
**Health informatics — Public key
infrastructure —**

**Part 2:
Certificate profile**

*Informatique de santé — Infrastructure de clé publique —
Partie 2: Profil de certificat*



PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 17090-2:2002

© ISO 2002

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

Printed in Switzerland

Contents

Page

Foreword	iv
Introduction.....	v
1 Scope	1
2 Normative references.....	1
3 Terms and definitions	1
4 Abbreviations	2
5 Healthcare CPs	2
5.1 Certificate types required for healthcare	2
5.2 CA certificates	2
5.3 Cross/Bridge certificates	3
5.4 End entity certificates	3
6 General certificate requirements	6
6.1 Certificate compliance	6
6.2 Common fields for each certificate type.....	7
6.3 Specifications for common fields.....	8
6.4 Requirements for each healthcare certificate type.....	10
7 Use of certificate extensions	13
7.1 Introduction	13
7.2 General extensions	13
7.3 Special subject directory attributes	14
7.4 Qualified certificate statements extension	16
7.5 Requirements for each health industry certificate type	16
Annex A (informative) Certificate profile examples	18
Bibliography.....	25

Foreword

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

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

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

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of normative document:

- an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;
- an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years with a view to deciding whether it should be confirmed for a further three years, revised to become an International Standard, or withdrawn. In the case of a confirmed ISO/PAS or ISO/TS, it is reviewed again after six years at which time it has to be either transposed into an International Standard or withdrawn.

Attention is drawn to the possibility that some of the elements of this part of ISO/TS 17090 may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TS 17090-2 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

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

- *Part 1: Framework and overview*
- *Part 2: Certificate profile*
- *Part 3: Policy management of certification authority*

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

Introduction

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

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

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

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

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

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

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

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

This three-part document is being issued in the Technical Specification series of publications (according to the ISO/IEC Directives, Part 1, 3.1.1.1) as a prospective standard for the use of PKI in the field of healthcare because there is an urgent need for guidance on how standards in this field should be used to meet an identified need. This document is not to be regarded as an International Standard. It is proposed for provisional application so that information and experience of its use in practice may be gathered. ISO/TC 215 intends to revise it into a full International Standard after a three-year period.

This Technical Specification describes the common technical, operational and policy requirements that need to be addressed to enable PKI to be used in protecting the exchange of healthcare information within a single domain, between domains and across jurisdictional boundaries. Its purpose is to create a platform for global interoperability.

It specifically supports PKI enabled communication across borders, but could also provide guidance for the establishment of healthcare PKIs nationally or regionally. The Internet is increasingly used as the vehicle of choice to support the movement of healthcare data between healthcare organizations and is the only realistic choice for cross-border communication in this sector.

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

ISO/TS 17090-1 defines the basic concepts of a healthcare public key infrastructure (PKI) and provides a scheme of interoperability requirements to establish a PKI enabled secure communication of health information.

ISO/TS 17090-2 provides healthcare specific profiles of digital certificates based on the International Standard X.509 and the profile of this specified in IETF/RFC 2459 for different types of certificates.

ISO/TS 17090-3 deals with management issues involved in implementing and operating a healthcare PKI. It defines a structure and minimum requirements for certificate policies (CPs) and a structure for associated certification practice statements. This part is based on the recommendations of the IETF/RFC 2527 *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* and identifies the principles needed in a healthcare security policy for cross border communication. It also defines the minimum levels of security required, concentrating on the aspects unique to healthcare.

Comments on the content of this document, as well as comments, suggestions and information on the application of these technical specifications may be forwarded to the ISO/TC 215 secretariat: tsandler@astm.org and the WG4 secretariat w4sec215@medis.or.jp.

Health informatics — Public key infrastructure —

Part 2: Certificate profile

1 Scope

This part of ISO/TS 17090 specifies the certificate profiles required to interchange healthcare information within a single organization, between different organizations and across jurisdictional boundaries. It details the use made of public key infrastructure (PKI) digital certificates in the health industry and focuses, in particular, on specific healthcare issues relating to certificate profiles.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/TS 17090. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO/TS 17090 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/TS 17090-1:2002, *Health informatics — Public key infrastructure — Part 1: Framework and overview*

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

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*

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

3 Terms and definitions

For the purposes of this part of ISO/TS 17090, the terms and definitions given in ISO/TS 17090-1:2002 apply.

4 Abbreviations

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

5 Healthcare CPs

5.1 Certificate types required for healthcare

Identity certificates shall be issued to:

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

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

5.2 CA certificates

5.2.1 Root CA certificates

Root CA certificates are used when the subject of the certificate is itself a CA, they are self-signed and are used in a healthcare PKI to issue certificates to relying parties, including subordinate CAs. The basic constraints field indicates whether the certificate is a CA, as well as the maximum allowable depth of a certification path through that CA.

