ISO/TC 215/WG 4
Health Informatics/Security

Reference number of working document: **ISO/TC 215/WG4/N83**

Date: 2001-03-05

Reference number of document: **ISO/DTS 17090-2**

Committee identification: ISO/TC 215

Secretariat: ANSI

Health Informatics – Public Key Infrastructure - Part 2: Certificate profile

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 2: Certificate profile

1 Scope

This part two of a three-part document focuses on specifying the certificate profiles required to interchange health care information within a single organisation, between organisations and across jurisdictional boundaries.

It contains a set of terms and definitions common to each part of this Technical Specification.. Part 2 of this specification takes RFC2459: *Internet X.509 Public Key Infrastructure Certificate and CRL Profile* as a starting point and adds detail to that specification to make it applicable in the health industry.

The specification details the use made of Public Key Infrastructure digital certificates in the health industry and focuses in particular, on the health care specific issues relating to Certificate Profiles

A set of Certificate Profiles applicable for health care are then identified and described using a set of tables to detail and compare profile requirements by certificate type. The profiles have additional content defined to support the needs of the different health care actors described in Part 1.

The tables specify the data items contained in each certificates and whether they are mandatory or optional, providing a contextual overview of how each Certificate profile relates to the others. The specification then goes on to provide Certificate Profile examples for each of the Certificate types defined.

The Technical Specification should be approached as a whole, with the three parts all making a contribution to defining how public key infrastructures 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.

Part 1 covers the basic concepts by defining a Health Industry Public Key Infrastructure (PKI), defining the concepts and stating the purpose of the specification. It describes the needed security services and references other standards and documents.

Part 3: "Policy management of certification authority" deals with 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 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 health care security policy for cross border communication. It also defines the minimum levels of security required, concentrating on the 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 ecipient 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 Health Care Certificate Profiles

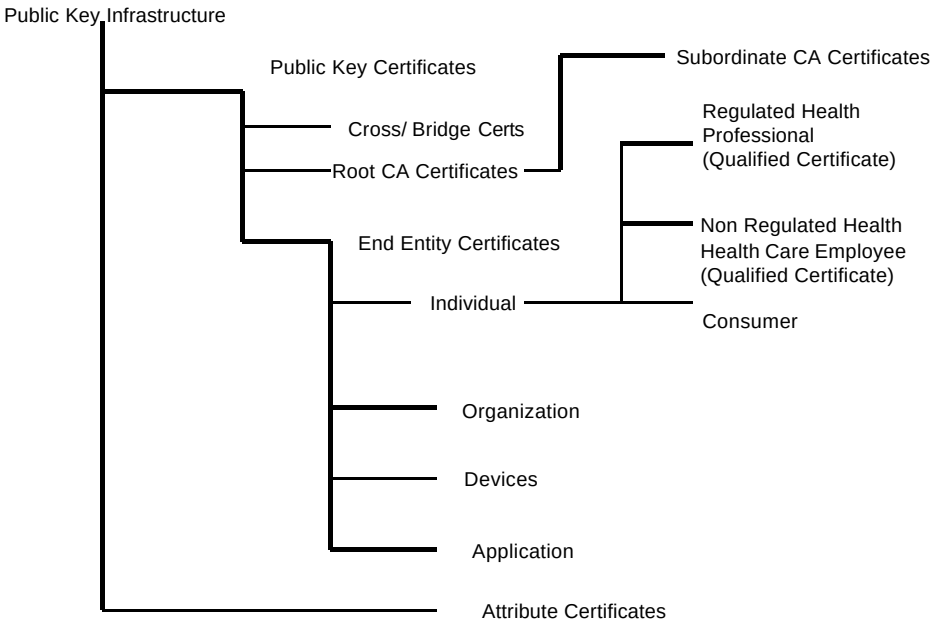
5.1 Certificate Types Required for Health Care

This technical specification supports the issuance of identity certificates to:

1. Individuals (regulated health professionals, health care non-regulated employees, sponsored health care providers, supporting organisation employees and patients/ consumers;
2. Organisations (health care organisations and supporting organisations)
3. Devices; and
4. Applications

