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)

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to deciding whether it should be confirmed for a further three years, revised to become an International Standard, or withdrawn.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.

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.

7.2.1.2.2 Certification revocation request

RAs can be instrumental in the handling of certificate revocation requests. In some health PKI implementations, RAs may be used to initiate or authenticate certificate revocation requests. Where applicable, they shall forward authenticated requests to the appropriate CA. The RA itself may initiate a revocation request (for example, if a regulated health professional is suspended for misconduct and the RA is a health profession registration board or licensing board). In either event, it is then the responsibility of the RA to authenticate the report. If, by applying the same criteria as the CA would have used, the RA is satisfied that the report is authentic, the RA shall send a signed message to the CA containing certificate identification information and, optionally, the stated reason for revoking that certificate.

7.2.1.2.3 Auditing

To provide assurance of the trusted nature of RAs and to provide information to personnel conducting internal audits, the actions of each RA shall be auditable. Audit records and audit trails shall be generated for events in accordance with the relevant policy.

7.2.1.2.4 Archiving

It may be important in the future to know how or why a certificate was produced. The RAs within healthcare PKIs or their CAs shall archive such events as requests for the creation or revocation of certificates.

7.2.1.3 Certificate holder obligations

(2.1.3)

A certificate holder in a healthcare PKI shall:

— ensure the accuracy of representations in the certificate application and, by accepting the certificate, acknowledge that all information included in the certificate is true;

— protect their private keys and key tokens (if applicable) and take all reasonable measures to prevent their loss, disclosure, modification or unauthorized use;

— make every effort to prevent the loss, disclosure or unauthorized use of his/her private key;

— immediately notify the CA and/or RA of any actual or suspected loss, disclosure, or other compromise of his/her private key;

— notify the RA and/or CA of any change in certificate information, role or status in the healthcare organization;

— read either the CP or a PKI disclosure document that clearly sets out in plain language the responsibilities of the certificate holder;

— use key pairs in accordance with the CP;

— formally agree to these obligations by signing a certificate holder agreement.

It is recommended that a certificate holder in a healthcare PKI also attest to receipt of security training appropriate to the health information functions for which the certificate will be used.

7.2.1.4 Relying party obligations

(2.1.4)

A relying party to healthcare PKIs has a right to rely on a healthcare certificate only if:

— the purpose for which the certificate is used was appropriate under this policy;

— the reliance is reasonable and in good faith in light of all the circumstances known to the relying party at the time of reliance;

— the relying party confirmed the current validity of the certificate by checking that the certificate was not revoked or suspended;

— the relying party confirmed the current validity of digital signatures, where applicable;

— applicable limitations of liability and warranties are acknowledged.

7.2.1.5 Repository obligations

(2.1.5)

Certificates and CRLs shall be available to relying parties in accordance with the requirements of 7.4.4.9 of this part of ISO/TS 17090.

7.2.2 Liability

(2.2)

7.2.2.1 General

The extent of the liability in the situations listed in 7.2.2.2 below is part of an overall policy under which the CAs operate in the healthcare domains of their respective countries. These domains are, in turn, subject to government regulations and international agreements. Requirements follow for CA liability and RA liability. If used, attribute authority liability shall either be subsumed by the former liability or explicitly delineated.

7.2.2.2 CA liability

(2.2.1)

The liability of the CA in a healthcare PKI may be limited to acts of negligence on the part of the CA as follows.

a) A CA may assume no liability associated with the loss by the certificate holder of the private keys.

b) A CA may assume no liability associated with certificate holder generated keys, unless they were generated in full accordance with the guidelines of a healthcare PKI.

c) A CA may assume no liability associated with the compromise of the private keys it produces, unless it can be proved that the keys were compromised at the CA or that documented policies and procedures were not followed during the key generation process, resulting in a private key that is more susceptible to compromise or the actual revelation of the private key.

d) A CA may assume no liability associated with forged signatures, unless the forgery resulted from the documented policies and procedures of a healthcare PKI not being followed, or could be shown to permit the forgery.

e) A CA may limit its liability to the extent of the direct damages sustained by the relying party and caused by the failure of the CA to comply with the terms of this policy.

