TECHNICAL SPECIFICATION

ISO/TS 17090-1

First edition
2002-10-15

Health informatics — Public key infrastructure —

Part 1: Framework and overview

Informatique de santé — Infrastructure de clé publique — Partie 1: Cadre et vue d'ensemble

Reference number
ISO/TS 17090-1:2002(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.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to deciding whether it should be confirmed for a further three years, revised to become an International Standard, or withdrawn.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 17090-1 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*

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

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) 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 the 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.

Health informatics — Public key infrastructure —

Part 1:
Framework and overview

1 Scope

This part of ISO/TS 17090 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. It also identifies the major stakeholders who are communicating in health, as well as the main security services required for health communication where PKI may be required.

This part of ISO/TS 17090 gives a brief introduction to public key cryptography and the basic components of a healthcare PKI. It further introduces different types of certificates, public key identity certificates and associated attribute certificates, for relying parties, self-signed certification authority (CA) certificates, and CA hierarchies and bridging structures.

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 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

ISO/IEC 9594-8:2001, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks — Part 8*

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

ISO/TS 17090-3:2002, *Health informatics — Public key infrastructure — Part 3: Policy management of certification authority*

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

INTERNET-DRAFT October 1999 4.1, *X.509 Attribute Certificate*

3 Terms and definitions

For the purposes of this part of ISO/TS 17090, the following terms and definitions apply.

3.1 Healthcare context terms

3.1.1
application
identifiable computer running software process that is the holder of a private encipherment key

NOTE 1 Application, in this context, can be any software process used in healthcare information systems including those without any direct role in treatment or diagnosis.

NOTE 2 In some jurisdictions, including software processes can be regulated medical devices.

3.1.2
device
identifiable computer controlled apparatus or instrument that is the holder of a private encipherment key

NOTE 1 This includes the class of regulated medical devices that meet the above definition.

NOTE 2 Device, in this context, is any device used in healthcare information systems, including those without any direct role in treatment or diagnosis.

3.1.3
healthcare actor
regulated health professional, non-regulated health professional, sponsored healthcare provider, supporting organization employee, patient/consumer, healthcare organization, device or application that acts in a health related communication and requires a certificate for a PKI enabled security service

3.1.4
healthcare organization
officially registered organization that has a main activity related to healthcare services or health promotion

EXAMPLES Hospitals, Internet healthcare web site providers and healthcare research institutions.

NOTE 1 The organization is recognized to be legally liable for its activities but need not be registered for its specific role in health.

NOTE 2 An internal part of an organization is called here an organizational unit, as in X.501.

3.1.5
non-regulated health professional
person employed by a healthcare organization who is not a health professional

EXAMPLES Receptionist or secretary who organizes appointments, or a business manager who is responsible for validating patient health insurance.

NOTE The fact that the employee is not authorized by a body independent of the employer in his professional capacity does, of course, not imply that the employee is not professional in conducting his services.

3.1.6
patient
consumer
person who is the receiver of health related services and who is an actor in a health information system

3.1.7
privacy
freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual

[ISO/IEC 2382-8:1998]

3.1.8
regulated health professional
person who is authorized by a nationally recognized body to be qualified to perform certain health services

EXAMPLES Physicians, registered nurses and pharmacists.

NOTE 1 The types of registering or accrediting bodies differ in different countries and for different professions. Nationally recognized bodies include local or regional governmental agencies, independent professional associations and other formally and nationally recognized organizations. They may be exclusive or non-exclusive in their territory.

NOTE 2 A nationally recognized body in this definition does not imply one nationally controlled system of professional registration but, in order to facilitate international communication, it would be preferable for one nationwide directory of recognized health professional registration bodies to exist.

3.1.9
sponsored healthcare provider
health services provider who is not a regulated professional in the jurisdiction of his/her practice, but who is active in his/her healthcare community and sponsored by a regulated healthcare organization

EXAMPLES A drug and alcohol education officer who is working with a particular ethnic group, or a healthcare aid worker in a developing country.

3.1.10
supporting organization
officially registered organization which is providing services to a healthcare organization, but which is not providing healthcare services

EXAMPLES Healthcare financing bodies such as insurance institutions, suppliers of pharmaceuticals and other goods.

3.1.11
supporting organization employee
person employed by a supporting organization

EXAMPLES Medical records transcriptionists, healthcare insurance claims adjudicators and pharmaceutical order entry clerks.