The specification also allows for the roles of health professionals and organisations to be captured; either in the identity certificate itself (in a certificate extension) or in an associated attribute certificate. The different kinds of certificates and how they relate to each other are shown in Figure 1 below:

Figure 1 – Health Care Certificate Types



5.2 Certification Authority Certificates

5.2.1 Root Certification Authority Certificates

These are certificates used when the subject of the Certificate is itself a Certification Authority. CA Certificates are self-signed. The Basic Constraints Field indicates whether the Certificate is a CA and it also indicates the maximum allowable depth of a certification path through that CA. They are used in a health care PKI to issue certificates to relying parties, including subordinate Certification Authorities.

5.2.2 Subordinate Certification Authority Certificates

These are certificates 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.

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 this technical specification provides for “islands of trust” in each health industry domain, based on specialty, 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 standard to be embodied in their Policies and associated practice statements. When this occurs a relying party may accept a certificate from a CA outside their own domain. This could be particularly useful for organisations like state or provincial health authorities to allow 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 e-mail and others required in the health industry.

5.4 End Entity Certificates

End Entity Certificates are issued to entities that may include individuals, organisations, 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. This specification introduces three types of individual identity certificates. These are:

a) Regulated Health Professional Identity Certificate

Each certificate holder is a health professional who, in order to practice their profession requires a license or registration from a government body [see Part 1, Section 5.1]. These certificates may be qualified certificates [see Section 8.2]

B) NON REGULATED HEALTH PROFESSIONAL IDENTIFY CERTIFICATE

Each certificate holder is a health employee who is not subject to registration or licensing from a government body [see Part 1, Section 5.1]. These certificates may be qualified certificates.

C) Sponsored Health Care Provider Identity Certificate

Each certificate holder is an individual who is active in his/her health care community and is sponsored by a regulated health care organization or professional. These certificates may be qualified certificates.

D) Supporting Organisation Employee Identity Certificate

Each certificate holder is an individual who is active in his/ her community and is sponsored by a regulated health care organization or professional. These certificates may be qualified certificates.

E) Patient/ Consumer Identity Certificate

Each certificate holder is an individual person who at some stage is about to receive, is receivi ng 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 organisation that is involved in the health industry may hold a certificate to identify itself or to use for encryption purposes. As in IETF, RFC2527 provision is made in this technical specification for organisational 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 specification concentrates on the providers but recognizes that patients/ consumers will increasingly require the services of a PKI in managing their own health care.

5.4.5 Attribute Certificate

An Attribute Certificate (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 access control information associated with the AC owner. The IETF Attribute Certificate Internet Draft specifies the AC in detail.

Within the health industry context attribute certificates can fulfil the valuable role of communicating authorisation information. Authorisation information is distinct from information on health-care roles or licences, which may be appropriately included in a PKC. Role or licence implies an authorisation level, but they are not necessarily authorisation information in themselves.

The syntax of an attribute certificate 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          UniqueIdentifier OPTIONAL,
        extensions              Extensions OPTIONAL }

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

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

CertificateSerialNumber ::= INTEGER

UniqueIdentifier ::= 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 attribute certificate are used as follows:

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

The **owner** field conveys the identity of the attribute certificate's owner. Use of the issuer name and serial number of a specific public key certificate 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 owner, 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 attribute certificate. Also, some of the options in **GeneralNames** (e.g. **IPAddress**) are inappropriate for use in naming an attribute certificate owner which is a role rather than an individual entity. General name forms should be restricted to distinguished name, RFC 822 (email) address, and (for role names) object identifiers.

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

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

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

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

The **attributes** field contains the attributes associated with the owner which are being certified (e.g. the privileges).

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

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

Refer to ISO/DTS 17090-Part 1, Section 8.3 for a detailed discussion on the use of Attribute Certificates in health care.