The liability of the CA in a healthcare PKI shall not be limited in regard to the following.

a) A CA shall be liable for the compromise of a private key during the key distribution process.

b) A CA shall be liable for the wrongful binding of an individual's identity with an associated digital signature and other accreditation information, unless it can be proved that the documented policies and procedures for identification and authentication were followed. This liability shall extend to circumstances where a CA knew or suspected, or should have known or suspected, that the binding might be wrongful.

c) A CA shall be liable for not revoking certificates according to its revocation policy.

d) A CA shall be liable for revoking a certificate for a reason not specified in its revocation policy.

7.2.2.3 RA liability

(2.2.2)

The liability of an RA in a healthcare PKI may be limited to acts of negligence on the part of the RA.

The liability of an RA in a healthcare PKI shall not be limited in regard to the following.

a) An RA is liable for the wrongful binding of an individual's identity and other accreditation information with an associated digital signature, unless it can be proved that the documented policies and procedures for identification and authentication were followed. This liability shall extend to circumstances where an RA knew or suspected, or should have known or suspected, that the subject information on which the binding was made might be wrongful.

b) An RA is liable for not revoking certificates according to its revocation policy.

c) A RA is liable for revoking a certificate for a reason not specified in its revocation policy.

7.2.3 Financial responsibility

(2.3)

7.2.3.1 Indemnification by relying parties

Indemnification by relying parties shall be in accordance with 2.3.1 of IETF/RFC 2527.

7.2.3.2 Fiduciary relationships

Fiduciary relationships shall be in accordance with 2.3.2 of IETF/RFC 2527.

7.2.3.3 Administrative processes

Administrative processes shall be in accordance with 2.3.3 of IETF/RFC 2527.

7.2.4 Interpretation and enforcement

(2.4)

7.2.4.1 Governing law

(2.4.1)

Healthcare PKIs shall comply with local and international legal requirements in accordance with ISO 17799-1:2000 (or its equivalent) or approved accreditation or licensing criteria.

7.2.4.2 Severability, survival, merger, notice

(2.4.2)

The healthcare CP shall stipulate that, should it be determined that one section of the CP is incorrect or invalid, other sections shall remain in effect until the policy is updated.

If the CA or RA merges with another organization, the new organization remains liable for the course of the original agreement.

7.2.4.3 Dispute resolution procedures

Dispute resolution procedures shall be in accordance with 2.4.3 of IETF/RFC 2527.

7.2.5 Fees

(2.5)

Fees shall be in accordance with 2.5 of IETF/RFC 2527.

7.2.6 Publication and repository

(2.6)

7.2.6.1 Publication of CA information

(2.6.1)

All CAs within healthcare PKIs 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 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.

7.2.6.2 Frequency of publication

(2.6.2)

CAs shall publish information, whenever such information has been modified. Information on certificate revocation shall be in accordance with 7.4.4 of this part of ISO/TS 17090.

7.2.6.3 Access controls

(2.6.3)

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

7.2.6.4 Repositories

(2.6.4)

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 17799:2000 (or its equivalent) or approved accreditation or licensing criteria.

7.2.7 Compliance audit

(2.7)

Compliance audit is an essential component of many PKI interoperability models (see, for example, 9.2.4 of ISO/TS 17090-1).

7.2.7.1 Frequency of CA compliance audit

(2.7.1)

A CA issuing certificates pursuant to a healthcare PKI policy shall establish to the satisfaction of any relying party that it fully complies with the requirements of this policy. A CA compliance audit shall be carried out by a qualified independent third party within intervals that are no more than one year apart.

7.2.7.2 Identity/Qualifications of auditor

(2.7.2)

The auditor shall be a qualified information systems auditor to the extent necessary for admission to the relevant professional body (such as accreditation to ISO 9000). The auditor shall possess significant PKI experience. Where a formal accreditation body exists, the auditor shall meet that body's requirements.

7.2.7.3 Auditor's relationship to audited party

(2.7.3)

The auditor shall be completely independent of the audited party by belonging to a separate organization from the CA. The auditor shall have no financial interest in the audited party.

7.2.7.4 Topics covered by audit

(2.7.4)

Events such as certificate holder registration, certificate registration, compromised key reports and certificate revocation shall be audited. The audit will generally cover compliance to CPs and to associated CPSs.

7.2.7.5 Actions taken as a result of deficiency

(2.7.5)

7.2.7.5.1 General

If irregularities are found in an audit, the CA shall take corrective action. Where a CA fails to take appropriate action in response to the audit, the CA's governing body may:

— indicate the irregularities, but allow the CA to continue operations until the next audit; or

— allow the CA to continue operations for a maximum of thirty days pending correction of any problems prior to revocation; or

— revoke the CA's certificate.

