INTERNATIONAL STANDARD

ISO 17090-3

First edition
2008-02-15

Health informatics — Public key infrastructure —

Part 3: Policy management of certification authority

Informatique de santé — Infrastructure de clé publique —

Partie 3: Gestion politique d'autorité de certification

Reference number
ISO 17090-3:2008(E)

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

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

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

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

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

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

— *Part 1: Overview of digital certificate services*

— *Part 2: Certificate profile*

— *Part 3: Policy management of certification authority*

Introduction

The healthcare industry is faced with the challenge of reducing costs by moving from paper-based processes to automated electronic processes. New models of healthcare delivery are emphasizing the need for patient information to be shared among a growing number of specialist healthcare providers and across traditional organizational boundaries.

Healthcare information concerning individual citizens is commonly interchanged by means of electronic mail, remote database access, electronic data interchange and other applications. The Internet provides a highly cost-effective and accessible means of interchanging information, but it is also an insecure vehicle that demands additional measures be taken to maintain the privacy and confidentiality of information. Threats to the security of health information through unauthorized access (either inadvertent or deliberate) are increasing. It is essential to have available to the healthcare system reliable information security services that minimize the risk of unauthorized access.

How does the healthcare industry provide appropriate protection for the data conveyed across the Internet in a practical, cost-effective way? Public key infrastructure (PKI) and digital certificate technology seek to address this challenge.

The proper deployment of digital certificates requires a blend of technology, policy and administrative processes that enable the exchange of sensitive data in an unsecured environment by the use of “public key cryptography” to protect information in transit and “certificates” to confirm the identity of a person or entity. In healthcare environments, this technology uses authentication, encipherment and digital signatures to facilitate confidential access to, and movement of, individual health records to meet both clinical and administrative needs. The services offered by the deployment of digital certificates (including encipherment, information integrity and digital signatures) are able to address many of these security issues. This is especially the case if digital certificates are used in conjunction with an accredited information security standard. Many individual organizations around the world have started to use digital certificates for this purpose.

Interoperability of digital certificate technology and supporting policies, procedures and practices is of fundamental importance if information is to be exchanged between organizations and between jurisdictions in support of healthcare applications (for example between a hospital and a community physician working with the same patient).

Achieving interoperability between different digital certificate implementations requires the establishment of a framework of trust, under which parties responsible for protecting an individual’s information rights may rely on the policies and practices and, by extension, the validity of digital certificates issued by other established authorities.

Many countries are deploying digital certificates to support secure communications within their national boundaries. Inconsistencies will arise in policies and procedures between the certification authorities (CAs) and the registration authorities (RAs) of different countries if standards development activity is restricted to within national boundaries.

Digital certificate technology is still evolving in certain aspects that are not specific to healthcare. Important standardization efforts and, in some cases, supporting legislation are ongoing. On the other hand, healthcare providers in many countries are already using or planning to use digital certificates. ISO 17090 seeks to address the need for guidance of these rapid international developments.

ISO 17090 describes the common technical, operational and policy requirements that need to be addressed to enable digital certificates to be used in protecting the exchange of healthcare information within a single domain, between domains and across jurisdictional boundaries. Its purpose is to create a platform for global interoperability. It specifically supports digital certificate-enabled communication across borders, but could also provide guidance for the national or regional deployment of digital certificates in healthcare. The Internet

is increasingly used as the vehicle of choice to support the movement of healthcare data between healthcare organizations and is the only realistic choice for cross-border communication in this sector.

ISO 17090 should be approached as a whole, with the three parts all making a contribution to defining how digital certificates can be used to provide security services in the health industry, including authentication, confidentiality, data integrity and the technical capacity to support the quality of digital signature.

ISO 17090-1 defines the basic concepts underlying the use of digital certificates in healthcare and provides a scheme of interoperability requirements to establish digital certificate-enabled secure communication of health information.

ISO 17090-2 provides healthcare-specific profiles of digital certificates based on the international standard X.509 and the profile of this, specified in IETF/RFC 3280 for different types of certificates.

This part of ISO 17909 deals with management issues involved in implementing and using digital certificates in healthcare. It defines a structure and minimum requirements for certificate policies (CPs) and a structure for associated certification practice statements. This part of ISO 17090 is based on the recommendations of the informational IETF/RFC 3647, and identifies the principles needed in a healthcare security policy for cross border communication. It also defines the minimum levels of security required, concentrating on the aspects unique to healthcare.

