ISO/TC 215/WG 4
Health Informatics/Security

Reference number of working document: **ISO/TC 215/WG4/N84**

Date: 2001-03-05

Reference number of document: **ISO/DTS 17090-3**

Committee identification: ISO/TC 215

Secretariat: ANSI

Health informatics – Public Key Infrastructure - Part 3: Policy management of certification authority

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Document type: Technical Specification
Document stage: (20) Preparation

This is a final working draft from the Task Force proposed to be approved by ISO/TC215/WG 4 on 2001-03-28 as the Draft Technical Specification to be submitted to ballot

Document language: E

International Standards Organisation Technical Committee 215, Health Informatics
Working Group 4: Security

Contact person

Convenor: Gunnar Klein, HSS
Box 70 487, S-107 26 Stockholm, Sweden
e-mail: wg4.isotc215@hss.se

Secretariat: Nagaki Ohyama, Tokyo Institute of Technology Imaging
Science and Engineering Laboratory
4259 Nagatsuta, Midori-ku, Yokahama 226-8503, Japan
e-mail: wg4kita@medis.or.jp

WG4/Task Force PKI. Managed by John Lewis

e-mail: jlewi@bigpond.com

Contents

Foreword

ISO (the International Standards Organisation) 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 organisations, 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, Edition 4.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by 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 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/TS is reviewed every three years with a view to deciding whether it can be transformed into an International Standard.

Attention is drawn to the possibility that some elements of this Technical Specification/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 was prepared by Technical Committee ISO/TC 215, “Health informatics”, WG4 “Security”.

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 Certificate Authority

Introduction

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

Health care 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 unauthorised access (either inadvertent or deliberate) are increasing. It is essential to have available to the health care system reliable information security services which minimise the risk of unauthorised access.

How does the health care 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 health care 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) can 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 organisations 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 organisations and between jurisdictions in support of health care 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 public key infrastructures to support secure communications within their national boundaries. Inconsistencies will arise in policies and procedures between the Certification and Registration Authorities of different countries, if PKI standards development activity is restricted to within national boundaries.

Public Key Infrastructure technology is still rapidly evolving in certain aspects that are not specific to health care. Important standardization efforts and in some cases supporting legislation are ongoing. On the other hand health care 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. ISO/TC 215 intends to revise it into a full international standard after a three year period.

Health informatics – Public key infrastructure – Part 3: Policy Management of Certification Authority

1 Scope

This three-part ISO Technical Specification (ISO/TS) describes the common technical, operational and policy requirements that need to be addressed to enable Public Key Infrastructures (PKI) to be used in protecting the exchange of health care information within a single domain, between domains and across jurisdictional boundaries.

The purpose of this technical specification is to create a platform for global interoperability. It specifically supports PKI enabled communication across borders but the specification could also provide guidance for the establishment of health care PKIs nationally or regionally. The Internet is increasingly used as the vehicle of choice to support the movement of health care data between health care organisations and is the only realistic choice for cross-border communication in this sector.

This ISO/TS provides health care specific profiles of existing security standards from ISO/IEC and the Internet Engineering Task Force (IETF). The use of this ISO/TS is not however restricted to Internet transport.

The specification addresses the following types of end-entity Certificate holders:

Regulated health care professionals

Health care non-regulated employee

Sponsored health care providers (that are not regulated)

Patients/consumers

Health care organisations

Supporting organisations

Supporting organisation employee

Devices

Applications

These are defined further in Part 1, Section 5.3.

Part 1: "*Framework and overview"* of the ISO/TS defines the basic concepts needed to describe a health care PKI and provide a scheme of interoperability requirements to establish a PKI enabled secure communication of health information.

It starts with a model of the major stakeholders that are communicating in health with some detailed scenarios highlighting the need for PKI in an informative annex. This ISO/TC further describes the major security services required for health communication where PKI may be required. The document gives a brief introduction to public key cryptography and the basic components of a health care PKI. It further introduces different types of certificates, public key identity certificates and associated attribute certificates, for relying parties as described above, self-signed CA certificates, and CA hierarchies and bridging structures.

Part 2: "Certificate profile" specifies health care 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.

This part, *Part 3: "Policy management of certificate authority*", deals with certificate management issues involved in implementing and operating a health care PKI. It defines a structure and minimum requirements for Certificate Policies and a structure for associated certification practice statements. This parts 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 health care security policy for cross border communication. It also defines the minimum levels of security required, concentrating on aspects unique to

health care.

2 Normative references

This ISO Technical Specification incorporates by dated or undated reference, provisions from other publications. These normative references are cited in the appropriate places in the text, and the publications are listed hereafter. For dated references, subsequent amendments and revisions of any of these publications apply to this ISO Technical Specification only when incorporated in it by amendment and revision. For undated references, the latest edition of the publication referred to applies.

ISO/IEC 2382-8:1998	Information technology – Vocabulary -- Part 8: Security
ISO/IEC 7498-2	Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture
ISO/IEC 8824-1:1995	Information Technology - Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1). - Part 1: Specification of the basic notation
ISO/IEC 10181-1	Information technology – Open Systems Interconnection – Security frameworks for open systems – Overview.
ISO/IEC TR13335	Guidelines for management of IT Security – Part 1, Concepts and models for IT security.
ISO/IEC 14516	Information technology – Security techniques – Guidelines on the use and management of Trusted Third Party services
ISO/IEC 15945	Information technology – Security techniques – Specification of TTP services to support the application digital signatures
ISO/IEC 17799:2000	Information technology -- Code of practice for information security management
ITU-T X.509:1997	Recommendation X.509: The Directory - Authentication Framework. Equivalent to ISO/IEC 9594-8
IETF/RFC 2459	Internet X.509 Public Key Infrastructure: Certificate and CRL Profile
IETF/RFC 2527	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
IETF/RFC 3039	Internet X.509 Public Key Infrastructure Qualified Certificates Profile
ENV 13608-1	Health informatics - Security for healthcare communication - Concepts and terminology

3 Terms and definitions

For the purposes of this ISO Technical Specification, the following definitions apply:

3.1 Health care context terms

Please note that there are many different terms used to describe these concepts for different purposes available from CEN, HL-7 and various national organisations. The following definitions are not meant to be universal in ISO work in health informatics, only to facilitate the understanding of this ISO/TS.

3.1.1

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

NOTE 1: in this context it may be any software process used in health care information systems including those without any direct role in treatment or diagnosis.