5.2.2 Subordinate CA certificates

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

Public key infrastructure

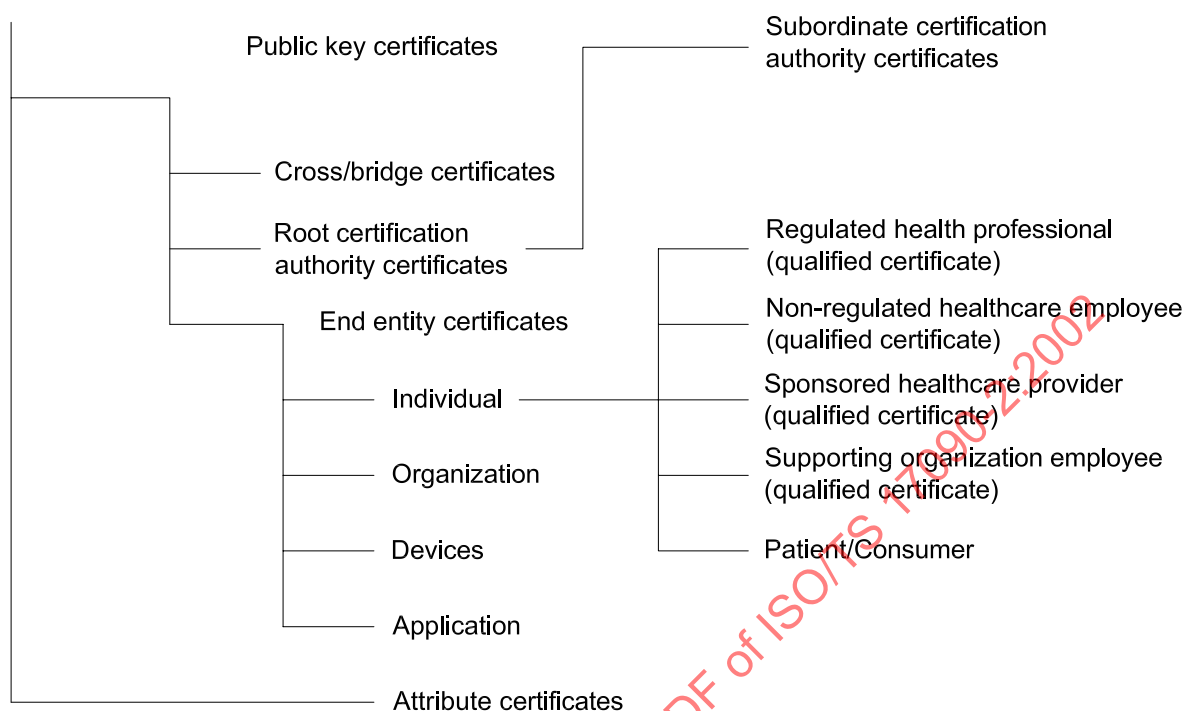


Figure 1 — Healthcare certificate types

5.3 Cross/Bridge certificates

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

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

5.4 End entity certificates

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

5.4.1 Individual identity certificates

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

a) regulated health professional:

- each certificate holder is a health professional who, in order to practice his/her profession requires a license or registration from a government body (see 5.1 of ISO/TS 17090-1:2002). These certificates may be qualified certificates (see 8.2 of ISO/TS 17090-1:2002 and 7.3 below);

b) non-regulated health professional:

- each certificate holder is a health professional who is not subject to registration or licensing from a government body (see 5.1 of ISO/TS 17090-1:2002). These certificates may be qualified certificates;

c) sponsored healthcare provider:

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

d) supporting organization employee:

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

e) patient/consumer:

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

5.4.2 Organization identity certificate

An organization that is involved in the health industry may hold a certificate to identify itself or to use for encryption purposes. In accordance with IETF/RFC 2527, provision is made in this part of ISO/TS 17090 for an organizational unit name.

5.4.3 Device identity certificate

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

5.4.4 Application certificate

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

This part of ISO/TS 17090 concentrates on the providers, but recognizes that patients/consumers will increasingly require the services of a PKI in managing their own healthcare.

5.4.5 AC

An AC is a digitally signed (or certified) set of attributes. An AC is a structure similar to a PKC; the main difference being that it contains no public key. An AC may contain attributes that specify group membership, role, security clearance and other information associated with the AC holder that could be used for access control. The AC shall be in accordance with the specifications given in INTERNET-DRAFT October 1999 4.1, *X.509 Attribute Certificate*.

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

The syntax of an AC is specified in X.509:

AttributeCertificate ::= SIGNED { AttributeCertificateInfo }

AttributeCertificateInfo ::= SEQUENCE {
version **Version** **DEFAULT v1,**
owner **SEQUENCE {**
 baseCertificateId [0] **IssuerSerial** **OPTIONAL,**
 entityName [1] **GeneralNames** **OPTIONAL,**
 objectDigestInfo [2] **ObjectDigestInfo** **OPTIONAL },**
issuer **SEQUENCE {**
 baseCertificateId **IssuerSerial** **OPTIONAL,**
 issuerName [0] **GeneralNames** **OPTIONAL },**
signature **AlgorithmIdentifier,**
serialNumber **CertificateSerialNumber,**
attCertValidityPeriod **AttCertValidityPeriod,**
attributes **SEQUENCE OF Attribute,**
issuerUniqueID **UniquelIdentifier** **OPTIONAL,**
extensions **Extensions** **OPTIONAL }**

Version ::= INTEGER { v1(0), v2(1) }

IssuerSerial ::= SEQUENCE {
issuer **GeneralNames,**
serialNumber **CertificateSerialNumber,**
issuerUID **UniquelIdentifier** **OPTIONAL }**

CertificateSerialNumber ::= INTEGER

UniquelIdentifier ::= BIT STRING

ATTRIBUTE ::= CLASS {
 &id **OBJECT IDENTIFIER** **UNIQUE,**
 &singleValued **BOOLEAN** **DEFAULT FALSE,**
 &Syntax **}**

Attribute ::= SEQUENCE {
 attrType **ATTRIBUTE.&id ({SupportedAttrs}),**
 attrValues **ATTRIBUTE.&Syntax ({SupportedAttrs} {@attrType}) }**

ObjectDigestInfo ::= SEQUENCE {
 digestAlgorithm **AlgorithmIdentifier,**
 objectDigest **OCTET STRING }**

AttCertValidityPeriod ::= SEQUENCE {
 notBefore **GeneralizedTime,**
 notAfter **GeneralizedTime }**

The components of the AC are used as follows.