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

Health informatics — Public key infrastructure —

Part 3:
Policy management of certification authority

1 Scope

This part of ISO 17090 gives guidelines for certificate management issues involved in deploying digital certificates in healthcare. It specifies a structure and minimum requirements for certificate policies, as well as a structure for associated certification practice statements.

This part of ISO 17090 also identifies the principles needed in a healthcare security policy for cross-border communication and defines the minimum levels of security required, concentrating on aspects unique to healthcare.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 17090-1:2008, *Health informatics — Public key infrastructure — Part 1: Overview of digital certificate services*

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

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

IETF/RFC 3647, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*

IETF/RFC 4211, *Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 17090-1 apply.

4 Abbreviations

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

5 Requirements for digital certificate policy management in a healthcare context

5.1 General

Deployment of digital certificates in healthcare shall meet the following objectives in order to be effective in securing the communication of personal health information:

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

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

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

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

To do this, each CA issuing digital certificates for use in healthcare shall operate according to an explicit set of publicly stated policies that promote the above objectives.

5.2 Need for a high level of assurance

Security services required for health applications are specified in Clause 6 of ISO 17090-1:2008. For each of these security services (authentication, integrity, confidentiality, digital signature, authorization, access control), a high level of assurance is required.

5.3 Need for a high level of infrastructure availability

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

5.4 Need for a high level of trust

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

5.5 Need for Internet compatibility

As the purpose of this part of ISO 17090 is to define the essential elements of a healthcare digital certificate deployment to support the secure transmission of healthcare information across national or regional boundaries, it is based as much as possible upon Internet standards so as to effectively span those boundaries.

5.6 Need to facilitate evaluation and comparison of CPs

Approaches for using digital certificates to facilitate the secure exchange of health information across national boundaries are discussed in 9.2 of ISO 17090-1:2008. These approaches (such as cross-recognition and cross-certification) are greatly facilitated if healthcare CPs follow a consistent format so that comparisons may be readily drawn between the provisions of one CP and another.

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

6 Structure of healthcare CPs and healthcare CPSs

6.1 General requirements for CPs

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

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

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

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

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

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

— distributing certificates to certificate holders and to directories;

— accepting information about possible private key compromise;

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

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

— cross-certifying with other CAs;

— security controls and auditing.

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

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

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

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

a) Each digital certificate issued in accordance with this part of ISO 17090 shall contain at least one registered CP OID, which identifies the CP under which the certificate was issued.

b) The structure of CPs shall be in accordance with IETF/RFC 3647.

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

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

6.2 General requirements for CPSs

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

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

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

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

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

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

6.3 Relationship between a CP and a CPS

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

6.4 Applicability

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

7 Minimum requirements for a healthcare CP

7.1 General requirements

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

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

7.2 Publication and repository responsibilities

7.2.1 Repositories

(2.1)

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

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

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

7.2.2 Publication of certification information

(2.2)

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

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

— each certificate issued or renewed under this policy;

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

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

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

— on a web site available to all relying parties or

— via an electronic mail request.

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

7.2.3 Frequency of publication

(2.3)

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

7.2.4 Access controls on repositories

(2.4)

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

7.3 Identification and authentication

7.3.1 Initial registration

7.3.1.1 Types of name

(3.1.1)

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

7.3.1.2 Need for names to be meaningful

(3.1.2)

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

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

7.3.1.3 Anonymity or pseudonymity

(3.1.3)

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

7.3.1.4 Rules for interpreting various name forms

(3.1.4)

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

7.3.1.5 Uniqueness of names

(3.1.5)

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

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

7.3.1.6 Recognition, authentication and role of trademarks

(3.1.6)

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

7.3.2 Initial identity validation

7.3.2.1 Method to prove possession of private key

(3.2.1)

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

7.3.2.2 Authentication of identity of organizations

(3.2.2)

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

7.3.2.3 Authentication of identity of individuals

(3.2.3)

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

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

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.

7.3.2.4 Non-verified subscriber information

(3.2.4)

Non-verified subscriber information shall be specified in accordance with 3.2.4 of IETF/RFC 3647.