NOTE 2: in some jurisdictions including software processes may be regulated medical devices

3.1.2

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

NOTE: This includes the class of regulated medical devices that meet the above definition. Device in this context is any device used in health care information systems including those without any direct role in treatment or diagnosis

3.1.3

health care actor
health professional, health care employee, patient/consumer, sponsored health care provider, health care organisation, device or application that acts in a health related communication and requires a certificate for a PKI enabled security service

3.1.4

health care organisation
an officially registered organisation that has a main activity related to health care services or health promotion

NOTE 1: Examples include hospitals, Internet health care website providers, and health care research institutions.

NOTE 2: The organisation should be recognised to be legally liable for their activities but need not be registered for their specific role in health. An internal part of an organisation is here called organisational unit as in X.501.

3.1.5

health care non-regulated employee
person employed by a health care organisation that is not a health professional. Examples include a receptionist or secretary who organises appointments, or a business manager who is responsible for validating patient health insurance.

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

3.1.6

health professional
person that is authorised by a nationally recognised body to be qualified to perform certain health services

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

NOTE 2: A nationally recognised body in this definition does not imply one nationally controlled system of professional registration but in order to facilitate international communication it would be preferable that one nation-wide directory of recognised health professional registration bodies exists.

NOTE 3: Examples of health professionals are physicians, registered nurses and pharmacists.

3.1.7

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

3.1.8

privacy
freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual [ISO/IEC 2382-8]

3.1.9

sponsored health care provider
health services provider who is not a regulated professional in the jurisdiction of his/her practice but who is active in his/her health care community and sponsored by a regulated health care organisation

NOTE: Examples would be a drug and alcohol education officer who is working with a particular ethnic group, or a health care aid worker in a developing country

3.1.10

supporting organisation
an officially registered organisation that is providing services to a health care organisation but which is not providing health care services

NOTE : Examples include health care financing bodies such as insurance institutions, suppliers of pharmaceuticals and other goods

3.1.11

supporting organisation employee
person employed by a supporting organization

NOTE: Examples include medical records transcriptionists, health care insurance claims adjudicators and pharmaceutical order entry clerks.

3.2 Security services terms

3.2.1

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

authorized ways [ISO/IEC 2382-8]

3.2.2

accountability
the property that ensures that the actions of an entity may be traced uniquely to the entity [ISO 7498-2]

3.2.3

asymmetric cryptographic algorithm
an algorithm for performing encipherment or the corresponding decipherment in which the keys used for encipherment and decipherment differ [ISO 10181-1]

3.2.4

authentication
process of reliably identifying security subjects by securely associating an identifier and its authenticator. See also data origin authentication and peer entity authentication [ISO 7498-2]

3.2.5

authorization
the granting of rights, which includes the granting of access based on access rights [ISO 7498-2]

3.2.6

availability
property of being accessible and useable upon demand by an authorised entity [ISO 7498-2]

3.2.7

ciphertext
data produced through the use of encipherment. The semantic content of the resulting data is not available [ISO 7498-2]

3.2.8

confidentiality
the property that information is not made available or disclosed to unauthorised individuals, entities, or processes [ISO 7498-2]

3.2.9

cryptography
the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use [ISO 7498-2]

3.2.10

cryptographic algorithm
cipher
A method for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. [ISO 7498-2]

3.2.11

data integrity
the property that data has not been altered or destroyed in an unauthorised manner [ISO 7498-2]

3.2.12

data origin authentication
the corroboration that the source of data received is as claimed [ISO 7498-2]

3.2.13

decipherment
decryption
the process of obtaining, from a ciphertext, the original corresponding data [ISO/IEC 2382-8]

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

3.2.14

digital signature
data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient [ISO 7498-2]

3.2.15

encipherment
encryption
the cryptographic transformation of data (see cryptography) to produce ciphertext [ISO 7498-2]

3.2.16

identification
the performance of tests to enable a data processing system to recognize entities [ISO/IEC 2382-8]

3.2.17

identifier
piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator [ENV 13608-1]

3.2.18

integrity
proof that the message content has not altered, deliberately or accidentally in any way, during transmission [ISO/IEC 7498-2]

3.2.19

key
a sequence of symbols that controls the operations of encipherment and decipherment [ISO 7498-2]

3.2.20

key management
the generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy [ISO 7498-2]

3.2.21

non-repudiation
this service provides proof of the integrity and origin of data (both in an unforgeable relationship) which can be verified by any party [ASTM]

3.2.22

private key
a key that is used with an asymmetric cryptographic algorithm and whose possession is restricted (usually to only one entity) [ISO 10181-1]

3.2.23

public key
a key that is used with an asymmetric cryptographic algorithm and that can be made publicly available [ISO 10181-1]

3.2.24

role
a set of behaviours that is associated with a task

3.2.25

security
the combination of availability, confidentiality, integrity and accountability [ENV 13608-1]

3.2.26

security policy
a plan or course of action adopted for providing computer security [ISO/IEC 2382-8]

3.2.27

security service
A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers [ISO 7498-2]

3.3 Public key infrastructure related terms

3.3.1

attribute authority
AA
An authority which assigns privileges by issuing attribute certificates [X.509]

3.3.2

attribute certificate
a data structure, digitally signed by an Attribute Authority, that binds some attribute values with identification about its holder [X.509]

3.3.3

authority certificate
a certificate issued to a Certification Authority or an Attribute Authority [adapted from X.509]

3.3.4

certificate
public key certificate

3.3.5

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

3.3.6

certificate extension

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

NOTE: Certificate extensions may be either:

critical - a certificate using system MUST reject the certificate if it encounters a critical extension it does not recognize.

non-critical extension - may be ignored if it is not recognized.

3.3.7

certificate generation
act of creating certificates

3.3.8

certificate management
procedures relating to certificates: certificate generation, certificate distribution, certificate archiving and revocation

3.3.9

certificate profile
specifies the structure and permissible content of a certificate type

3.3.10

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

3.3.11

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

3.3.12

certificate verification
verifying that a certificate is authentic

3.3.13

certification
procedure by which a third party gives assurance that all or part of a data processing system conforms to security requirements [ISO/IEC 2382-8]

3.3.14

certification authority
CA
certificate issuer
an authority trusted by one or more relying parties to create and assign certificates. Optionally the certification authority may create the relying parties' keys [ISO 9594-8]

NOTE: Authority in the CA term does not imply any government authorisation only that it is trusted. Certificate issuer may be a better term but CA is used very broadly.