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

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

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

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

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

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

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

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

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

Details on the use of ACs in healthcare are specified in 8.3 of ISO/TS 17090-1:2002.

5.4.6 Role certificates

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

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

The following are all possible:

- any number of roles can be defined by any AA;
- the role itself and the members of a role can be defined and administered separately, by separate AAs;
- the privileges assigned to a given role may be placed into one or more ACs;
- a member of a role may be assigned only a subset of the privileges associated with a role, if desired;
- role membership may be delegated; and
- roles and membership may be assigned any suitable lifetime.

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

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

6 General certificate requirements

6.1 Certificate compliance

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

- a) Certificates shall be X.509 version 3 certificates.

- b) Certificates shall be in accordance with IETF/RFC 2459. Deviations from IETF/RFC 2459 are only allowed if they are aligned with proposed solutions to known problems with IETF/RFC 2459.
- c) For individual identity, certificates should be in accordance with the IETF/RFC 3039. Deviations should only be allowed if they are aligned with proposed solutions to known problems.
- d) The signature field shall identify the signature algorithms used.
- e) The certified public key shall have a minimum key-length field depending on the algorithm used. Key sizes shall be in accordance with those specified in clause 6 of ISO/TS 17090-3:2002.
- f) Digital certificates shall not be issued for the purposes of non-repudiation and digital signature. In addition, digital signatures shall not be used for the purpose of encipherment (see 7.2).

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

Certificate ::= SIGNED { SEQUENCE {

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

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

6.2 Common fields for each certificate type

- 1 **serialNumber** is an integer assigned by the CA to each certificate. Its intention is to uniquely identify each certificate.
The value of **serialNumber** shall be unique for each certificate issued by a given CA (i.e. the issuer name and serial number identify a unique certificate).
- 2 **signature** contains the algorithm identifier for the algorithm used by the CA to sign the certificate.
- 3 **issuer** identifies the name of the entity that has signed and issued the certificate. The field shall be populated with an appropriate ISO name structure according to the object class *Organizational Role*, located under an organization or under an organizational unit.
- 4 **validity** is the time interval during which the CA warrants that it will maintain information about the status of the certificate. For regulated health professionals, the validity period shall not exceed the validity period for the professional licence.

Note on time format:

The Distinguished Encoding Rules (DER) allow several methods for formatting UTCTime and GeneralizedTime. It is important that all implementations use the same format to minimize signature verification problems. Where the year is greater or equal to 2050 the time shall be encoded using GeneralizedTime. To ensure that UTCTime encodings are consistently formatted, UTCTime should be encoded using the "Z" format and the seconds field shall not be omitted, even if it is 00 (i.e. the format shall be YYYYMMDDHHMMSSZ). Where so encoded, the year field YY shall be interpreted as 19YY when YY is greater than or equal to 50 and as 20YY when YY is less than 50. When GeneralizedTime is used, it should be encoded in the "Z" format and the seconds field should be included (i.e. the format should be YYYYMMDDHHMMSSZ).

- 5 **subject** identifies the name of the entity associated with the public key found in the subject public key field.
- 6 **subjectPublicKeyInfo** is used to carry the public key and identify the algorithm with which the key is used.

7 **issuerUniquelIdentifier** is an optional bit string used to uniquely identify an issuer.

(In accordance with RFC 2459, this Technical Specification recommends that this field should not be used.)

8 **subjectUniquelIdentifier** is an optional bit string used to uniquely identify a subject.

(In agreement with RFC 2459, this Technical Specification recommends that this field should not be used.)

9 **extensions** — a SEQUENCE of one or more extensions shall be present.

The signature of the certificate is appended to the certificate data type by means of the standard signed data type defined in X.509.

6.3 Specifications for common fields

6.3.1 General

Specific requirements for information content in basic certificate fields, which are not already specified by IETF/RFC 2459 or draft-ietf-pkix-qc-02, are as follows.

6.3.2 Signature

It is recommended that the signature field contain one of the following values:

1. md5WithRSAEncryption (1.2.840.113549.1.1.4)
2. sha1WithRSAEncryption (1.2.840.113549.1.1.5)
3. dsa-with-sha1 (1.2.840.10040.4.3)
4. md2WithRSAEncryption (1.2.840.113549.1.1.2)
5. Ecdsa [1, 2, 840, 10045, 2, 1]}

6.3.3 Validity

Validity dates shall be in accordance with IETF/RFC 2459. This part of ISO/TS 17090 has adopted reasonable constraints for health certificate validity periods as specified in 6.1 of ISO/TS 17090-3:2002.

Certificate's **notBefore time** expresses the exact moment from which the CA will maintain and publish accurate information about the status of the certificate.

6.3.4 Subject public key information

The algorithm identifier shall be identified, e.g.

1. RSA

pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) 1 }
rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1 }

2. Diffie-Hellman

The Diffie-Hellman OID supported by this profile is defined by ANSI
X9.42 [X9.42].

dhpublicnumber OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) ansi-x942(10046) number-type(2) 1 }

3. DSA

The DSA OID supported by this profile is

id-dsa ID ::= { iso(1) member-body(2) us(840) x9-57(10040)

x9cm(4) 1 }

4. *Elliptic Curve*

Ecdsa [1, 2, 840, 10045, 2, 1] }

Refer to ISO/TS 17090 — Part 3, Section 6 for specification of key sizes.

6.3.5 Issuer name field

The issuer name, stored in the issuer name field, shall, with the amendments and constraints specified below, be consistent with an appropriate ISO name structure according to the object class *Organizational Role*, located under an organization or under an organizational unit.