7.3.2.5 Validation of authority

(3.2.5)

Validation of authority shall be specified in accordance with 3.2.5 of IETF/RFC 3647.

7.3.2.6 Criteria for interoperation

(3.2.6)

Criteria for interoperation shall be specified in accordance with 3.2.6 of IETF/RFC 3647 and ISO 17090-2.

7.3.3 Identification and authentication for re-keying requests

7.3.3.1 Identification and authentication for routine re-key

(3.3.1)

7.3.3.1.1 CA routine re-keying

Routine re-keying or re-issue of CA certificates shall be carried out based on the original documentation used when the original record was created.

7.3.3.1.2 RA routine re-keying

Routine re-keying or re-issue of RA certificates shall be carried out based on the original documentation used when the original record was created.

7.3.3.1.3 Certificate holder routine re-keying

Routine re-keying of certificate holder information shall be carried out by referring back to the original documentation or records used when the original record was created, including reliance on a current valid unexpired key.

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

7.3.3.2 Re-key after revocation

(3.3.2)

7.3.3.2.1 CA re-key after revocation

Re-keying of information after a certificate has been revoked shall require presentation again of the original information originally used to accredit the CA.

7.3.3.2.2 RA re-key after revocation

Re-keying of information after a certificate has been revoked shall require presentation again of the original information originally used to accredit the RA.

7.3.3.2.3 Certificate holder re-key after revocation

Routine re-keying 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 Identification and authentication for revocation request

(3.4)

7.3.4.1 CA

A CA, when making a revocation request under a healthcare CP 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, when making a revocation request to a CA for a digital certificate issued under a healthcare CP, 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 of a digital certificate issued under a healthcare CP, when making a revocation request to a CA, shall:

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

— state the reasons why the certificate should be revoked;

— securely send the revocation request to the relevant domain CA.

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

7.4 Certificate life-cycle operational requirements

7.4.1 Certificate application

7.4.1.1 Who can submit a certificate application

(4.1.1)

Criteria for who can submit a certificate application shall be specified in accordance with 4.1.1 of IETF/RFC 3647.

7.4.1.2 Enrollment process and responsibilities

(4.1.2)

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, independent 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, revocation requests, and other authenticated communications with certificate holders, 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) in accordance with 7.3.4.2.

A certificate holder in a healthcare deployment of digital certificates 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.

7.4.2 Certificate application processing

7.4.2.1 Performing identification and authentication functions

(4.2.1)

Criteria for performing identification and authentication functions shall be specified in accordance with 4.2.1 of IETF/RFC 3647.

7.4.2.2 Approval or rejection of certificate applications

(4.2.2)

Criteria for approval or rejection of certificate applications shall be specified in accordance with 4.2.2 of IETF/RFC 3647.

7.4.2.3 Time to process certificate applications

(4.2.3)

It is recommended that the CA state a maximum period of time by which a certificate holder has to complete the key activation process after the initiation of the certificate issuance process.

7.4.3 Certificate issuance

7.4.3.1 CA actions during certificate issuance

(4.3.1)

Certificate re-key procedures shall be specified in accordance with 4.7 of IETF/RFC 3647.

7.4.3.2 Notifications to certificate holders by the CA of issuance of the certificate

(4.3.2)

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

7.4.4 Certificate acceptance

7.4.4.1 Conduct constituting certificate acceptance

(4.4.1)

A certificate holder in a healthcare deployment of digital certificates shall:

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

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

7.4.4.2 Publication of the certificate by the CA

(4.4.2)

See 7.2.2.

7.4.4.3 Notification of certificate issuance by the CA to other entities

(4.4.3)

Criteria for notification of certificate issuance by the CA to other entities shall be specified in accordance with 4.4.3 of IETF/RFC 3647.

7.4.5 Key pair and certificate usage

7.4.5.1 Certificate holder private key and certificate usage

(4.5.1)

A certificate holder in a healthcare deployment of digital certificates shall:

— 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;

— use key pairs in accordance with the CP.

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

7.4.5.2 Relying party public key and certificate usage

(4.5.2)

A relying party 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.

7.4.6 Certificate renewal

(4.6)

The issuing CA shall ensure that any procedures for the renewal of a certificate shall conform to the relevant provisions of this CP.

7.4.6.1 Circumstances for certificate renewal

(4.6.1)

Circumstances for certificate renewal shall be specified in accordance with 4.6.1 of IETF/RFC 3647.