3.2 Security services terms

3.2.1
access control
means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways

[ISO/IEC 2382-8:1998]

3.2.2
accountability
property that ensures that the actions of an entity may be traced uniquely to the entity

[ISO 7498-2:1989]

3.2.3
asymmetric cryptographic algorithm
algorithm for performing encipherment or the corresponding decipherment in which the keys used for encipherment and decipherment differ

[ISO 10181-1:1996]

3.2.4
authentication
process of reliably identifying security subjects by securely associating an identifier and its authenticator

[ISO 7498-2:1989]

NOTE See also data origin authentication and peer entity authentication.

3.2.5
authorization
granting of rights, which includes the granting of access based on access rights

[ISO 7498-2:1989]

3.2.6
availability
property of being accessible and useable upon demand by an authorized entity

[ISO 7498-2:1989]

3.2.7
ciphertext
data produced through the use of encipherment, the semantic content of which is not available

NOTE Adapted from ISO 7498-2:1989.

3.2.8
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO 7498-2:1989]

3.2.9
cryptography
discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use

[ISO 7498-2:1989]

3.2.10
cryptographic algorithm
cipher
method for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use

[ISO 7498-2:1989]

3.2.11
data integrity
property that data has not been altered or destroyed in an unauthorized manner

[ISO 7498-2:1989]

3.2.12
data origin authentication
corroboration that the source of data received is as claimed

[ISO 7498-2:1989]

3.2.13
decipherment
decryption
process of obtaining, from a ciphertext, the original corresponding data

[ISO/IEC 2382-8:1989]

NOTE A ciphertext may be enciphered a second time, in which case a single decipherment does not produce the original plaintext.

3.2.14
digital signature
data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient

[ISO 7498-2:1989]

NOTE See cryptography.

3.2.15
encipherment
encryption
cryptographic transformation of data to produce ciphertext

[ISO 7498-2:1989]

NOTE See cryptography.

3.2.16
identification
performance of tests to enable a data processing system to recognize entities

[ISO/IEC 2382-8:1998]

3.2.17
identifier
piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator

[ENV 13608-1]

3.2.18
integrity
proof that the message content has not been altered, deliberately or accidentally, in any way during transmission

NOTE Adapted from ISO 7498-2:1989.

3.2.19
key
sequence of symbols that controls the operations of encipherment and decipherment

[ISO 7498-2:1989]

3.2.20
key management
generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy

[ISO 7498-2:1989]

3.2.21
non-repudiation
service providing proof of the integrity and origin of data (both in an unforgeable relationship), which can be verified by any party

NOTE Adapted from ASTM [13].

3.2.22
private key
key that is used with an asymmetric cryptographic algorithm and whose possession is restricted (usually to only one entity)

[ISO 10181-1:1996]

3.2.23
public key
key that is used with an asymmetric cryptographic algorithm and that can be made publicly available

[ISO 10181-1:1996]

3.2.24
role
set of behaviours that is associated with a task

3.2.25
security
combination of availability, confidentiality, integrity and accountability

[ENV 13608-1]

3.2.26
security policy
plan or course of action adopted for providing computer security

[ISO/IEC 2382-8:1998]

3.2.27
security service
service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers

[ISO 7498-2:1989]

3.3 Public key infrastructure related terms

3.3.1
attribute authority
AA
authority which assigns privileges by issuing attribute certificates

[X.509]

3.3.2
attribute certificate
data structure, digitally signed by an attribute authority, that binds some attribute values with identification about its holder

[X.509]

3.3.3
authority certificate
certificate issued to a certification authority or to an attribute authority

NOTE Adapted from X.509.

3.3.4
certificate
public key certificate

3.3.5
certificate distribution
act of publishing certificates and transferring certificates to security subjects

3.3.6
certificate extension
extension fields (known as extensions) in X.509 certificates that provide methods for associating additional attributes with users or public keys and for managing the certification hierarchy

NOTE Certificate extensions may be either critical (i.e. a certificate-using system has to reject the certificate if it encounters a critical extension it does not recognize) or non-critical (i.e. it may be ignored if the extension is not recognized).

3.3.7
certificate generation
act of creating certificates

3.3.8
certificate management
procedures relating to certificates, i.e. certificate generation, certificate distribution, certificate archiving and revocation

3.3.9
certificate profile
specification of the structure and permissible content of a certificate type

3.3.10
certificate revocation
act of removing any reliable link between a certificate and its related owner (or security subject owner) because the certificate is not trusted any more, even though it is unexpired

3.3.11
certificate holder
entity that is named as the subject of a valid certificate

3.3.12
certificate verification
verifying that a certificate is authentic

3.3.13
certification
procedure by which a third party gives assurance that all or part of a data processing system conforms to security requirements

[ISO/IEC 2382-8:1998]