Contents of the issuer name field for each certificate type is specified in 6.4.

1. **countryName:** The *countryName* shall contain the two character ISO country identifiers.

EXAMPLE *countryName* = "US"

This field is mandatory, as it is critical in the healthcare field to know the country of origin of a certificate presented with a request for access to personal health information. Different countries have varying privacy laws and practices to protect client/consumer policy and knowing the country a request has originated from will assist any decision on whether to grant it.

2. **localityName:** *localityName* may be used to store at least one locality name value. The specification will specify use of two levels of locality name. The top level specifies the PKI for the country participating followed by a geographic locality name value. Within the certificate issuer name the *localityName* may be omitted and only the geographic *localityName* may be used.

EXAMPLE *localityName* = "California"

3. **organizationName:** The *organizationName* field, which refers to the name of the sponsoring healthcare organization in the case of end entities and the organization name of the CA in the case of CA certificates, shall contain the full registered name or the organization, as specified by the participating PKI.

EXAMPLE *organizationName* = "California Hospital Authority"

4. **organizationalUnitName:** The *organizationalUnitName* field may, when present, be used to store a name of an organizational unit/department under the specified organization. Organizational units may be specified in several levels by including more than one field value. When present, the *organizationalUnitName* shall be selected in a way that prevents name ambiguity within the CA domain.

EXAMPLE *organizationalUnitName* = "Midtown Hospital Radiology"

5. **commonName:** The purpose of this field is to describe the name by which the subject is commonly known. This field is often used, together with subject *commonName*, by standard software components when presenting a certificate to a user. The presented name shall therefore be informative, providing a good understanding of the certificate issuer and the purpose of the certificate. It is further recommended to include a name of the governing certificate policy in the *commonName* field value. This is in addition to referring to the policy using the OID.

EXAMPLE *commonName* = "Patient Health Information Policy"

6.3.6 The subject name field

The subject name, stored in the subject name field, shall, with the amendments and constraints defined below, be consistent with an appropriate ISO name structure according to the object class *Organizational Role*, located under an organization or under an organizational unit.

Qualifications and titles of healthcare actors will be reflected in the certificate extension — HCRole field.

Contents of the Subject Name field for each certificate type are specified in 6.4.

1. **countryName:** The *countryName* shall contain the two character ISO country identifier.

EXAMPLE *countryName* = "US"

The population of this field should reflect the particular country's practice.

This field is mandatory for CAs, regulated and non-regulated health professionals, sponsored healthcare providers, supporting organization employees and organizations, as it is critical in the healthcare field to know the country of origin of an entity that is the subject of a certificate presented with a request for access to personal health information. Different countries have varying privacy laws and practices to protect client/consumer policy and knowing from which country the request has originated will assist any decision on whether to grant it.

2. *localityName*: *localityName* may be used to store at least one locality name value. Two levels of locality name are specified, with the top level being the PKI for the country participating. This is followed by a geographic locality name value. Within the certificate subject name the *localityName* may be omitted and only the geographic *localityName* may be used.

EXAMPLE *localityName* = "California"

3. *organizationName*: The *organizationName* field, which refers to the name of the sponsoring healthcare organization in the case of end entities and the organization name of the CA in the case of CA certificates, shall contain the full registered name or the organization, as specified by the participating PKI.

EXAMPLE *organizationName* = "Midtown General Hospital"

4. *organizationalUnitName*: The *organizationalUnitName* field may, when present, be used to store a name of an organizational unit/department under the specified organization. Organizational units may be specified in several levels by including more than one field value. When present, the *organizationalUnitName* shall be selected in a way that prevents name ambiguity.

EXAMPLE *organizationalUnitName* = "Midtown Hospital Radiology"

5. *commonName*: The purpose of this field is to describe the name by which the subject is commonly known. It shall be present and shall clearly identify the subject as it is known within the healthcare system.

EXAMPLE *commonName* = "Bruce Wayne"

This field is mandatory for persons and organizations that are the subject of certificates. It is essential to be able to identify the common name by which a person is known in the health system, if decisions are to be made on whether to allow them to access personal health information.

6. *surName*: This field is used to describe the surname by which the subject is known. It may be present. If present, it shall clearly identify the subject as it is known within the healthcare system.

EXAMPLE *commonName* = "Wayne"

7. *givenName*: The purpose of this field is to describe the given name by which the subject is commonly known. It may be present. It shall clearly identify the subject as it is known within the healthcare system.

EXAMPLE *givenName* = "Bruce"

8. *e-mail*: The primary recommended usage of this field is to record the subject's electronic mail address.

EXAMPLE *e-mail* = "jsmith@network.com.au"

6.4 Requirements for each healthcare certificate type

6.4.1 Issuer fields

Issuer field requirements for each healthcare certificate type are given in Table 1.

6.4.2 Subject fields

Subject field requirements for each healthcare certificate type are given in Table 2.

Table 1 — Issuer field requirements for each healthcare certificate type

Certificate elements	CA certificates		Identity certificates					Attribute certificate
	Certification authority certificate	Cross/Bridge certificate	Regulated health professional certificate	Non-regulated healthcare professional certificate ^b	Consumer certificate	Organization certificate	Devices certificate	Applications certificate
Issuer fields^a								
CountryName	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
LocalityName	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional
Organization_Name	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
Organizational_Unit Name	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional
CommonName	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Not applicable
^a This table refers to issuer ID elements that may vary between certificate types.								
^b The values for non-regulated health professional certificates also apply to sponsored healthcare provider certificates and supporting healthcare employees certificates.								