7.4.6.2 Who may request renewal

(4.6.2)

Criteria for who may request renewal shall be specified in accordance with 4.6.2 of IETF/RFC 3647.

7.4.6.3 Processing certificate renewal requests

(4.6.3)

Criteria for processing certificate renewal requests shall be specified in accordance with 4.6.3 of IETF/RFC 3647.

7.4.6.4 Notification to certificate holder of certificate renewal

(4.6.4)

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

7.4.6.5 Conduct constituting acceptance of a renewal certificate

(4.6.5)

Conduct constituting acceptance of a renewal certificate shall be in accordance with the provisions of 7.4.4.1.

7.4.6.6 Publication of the renewal certificate by the CA

(4.6.6)

See the provisions of 7.2.2.

7.4.6.7 Notification of certificate renewal by the CA to other entities

(4.6.7)

See the provisions of 7.4.4.3.

7.4.7 Certificate re-key

(4.7)

Certificate re-key procedures shall be in accordance with 7.3.3.

7.4.8 Certificate modification

7.4.8.1 Circumstances for certificate modification

(4.8.1)

The issuing CA shall modify a certificate:

— 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;

— 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.

7.4.8.2 Who may request certificate modification

(4.8.2)

The modification 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 health profession registration board or licensing board of a certificate holder who is a regulated healthcare professional;

— the sponsor of a sponsored healthcare provider;

— personnel of the issuing CA;

— personnel of an RA associated with the issuing CA.

7.4.8.3 Processing certificate modification requests

(4.8.3)

Criteria for processing certificate modification requests shall be specified in accordance with 4.8.3 of IETF/RFC 3647.

7.4.8.4 Notification to certificate holder of modified certificate issuance

(4.8.4)

Notification to certificate holder of modified certificate issuance shall be in accordance with 7.4.3.2.

7.4.8.5 Conduct constituting acceptance of a modified certificate

(4.8.5)

Conduct constituting acceptance of a modified certificate shall be in accordance with 7.4.4.1.

7.4.8.6 Publication of the modified certificate by the CA

(4.8.6)

Criteria for publication of the modified certificate by the CA shall be in accordance with 7.4.4.2.

7.4.8.7 Notification of modified certificate issuance by the CA to other entities

(4.8.7)

Notification of modified certificate issuance by the CA to other entities shall be in accordance with 7.4.4.3.

7.4.9 Certificate revocation and suspension

(4.9)

RAs can be instrumental in the handling of certificate revocation requests. In some health digital certificate 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 securely send a message to the CA containing certificate identification information and, optionally, the stated reason for revoking that certificate.

It is recommended that the address of the CRL distribution points be defined in the certificate in accordance with 7.2.8 of ISO 17090-2:2008.

7.4.9.1 Circumstances for revocation

(4.9.1)

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.

7.4.9.2 Who can request revocation

(4.9.2)

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.

7.4.9.3 Procedure for revocation request

(4.9.3)

When a revocation request is received by the CA in accordance with 7.3.4, 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, confirm that the requestor has sufficient authority to effect revocation;

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

7.4.9.4 Revocation request grace period

(4.9.4)

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

7.4.9.5 Time within which a CA must process the revocation request

(4.9.5)

Revocation of a certificate shall be initiated immediately by the CA upon receipt of request.

7.4.9.6 Revocation checking requirements for relying parties

(4.9.6)

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

7.4.9.7 CRL issuance frequency

(4.9.7)

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

7.4.9.8 Maximum latency for CRLs

(4.9.8)

Criteria for maximum latency for CRLs shall be specified in accordance with 4.9.8 of IETF/RFC 3647.

7.4.9.9 On-line revocation/status checking availability

(4.9.9)

The CA should make its revocation/status checking service (e.g. CRL or OCSP) available to match the business hours of its relying parties.

7.4.9.10 On-line revocation checking requirements

(4.9.10)

On-line revocation checking (e.g. with OCSP) 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.

7.4.9.11 Other forms of revocation advertisements available

(4.9.11)

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

7.4.9.12 Special requirements regarding key compromise

(4.9.12)

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

7.4.9.13 Circumstances for suspension

(4.9.13)

Within a healthcare CP, 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 suspension request;

— other circumstances determined within local healthcare digital certificate domains.