3.3.15

certificate policy
a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements[X.509]

3.3.16

certification practices statement
CPS
a statement of the practices which a certification authority employs in issuing certificates [RFC2527]

3.3.17

public key certificate
X.509 public key certificates (PKCs) [X.509], bind an identity and a public key. The identity may be used to support identity-based access control decisions after the client proves that it has access to the private key that corresponds to the public key contained in the PKC [RFC2459]

3.3.18

public key infrastructure
PKI
an infrastructure used in the relation between a key holder and a relying party that allows a relying party to use a certificate relating to the key holder for at least one application using a public key dependent security service. PKI includes a Certification Authority, a certificate data structure, means for the relying party to obtain current information on the revocation status of the certificate, a certification policy and methods to validate the certification practice

3.3.19

registration authority
RA
an entity which establishes the identities of relying parties and registers their certification requirements with a Certification Authority

3.3.20

relying party
a recipient of a certificate who acts in reliance on that certificate and/or digital signature verified using that certificate [RFC 2527]

3.3.21

third party
party other than data originator, or data recipient, required to perform a security function as part of a communication protocol.

3.3.22

trusted third party
TTP
a third party which is considered trusted for purposes of a security protocol [ENV 13608-1]

NOTE: This term is used in many ISO/IEC standards and other documents describing mainly the services of a CA. The concept is however broader and includes services like time stamping and possibly escrowing

4 Abbreviations

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
PKC	Public Key Certificate
PKI	Public Key Infrastructure
RA	Registration Authority
TTP	Trusted Third Party

5 Requirements for PKI Policy Management in a Health care Context

For PKI to be effective in securing the communication of personal health information, a health care PKI must achieve the following objectives:

1. the reliable and secure binding of unique and distinguished names to individuals, organisations, applications, and devices that participate in the electronic exchange of personal health information

2. the reliable and secure binding of professional roles in health care to individuals, organisations 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.

3. (optionally) the reliable and secure binding of attributes to individuals, organisations, 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.

All of the above must 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 health care PKI.

To do this, each Certification Authority in a Health Care PKI must operate according to an explicit set of publicly stated policies that promote the objectives above.

5.1 Need for a High Level of Assurance

Part I of this technical specification lists the security services required for health applications (section 6). For each of these security services (authentication, integrity, confidentiality, digital signature, authorization, access control), a high level of assurance is required.

5.2 Need for a High Level of Infrastructure Availability

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

5.3 Need for a High Level of Trust

Unlike e-commerce (where a vendor and customer are often the only parties to an electronic transaction who rely upon its security and integrity), health care applications that store or transmit personal health information may implicitly require the trust of the patients whose information is being exchanged trust of the general public, as well as the trust of the general public. Neither health care providers nor patients will likely cooperate in the electronic exchange of personal health information if such exchanges are believed to be insecure.

5.4 Need for Internet Compatibility

As the purpose of this technical specification is to define the essential elements of a health care PKI to support the secure transmission of health care information across national boundaries, this specification is based as much as possible upon Internet standards so as to effectively span those boundaries.

5.5 Need to Facilitate Evaluation and Comparison of Certificate Policies

Part I section 9.2 discusses approaches for using PKI to facilitate the secure exchange of health information across national boundaries. These approaches (such as cross-recognition and cross-certification) are greatly facilitated if health care PKI certificate policies follow a consistent format so that comparisons may be readily drawn between

the provisions of one certificate policy and another.

Health care certificate policies also constitute a basis for accreditation of CAs (a CA being accredited to support one or more certificate policies which it proposes to implement). While accreditation criteria are beyond the scope of this technical specification, the entire process of accreditation of health care CAs is expedited by the consistency of format and the minimum standards which this technical specification promotes.

6 Structure of Health care Certificate Policies and Health care Certification Practice Statements

6.1 General Requirements for Certificate Policies

When a Certification Authority (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 certificate policy object identifier (OID), which identifies the certificate policy 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 Certificate Policy (CP) in establishing trust in a public key certificate, it is fundamental that the CP be understood and consulted not only by Certificate holders but any Relying Party. Certificate holders and relying parties must therefore have ready and reliable access to the CP under which a certificate was issued.

The following requirements apply to all certificate policies specified in accordance with this document:

1. Each PKI certificate issued in accordance with this standard SHALL contain a registered certificate policy object identifier (OID), which identifies the certificate policy under which the certificate was issued.

2. Certificate policies SHALL comply with *IETF RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*.

3. Certificate policies SHALL be accessible to Certificate holders and relying parties.

While Certificate Policy documents are essential for describing and governing certificate policies 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 Certificate Policy that require emphasis and disclosure. Section 8 below contains a model PKI Disclosure Statement that is intended to serve as this concise statement.

6.2 General Requirements for Certification Practice Statements

A Certification Practice Statement (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 certificate policy.

The following requirements apply to all certification practice statements specified in accordance with this document:

1. Certification practice statements SHALL be in compliance with *IETF RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*.
2. A CA with a single CPS MAY support multiple certificate policies (used for different application purposes and/or by different groups of relying parties).
3. A number of CAs with non-identical certification practice statements MAY support the same certificate policy.

4. a CA MAY choose not to make its CPS accessible to Certificate holders or relying parties.

6.3 Relationship Between a Certificate Policy and a Certification Practice Statement

A CP states what assurance can be placed in a certificate. A CPS states how a CA establishes that assurance. A certificate policy may apply more broadly than to just a single organisation; a CPS applies only to a single CA. Certificate policies 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 technical specification applies to certificate policies and certification practice statements that are used for the purpose of issuing health care certificates as these certificates are defined in Part II, section 4.

7 Minimum Requirements for a Health care PKI Certificate Policy

7.1 General requirements

A certificate policy SHALL meet all the following requirements in order to comply with this Technical Specification. Numbers refer to the sections of IETF RFC 2527.

7.2 CA-RA requirements

7.2.1 Obligations [IETF RFC 2527 Section 2.1]

7.2.1.1 CA Obligations [IETF RFC 2527 Section 2.1.1]

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 Certificate Policy and with the CA's Certification Practices Statement.

A CA within a health care 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 as defined in Part 2, Section 6.
- 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 Certificate Authorities.
- Security controls and auditing.

In order to perform this function 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.

7.2.1.1.1 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 organisation in the case

of device or application certificates.