Table 2 — Subject field requirements for each healthcare certificate type

Certificate elements	CA certificates		Identity certificates					Attribute certificate	
	Certification authority certificate	Cross/Bridge certificate	Regulated health professional certificate	Non-regulated healthcare professional certificate ^b	Consumer certificate	Organization certificate	Devices certificate		Applications certificate
Subject fields ^a									
CountryName	Mandatory	Mandatory	Mandatory	Mandatory	Optional	Mandatory	Optional	Optional	Optional
LocalityName	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional
Organization_Name	Mandatory	Mandatory	Optional	Optional	Optional	Mandatory	Optional	Optional	Optional
Organizational_Unit Name	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional
CommonName	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Optional	Optional	Optional
GivenName	Not applicable	Not applicable	Optional	Optional	Optional	Not applicable	Not applicable	Not applicable	Optional
Surname	Not applicable	Not applicable	Optional	Optional	Optional	Not applicable	Not applicable	Not applicable	Optional
Electronic mail	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional
^a This table refers to subject ID field elements that may vary between certificate types.									
^b The values for non-regulated health professional certificate also apply to sponsored healthcare provider certificates and supporting healthcare employee certificates.									

7 Use of certificate extensions

7.1 Introduction

Requirements that implementations shall have of certificate extensions in X.509 version 3 certificates for a healthcare PKI are given below. More detailed information about these extensions is given in IETF/RFC 2459 and IETF/RFC 3039.

7.2 General extensions

7.2.1 authorityKeyIdentifier

This extension shall identify the public key to be used to verify the signature of the certificate. It enables distinct keys, used by one CA, to be distinguished (e.g. as key updating occurs).

Only the **keyIdentifier** element of the authorityKeyIdentifier extension shall be used.

This is a non-critical extension. It is recommended that it be mandatory.

7.2.2 subjectKeyIdentifier

This extension is used to identify the public key held in the subjectPublicKeyInfo field of the certificate.

IETF/RFC 2459 contains guidelines on how the keyIdentifier element may be derived from the public key. Any algorithm is allowed, however, as long as the identifier satisfies the property of being a unique representation of the key.

This is a mandatory and non-critical extension for all end-entity certificates and all CA certificates within the healthcare chain of trust.

7.2.3 keyUsage

This extension shall identify the basic key usage associated with the public key in the certificate. The use of single key pairs for both encipherment and digital signature is discouraged and a key usage of dataEncipherment together with a key usage of digitalSignature or nonRepudiation for each certificate shall not be specified.

This extension shall be mandatory. It is recommended (as in IETF/RFC 2459) that this extension be critical.

7.2.4 privateKeyUsagePeriod

The use of this extension is not recommended.

The default private key usage period in absence of this extension is the validity period of the certificate.

7.2.5 certificatePolicies

The certificatePolicies extension shall contain an objectIdentifier of a standardized certificate CA-policy as specified in ISO/TS 17090-3:2002.

This is a mandatory and non-critical extension.

7.2.6 subjectAltName

It is recommended that this extension be present in the certificate. It is recommended that directoryName be included and be set to a UTF8String for the purpose of providing international character set support for a subject distinguished name.

This is a mandatory and non-critical extension.

7.2.7 basicConstraints

The basicConstraints extension contains a boolean used to specify whether or not the subject can act as a CA, using the certified key to sign certificates. If so, a certification path length constraint may also be specified.

CA certificates shall include a **basicConstraints** extension with the **CA** value set to **TRUE**.

This extension may either be critical or non-critical.

End entity certificates (individual regulated health professional, non-regulated healthcare employee, sponsored healthcare provider, supporting healthcare employee, consumer, organization, application and devices certificates) shall not include this extension.

7.2.8 CRLDistributionPoints

IETF/RFC 2459 recommends support for this extension by CAs and applications. For healthcare implementations that rely upon CRL distribution points, the extension shall identify the location of the associated CRL (or ARL for CA certificates) in the PKI directory and shall be a mandatory and non-critical extension.

7.2.9 ExtKeyUsage

This field indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension field.

This extension is optional and non-critical.

7.2.10 Authority information access

The authorityInfoAccess extension indicates how to access CA information and services. The location of CRLs is not specified in this extension. The extension is comprised of a sequence of access methods and access locations. Each entry in the sequence describes the format and location of additional information about the CA. The type and format of the information is specified by the access method, and the access location specifies the location of the information.

This extension is optional and non-critical.

7.3 Special subject directory attributes

7.3.1 hcRole attribute

The hcRole attribute allows the encoding of regulated and non-regulated health professional role data. It is recommended that it be implemented, as it will provide international interoperability in certification of healthcare roles. It allows multiple certificates to be issued and enables a range of classification tables to be associated with the field. The proposed field has an extension mechanism to allow for national or regional healthcare role coding schemes.

This field is needed in an identity certificate as the certificate holder's healthcare role forms an integral part of his/her identity. Once verified, further information is more appropriately placed in an AC as discussed in 8.4 of ISO/TS 17090-1:2002.