7.4.9.14 Who can request suspension

(4.9.14)

Where a CA supports suspension, the suspension 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;

— a relying party.

7.4.9.15 Procedures for suspending certificates

(4.9.15)

When a suspension request is received by the CA, in accordance with 7.4.9.13 and 7.4.9.14, 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 to be true, suspend the certificate.

7.4.9.16 Limits on suspension period

(4.9.16)

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.

7.4.9.17 Notification of certificate suspension

(4.9.17)

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

7.4.10 Certificate status services

7.4.10.1 Operational characteristics

(4.10.1)

Criteria for operational characteristics shall be specified in accordance with 4.10.1 of IETF/RFC 3647.

7.4.10.2 Service availability

(4.10.2)

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

7.4.10.3 Operational features

(4.10.3)

Criteria for operational features shall be specified in accordance with 4.10.3 of IETF/RFC 3647.

7.4.11 End of subscription

(4.11)

Criteria for end of subscription shall be specified in accordance with 4.11 of IETF/RFC 3647.

7.4.12 Private key escrow

(4.12)

Private keys used for authentication or digital signature shall not be escrowed, except where required by law.

7.5 Physical controls

(5)

7.5.1 General

Physical, procedural and personnel security controls shall be in accordance with ISO/IEC 27002 (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/IEC 27002 (or its equivalent).

7.5.3 Procedural controls

(5.2)

Procedural controls shall be in accordance with ISO/IEC 27002 (or its equivalent).

7.5.4 Personnel controls

(5.3)

Personnel controls shall be in accordance with ISO/IEC 27002 (or its equivalent).

7.5.5 Security audit logging procedures

(5.4)

Security audit logging procedures shall be in accordance with ISO/IEC 27002.

7.5.6 Record archive

7.5.6.1 General

(5.5)

Records shall be archived in accordance with ISO/IEC 27002 and in accordance with national law, regulations and accepted practice for the retention of archives. Health information is re-usable and can exist for as long as (and longer than) the person to whom it refers. This creates a special need for long-term preservation of digitally signed records, and a valuable role for the time-stamp and long-term non-repudiation technologies that can support this.

7.5.6.2 Types of record archived

(5.5.1)

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

7.5.6.3 Retention period for archive

(5.5.2)

Criteria for retention period shall be specified in accordance with 5.5.2 of IETF/RFC 3647. As noted above, health information is re-usable and can exist for as long as (and longer than) the person to whom it refers. This creates a special need for long-term preservation of digital signatures.

7.5.7 Key changeover

(5.6)

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

7.5.8 Compromise and disaster recovery

(5.7)

Security audit procedures shall be in accordance with ISO/IEC 27002.

7.5.9 CA termination

(5.8)

In the event that a CA ceases operation, it shall notify its certificate holders immediately upon the termination of operations and arrange for final publication of the CRL and 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.

7.6 Technical security controls

(6)

7.6.1 Key pair generation and installation

7.6.1.1 Key pair generation

(6.1.1)

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

— the CA,

— another TTP 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.

Key generation shall be provided in a secure manner.

7.6.1.2 Private key delivery to certificate holder

(6.1.2)

If the private decipherment key is not generated by the prospective certificate holder, it shall be delivered to the certificate holder either in an on-line transaction in accordance with IETF/RFC 4211, 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 7.6.2.5.

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 delivered to the CA either in an on-line transaction in accordance with IETF/RFC 4211, or via an equally secure manner.

7.6.1.4 CA public key delivery to relying parties

(6.1.4)

As the public key is bound to the CA's signing certificate, the public key shall be available to relying parties with access to the certificate repository.

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 2 048 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 1 024 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 parameter generation and quality checking

(6.1.6)

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

It shall be the role of the auditing organization to verify the parameter quality of the operational system.

7.6.1.7 Key usage purposes in accordance with the X.509 v3 key usage field

(6.1.7)

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)

7.6.2.1 General

This part of ISO 17090 recommends that two key pairs exist – one pair for encipherment where the CA could back up the private key and an authentication or digital signature key pair where the private key would never be escrowed.

7.6.2.2 Cryptographic module standards and controls

(6.2.1)

CA signing keys shall be compliant with US FIPS[12] 140-2 level 2 (or its equivalent). Where a healthcare organization's CA does not cross-certify (a small hospital, say), level 2 compliance is sufficient as long as a CP allows it. For inter-organizational trust, the CA shall be compliant with level 3 or higher.