Any decision regarding which of these actions to take shall be based on the severity of the irregularities. However, the CA cannot be shut down as this may disrupt services.

7.2.7.5.2 Critical failure category

Inability of a CA to comply with essential sections of the CPS as determined by a CA accreditation body (where such accreditation exists within the jurisdiction in which the CA operates) shall be classified as a critical failure. For example, the detection of a CA having cut back on expensive procedures resulting in their certificates being compromised shall be classified as a critical failure.

Where the CA has been accredited in its jurisdiction, it is recommended that accreditation be withdrawn immediately.

7.2.7.5.3 Major failure category

A CA failing to comply with important element(s) of the CPS, which was assessed as part of the assurance process, shall be classified as a major failure. For example, the identification of a CA not maintaining sufficient business continuity practices shall be classified as a major failure.

Escalation of the problem to a critical failure shall be imposed if additional events impact on the CA simultaneously or if the CA fails to rectify the compliance problem within several days.

7.2.7.5.4 Partial failure category

Any compliance breach against the CPS, which is assessed as part of the assurance process as not being reasonably likely to turn into a major failure but which could impact on the integrity of the CA's operations, shall be classified as a partial failure. For example, out-of-date security policies and procedures shall be classified as a partial failure.

Escalation of the problem to the major failure category shall be imposed if additional failures within this category are detected or if the CA fails to rectify the compliance problem within 30 days.

7.2.7.5.5 Minor failure category

Compliance failures which are viewed as being unlikely to turn into a partial failure, but which should be addressed to reduce the overall impact on the integrity of the CA's operations should be classified as minor failures. For example, administrative failings (i.e. inaccurate billing) should be classified as being a minor failure.

Escalation of the problem to the partial failure category shall be imposed if additional failures within this category are detected or if the CA fails to rectify the compliance problem before the next scheduled audit.

7.2.7.6 Communication of audit results

(2.7.6)

Certificate holders and relying parties shall immediately be notifed of any CA or RA that is found by an auditor to be deficient.

7.2.8 Confidentiality

(2.8)

7.2.8.1 Information to be kept confidential

(2.8.1)

The following information shall be kept confidential:

— personal information of certificate holders and registration authorities collected for identification purposes, but which is not included in the certificate (e.g. personal identification, background checks, home address, contact details). Some of this information may, with the consent of the certificate holder, be included in the directory listing for that certificate holder;

— private keys.

7.2.8.2 Information not to be considered as confidential

(2.8.2)

The following information shall not be considered as confidential:

— public key;

— role of regulated or non-regulated health professional;

— healthcare speciality.

7.2.8.3 Disclosure of certificate revocation/suspension

(2.8.3)

The CA shall keep confidential information pertaining to the reason for a certificate holder's certificate revocation or suspension.

7.2.8.4 Release to law enforcement officials

(2.8.4)

Confidential information shall only be released with the explicit consent of the certificate holder or as required under the CA or RA country's law.

7.2.8.5 Release as part of civil discovery

(2.8.5)

Confidential information shall only be released with the explicit consent of the certificate holder or on presentation of an order from a recognized court of law under the CA or RA country's law.

7.2.8.6 Disclosure upon certificate holder's request

(2.8.6)

Confidential information shall be disclosed to parties nominated by the certificate holder following a request either by authenticated electronic mail (bearing the certificate holder's digital signature) or by signed written authority from the requesting certificate holder.

7.2.8.7 Other information release circumstances

(2.8.7)

Confidential information shall only be disclosed following the presentation of an order from a recognized court of law under the CA or RA country's law.

7.2.9 Intellectual property rights

(2.9)

Intellectual property rights shall be in accordance with 2.9 of IETF/RFC 2527.

7.3 Identification and authentication

(3)

7.3.1 Initial registration

(3.1)

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/TS 17090-2:2002.

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. This does not preclude the use of pseudonyms in certificates issued to patients/consumers.

7.3.1.3 Recognition, authentication and role of trademarks

(3.1.3)

Recognition, authentication and the role of trademarks shall be in accordance with 3.1.3 of IETF/RFC 2527.

7.3.1.4 Uniqueness of names

(3.1.4)

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

7.3.1.5 Name claim dispute resolution procedure

(3.1.5)

A CP shall have a name claim dispute resolution procedure to apply in those situations where name claim disputes arise.

