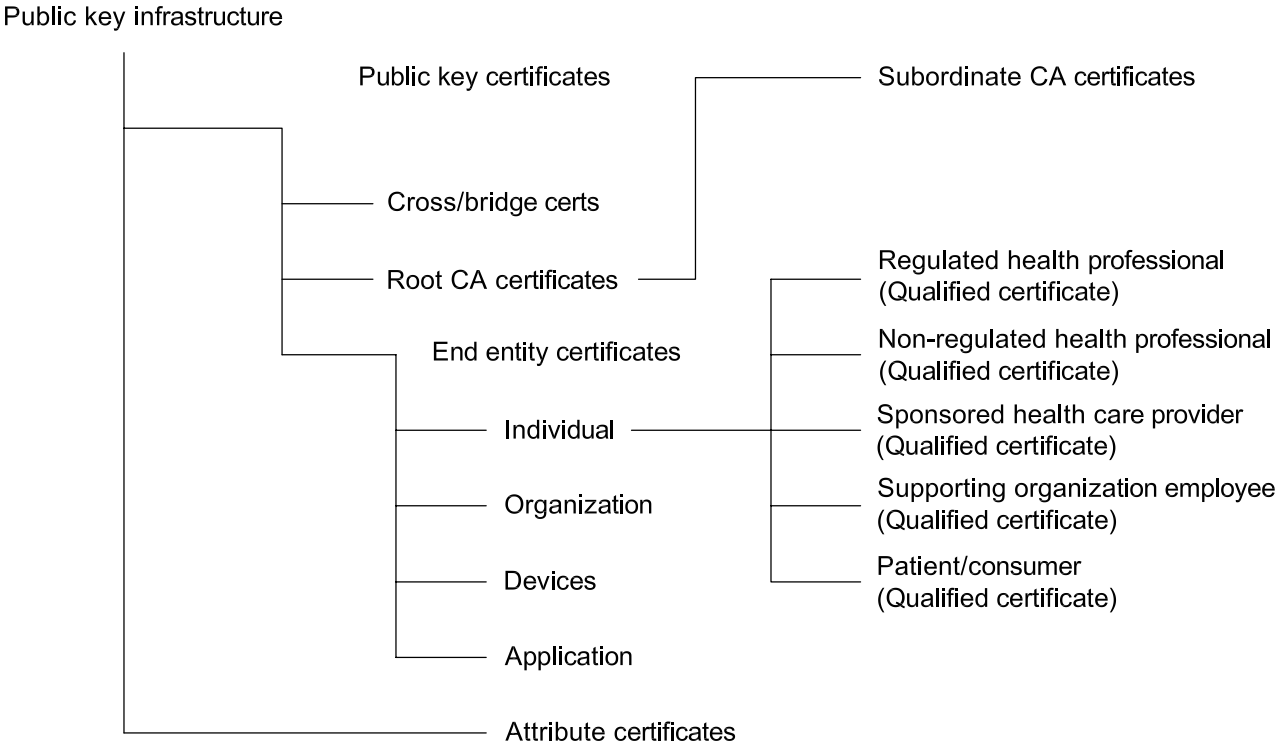

Figure 1 — Healthcare certificate types

5.3 Cross/bridge certificates

In an Internet environment, it is not feasible to expect the health industry in cross-border and jurisdictional situations to trust a top level CA. Instead, "islands of trust" shall be provided in each health industry domain, based on speciality, jurisdiction, setting or geography which trust a particular CA. Each central root CA for each "island of trust" can then cross-certify another root. In these situations, a group of CAs may agree on a minimum set of standards to be embodied in their policies and associated practice statements. When this occurs, a relying party may accept a certificate from a CA outside its own domain. This could be particularly useful for organizations such as state or provincial health authorities to enable the transfer of information across boundaries.

Cross/bridge certificates are certificate types that cross-certify different CA domains. This supports the large-scale deployment of public key applications, such as secure electronic mail and others required in the health industry.

5.4 End-entity certificates

5.4.1 General

End-entity certificates are issued to entities that may include individuals, organizations, applications or devices. They are called end-entity certificates because there are no further entities beneath them relying on that certificate.

5.4.2 Individual identity certificates

Individual identity certificates are a particular subtype of end-entity certificates that are issued to individual persons for the purpose of authentication. The following five types of healthcare actors are recognized as being individuals:

a) regulated health professional:

— each certificate holder is a health professional who, in order to practice his/her profession requires a license or registration from a government body (see 5.1 of ISO 17090-1:2008); these certificates may be qualified certificates (see 8.2 of ISO 17090-1:2008 and 7.3 below);

b) non-regulated health professional:

— each certificate holder is a health professional who is not subject to registration or licensing from a government body (see 5.1 of ISO 17090-1:2008); these certificates may be qualified certificates;

c) sponsored healthcare provider:

— each certificate holder is an individual who is active in his/her healthcare community and is sponsored by a regulated healthcare organization or professional; these certificates may be qualified certificates;

d) supporting organization employee:

— each certificate holder is an individual who is a person employed by a healthcare organization or a supporting organization; these certificates may be qualified certificates;

e) patient/consumer:

— each certificate holder is an individual person who, at some stage, is about to receive, is receiving or has received the services of a regulated or non-regulated health professional; these may be qualified certificates.

5.4.3 Organization identity certificate

An organization that is involved in the health industry may hold a certificate to identify itself or to use for encryption purposes. In accordance with IETF/RFC 3647, provision is made in this part of ISO 17090 for an organizational unit name.

5.4.4 Device identity certificate

A device can be a computer server, a medical machine, such as a radiology machine, a vital signs monitoring device or a prosthetic device that needs to be individually identified and authenticated.