5.4.6 Role Certificates

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

Many environments which 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:

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

An entity is assigned an attribute certificate containing an attribute asserting that the entity occupies a certain role. That certificate has an extension pointing to another attribute certificate which defines the role (i.e., this role certificate specifies the role as owner 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 will apply for all certificates specified in this document::

1 Certificates SHALL be X.509 version 3 certificates.

2 Certificates SHALL be compliant with *RFC 2459* . Deviations from RFC2459 are only allowed if they are aligned with proposed solutions to known problems with *RFC2459*.

3 Individual Identity It is RECOMMENDED that Certificates according to this section be compliant with the *IETF/RFC 3039 Qualified Certificates Profile*. It is RECOMMENDED that Deviations only be allowed if they are aligned with proposed solutions to known problems.

4 The signature field SHALL identify the signature algorithms used

5 The certified public key SHALL have a minimum key-length field depending on the algorithm used. Refer to Part 3, Section 6 for specification of key sizes

6 Digital certificates SHALL NOT be issued for the purposes of non-repudiation and digital signature. Also digital signatures SHALL NOT be used for the purpose of encipherment. See Section 7.1 - General Extensions, for the Key Usage .Extension

The common elements in all Health Care PKI Certificates identified above in Figure1 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. I 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.

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

(In agreement with RFC2459, this technical specification RECOMMENDS this field not be used)

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

(In agreement with RFC2459, this technical specification RECOMMENDS this field not be used)

9 **extensions** - a SEQUENCE of one or more extensions SHALL be present.

10 **timeformat**

The Distinguished Encoding Rules (DER) allow several methods for formatting UTCTime and GeneralizedTime. It is important that all implementations use the same format to minimise signature verification problems. Where the year is greater or equal to 2050 the time SHALL be encoded using GeneralizedTime. To ensure that UTCTimes are consistently format it is RECOMMENDED that UTCTime be encoded using the “Z” format and that the seconds field shall not be omitted, even if it is 00 (i.e., the format shall be YYYYMMDDHMMSSZ). 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. It is RECOMMENDED that when GeneralizedTime is used it be encoded in the “Z” format and that the seconds field be included (i.e. the format should be YYYYMMDDHHMMSSZ).

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 Certificate fields and related information

This section contains specific requirements for information content in basic certificate fields, which are not already specified by RFC 2459 or draft-ietf-pkix-qc-02.

6.3.1 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)

6.3.2 Validity

Refer to RFC2459 for validity dates. This Technical Specification has adopted reasonable constraints for Health Certificate Validity Periods . Refer to ISO/DTS 17090 - Part 3, Policy Validity Period Section 6.1

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

6.3.2 Subject public key info

The algorithm identifier SHALL be identified eg.

1. RSA

kcs-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

6.3.3 Issuer name field

The issuer name, stored in the issuer 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.

See Section 6.4 below for a detailed specification on what the Issuer Name field SHALL contain for each certificate type.

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

Example: *countryName* = “US”

This field is **MANDATORY** as it is critical in the health care 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 inform 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* , which refers to the name of the sponsoring health care organisation in the case of End Entities and the organisation name of the CA in the case of CA Certificates, the field 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”

6.3.4 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 health care professionals will be reflected in the Certificate Extension - HCRole field

Refer to Section 6.4 below for a detailed specification on what the Subject Name field SHALL contain for each certificate type.

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

Example: *countryName* = “US”

It is RECOMMENDED that the population of this field reflect the particular country’s practice.

This field is MANDATORY for CAs, Health Professionals and Organisations as it is critical in the health care field to know the country of origin of a 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 the country a request has originated from will inform any decision on whether to grant it.

2. ***localityName*****:** *localityName* atmay be used to store at least one locality name value. The specification will specify use of two levels of locality name where the top level specifies 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* , which refers to the name of the sponsoring health care organisation in the case of End Entities and the organisation name of the CA in the Case of CA Certificates, the field 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. It SHALL clearly identify the subject as they are known within the health care system.

Example: *commonName* = “Bruce Wayne”

This field is MANDATORY for persons and organisations 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 they are known within the health care 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 they are known within the health care system.

Example: *givenName* = “Bruce”

8. ***e-mail:*** the primary RECOMMENDED usage of this field is to record the subject’s email address.