This part of ISO/TS 17090 allows for the assertion of regional data including professional identifiers such as registration numbers, billing numbers and patient identifiers. See REGIONAL-DATA below.

```
hcRole ATTRIBUTE ::= {
    WITH SYNTAX          HCActorData
    EQUALITY MATCHING RULE hcActorMatch
    SUBSTRINGS MATCHING RULE hcActorSubstringsMatch
    ID                    id-hcpki-at-healthcareactor}
```

Assignment of object identifier values

The following values are assigned in this Technical Specification:

```
{iso (1) standard (0) hcpki (17090)}
  id-hcpki OBJECT IDENTIFIER ::= 1.0.17090

id-hcpki-at OBJECT IDENTIFIER ::= {id-hcpki 0 }
  id-hcpki-at OBJECT IDENTIFIER ::= 1.0.17090.0

id-hcpki-at-healthcareactor OBJECT IDENTIFIER ::= {id-hcpki-at 1}
  id-hcpki-at-healthcareactor OBJECT IDENTIFIER ::= 1.0.17090.0.1

id-hcpki-cd OBJECT IDENTIFIER ::= {id-hcpki 1}
  id-hcpki-cd OBJECT IDENTIFIER ::= 1.0.17090.1
```

Definition of data types:

```
HCActorData ::= SET OF HCActor

HCActor ::= SEQUENCE {
  codedData [0] CodedData OPTIONAL,
  RegionalHCActorData [1]
    SEQUENCE OF RegionalData OPTIONAL }

CodedData ::= SET {
  codingSchemeReference [0] OBJECT IDENTIFIER,
  ---- Contains the ISO coding scheme Reference

  ---- or local coding scheme reference achieving ISO registration.

  ---- The ISO coding scheme OID is id-hcpki (defined above).

  ---- At least ONE of the following SHALL be present:

  codeDataValue [1] NumericString OPTIONAL,
  codeDataFreeText [2] DirectoryString OPTIONAL }

RegionalData ::= SEQUENCE {
  type REGIONALDATA.&id({SupportedRegionalData}),
  value REGIONALDATA.&Type({SupportedRegionalData}{@type}) }
```

Definition of REGIONALDATA object class:

```
REGIONALDATA ::= CLASS {
  &Type,
  &idOBJECT IDENTIFIER UNIQUE }
WITH SYNTAX {
  WITH SYNTAX &Type
  ID &id }
```

Definition of SupportedRegionalData object class set

```
SupportedRegionalData REGIONALDATA ::=
  {coded,
    ... -expect additional regional/national objects to be defined}
```

Definition of coded information object:

```
coded ::= REGIONAL-DATA {  
    WITH SYNTAX CodedRegionalData  
    ID id-hcpki-cd}  
  
CodedRegionalData ::= SEQUENCE {  
    country[0] PrintableString (SIZE (2)),  
        -- ISO3166 code of country of issuing authority.  
  
    issuingAuthority [1] DirectoryString,  
  
        -- Identifier of issuing authority as Regional Entity. -- -- Could be  
        implemented as a true identifier or a  
  
        -- Directory lookup string (to be determined)  
  
    hcMajorClassCode [2] CodedData,  
    hcMinorClassCode [3] CodedData OPTIONAL
```

Codes to be used for this field, e.g. ASTM E1986-98 Data User Role Name.

It is recommended that The **HcProfessionalData** be taken from the appropriate national coding scheme.

This extension is optional and non-critical.

7.3.2 subjectDirectoryAttributes

It is recommended that this extension be present in individual identity certificates. In such certificates it may contain an hcRole attribute (see 7.3.1). In addition, subjectDirectoryAttributes may contain other attributes not specified by this Technical Specification.

The extension shall be marked non-critical. Since the certificate is used for both authentication and role assigning purposes, its use shall be mandatory for regulated health professional certificates and non-regulated health professional certificates. It shall be optional for other certificate types.

7.4 Qualified certificate statements extension

It is recommended that certificates for regulated health professionals and for non-regulated health professionals contain a qcStatement. Certificates for patients/consumers, for sponsored healthcare providers and for supporting organization employees may contain a qcStatement subject directory attribute. Certificates for devices and applications shall not contain this subject directory attribute. The detailed specification is given in IETF/RFC 3039.

It is recommended that complying applications be able to support the qcStatements extension.

The extension is optional and non-critical.

7.5 Requirements for each health industry certificate type

7.5.1 Extension fields

Extension field requirements for each health industry certificate type are given in Table 3.

Table 3 — Extension field requirements for each health industry certificate type

Certificate elements	CA certificates		Identity certificates					Attribute certificates
	Certification authority certificate	Cross/Bridge certificate	Regulated health professional	Non-regulated health professional	Consumer	Organization	Device	Application
General extensions								
authorityKeyIdentifier ^a	Mandatory ^a	Mandatory ^a	Mandatory ^a	Mandatory ^a	Mandatory ^a	Mandatory ^a	Mandatory	Mandatory ^a
subjectKeyIdentifier	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
keyUsage	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
privateKeyUsagePeriod	Absent	Absent	Absent	Absent	Absent	Absent	Absent	Absent
certificatePolicies	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
subjectAltName	Absent	Absent	Optional	Optional	Optional	Optional	Optional	Optional
subjectDirectoryAttributes ^b	Absent	Absent	Mandatory ^b	Mandatory ^b	Optional	Absent	Absent	Absent
basicConstraints	Mandatory and critical	Mandatory and critical	Absent	Absent	Absent	Absent	Absent	Absent
CRLDistributionPoints	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
ExtKeyUsage	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional
Other extensions								
Authority information access	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional
qcStatements extension	Absent	Absent	Mandatory	Mandatory	Mandatory	Absent	Absent	Absent
Hcrole ^b	Absent	Absent	Mandatory ^b	Mandatory ^b	Optional	Optional	Optional	Absent

^a It is recommended that this field be mandatory.

^b The use of hcRole in certificates for regulated health professionals and non-regulated professionals requires that the subjectDirectoryAttributes be mandatory.

Annex A (informative)

Certificate profile examples

A.1 Introduction

Some basic examples of each type of certificate are detailed below for illustrative purposes. These examples are not normative. The ASN.1 code and normative text is found in the main text of this part of ISO/TS 17090.