Other certificates shall be compliant with US FIPS 140-2 level 1 or higher (or its equivalent).

Cryptographic module engineering controls shall be in accordance with ISO/IEC 27002 (or its equivalent), or with approved accreditation or licensing criteria.

7.6.2.3 Private key (n out of m) multi-person control

(6.2.2)

Where the certificate holder is a healthcare organization or supporting organization, the private key may be split into more than one part under the control of different persons.

7.6.2.4 Private key escrow

(6.2.3)

Private keys used for authentication or digital signature shall not be escrowed, except where required by law.

7.6.2.5 Private key backup

(6.2.4)

It is recommended that the certificate holder back up private keys where possible, e.g. where the private key is stored in a software token.

Private authentication or digital signature keys shall be backed up entirely within the control of the certificate holder. Backed-up keys shall be held within the certificate holder's environment (workplace, department or organization).

The certificate holder may consent to the CA backing up and retaining a copy of his/her private decipherment key. Such backup shall be carried out by a certified process. Private keys shall be backed up at a level of protection no lower than that required for the primary copy.

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.

7.6.2.6 Private key archive

(6.2.5)

Where the CA, with the consent of a certificate holder, has backed up a private key, this key shall be retained for a period at least as long as the mandatory retention time of personal health records in the CA's jurisdiction.

7.6.2.7 Private key transfer into or from a cryptographic module

(6.2.6)

If the private decipherment key is not generated in the entity's cryptographic module, it shall be entered into the module in accordance with IETF/RFC 4211, or via an equally secure manner.

7.6.2.8 Private key storage on cryptographic module

(6.2.7)

If the private decipherment key is not generated in the entity's cryptographic module, it shall be entered into the module in accordance with IETF/RFC 4211, or via an equally secure manner.

7.6.2.9 Method of activating private key

(6.2.8)

For digital certificates issued under a healthcare CP, only the certificate holder can activate the private key. The certificate holder shall be authenticated to the cryptographic module or application protecting the private key before the activation of the private key. This authentication may be in the form of a password, passphrase, PIN or biometric. When deactivated, private keys shall be kept in encrypted form only.

7.6.2.10 Method of deactivating private key

(6.2.9)

When keys are deactivated, they shall be cleared from memory before the memory is de-allocated. Any disk space, where keys were stored, shall be overwritten before the space is released to the operating system. The cryptographic module shall automatically de-activate the private key after a pre-set period of inactivity.

7.6.2.11 Method of destroying private key

(6.2.10)

Upon termination of use of a private key, all copies of the private key in computer memory and shared disk space shall be securely destroyed by overwriting multiple times. Private key destruction procedures shall be described in the CPS or a publicly available document.

7.6.2.12 Cryptograhic Module Rating

(6.2.11)

CA signing keys shall be compliant with US FIPS 140-2 level 2 (or its equivalent).

Other certificates shall be compliant with US FIPS 140-2 level 1 (or its equivalent).

7.6.3 Other aspects of key management

(6.3)

7.6.3.1 Public key archive

(6.3.1)

PKCs and CRLs will need to be archived with a TTP to allow verification of a signature at a future date. The CA shall be responsible for ensuring that public key certifcates and CRLs are archived.

7.6.3.2 Certificate operational periods and key pair usage periods

(6.3.2)

For regulated health professionals, the CA shall ensure that the validity period of the certificate does not exceed the validity period of the professional licence. To accomplish this, the CA shall either set the certificate validity so as not to exceed the period for the professional licence or else reliably confirm the renewal of the professional license prior to the license expiry date and revoke or suspend the certificate if the professional license has not been renewed.

Non-CA public and private key usage shall not exceed three years, after which a new key pair shall be issued. Attribute certificates may have a shorter validity period, depending on the business need.

CA public and private keys usage shall not exceed ten years, after which a new key pair shall be issued.

7.6.3.3 Restrictions on CA's private key use

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

7.6.4 Activation data

(6.4)

Activation data shall be unique, unpredictable and conveyed to the certificate holder in a secure manner.