Example: *serialNumber* = “jsmith@network.com.au”

6.4 Issuer Field Requirements for each Health Care Certificate Type

Certificate Elements	CA Certificates		Identity Certificates						Attribute Certificate
	Certification Authority Certificate	Bridge Certificate	Regulated Health Professional Certificate	Non Regulated Health Care Employee Certificate **	Consumer Certificate	Organization Certificate	Devices Certificate	Applications Certificate	
Issuer Fields									
CountryName	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Optional
LocalityName	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional
Organization_Name	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Optional
Organizational_UnitName	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional
CommonName	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Not Applicable

Footnote: Table refers to Subject ID and Issuer ID that may vary between Certificate Types.

** The values for Non-Regulated Health Care Employee Certificate also apply to *Sponsored Health Care Provider* Certificates and *Supporting Health Care Employee* Certificates

6.5 Subject Field Requirements Requirements for each Health Care Certificate Type (Continued)

Certificate Elements	CA Certificates		Identity Certificates						Attribute Certificate
	Certification Authority Certificate	Cross Bridge	Regulated Health Professional Certificate	Non Regulated Health Professional Certificate **	Consumer Certificate	Organization Certificate	Device Certificate	Application Certificate	
SUBJECT Fields									
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
e-mail	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional

Footnote: Table refers to Subject ID and Issuer ID that may vary between Certificate Types.
** The values for Non-Regulated Health Care Employee Certificate also apply to *Sponsored Health Care Provider Certificates* and *Supporting Health Care Employee Certificates*

7 Use of Certificate Extensions

This section provides requirements that implementations SHALL have of certificate extensions in X.509 version 3 certificates for a health care PKI. More detailed information about the extensions listed in this section can be found in RFC2459 and RFC3039.

7.1 General Extensions

7.1.1 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 **mandatory** and **non-critical** extension.

7.1.2 subjectKeyIdentifier

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

RFC2459 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.

7.1.3 keyUsage

This extension SHALL identify the basic key usage associated with the public key in the certificate. As this technical specification disparages the use of single key pairs for both encipherment and digital signature, each certificate SHALL NOT specify a key usage of dataEncipherment together with a key usage of digitalSignature or nonRepudiation.

This extension SHALL be mandatory. It is RECOMMENDED (as in IETF RFC 2459) that this extension be **critical**.

7.1.4 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.

7.1.5 certificatePolicies

The certificatepolicies extension SHALL contain an objectidentifier of a standardised Certificate CA-policy as specified in Part 3 of this Technical Specification.

This is a **mandatory** and **non-critical** extension.

7.1.6 subjectAltName

Replace text with:

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.

7.1.7 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 Health Care Employee, Sponsored Health Care, Supporting Health Care Employee, Consumer, Organization, Application and Devices Certificates) SHALL NOT include this extension.

7.1.8 CRLDistributionPoints

It is RECOMMENDED that this extension be present in all Certificates. The extension SHALL identify the location of the associated CRL (or ARL for CA certificates) in the PKI directory.

This is a **mandatory** and **non-critical** extension.

7.1.9 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**.

7.1.10 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**

7.2 Special Subject Directory Attributes

7.2.1 HcRole Attribute

The *hcRole* attribute allows the encoding of regulated and non-regulated health care professional role data, and it is RECOMMENDED that if implemented, provide international interoperability in certification of health care 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 health care role coding schemes.

This field is required in an identity certificate as verifying a health care actor's identity is likely to require information about the specialty or role that actor fulfils. Information about whether an actor is a Surgeon as well as a Physician is also less subject to change over time and is therefore appropriate to place in an identity certificate. It remains the recommendation of this Technical Specification that information to support authorisation and access control decisions is more appropriately placed on Attribute Certificates.

```
hcRole ATTRIBUTE    ::=     {
            WITH SYNTAX             HCactorData
        EQUALITY MATCHING RULE  hCactorMatch
        SUBSTRINGS MATCHING RULE        hCactorSubstringsMatch
        ID                              id-at-th2-healthcareactor }
```