A.2 EXAMPLE 1: Consumer certificate profile

NOTE The following example is for illustrative purposes only and is not intended to state the future format of UK National Health Service (NHS) certificates.

Bill Smith, NHS number 368964278, Date of certificate issuance: 1 August 2001, Date of certificate expiration: 1 August 2006

Version		(2 – decimal code for version 3 certificates)
SerialNumber		(unique CA generated decimal number)
Signature		(sha-1WithRSAEncryption {1,2,840,113549,1,1,5})
Issuer	countryName	(UK)
	localityName	(London)
	organizationName	(Dept. of Health)
	organizationalUnit	(National Health Service)
	commonName	(Patient Certificate v1)
	serialNumber	{serialNumber of the issuer}
Validity		(validity period coded as UTCtime: not before 010801000000z not after 060801000000z)
Subject	countryName	(UK)
	localityName	(London)
	organizationName	(NHS)
	organizationalUnit	(Patient Registration)
	commonName	(Smith, Bill)
	surName	(Smith)
	givenName	(William)
	e-mail	(bSmith@uknet.com)
subjectPublicKeyInfo	algorithm	(public RSA key, 1024 bit {1,2,840,113549,1,1,1})
	subjectPublicKey	(Subject's PUBLIC KEY)
Extensions		
authorityKeyIdentifier		(unique identifier of CA public key)
subjectKeyIdentifier		(unique identifier of subject public key)
keyUsage		(digitalSignature)
certificatePolicies	policyIdentifier	OBJECT IDENTIFIER ::= <i>Policy-OID-for-Patient-Certificate-v1</i>
	cRLDistributionPoints	(http://crl.location.nhs.uk)
authorityInformationAccess		(http://ocspserver.nhs.uk/OCSP_SERVER:5555)
subjectDirectoryAttributes	hcRole	OBJECT IDENTIFIER ::= <i>id-hcpki-at-healthcareactor</i>
	hcActorData	SET OF {

```

codedData CodedData ::= {
    codingSchemeReference OBJECT IDENTIFIER ::= id-hcpki,
    codeDataValue NUMERIC STRING ::= the-code-for-patient,
    codeDataFreeText DirectoryString ::= optional-data }
regionalHCData Sequence of RegionalData ::= {
    type OBJECT IDENTIFIER ::= OID-for-this-regional-encoding,
    country PrintableString (SIZE (2) ::= ISO-country-code-for-UK,
    issuingAuthority DirectoryString ::= (c=UK, National Health Service,
        ou=patients),
    hcMajorClassCode CodedData ::= {
        codingSchemeReference OBJECT IDENTIFIER ::=
            Coding-Scheme-for-Type-OID,
        codeDataValue NUMERIC STRING ::= Type-OID-for-patient,
        codeDataFreeText UTF8String ::= "patient ID 368964278" } }

```

A.3 EXAMPLE 2: Non-regulated health professional certificate profile

NOTE The following example is for illustrative purposes only and is not intended to state the future format of health certificates issued in the State of California.

Betty Smith, "Certified Medical Transcriptionist (CMT)"; CMT are issued by the American Association of Medical Transcriptionist.

Version	(2 – decimal code for version 3 certificates)
SerialNumber	(unique CA generated decimal number)
Signature	(sha-1WithRSAEncryption {1,2,840,113549,1,1,5})
Issuer	
	countryName (US)
	localityName (California)
	organizationName (Name-of-CA-for-California-Health-Care)
	commonName (Name-of-CA-for-California-Health-Care)
Validity	(validity period coded as UTCTime)
Subject	
	countryName (US)
	localityName (California)
	organizationName (CertHolderOrganization)
	commonName (Smith, Betty)
	surname (Smith)
	givenName (Betty)
subjectPublicKeyInfo	
	algorithm (public RSA key, 1024 bit {1,2,840,113549,1,1,1})
	subjectPublicKey (Subject's PUBLIC KEY)
Extensions	
authorityKeyIdentifier	(unique identifier of CA public key)
subjectKeyIdentifier	(unique identifier of subject public key)
keyUsage	(digitalSignature or non-repudiation or keyEncipherment)
certificatePolicies	(appropriate policy OID)
cRLDistributionPoints	(CRL X.500 entry location)
subjectDirectoryAttributes	
	(hcRole OBJECT IDENTIFIER ::= <i>id-hcpki-at-healthcareactor</i>)
	hcActorData SET OF {
	codedData CodedData ::= {
	codingSchemeReference OBJECT IDENTIFIER ::= <i>id-hcpki</i> ,
	codeDataValue NUMERIC STRING ::= <i>the-code-for-transcriptionist-role</i> ,
	codeDataFreeText DirectoryString ::= <i>optional-data</i> }
	regionalHCData Sequence of RegionalData ::= {
	type OBJECT IDENTIFIER ::= OID-for-this-regional-encoding,
	country PrintableString (SIZE (2) ::= ISO-country-code-for-USA,
	issuingAuthority DirectoryString ::= (C=US,

OU= American Association of Medical Transcriptionists),
nameAsIssued DirectoryString ::= (CN= Elizabeth Smith)
hcMajorClassCode CodedData ::= {
 codingSchemeReference OBJECT IDENTIFIER ::= ASTM-Coding-Scheme-for-Type,
 codeDataValue NUMERIC STRING ::= ASTM-Type-OID-for-transcriptionist}
 codeDataFreeText UTF8String ::= "license number 1234567"} }

A.4 EXAMPLE 3: Regulated health professional certificate profile

NOTE The following example is for illustrative purposes only and is not intended to state the future format of health certificates issued in the State of California.

John Stuart Woolley aka Tink Woolley; license issued by State of California Medical License Board, license number 20A4073, license status code 17 ('01' is 'active and current'), issue date 22 March 2000 — expiration date 21 March 2002.