An issuing CA SHALL make Certification Revocation Lists (CRLs) available to relying parties in accordance with section 4.4.

7.2.1.1.2 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 Certificate Policy (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 Certificate Policy. Such notice MAY be in the form of a Certificate holder Agreement. Such notice SHALL include a description of the allowed 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.

7.2.1.1.3 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.

7.2.1.1.4 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. The address of the CRL SHALL be defined in the certificate (see ISO/TS 17090 - Part 2, section 8.1).

7.2.1.1.5 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 Sections 7.6.2, 7.6.3 and 7.6.4.

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 Section 7.6.2. The CA SHALL NOT disclose private decipherment keys to any other party without the prior consent of the Certificate holder unless required by law. Despite the foregoing, because a non-regulated health care employee or a supporting organisation 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 care employee or a supporting organisation employee.

7.2.1.1.6 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 Registration Authority Obligations [IETF RFC 2527 Section 2.1.2]

The CA MAY delegate identification and authentication functions, for which it is responsible, to a registration authority (RA). The prime function that a health care organisation RA performs is verification of a Certificate holder's identity and health care role during initial registration. The RA SHALL follow the same set of rules and

methods of authentication as the CA uses itself. RA's 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 must have their certificates created by a trusted source. As RAs perform authentication functions for CAs, they must 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 must be trusted to pass certificate revocation requests to a CA in an accurate and timely fashion.

It is RECOMMENDED that Registration Authorities be individually accountable for actions performed on behalf of the CA. The RA SHALL:

1. Ensure that its signing private key is used only to sign certificate requests, if the RA is performing its duties on-line.

2. Certify to the CA that it has authenticated the identity of the Certificate holder.

3. Securely transmit and store certificate application information and records of registration.

4. Initiate a revocation request (where applicable) according to section 7.3.4.2.

7.2.1.2.1 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 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 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 the stated reason for revoking that certificate.

7.2.1.2.2 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 must be generated for events in accordance with relevant policy.

7.2.1.2.3 Archiving

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

7.2.1.3 Certificate holder Obligations [IETF RFC 2527 Section 2.1.3]

A Certificate holder in a Health care PKI SHALL:

1. Ensure the accuracy of representations in the certificate application and, by accepting the certificate, acknowledge that all information included in the certificate are true.

2. Protect their private keys and key tokens (if applicable) and take all reasonable measures to prevent their loss, disclosure, modification or unauthorized use.

3. Make all efforts to prevent the loss, disclosure or unauthorized use of his/her private key.

4. Immediately notify the CA and/or RA of any actual or suspected loss, disclosure, or other compromise of

his/her private key.

5. notify the RA and/or CA of any change in certificate information, role or status in the health care organisation.

6. Read either the Certificate Policy (CP) or a PKI disclosure document that clearly sets out in plain language the responsibilities of the Certificate holder.

7. Use key pairs in accordance with the CP.

8. Formally agree to these obligations by signing a Certificate holder agreement.

It is RECOMMENDED that a Certificate holder in a Health care 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 [IETF RFC 2527 Section 2.1.4]

A relying party to Health care PKIs has a right to rely on a health care certificate only if:

1. The purpose for which the certificate is used was appropriate under this policy .

2. The reliance is reasonable and in good faith in light of all the circumstances known to the Relying Party at the time of reliance.

3. The Relying Party confirmed the current validity of the certificate by checking that the certificate was not revoked or suspended.

4. The Relying Party confirmed the current validity of Digital signatures where applicable.

5. Applicable limitations of liability and warranties are acknowledged.

7.2.1.5 Repository Obligations [IETF RFC 2527 Section 2.1.5]

Certificates and CRLs SHALL be available to Relying Parties in accordance with the requirements of Section 7.4.4.9.

7.2.2 Liability [IETF RFC 2527 Section *2.2*]

The extent of the liability in the situations listed below in 7.2.2.1 is part of an overall policy under which the CAs operate in the health care domains of their respective countries. These domains are in turn subject to government regulations and international agreements.

7.2.2.1 CA Liability [IETF RFC 2527 Section 2.2.1]

The liability of the CA in a health care PKI MAY be limited to acts of negligence on the part of the CA. In particular:

1. A CA MAY assume no liability associated with the loss by the Certificate holder of the private keys.

2. A CA MAY assume no liability associated with Certificate holder generated keys unless they were generated fully in accordance with the guidelines of a health care PKI.

3. 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.

4. A CA MAY assume no liability associated with forged signatures unless the forgery resulted from the

documented policies and procedures of a health care PKI not being followed, or could be shown to permit the forgery.

5. 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 health care PKI SHALL NOT be limited in regard to the following:

6. A CA SHALL be liable for the compromise of a private key during the key distribution process.

7. 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.

8. A CA SHALL be liable for not revoking certificates according to its revocation policy.

9. A CA SHALL be liable for revoking a certificate for a reason not specified in its revocation policy.

7.2.2.2 RA Liability [IETF RFC 2527 Section 2.2.2]

The liability of an RA in a health care PKI MAY be limited to acts of negligence on the part of the RA.

The liability of an RA in a health care PKI SHALL NOT be limited in regard to the following:

1. 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.

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

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

7.2.3 Financial Responsibility [IETF RFC 2527 Section 2.3]

7.2.3.1 Indemnification by Relying Parties [IETF RFC 2527 Section 2.3.1]

This technical specification makes no further stipulation

7.2.3.2 Fiduciary Relationships [IETF RFC 2527 Section 2.3.2]

This technical specification makes no further stipulation

7.2.3.3 Administrative Processes [IETF RFC 2527 Section 2.3.3]

This technical specification makes no further stipulation

7.2.4 Interpretation and Enforcement [IETF RFC 2527 Section 2.4]

7.2.4.1 Governing Law [IETF RFC 2527 Section 2.4.1]

Health care PKIs SHALL comply with local and international legal requirements in accordance with a standard equivalent to but not less than ISO 17799-1:2000 or approved accreditation or licensing criteria.

7.2.4.2 Severability, Survival, Merger, Notice [IETF RFC 2527 Section 2.4.2]

Health care 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 organisation the new organisation remains liable for the course of the original agreement.

7.2.4.3 Dispute Resolution Procedures [IETF RFC 2527 Section 2.4.3]

This technical specification makes no further stipulation.

7.2.5 Fees [IETF RFC 2527 Section 2.5]

This technical specification makes no further stipulation.