Preliminary object identifiers:

```
id-th2                          OBJECT IDENTIFIER ::= 1.2.826.0.1.3344810.3
id-th2-at                               OBJECT IDENTIFIER ::= {id-th2 0 }
id-at-th2-healthcareactor       OBJECT IDENTIFIER ::= {id-th2-at 1}
id-th2-cd                       OBJECT IDENTIFIER ::= {id-th2 1 }
```

Definition of data types:

```
HCActordata     ::= CLASSIFICATIONSCHEME

HcProfessions   ::= SEQUENCE {
codedData                       [0] CodedData OPTIONAL,
REGIONALHcProfessionalData      [1] SEQUENCE OF REGIONALData OPTIONAL }

REGIONALData            ::= SEQUENCE {
        type            REGIONALDATA.& id,
        value   REGIONALDATA.&Type}

CodedData       ::= SET {
codingSchemeReference       [0] OBJECT IDENTIFIER,
----- Contains the ISO coding scheme Reference or local coding scheme reference
---- achieving ISO registration) will be OID id-th2
---- at least ONE of the following SHALL be present

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

REGIONAL-DATA   ::=   CLASS {
        &Type,
        &id     OBJECT IDENTIFIER UNIQUE }
WITH SYNTAX {
        WITH SYNTAX  &Type
        ID                      &id }

coded           ::= REGIONAL-DATA {
        WITH SYNTAX  CodedREGIONALData
        ID                      id-th2-cd }

CodedREGIONALData  ::= SEQUENCE {
country         [0] PrintableString (SIZE (2)),
----- ISO3166 code of country of issuing authority.
professionalIssuingAuthority    [1] DirectoryString,
----- Identifier of issuing authority as Regional Entity. Could be implemented
----- as a true identifier or a Directory lookup string (to be determined)
HCareMajorClassCode [2] CodedData,
HCareMinorClassCode             [3] CodedData OPTIONAL
```

Codes to be used the field **eg.** 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**

7.2.2 subjectDirectoryAttributes

It is RECOMMENDED that this extension be present in individual identity certificates. In such certificates it MAY contain a hcRole attribute (see Section 7.2.1) and may contain a qcStatement attribute (see Section 7.2). 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·

7.3 Qualified certificate statements extension

It is RECOMMENDED that certificates for health professionals and for non-regulated health care providers contain a qcStatement subject directory attribute. Certificates for patients/ consumers, for sponsored health care 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.

Refer to the IETF RFC 3039 Internet X.509 Public Key Infrastructure Qualified Certificates Profile for the detailed specification.

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

The extension is **optional** and **non-critical**.

.

7.4 Extension Field Requirements for each Health Industry Certificate Type

Certificate Elements	CA Certificates		Identity Certificates						Attribute Certificate
	Certification Authority Certificate	Cross Certificate	Regulated Health Professional Certificate	Non Regulated Health Professional Certificate	Consumer Certificate	Organization Certificate	Device Certificate	Application Certificate	
Standard Extensions									
authorityKeyIdentifier	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Optional
subjectKeyIdentifier	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Optional
keyUsage	Mandatory	Mandatory	Mandatory	**Mandatory**	Mandatory	Mandatory	Mandatory	Mandatory	Optional
privateKeyUsagePeriod	Absent	Absent	Absent	**Absent**	Absent	Absent	Absent	Absent	Optional
certificatePolicies	Mandatory	Mandatory	Mandatory	**Mandatory**	Mandatory	Mandatory	Mandatory	Mandatory	Optional
subjectAltName	Absent	Absent	Optional	Optional	Optional	Optional	Optional	Optional	Optional

subjectDirectoryAttributes	Absent	Absent	Mandatory	**Mandatory**	Optional	Absent	Absent	Absent	Optional
basicConstraints	Mandatory & Critical	Mandatory & Critical	Absent	**Absent**	Absent	Absent	Absent	Absent	Optional
CRLDistributionPoints	Mandatory	Mandatory	Mandatory	**Mandatory**	Mandatory	Mandatory	Mandatory	Mandatory	Optional
ExtKeyUsage	Optional	Optional	Absent	**Absent**	Absent	Absent	Absent	Absent	Optional
Private extensions									Optional
Authority Information Access	Optional	Optional	Optional	**Optional**	Optional	Optional	Optional	Optional	Optional
qcStatements extension	Absent	Absent	Mandatory	**Mandatory**	Optional	Absent	Absent	Absent	Optional

Hcrole	Absent	Absent	Mandatory	Mandatory	**Optional**	Absent	Absent	Absent	Absent

Footnote: Table refers to Subject ID and Issuer ID that may vary between Certificate Types.