Version (2 – decimal code for version 3 certificates)
SerialNumber (unique number)
Signature (sha-1WithRSAEncryption {1,2,840,113549,1,1,5})
Issuer

countryName	(US=United States of America)
localityName	(California)
organizationName	(Name-of-CA-for-California-Health-Care)
commonName	(Name-of-CA-for-California-Health-Care)

Validity
Subject

countryName	(US=United States of America)
localityName	(California)
organizationName	(CertHolderOrganization)
commonName	(Woolley, Tink)
surname	(Woolley)
givenName	(John Stuart)

subjectPublicKeyInfo

algorithm	(public RSA key, 1024 bit {1,2,840,113549,1,1,1})
subjectPublicKey	(Subject's PUBLIC KEY)

Extensions

authorityKeyIdentifier	(unique identifier of CA public key)
subjectKeyIdentifier	(unique identifier of subject public key)
keyUsage	(digitalSignature or non-repudiation or keyEncipherment)
certificatePolicies	(appropriate policy OID)
cRLDistributionPoints	(CRL X.500 entry location)

subjectDirectoryAttributes

(**hcRole** OBJECT IDENTIFIER ::= id-hcpki-at-healthcareactor
hcActorData SET OF {
 codedData CodedData ::= {
 codingSchemeReference OBJECT IDENTIFIER ::= id-hcpki,
 codeDataValue NUMERIC STRING ::= the-code-for-physician-role,
 codeDataFreeText DirectoryString ::= optional-data}
 regionalHCDData Sequence of RegionalData ::= {
 type OBJECT IDENTIFIER ::= OID-for-this-regional-encoding,
 country PrintableString (SIZE (2)) ::= ISO-country-code-for-USA,
 issuingAuthority DirectoryString ::= (C=US, L=CA, OU=California Medical License Board),
 nameAsIssued DirectoryString ::= (CN= John Stuart Woolley)
 hcMajorClassCode CodedData ::= {
 codingSchemeReference OBJECT IDENTIFIER ::= ASTM-Coding-Scheme-for-Type-OID,
 codeDataValue NUMERIC STRING ::= ASTM-Type-OID-for-physician}
 codeDataFreeText UTF8String ::= "license number 20A4073"
 hcMinorClassCode CodedData ::= {
 codingSchemeReference OBJECT IDENTIFIER ::= ASTM-Coding-Scheme-for-License-Status-OID,
 codeDataValue NUMERIC STRING ::= 0 (unrestricted)
 codeDataFreeText UTF8String ::= "unrestricted"} }

Note that, in this example, a license number and license status have been encoded as regional data. Such regional data is optional, and the decision to include or exclude such regional data is left up to the issuing CA.

A.5 EXAMPLE 4: Sponsored healthcare provider certificate profile

NOTE The following example is for illustrative purposes only and is not intended to state the future format of health certificates issued in the Province of Ontario, Canada.

Julie LeClerk, midwife in the province of Ontario.

Version	(2 – decimal code for version 3 certificates)
SerialNumber	(unique number)
Signature	(sha-1WithRSAEncryption {1,2,840,113549,1,1,5})
Issuer	countryName (CA=Canada) localityName (Ontario) organizationName (Name-of-CA-for-Ontario-Health-Care) commonName (Name-of-CA-for-Ontario-Health-Care) (validity period coded as UTCTime)
Validity	
Subject	countryName (CA=Canada) localityName (Ontario) organizationName (CertHolderOrganization) commonName (LeClerk, Julie) surname (LeClerk) givenName (Julie)
subjectPublicKeyInfo	
algorithm	(public RSA key, 1024 bit {1,2,840,113549,1,1,1})
subjectPublicKey	(Subject's PUBLIC KEY)
Extensions	
authorityKeyIdentifier	(unique identifier of CA public key)
subjectKeyIdentifier	(unique identifier of subject public key)
keyUsage	(digitalSignature or non-repudiation or keyEncipherment)
certificatePolicies	(appropriate policy OID)
cRLDistributionPoints	(CRL X.500 entry location)
subjectDirectoryAttributes	(hcRole OBJECT IDENTIFIER ::= id-hcpki-at-healthcareactor hcActorData SET OF { codedData CodedData ::= { codingSchemeReference OBJECT IDENTIFIER ::= <i>id-hcpki</i> , codeDataValue NUMERIC STRING ::= <i>the-code-for-midwife-role</i> , codeDataFreeText DirectoryString ::= <i>optional-data</i> } regionalHCData Sequence of RegionalData ::= { type OBJECT IDENTIFIER ::= <i>OID-for-this-regional-encoding</i> , country PrintableString (SIZE (2) ::= <i>ISO-country-code-for-Canada</i> , issuingAuthority DirectoryString ::= (C=CA, OU= <i>Name-of-CA-for-Ontario-Health-Care</i>), hcMajorClassCode CodedData ::= { codingSchemeReference OBJECT IDENTIFIER ::= <i>ISO-Role-Coding-Scheme</i> , codeDataValue NUMERIC STRING ::= <i>the-code-for-midwife-role</i> } codeDataFreeText UTF8String ::= <i>"optional printable data"</i> }) }

A.6 EXAMPLE 5: Supporting organization employee certificate profile

NOTE The following example is for illustrative purposes only and is not intended to state the future format of health certificates issued in the State of California.

Sally R Jones, administrative billing clerk, employed by American Health Systems

Version	(2 – decimal code for version 3 certificates)
SerialNumber	(unique number)
Signature	(sha-1WithRSAEncryption {1,2,840,113549,1,1,5})