7.3.1.6 Method to prove possession of private key

(3.1.7)

Key holders shall be required to prove possession of their private key by electronically signing any request they may make to the CA and may also be periodically required to sign a challenge from the CA.

7.3.1.7 Authentication of identity of organizations

(3.1.8)

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.

7.3.1.8 Authentication of identity of individuals

(3.1.9)

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/TS 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.

Non-regulated health professionals, in order that they establish their employment and authenticate their healthcare role, shall present to the RA proof of sponsorship or employment from their sponsoring health organizations or sponsoring (regulated) health professionals.

Sponsored healthcare providers, in order that they establish that they are active in their healthcare community and in order that they authenticate their healthcare role, shall present to the RA proof of sponsorship from their sponsoring health organizations or sponsoring (regulated) health professionals.

Supporting organization employees, in order that they establish their employment and authenticate their healthcare role, shall present to the RA proof of employment by their supporting health organizations.

7.3.2 Routine rekeying

(3.2)

7.3.2.1 CA routine rekeying

Routine rekeying of CA information shall be carried out based on the original documentation used when the original record was created.

7.3.2.2 RA routine rekeying

Routine rekeying of RA information shall be carried out based on the original documentation used when the original record was created.

7.3.2.3 Certificate holder routine rekeying

Routine rekeying of certificate holder information shall be carried out by referring back to the original documentation or records used when the original record was created.

If the original documentation has lapsed or been discarded, substitute documentation may be used.

7.3.3 Rekey after revocation — No key compromise

(3.3)

7.3.3.1 CA rekey after revocation — No key compromise

Rekeying of information after a certificate has been revoked for reasons other than a key compromise shall require presentation again of the original information originally used to accredit the CA.

7.3.3.2 RA rekey after revocation — No key compromise

Rekeying of information after a certificate has been revoked for reasons other than a key compromise shall require presentation again of the original information originally used to accredit the RA.

7.3.3.3 Certificate holder rekey after revocation — No key compromise

Routine rekeying of certificate holder information shall require either presentation of the original documentation used when the original record was created or reference to the original records used. If the original documentation has lapsed or been discarded, substitute documentation may be used.

7.3.4 Revocation request

(3.4)

7.3.4.1 CA

A CA within a healthcare PKI, when making a revocation request to another CA, shall:

— identify the certificate;

— state the reasons why the certificate should be revoked;

— sign the request with its private key, encrypt the message and send it to the relevant domain CA.

7.3.4.2 RA

An RA within a healthcare PKI, when making a revocation request to a certification authority, shall:

— identify the certificate that it is requesting to have revoked;

— state the reasons why the certificate should be revoked;

— sign the request with its private key, encrypt the message and send it to the relevant domain CA.

7.3.4.3 Certificate holder

A certificate holder within a healthcare PKI, when making a revocation request to a certification authority, shall:

— identify the certificate that the certificate holder is requesting to have revoked;

— state the reasons why the certificate should be revoked;

— sign the request with its private key, encrypt the message and send it to the relevant domain CA.

It should be noted that, requiring a signed request for revocation is not contradictory, even in the case of suspected key compromise: either the revocation request genuinely comes from the certificate holder, or a third party is using a compromised key to initiate the request, in which case the key should be revoked anyway.

If the token containing the private key has been lost or stolen (and the certificate holder cannot therefore initiate a digitally signed request by some other means) the revocation request shall be accompanied by equivalent evidence of identity to that originally provided to obtain the certificate.

7.4 Operational requirements

(4)

7.4.1 Certificate application

Certificate application shall be in accordance with 4.1 of IETF/RFC 2527.

7.4.2 Certificate issuance

Certificate issuance shall be in accordance with 4.2 of IETF/RFC 2527.

7.4.3 Certificate acceptance

(4.3)

Certificate acceptance shall be in accordance with 4.3 of IETF/RFC 2527.

7.4.4 Certificate suspension and revocation

(4.4)

7.4.4.1 Circumstances for revocation

(4.4.1)

The issuing CA shall revoke a certificate:

— upon failure of the certificate holder, the employer (in the case of a non-regulated health professional or supporting organization employee), or the sponsor (in the case of a sponsored healthcare provider) to meet obligations under this policy, any applicable CPS, or any other agreement, regulation or law applicable to the certificate that may be in force;

— upon knowledge or reasonable suspicion of compromise of a private key;

— if relevant subject information contained in the certificate is no longer accurate;

— if a certificate holder's organizational affiliation changes, e.g. a regulated health professional resigning from a particular organization;

— if the CA determines that the certificate was not properly issued in accordance with this policy and/or any applicable CPS;

— for any reason, upon request of a certificate holder or sponsor of a sponsored healthcare provider.