Annex A. (informative) Certificate Profile Examples

Some basic examples of each type of Certificate are detailed below for information:

A.1 EXAMPLE 1 Non-Regulated Health Care Employee Certificate Profile

Version	(3)	
SerialNumber	(unique number)	
Signature	(sha-1WithRSAEncryption {1,2,840,113549,1,1,5})	
Issuer		
	countryName	(US=United States of America)
	localityName	(Ex.= California)
	organizationName	(Ex California Health Authority)
	commonName	(Ex.CA Health Care PKI US / policy v01)
Validity		(validity period coded as UTCTime)
Subject		
	countryName	(US=United States of America)
	localityName	(Ex. .= California)
	organizationName	(Ex Midtown Hospital)
	commonName	(Ex. John Citizen)
	surname	(Ex Citizen)
	givenName	(Ex. John)
subjectPublicKeyInfo	(public RSA key, 1024 bit {1,2,840,113549,1,1,1})	
Extensions		
	authorityKeyIdentifier	(unique identifier of CA public key)
	subjectKeyIdentifier	(unique identifier of subject public key)
	keyUsage	(digitalSignature | non-repudiation | keyEncpherment)
	certificatePolicies	(appropriate policy OID)
	cRLDistriburionPoints	(CRL X.500 entry location)
j	**hcRole**	(bookings clerk)

A.2 EXAMPLE 2 Consumer Certificate Profile

Version (3)

SerialNumber (unique number)

Signature (sha-1WithRSAEncryption {1,2,840,113549,1,1,5})

Issuer

	countryName	(US=United States of America)
	localityName	(Ex.= California)
	commonName	(Ex.CA Health Care PKI US / policy v01)

Validity (validity period coded as UTCTime)

Subject

	countryName	(US=United States of America)
	localityName	(Ex. .= California)
	organizationName	(Ex Midtown Hospital)
	commonName	(Ex. John Citizen)
	surname	(Ex Citizen)
	givenName	(Ex. John)

subjectPublicKeyInfo (public RSA key, 1024 bit {1,2,840,113549,1,1,1})

Extensions

	authorityKeyIdentifier	(unique identifier of CA public key)
	subjectKeyIdentifier	(unique identifier of subject public key)
	keyUsage	(digitalSignature | non-repudiation | keyEncpherment)
	certificatePolicies	(appropriate policy OID)
	cRLDistriburionPoints	(CRL X.500 entry location)
j	**hcRole**	(dialysis)

A.3 EXAMPLE 3 Regulated Health Professional Certificate Profile

Version (3)

SerialNumber (unique number)

Signature (sha-1WithRSAEncryption {1,2,840,113549,1,1,5})

Issuer

countryName	(US=United States of America)
localityName	(Ex.= California)
organizationName	(Ex California Health Authority)
commonName	(Ex.CA Health Care PKI US / policy v01)

Validity (validity period coded as UTCTime)

Subject

countryName	(US=United States of America)
localityName	(Ex. .= California)
organizationName	(Ex Midtown Hospital)
commonName	(Van der Lay, Art)
surname	(Van der Lay)
givenName	(Art)

subjectPublicKeyInfo (public RSA key, 1024 bit {1,2,840,113549,1,1,1})

Extensions

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

A.4 EXAMPLE 4 Organization Certificate Profile

Version (3)

SerialNumber (unique number)

Signature (sha-1WithRSAEncryption {1,2,840,113549,1,1,5})

Issuer

countryName (US=United States of America)

localityName (Ex.= California)

organizationName (Ex California Hospital Authority)

commonName (Ex. Health PKI / policy v01)