7.2.6 Publication and Repository [IETF RFC 2527 Section 2.6]

7.2.6.1 Publication of CA Information [IETF RFC 2527 Section 2.6.1]

All CAs within Health care PKIs SHALL make available to their Certificate holders and relying parties:

1. the URL of an available web site maintained by, or on behalf of, the CA, containing their certificate policies.
2. each certificate issued under this policy.
3. the current status of each certificates issued under this policy.
4. 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 [IETF RFC 2527 Section 2.6.2]

CAs SHALL publish information, whenever such information has been modified. Information on certificate revocation SHALL be in accordance with section 7.4.4.

7.2.6.3 Access Controls [IETF RFC 2527 Section 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 [IETF RFC 2527 Section 2.6.4]

Information maintained about Certificate holders in RA or CA repositories SHALL be:

1. Kept current and up to date (within one day of changes being verified and earlier depending on

circumstances)

2. Be managed in accordance with a standard equivalent to but not less than ISO 17799-1:2000 or approved accreditation or licensing criteria.

7.2.7 Compliance Audit [IETF RFC 2527 Section 2.7]

Compliance audit is an essential component of many PKI interoperability models (see for example, Part 1, Section 9.2, Option 3 – Cross Recognition).

7.2.7.1 Frequency of CA Compliance Audit [IETF RFC 2527 Section 2.7.1]

A CA issuing certificates pursuant to a Health care 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 done by a qualified independent third party within intervals that are no more than one year apart.

7.2.7.2 Identity/Qualifications of Auditor [IETF RFC 2527 Section 2.7.2]

The auditor SHALL be qualified as an Information Systems Auditor to the extent necessary for admission to the relevant professional body (such as accreditation to ISO9000). 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 [IETF RFC 2527 Section 2.7.3]

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

7.2.7.4 Topics Covered by Audit [IETF RFC 2527 Section 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 Certificate Policies and to associated Certification Practice Statements.

7.2.7.5 Actions Taken as a Result of Deficiency [IETF RFC 2527 Section 2.7.5]

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:

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

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

3. revoke the CA's certificate. (Note: the CA cannot be shut down as this may disrupt services)

Any decision regarding which of these actions to take SHALL be based on the severity of the irregularities.

Failure Category—Critical

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

Where the CA has been accredited in its jurisdiction, it is RECOMMENDED that accreditation be withdrawn immediately. It is RECOMMENDED that the CA's certificate be revoked as in item 1 above.

Failure Category – Major

A Certification Authority fails to comply with important element(s) of the Certification Practice Statement, which was assessed as part of the assurance process, SHALL be classified as a Major failure. For example, the identification of a Certification Authority not maintaining sufficient business continuity practices SHALL be classified as being a Major failure.

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

Failure Category – Partial

Any compliance breach against the Certification Practice Statement, 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 Certification Authority's operations SHALL be classified as a Partial failure. For example, out-of-date security policies and procedures SHALL be classified as being 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.

Failure Category—Minor

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 Certification Authority'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 [IETF RFC 2527 Section 2.7.6]

Any CA or RA that is found by an auditor to be deficient SHALL immediately notify Certificate holders and relying parties.

7.2.8 Confidentiality [IETF RFC 2527 Section 2.8]

7.2.8.1 Types of Information to be Kept Confidential [IETF RFC 2527 Section 2.8.1]

1. Personal information of Certificate holders and registration authorities collected for authentication purposes but which is not included in the certificate SHALL be kept confidential (e.g., personal identification, background checks, home address, contact details).

2. Private keys.

7.2.8.2 Types of Information Not Considered Confidential [IETF RFC 2527 Section 2.8.2]

1. Public key

2. Role of health professional

3. Health care specialty

7.2.8.3 Disclosure of Certificate Revocation/Suspension [IETF RFC 2527 Section 2.8.3]

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

7.2.8.4 Release to Law Enforcement Officials [IETF RFC 2527 Section 2.8.4]

Confidential information SHALL only be released on the presentation of a warrant or equivalent order from a recognised court of law under the CA or RA country's law or with the explicit consent of the Certificate holder.

7.2.8.5 Release as Part of Civil Discovery [IETF RFC 2527 Section 2.8.5]

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

7.2.8.6 Disclosure Upon Certificate holder's Request [IETF RFC 2527 Section 2.8.6]

Confidential information SHALL be disclosed to parties nominated by the Certificate holder following a request either by authenticated e-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 [IETF RFC 2527 Section 2.8.7]

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

7.2.9 Intellectual Property Rights [IETF RFC 2527 Section 2.9]

This technical specification makes no further stipulation.

7.3 Identification and Authentication [IETF RFC 2527 Section 3]

7.3.1 Initial Registration [IETF RFC 2527 Section 3.1]

7.3.1.1 Types of Name [IETF RFC 2527 Section 3.1.1]

The subject names used for certificates issued under this policy SHALL be in accordance with Part 2 of this standard.

7.3.1.2 Need for Names to be Meaningful [IETF RFC 2527 Section 3.1.2]

The effective use of certificates requires that the relative distinguished names that appear in 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 [IETF RFC 2527 Section 3.1.2]

This technical specification makes no further stipulation.

7.3.1.4 Uniqueness of Names [IETF RFC 2527 Section 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 [IETF RFC 2527 Section 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 [IETF RFC 2527 Section 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 [IETF RFC 2527 Section 3.1.8]

Health care organisations, supporting organisations, or persons acting on behalf of organisations or devices SHALL present to the RA evidence of their existence and health care role by presenting documentation appropriate to their Country, State or Provincial Government. The CA or the RA 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 organisation.

7.3.1.8 Authentication of Identity of Individuals [IETF RFC 2527 Section 3.1.9]

Individuals, including health professionals, non-regulated health care employees, sponsored health care providers, supporting organisation employees, and patients/consumers, SHALL authenticate their identity to an RA prior to certificate issuance. This technical specification RECOMMENDS the same proof of identity that would be necessary for such individuals to be issued a passport, or a procedure of equivalent rigour.

Health professionals, in order that they authenticate their health care license, role and medical specialty (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 care employees, in order that they establish their employment and authenticate their health care role, SHALL present to the RA proof of sponsorship or employment from their sponsoring health organisations or sponsoring health professionals.

Sponsored health care providers, in order that they establish that they are active in their health care community and in order that they authenticate their health care role, SHALL present to the RA proof of sponsorship from their sponsoring health organisations or sponsoring health professionals.