Certificate holders, RAs and sponsors have a duty to inform the CA if they become aware of inaccuracy of the subject information in the certificate.

7.4.4.2 Who can request revocation

(4.4.2)

The revocation of a certificate shall be requested by one or more of the following:

— the certificate holder in whose name the certificate was issued;

— the individual or organization that made the application for the certificate on behalf of a device or application;

— the sponsor of a sponsored healthcare provider;

— personnel of the issuing CA;

— personnel of an RA associated with the issuing CA.

7.4.4.3 Procedure for revocation request

(4.4.3)

When a revocation request is received by the CA, in accordance with 3.4 of IETF/RFC 2527, the CA shall:

— confirm that the entity requesting revocation is the certificate holder listed in the certificate to be revoked;

— if the requestor is acting as an agent of the certificate holder, that the requestor has sufficient authority to effect revocation;

— verify the reasons given for revocation and, if they prove be true, revoke the certificate.

7.4.4.4 Revocation request grace period

(4.4.4)

Any action taken as a result of a request for the revocation of a certificate shall be initiated immediately upon receipt.

7.4.4.5 Circumstances for suspension

(4.4.5)

Within healthcare PKIs, a CA may support suspension. The identified circumstances that will justify certificate suspension include:

— suspected compromise of private keys, in which case suspension will occur during investigation;

— pending clarification of information on the certificate;

— a certificate holder requests suspension;

— other circumstances determined within local healthcare PKI domains.

7.4.4.6 Who can request suspension

(4.4.6)

Where a CA supports suspension, the suspension of a certificate shall be requested by one or more of:

— the certificate holder in whose name the certificate was issued;

— the individual or organization that made the application for the certificate on behalf of a device or application;

— the sponsor of a sponsored healthcare provider;

— personnel of the issuing CA;

— personnel of an RA associated with the issuing CA;

— a relying party.

7.4.4.7 Procedures for suspending certificates

(4.4.7)

When a suspension request is received by the CA, in accordance with 7.4.4.5 of this part of ISO/TS 17090, the CA shall:

— confirm the identity of the requestor, where the suspension request is purported to be from the certificate holder, or from the individual or organization that made the application for the certificate on behalf of a device or application, or from the sponsor of a sponsored healthcare provider;

— confirm the identity of the requestor, where the suspension request is purported to be from the individual or organization that made the application for the certificate on behalf of a device or application;

— confirm that the requestor has sufficient authority to effect suspension, if the requestor is acting as the sponsor of the certificate holder;

— verify the reasons given for suspension and, if they prove be true, suspend the certificate.

7.4.4.8 Limits on suspension period

(4.4.8)

The suspension period for certificates shall be limited to the time of any investigation required (e.g. to verify information). It is recommended that suspensions last no longer than ten working days.

7.4.4.9 CRL issuance frequency

(4.4.9)

Notice of revocation shall be published promptly (on the day of issue) and updated whenever changes are made to the CRL.

7.4.4.10 CRL checking requirements

(4.4.10)

Relying parties should check the CRL whenever they begin using another entities' public key. The CRL should be checked at least daily for revocations.

7.4.4.11 On-line revocation/status checking availability

(4.4.11)

The CA should make its CRL checking service available to match the business hours of its relying parties.

7.4.4.12 On-line revocation checking requirements

(4.4.12)

On-line revocation checking will require certificate holders to establish secure communication with an on-line certificate status-checking server, which has the capacity of signing responses: this may be the CA. In this way, the authenticity of the CA will be verified. It may also be possible to use validation authorities or outsourced directories rather than the issuing CA.

7.4.4.13 Other forms of revocation advertisements available

Other forms of revocation advertisements available shall be in accordance with 4.4.13 of IETF/RFC 2527.

7.4.4.14 Checking requirements for other forms of revocation advertisements

Checking requirements for other forms of revocation advertisements shall be in accordance with 4.4.14 of IETF/RFC 2527.

7.4.4.15 Special requirements regarding key compromise

(4.4.15)

In the event of the compromise of a CA signing key, the CA shall immediately notify CAs to whom it has issued cross-certificates.