Validity (validity period coded as UTCTime)

Subject

countryName (US = United States of America)

localityName (Ex. Region = California)

organizationName (Ex Midtown Hospital)

subjectPublicKeyInfo (public RSA key, 1024 bit {1,2,840,113549,1,1,1})

Extensions

authorityKeyIdentifier (unique identifier of CA public key)

subjectKeyIdentifier (unique identifier of subject public key)

keyUsage (digitalSignature | non-repudiation | keyEncpherment)

certificatePolicies (appropriate policy OID)

cRLDistriburionPoints (CRL X.500 entry location)

A.5 EXAMPLE 5 Attribute Certificate Profile

Version (3)

SerialNumber (unique number)

Signature (sha-1WithRSAEncryption {1,2,840,113549,1,1,5})

baseCertificateID 339393322281

entityName Dr Benjamin Casey

Optional

AttCertValidity Period

Attributes Surgeryrecordaccess,

Issuer

countryName (US= United States of America)

localityName (Ex California)

organizationName (Ex California Hospital Authority)

commonName (Ex. CA - / policy v01)

Validity (validity period coded as UTCTime)

Subject

countryName (US= United States of America)

localityName (Ex. Region = California)

organizationName (Ex Midtown Hospital)

commonName (Ex. Midtown Secure Server 01)

subjectPublicKeyInfo (public RSA key, 1024 bit {1,2,840,113549,1,1,1})

Extensions

authorityKeyIdentifier (unique identifier of CA public key)

subjectKeyIdentifier (unique identifier of subject public key)

keyUsage (digitalSignature | non-repudiation | keyEncpherment)

certificatePolicies (appropriate policy OID)

cRLDistriburionPoints (CRL X.500 entry location)

A.6 EXAMPLE 6 CA Certificate Profile

Version (3)

SerialNumber (unique number)

Signature (sha-1WithRSAEncryption {1,2,840,113549,1,1,5})

Issuer

countryName	(US=United States of America)
localityName	(Ex. Region California)
organizationName	(Ex California Hospitals Authority)
commonName	(Ex. CA – Health PKI US-CT/ policy v01)

Validity (validity period coded as UTCTime)

Subject

countryName	(US=United States of America)
localityName	(Ex. Region California)
organizationName	(Ex El Cerrito Health Authority)
commonName	(Ex. CalifHA PKI US CT/ policy V.03)

subjectPublicKeyInfo (public RSA key, 1024 bit {1,2,840,113549,1,1,1})

Extensions

authorityKeyIdentifier	(unique identifier of CA public key)
subjectKeyIdentifier	(unique identifier of subject public key)
keyUsage	(CRL and certificate signing)
certificatePolicies	(appropriate policy OID)
basicConstraints	(CA = true)
cRLDistriburionPoints	(CRL X.500 entry location)

A.7 EXAMPLE 7 Bridge Certificate Profile

Version (3)

SerialNumber (unique number)

Signature (sha-1WithRSAEncryption {1,2,840,113549,1,1,5})

Issuer

countryName	(US=United States of America)
localityName	(Ex. Region California)
organizationName	(Ex California Hospitals Authority)
commonName	(Ex. CA – Health PKI US-CT/ policy v01)

Validity (validity period coded as UTCTime)

Subject

countryName	(US=United States of America)
localityName	(Ex. Region Washington)
organizationName	(Ex Washington Health Authority)
commonName	(Ex. CalifHA PKI US CT/ policy V.03)

subjectPublicKeyInfo (public RSA key, 1024 bit {1,2,840,113549,1,1,1})

Extensions

authorityKeyIdentifier	(unique identifier of CA public key)
subjectKeyIdentifier	(unique identifier of subject public key)
keyUsage	(CRL and certificate signing)
certificatePolicies	(appropriate policy OID)
basicConstraints	(CA = true)
cRLDistriburionPoints	(CRL X.500 entry location)

Annex B (Informative) Bibliography

Rich Ankney, CertCo, Privilege Management Infrastructure, v 0.4, 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.