Supporting organisation employees, in order that they establish their employment and authenticate their health care role, SHALL present to the RA proof of employment by their supporting health organisations.

7.3.2 Routine Rekeying [IETF RFC 2527 Section 3.2]

7.3.2.1 Certification Authority Routine Rekeying

Routine rekeying of Certification Authority information SHALL be done based on the original documentation used when the original record was created.

7.3.2.2 Registration Authority Routine Rekeying

Routine rekeying of Registration Authority information SHALL be done based on the original documentation used when the original record was created.

7.3.2.3 Certificate holder Routine Rekeying

Routing rekeying of Certificate holder information SHALL be done 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 [IETF RFC 2527 Section 3.3]

7. 3.3.1 Certification Authority Rekey after Revocation -- No Key Compromise

Rekeying of information after a Certificate has been revoked for reasons other than a key compromise SHALL require re-presentation of the original information originally used to accredit the Certification Authority.

7.3.3.2 Registration Authority Rekey after Revocation -- No Key Compromise

Rekeying of information after a Certificate has been revoked for reasons other than a key compromise, SHALL require re-presentation of the original information originally used to accredit the Registration Authority.

7.3.3.3 Certificate holder Rekey after Revocation -- No Key Compromise

Routing rekeying of Certificate holder information SHALL require either presentation of the original documentation used when the original record was created or else 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 [IETF RFC 2527 Section 3.4]

7.3.4.1 Certification Authority

A Certification Authority within a health care public key infrastructure, when making a revocation request to another Certification Authority, SHALL:

1. Identify the Certificate.
2. State the reasons why the Certificate should be revoked.
3. Sign the request with their private key, encrypt the message and send it to the relevant domain CA.

7.3.4.2 Registration Authority

A Registration Authority within a health care 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 their private key, encrypt the message and send it to the relevant domain CA.

7.3.4.3 Certificate holder

A Certificate holder within a health care public key infrastructure, when making a revocation request to a certification authority, SHALL:

1. Identify the Certificate that it is requesting to have revoked.

2. State the reasons why the Certificate should be revoked.

3. Sign the request with their 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 else 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, accompanied by equivalent evidence of identity to that originally provided to obtain the certificate.

7.4 OPERATIONAL REQUIREMENTS [IETF RFC 2527 Section 4]

7.4.1 Certificate Application [IETF RFC 2527 Section 4.1]

7.4.2 Certificate Issuance [IETF RFC 2527 Section 4.2]

7.4.3 Certificate Acceptance [IETF RFC 2527 Section 4.3]

7.4.4 Certificate Suspension and Revocation [IETF RFC 2527 Section 4.4]

7.4.4.1 Circumstances for Revocation [IETF RFC 2527 Section 4.4.1]

The issuing CA SHALL revoke a certificate:

a) Upon failure of the Certificate holder, the employer (in the case of a non-regulated employee or supporting organisation employee), or the sponsor (in the case of a sponsored health care provider) to meet obligations under this policy, any applicable Certification Practice Statement, or any other agreement, regulation, or law applicable to the certificate that may be in force.

b) Upon knowledge or reasonable suspicion of compromise of a private key.

c) If relevant subject information contained in the certificate is no longer accurate.

d) if a Certificate holder's organisational affiliation changes, e.g., a health professional resigning from a particular organisation.

e) If the CA determines that the certificate was not properly issued in accordance with this policy and/or any applicable Certification Practice Statement.

f) For any reason, upon request of a Certificate holder or sponsor of a sponsored health care provider.

Certificate holders, RA 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 [IETF RFC 2527 Section 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 organisation which made the application for the certificate on behalf of a device or application.

- the sponsor of a sponsored health care provider.
- personnel of the Issuing CA.
- personnel of an RA associated with the Issuing CA.

7.4.4.3 Procedure for Revocation Request [IETF RFC 2527 Section 4.4.3]

When a revocation request is received by the CA, in accordance with Section 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, 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 [IETF RFC 2527 Section 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 [IETF RFC 2527 Section 4.4.5]

Within health care PKIs, a CA MAY support suspension. The identified circumstances that will justify certificate suspension include:

1. Suspected compromise of private keys. Suspension will occur during investigation.
2. Pending clarification of information on the certificate.
3. A Certificate holder requests suspension.
4. Other circumstances determined within local Health Care PKI domains.

7.4.4.6 Who Can Request Suspension [IETF RFC 2527 Section 4.4.6]

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

1. the Certificate holder in whose name the certificate was issued.
2. the individual or organisation which made the application for the certificate on behalf of a device or application.
3. the sponsor of a sponsored health care provider.
4. personnel of the Issuing CA.
5. personnel of an RA associated with the Issuing CA
6. a relying party.

7.4.4.7 Procedures for Suspending Certificates [IETF RFC 2527 Section 4.4.7]

When a suspension request is received by the CA, in accordance with Section 7.4.4.5., the CA SHALL:

1. confirm the identity of the requestor., where the suspension request is purported to be from the Certificate holder, or from the individual or organisation which made the application for the certificate on behalf of a device or application, or from the sponsor of a sponsored health care provider

2. confirm the identity of the requestor where the suspension request is purported to be from the individual or organisation which made the application for the certificate on behalf of a device or application

3. confirm that the requestor has sufficient authority to effect suspension, If the requestor is acting as the sponsor of the Certificate holder

4. Verify the reasons given for suspension and if they prove be true, suspend the certificate.

7.4.4.8 Limits on Suspension Period [IETF RFC 2527 Section 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 (if applicable) [IETF RFC 2527 Section 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 [IETF RFC 2527 Section 4.4.10]

Relying parties should check the CRL whenever they commence 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 [IETF RFC 2527 Section 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 [IETF RFC 2527 Section 4.4.12]

On line revocation checking will require Certificate holders to establish secure communication with an online 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 [IETF RFC 2527 Section 4.4.13]

This technical specification makes no further stipulation

7.4.4.14 Checking Requirements for Other Forms of Revocation Advertisements [IETF RFC 2527 Section 4.4.14]

This technical specification makes no further stipulation

7.4.4.15 Special Requirements Regarding Key Compromise [IETF RFC 2527 Section 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 [IETF RFC 2527 Section 4.5]

Security Audit procedures SHALL be in accordance with a standard equivalent to but not less than ISO 17799:2000.