5.4.5 Application certificate

An application is a computer information system, such as a hospital patient administration system, that needs to be individually identified and authenticated.

This part of ISO 17090 concentrates on the providers, but recognizes that patients/consumers will increasingly require the security services that digital certificates can provide in managing their own healthcare.

5.4.6 AC

An AC is a digitally signed (or certified) set of attributes. An AC is a structure similar to a PKC; the main difference being that it contains no public key. An AC may contain attributes that specify group membership, role, security clearance and other information associated with the AC holder that could be used for access control. The AC shall be in accordance with the specifications given in IETF/RFC 3281.

Within the health industry context, ACs can fulfil the valuable role of communicating authorization information. Authorization information is distinct from information on healthcare roles or licences, which may be appropriately included in a PKC. Role or licence implies an authorization level, but they are not necessarily authorization information in themselves. It is important to note that the detailed specification for ACs is still evolving and that this specification still needs to be more widely implemented in the software industry.

The syntax of an AC is specified in IETF/RFC 3281.

The components of the AC are used as follows.

The **version** number differentiates between different versions of the AC. If **objectDigestInfo** is present or if **issuer** is identified with **baseCertificateID**, **version** shall be **v2**.

The **owner** field conveys the identity of the AC's holder. Use of the issuer name and serial number of a specific PKC is required; use of the general name(s) is optional and use of the object digest is prohibited. There is a risk with use of **GeneralNames** by itself to identify the holder, in that there is insufficient binding of a name to a public key to enable the authentication process of the owner's identity to be bound to the use of an AC. In addition, some of the options in **GeneralNames** (e.g. **IPAddress**) are inappropriate for use in naming an AC holder which is a role rather than an individual entity. General name forms should be restricted to distinguished names, RFC 822 (electronic mail) addresses, and (for role names) object identifiers.

The **issuer** field conveys the identity of the AA that issued the certificate. Use of the issuer name and serial number of a specific PKC is required, and use of the general name(s) is optional.

The **signature** identifies the cryptographic algorithm used to digitally sign the AC.

The **serialNumber** is the serial number that uniquely identifies the AC within the scope of its issuer.

The **attrCertValidityPeriod** field conveys the time period during which the AC is considered valid, expressed in **GeneralizedTime** format.

The **attributes** field contains the certificate holder's attributes that are being certified (e.g. the privileges).

The **issuerUniqueID** may be used to identify the issuer of the AC in instances where the issuer name is not sufficient.

The **extensions** field allows addition of new fields to the AC.

Details on the use of ACs in healthcare are specified in 8.4 of ISO 17090-1:2008.

5.4.7 Role certificates

A user's AC may contain a reference to another AC that contains additional privileges. This provides an efficient mechanism for implementing privileged roles.

Many environments that have authorization requirements require the use of role-based privileges (typically in conjunction with identity-based privileges) for some aspect of their operation. Thus, a claimant may present something to the verifier demonstrating only that the claimant has a particular role (e.g. "manager" or "purchaser"). The verifier may know *a priori*, or may have to discover by some other means, the privileges associated with the asserted role in order to make a pass/fail authorization decision.

The following are all possible:

— any number of roles can be defined by any AA;

— the role itself and the members of a role can be defined and administered separately, by separate AAs;

— the privileges assigned to a given role may be placed into one or more ACs;

— a member of a role may be assigned only a subset of the privileges associated with a role, if desired;

— role membership may be delegated;

— roles and membership may be assigned any suitable lifetime.

An entity is assigned an AC containing an attribute asserting that the entity occupies a certain role. That certificate has an extension pointing to another AC that defines the role (i.e. this role certificate specifies the role as holder and contains a list of privileges assigned to that role). The issuer of the entity certificate may be independent of the issuer of the role certificate and these may be administered (expired, revoked and so on) entirely separately.

Not all forms of **GeneralName** are appropriate for use as role names. The most useful choices are object identifiers and distinguished names.

6 General certificate requirements

6.1 Certificate compliance

The following requirements shall apply for all certificates specified in this part of ISO 17090.

— Certificates shall be X.509 version 3 certificates.

— Certificates shall be in accordance with IETF/RFC 3280. Deviations from IETF/RFC 3280 are only allowed if they are aligned with proposed solutions to known problems with IETF/RFC 3280.

— For individual identity, certificates should be in accordance with the IETF/RFC 3739. Deviations should only be allowed if they are aligned with proposed solutions to known problems.

— The signature field shall identify the signature algorithms used.

— The certified public key shall have a minimum key-length field depending on the algorithm used. Key sizes shall be in accordance with those specified in section 7.6.1.5 of ISO 17090-3:2008.

— dataEncipherment key usage shall not be combined with either non-repudiation or digitalSignature key usage (see 7.2.3).

The common elements in all healthcare digital certificates identified in Figure 1 are described below. These are the common elements upon which the different kinds of certificates are built.

Certificate ::= SIGNED { SEQUENCE {

version	**[0]**	**Version DEFAULT v1,**
serialNumber		**CertificateSerialNumber,**
signature		**AlgorithmIdentifier,**
issuer		**Name,**
validity		**Validity,**
subject		**Name,**
subjectPublicKeyInfo		**SubjectPublicKeyInfo,**
issuerUniqueIdentifier	**[1]**	**IMPLICIT UniqueIdentifier OPTIONAL,**
subjectUniqueIdentifier	**[2]**	**IMPLICIT UniqueIdentifier OPTIONAL,**
extensions	**[3]**	**Extensions MANDATORY,**

version is the version of the encoded certificate. The certificate version shall be v3.