7.6.5 Computer security controls

(6.5)

Computer security controls shall be in accordance with ISO/IEC 27002 (or its equivalent), or with approved accreditation or licensing criteria, and shall cover the following issues:

— IETF/RFC 3647, 6.5.1, Specific computer security technical requirements;

— IETF/RFC 3647, 6.5.2, Computer security rating.

7.6.6 Life-cycle technical controls

(6.6)

Life-cycle technical controls shall be in accordance with ISO/IEC 27002 (or its equivalent), or with approved accreditation or licensing criteria, and shall cover the following issues:

— IETF/RFC 3647, 6.6.1, System development controls;

— IETF/RFC 3647, 6.6.2, Security management controls;

— IETF/RFC 3647, 6.6.3, Life-cycle security controls.

7.6.7 Network security controls

(6.7)

Network security controls shall be in accordance with ISO/IEC 27002 (or its equivalent) or with approved accreditation or licensing criteria.

7.6.8 Time stamping

(6.8)

Criteria for time stamping shall be specified in accordance with 6.8 of IETF/RFC 3647.

7.7 Certificate, CRL and OCSP profiles

(7)

Certificate, CRL and OCSP profiles (where applicable) shall be in accordance with ISO 17090-2.

7.8 Compliance audit

7.8.1 General

(8)

Compliance audit is an essential component of many digital certificate interoperability models (see, for example, 9.2.4 of ISO 17090-1:2008).

7.8.2 Frequency of CA compliance audit

(8.1)

A CA issuing certificates pursuant to a healthcare CP 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.

7.8.3 Identity/qualifications of auditor

(8.2)

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 digital certificate experience. Where a formal accreditation body exists, the auditor shall meet that body's requirements.

7.8.4 Auditor's relationship to audited party

(8.3)

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

7.8.5 Topics covered by audit

(8.4)

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.

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.

7.8.6 Actions taken as a result of deficiency

(8.5)

7.8.6.1 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.

7.8.6.2 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.

7.8.6.3 Major failure category

A CA failing to comply with important element(s) of the CPS, which was/were 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.

7.8.6.4 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 d.

7.8.6.5 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.

7.8.7 Communication of audit results

(8.6)

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

7.9 Other business and legal matters

(9)

7.9.1 Fees

(9.1)

Fees shall be specified in accordance with 9.1 of IETF/RFC 3647.

7.9.2 Financial responsibility

(9.2)

Financial responsibility shall be in accordance with 9.2 of IETF/RFC 3647.

7.9.3 Confidentiality of business information

(9.3)

Confidentiality of business information shall be specified in accordance with 9.3 of IETF/RFC 3647.

7.9.4 Privacy of personal information

(9.4)

7.9.4.1 Privacy plan

(9.4.1)

Criteria for privacy plan shall be specified in accordance with 9.4.1 of IETF/RFC 3647.

7.9.4.2 Information treated as private

(9.4.2)

The following information shall be treated as private and 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.

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

7.9.4.3 Information not deemed private

(9.4.3)

The following information shall not be treated as private or confidential:

— public key;

— role of a regulated or non-regulated health professional;

— healthcare speciality.

7.9.4.4 Responsibility to protect confidential information

(9.4.4)

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.

7.9.4.5 Notice and consent to use private information

(9.4.5)

Notice and consent to use private information shall be specified in accordance with 9.4.5 of IETF/RFC 3647.

7.9.4.6 Disclsoure pursuant to judicial or administrative process

(9.4.6)

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.

7.9.4.7 Other information release circumstances — Disclosure upon certificate holder's request

(9.4.7)

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.

Confidential information shall only be disclosed without written authority from the certificate holder following the presentation of an order from a recognized court of law under the CA or RA country's law.

7.9.5 Intellectual property rights

(9.5)

Intellectual property rights shall be specified in accordance with 9.5 of IETF/RFC 3647.

7.9.6 Representations and warranties

(9.6)

7.9.6.1 General

The extent of the liability in the situations listed in 7.9.6.2 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, AA liability shall either be subsumed by the former liability or explicitly delineated.

7.9.6.2 CA representations and warranties

(9.6.1)

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 RA, 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.

The liability of the CA issuing digital certificates for use in healthcare shall not be limited with 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.

7.9.6.3 RA representations and warranties

(9.6.2)

The liability of an RA registering potential certificate holders for use in healthcare shall not be limited with 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.