[Note 4.5.2 frequency: Lori to provide sentence or two on alignment with health care organisation audits.]

7.4.6 Records Archival [IETF RFC 2527 Section 4.6]

Records SHALL be archived in accordance with a standard equivalent to but not less than ISO 17799-1:2000.

7.4.7 Key Changeover [IETF RFC 2527 Section 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 [IETF RFC 2527 Section 4.8]

Security Audit procedures SHALL be in accordance with a standard equivalent to but not less than ISO 17799:2000

7.4.9 CA Termination [IETF RFC 2527 Section 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 CA's 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 [IETF RFC 2527 Section 5]

These SHALL be in accordance with a standard equivalent to but not less than ISO 17799:2000 or approved accreditation or licensing criteria. This will apply to Section 5. and cover the following issues:

7.5.1 Physical Controls [IETF RFC 2527 Section 5.1]

Physical controls SHALL be in accordance with a standard equivalent to but not less than ISO 17799:2000.

7.5.2 Procedural Controls [IETF RFC 2527 Section 5.2]

Procedural controls SHALL be in accordance with a standard equivalent to but not less than ISO 17799:2000.

7.5.3 Personnel Controls [IETF RFC 2527 Section 5.3]

Personnel controls SHALL be in accordance with a standard equivalent to but not less than ISO 17799:2000.

7.6 Technical Security Controls [IETF RFC 2527 Section 6]

7.6.1 Key Pair Generation and Installation [IETF RFC 2527 Section 6.1]

7.6.1.1 Key Pair Generation [IETF RFC 2527 Section 6.1.1]

A Certificate holder's public/ private key pair SHALL be generated by:

1. the CA, or
2. another trusted third party nominated by the CA, or
3. 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 [IETF RFC 2527 Section 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 *Certificate Management Protocol*, 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 section 7.6.2.4.

7.6.1.3 Public Key Delivery to Certificate Issuer [IETF RFC 2527 Section 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 *Certificate Management Protocol*, or via an equally secure manner.

7.6.1.4 CA Public Key Delivery to Certificate holders [IETF RFC 2527 Section 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. These are covered in RFC2527, Section 4.2.

7.6.1.5 Key Sizes [IETF RFC 2527 Section 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 [IETF RFC 2527 Section 6.1.6]

Public key parameters SHALL be generated by either the CA or the trusted third party key generation organisation.

7.6.1.7 Parameter Quality Checking [IETF RFC 2527 Section 6.1.7]

It SHALL be the role of the auditing organisation to check the parameter quality.

7.6.1.8 Hardware/Software Key Generation [IETF RFC 2527 Section 6.1.8]

This technical specification makes no further stipulation

7.6.1.9 Key Usage Purposes (as per X.509 v3 key usage field) [IETF RFC 2527 Section 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 [IETF RFC 2527 Section 6.2]

This technical specification RECOMMENDS that two key pairs should 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.

7.6.2.1 Standards for Cryptographic Module [IETF RFC 2527 Section 6.2.1]

CA signing keys SHALL be compliant with a standard equivalent to but not less than US FIPS 140-1 level 2.

Other certificates SHALL be compliant with a standard equivalent to but not less than US FIPS 140-1 level 1.

7.6.2.2 Private Key (n out of m) Multi-person Control [IETF RFC 2527 Section 6.2.2]

Where the Certificate holder is a health care organisation or supporting organisation, the private key MAY be split into more than one part under the control of different persons.

7.6.2.3 Private Key Escrow [IETF RFC 2527 Section 6.2.3]

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

7.6.2.4 Private Key Backup [IETF RFC 2527 Section 6.2.4]

Key backup requires having the private key duplicated and stored in a secure manner. The Certificate holder should backup private keys. It SHALL be carried out by a certified process and the backed up digital signature SHALL be accessible only to the key holder.

Private authentication or digital signature keys SHALL be backed up entirely within the control of the Certificate holder. Key backup SHALL be held within the Certificate holders' environment (workplace, department, or organisation).

The Certificate holder MAY consent to the CA backing up and retaining a copy of his/her private decipherment key.

Private key SHALL be backed at a level of protection no lower than that required for the primary copy

7.6.2.5 Private Key Archival [IETF RFC 2527 Section 6.2.5]

7.6.2.6 Private Key Entry into Cryptographic Module [IETF RFC 2527 Section 6.2.6]

If the private decipherment key is not generated in the Entity's cryptographic module, it SHALL be either entered into the module in accordance with IETF RFC 2511 Certificate Management Protocol, or via an equally secure manner.

7.6.2.7 Method of Activating Private Key [IETF RFC 2527 Section 6.2.7]

Within a health care PKI 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, pass phrase, or a token. When deactivated, private keys SHALL be kept in encrypted form only.

7.6.2.8 Method of Deactivating Private Key [IETF RFC 2527 Section 6.2.8]

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 over-written before the space is released to the operating system. The cryptographic module SHALL automatically deactivate the private key after a pre-set period of inactivity.

7.6.2.9 Method of Destroying Private Key [IETF RFC 2527 Section 6.2.9]

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 over-writing multiple times. Private key destruction procedures SHALL be described in the CPS or a publicly available document.

7.6.3 Other Aspects of Key Management [IETF RFC 2527 Section 6.3]

7.6.3.1 Public Key Archival [IETF RFC 2527 Section 6.3.1]

Public keys will need to be archived with a trusted third party to allow verification of a signature at a future date. The CA SHALL be responsible for ensuring public keys are archived.

7.6.3.2 Usage Periods for the Public and Private Keys [IETF RFC 2527 Section 6.3.2]

Non-CA public and private keys 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.

7.6.4 Activation Data [IETF RFC 2527 Section 6.4]

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

7.6.5 Computer Security Controls [IETF RFC 2527 Section 6.5]

These SHALL be in accordance with a standard equivalent to but not less than ISO 17799-1:2000 or approved accreditation or licensing criteria. and SHALL cover the following issues:

[IETF RFC 2527 Section 6.5.1 Specific computer security technical requirements

[IETF RFC 2527 Section 6.5.2 Computer security rating

7.6.6 Life Cycle Technical Controls [IETF RFC 2527 Section 6.6]

These SHALL be in accordance with a standard equivalent to but not less than ISO 17799-1:2000 or approved accreditation or licensing criteria and SHALL cover the following issues:

[IETF RFC 2527 Section 6.6.1 System development controls

[IETF RFC 2527 Section 6.6.2 Security management controls

[IETF RFC 2527 Section 6.6.3 Life cycle security ratings

7.6.7 Network Security Controls [IETF RFC 2527 Section 6.7]

This SHALL be in accordance with a standard equivalent to but not less than ISO 17799-1:2000 or approved accreditation or licensing criteria.