7.4.5 Security audit procedures

(4.5)

Security audit procedures shall be in accordance with ISO 17799:2000.

7.4.6 Records archival

(4.6)

Records shall be archived in accordance with ISO 17799:2000.

7.4.7 Key changeover

(4.7)

To enable certificate holders to seamlessly change over from one public key to another, the CA should issue the new certificate 30 days in advance of the changeover date and clearly inform certificate holders of the date from which they will need to use the new certificate.

7.4.8 Compromise and ensuring business continuity

(4.8)

Security audit procedures shall be in accordance with ISO 17799:2000.

7.4.9 CA termination

(4.9)

In the event that a CA ceases operation, it shall notify its certificate holders immediately upon the termination of operations and arrange for the continued retention of the CA's keys and information. It shall also notify all CAs with whom it is cross-certified.

In the event of a transfer of a CA's operations to another CA operating at a lower level of assurance, the certificates issued by the CA whose operations are being transferred shall be revoked through a CRL signed by that CA prior to the transfer.

In the event that a CA terminates, arrangements shall be made to ensure the secure archival or disposal of that CA's records.

7.5 Physical, procedural and personnel security controls

(5)

7.5.1 General

Physical, procedural and personnel security controls shall be in accordance with ISO 17799:2000 (or its equivalent) or with approved accreditation or licensing criteria.

7.5.2 Physical controls

(5.1)

Physical controls shall be in accordance with ISO 17799:2000 (or its equivalent).

7.5.3 Procedural controls

(5.2)

Procedural controls shall be in accordance with ISO 17799:2000 (or its equivalent).

7.5.4 Personnel controls

(5.3)

Personnel controls shall be in accordance with ISO 17799:2000 (or its equivalent).

7.6 Technical security controls

(6)

7.6.1 Key pair generation and installation

(6.1)

7.6.1.1 Key pair generation

(6.1.1)

A certificate holder's public/private key pair shall be generated by:

— the CA, or

— another trusted third party nominated by the CA, or

— the certificate holder by means of a key management function or application approved by the CA.

If the key pair is generated by a third party, it shall be mandatory for it to employ security measures (such as a hardware token) to prevent tampering with key pairs and compromise of generated private keys.

7.6.1.2 Private key delivery

(6.1.2)

If the private decipherment key is not generated by the prospective certificate holder, it shall be either delivered to the certificate holder in an on-line transaction in accordance with IETF/RFC 2511, or via an equally secure manner.

The CA or trusted third party key generating entity shall be able to prove that there are no copies of the private key in its possession after it hands over the original private key, except where such copies are kept for the purposes of key backup, in accordance with 7.6.2.4 of this part of ISO/TS 17090.

7.6.1.3 Public key delivery to certificate issuer

(6.1.3)

If the public encipherment key is not generated by the CA, it shall be either delivered to the CA in an on-line transaction in accordance with IETF/RFC 2511, or via an equally secure manner.

7.6.1.4 CA public key delivery to certificate holders

(6.1.4)

As the public key is bound to the certificate, the public key shall be sent to certificate holders with the certificate as soon as it is created. The same procedures shall apply to public key delivery as they do to certificate delivery and are covered in 4.2 of IETF/RFC 2527.

7.6.1.5 Key sizes

(6.1.5)

The minimum key size will depend on the algorithm used. The minimum key size for CA certificates shall be 2048 bits for the RSA algorithm. The minimum key size for CA certificates using other algorithms shall be such as to provide equivalent security. The minimum key size for non-CA certificates shall be 1024 bits for the RSA algorithm or its technological equivalent. The minimum key size for non-CA certificates using other algorithms shall be such as to provide equivalent security.

7.6.1.6 Public key parameters generation

(6.1.6)

Public key parameters shall be generated by either the CA or the trusted third party key generation organization.

7.6.1.7 Parameter quality checking

(6.1.7)

It shall be the role of the auditing organization to check the parameter quality.

7.6.1.8 Hardware/Software key generation

(6.1.8)

Key generation shall be provided in a secure manner.

7.6.1.9 Key usage purposes as per X.509 v3 key usage field

(6.1.9)

Authentication and digital signature keys shall only be used for identification and/or non-repudiation purposes. There shall be a separate pair of keys for encipherment purposes.

7.6.2 Private key protection

(6.2)