7.6.8 Cryptographic Module Engineering Controls [IETF RFC 2527 Section 6.8]

This SHALL be in accordance with a standard equivalent to but not less than ISO 17799-1:2000 or approved accreditation or licensing criteria.

7.7 Section 7 Certificate and CRL Profiles [IETF RFC 2527]

These SHALL be in accordance with ISO/TS 17090 - Part 2 of this technical specification.

7.8 Specific Administration [IETF RFC 2527 Section *8*]

7.8.1 Policy Change Procedures [IETF RFC 2527 Section 8.1]

Prior to making any changes to this certificate policy, the CA governing body SHALL notify all CAs that are directly cross-certified with the CA and request comments. The policy change SHALL be approved by the CA governing body.

7.8.2 Publication and Notification Procedures [IETF RFC 2527 Section 8.2]

An electronic copy of the Certificate Policy document, digital 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 e-mail request.

7.8.2 CPS Approval & Notification Procedures [IETF RFC 2527 Section 8.2]

The Certification Practice Statement precisely details the implementation of a CA service and the procedures for key life cycle management. It is more detailed than the CP and contains information that MAY need to remain confidential to ensure the CA's security.

The Certification Practice Statement SHALL be approved by the CA governing body.

8 Model PKI Disclosure Statement

8.1 Introduction

The Model PKI Disclosure Statement is designed for use by a CA issuing certificates as a supplemental disclosure document and notice of the elements of a Certificate Policy and/or Certification Practice Statement that require emphasis and disclosure. A PKI Disclosure Statement may assist a CA to respond to regulatory requirements and relying party concerns. Although Certificate Policy and Certification Practice Statement documents are essential for describing and governing certificate policies and practices, many PKI Certificate holders, especially consumers, find these documents difficult to understand.

The use of a PKI disclosure statement is RECOMENDED.

This Appendix provides an example of the structure for a PKI Disclosure Statement, illustrating information that should be disclosed.

8.2 Model PKI Disclosure Statement Structure

The PKI Disclosure Statement should contain a section for each defined statement type. Each section of a PKI Disclosure Statement contains a descriptive statement that MAY include hyperlinks to the relevant Certificate Policy / Certification Practice Statement sections.

STATEMENT TYPES	STATEMENT DESCRIPTIONS	CERTIFICATE POLICY REQUIREMENTS
CA contact info:	The name, location and relevant contact information for the CA.	
Certificate policy information and registration:	Registered certificate policy object identifier (OID),	Registered certificate policy object identifier (OID). Publication of Certificate Policy and Certification Practice Statement (Section 2.6).
Certificate level of assurance, validation procedures and use:	A description of the level of assurance of the certificate issued by the CA, corresponding validation procedures, and any restrictions on certificate use.	Any limitations on the certificate use.
Reliance limits:	The reliance limits, if any.	Any limitations on the certificate use (e.g., if the certificate can only be used for electronic signatures and the limits of relying on the certificate to support non-repudiation.
Obligations of Certificate holders:	The description of the Certificate holder obligations.	The Certificate holder's obligations as defined in Section 2.1.3.
Obligations of Relying Parties:	The extent to which Relying Parties are obligated to check certificate status, and "reasonably rely" on the certificate.	The relying party's obligations as defined in Section 2.1.4.

STATEMENT TYPES	STATEMENT DESCRIPTIONS	CERTIFICATE POLICY REQUIREMENTS
Limited warranty & disclaimer/Limitation of liability:	Summary of the warranty, disclaimers, limitations of liability and any applicable warranty or insurance programs.	Limitations of liability (see Section 2.2).
Applicable agreements, Certification Practice Statement, Certificate	Identification and references to applicable agreements, Certification Practice Statement, Certificate Policy and other relevant documents.	Qualified Certificate Policy being applied
Privacy policy:	A description of and reference to the applicable privacy laws and policy.	CAs under this policy are required to comply with the requirements of the country's Privacy Legislation.
Refund policy:	A description of and reference to the applicable refund policy.	
Applicable law, complaints and dispute resolution:	Statement of the choice of law, complaints procedure and dispute resolution mechanisms.	The procedures for complaints and dispute settlements. The applicable legal system.
CA audit:	A description of the audit process and the audit firm	Whether the CA has been certified to conform to its Certificate Policy.
Cross-certification	A description of cross-certification and identify other Certificate Authorities that are cross-certified with the CA.	Relevant policy governing cross-certification.
CA and repository licenses and trust marks:	Summary of any governmental licenses, seal programs.	

Annex A (Informative) Bibliography

Rich Ankney, CertCo, Privilege Management Infrastructure, v0.4, August 24, 1999

APEC Telecommunications Working Group , Business Facilitation Steering Group Electronic Authentication Task Group PKI Interoperability Expert Group, Achieving PKI Interoperability., September, 1999.

ASTM Draft Standard: Standard Guide for Model Certification Practice Statement for Health care**.** January 2000

Canadian Institute for Health Information: Digital Signature and Confidentiality Certificate Policies for Health PKI, 2000

Drummond Group, The Healthkey Program **,** PKI IN HEALTH CARE: RECOMMENDATIONS AND GUIDELINES FOR COMMUNITY-BASED TESTING, MAY 2000.

EESSI European Electronic Signature Standardisation Initiative (EESSI), Final Report of the EESSI Expert Team 20th July 1999

Feghhi Jalal, Feghhi Jalil, Williams Peter, Digital Certificates – Applied Internet Security, Addison-Wesley 1998.

Government of Canada, Criteria for Cross Certification, 2000

Klein, Gunnar, Lindstrom Valter, Norr Anders, Ribbegard Goran, Torlof, Per Technical Aspects of PKI, January 2000

Klein, Gunnar, Lindstrom Valter, Norr Anders, Ribbegard Goran, Sonnergren Elizabeth, Torlof, Per,
Infrastructure for Trust in Health Informatics, January 2000

Strategies for the Implementation of a Public Key Authentication Framework (PKAF) in Australia SAA MP75, Standards Australia

Wilson, Stephen, Audit Based Public Key Infrastructure, Price Waterhouse Coopers White Paper, November 2000.