BS ISO 17090-2:2015

BSI Standards Publication

Health informatics — Public key infrastructure

Part 2: Certificate profile

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of ISO 17090-2:2015. It supersedes BS ISO 17090-2:2008 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/35, Health informatics.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2015.
Published by BSI Standards Limited 2015

ISBN 978 0 580 81170 8

ICS 35.240.80

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2015.

Amendments/corrigenda issued since publication

Date	Text affected

BS ISO 17090-2:2015

INTERNATIONAL STANDARD

ISO 17090-2

Second edition
2015-11-15

Health informatics — Public key infrastructure —

Part 2: Certificate profile

Informatique de santé — Infrastructure de clé publique —

Partie 2: Profil de certificat

Reference number
ISO 17090-2:2015(E)

© ISO 2015

COPYRIGHT PROTECTED DOCUMENT

© ISO 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

© ISO 2015 – All rights reserved

© ISO 2015 – All rights reserved

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

The committee responsible for this document is ISO/TC 215, *Health informatics*.

This second edition cancels and replaces the first edition (ISO 17090-2:2008), which has been technically revised.

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

— *Part 1: Overview of digital certificate services*

— *Part 2: Certificate profile*

— *Part 3: Policy management of certification authority*

— *Part 4: Digital Signatures for healthcare documents*

The following document is under preparation:

— *Part 5: Authentication using Healthcare PKI credentials*

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

© ISO 2015 – All rights reserved

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.

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

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

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

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

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

This International Standard describes the common technical, operational and policy requirements that need to be addressed to enable digital certificates to be used in protecting the exchange of healthcare information within a single domain, between domains and across jurisdictional boundaries. Its purpose is to create a platform for global interoperability. It specifically supports digital certificate enabled communication across borders, but could also provide guidance for national or regional deployment of digital certificates in healthcare. The Internet is increasingly used as the vehicle of choice to support the movement of healthcare data between healthcare organizations and is the only realistic choice for cross-border communication in this sector.

© ISO 2015 – All rights reserved

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

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

ISO 17090-2 provides healthcare specific profiles of digital certificates based on the International Standard X.509 and the profile of this specified in IETF/RFC 5280 for different types of certificates.

ISO 17090-3 deals with management issues involved in implementing and using digital certificates in healthcare. It defines a structure and minimum requirements for certificate policies (CPs) and a structure for associated certification practice statements. This part is based on the recommendations of the IETF/RFC 3647 *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 International Standard, as well as comments, suggestions and information on the application of these standards may be forwarded to the ISO/TC 215 Secretariat: Lisa.Spellman@ahima.org or WG4 PKI project leader Ross Fraser at RossFraser@SextantSoftware.com.

© ISO 2015 – All rights reserved

INTERNATIONAL STANDARD **ISO 17090-2:2015(E)**

Health informatics — Public key infrastructure —

Part 2: Certificate profile

1 Scope

This part of ISO 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 digital certificates in the health industry and focuses, in particular, on specific healthcare issues relating to certificate profiles.

2 Normative references

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

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

ISO 17090-3:2008, *Health informatics — Public key infrastructure — Part 3: Policy management of certification authority*

IETF/RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

3 Terms and definitions

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

4 Abbreviated terms

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

© ISO 2015 – All rights reserved

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 to issue certificates to relying parties, including subordinate CAs. The basic constraints field indicates whether the certificate is a CA. The Root CA certificate is used to establish a chain of trust by Internet browsers and other applications that rely on PKI for entity identification and authentication.

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. The Subordinate CA certificate is used, along with other certificates, to establish a chain of trust by Internet browsers and other applications that rely on PKI for entity identification and authentication.

© ISO 2015 – All rights reserved

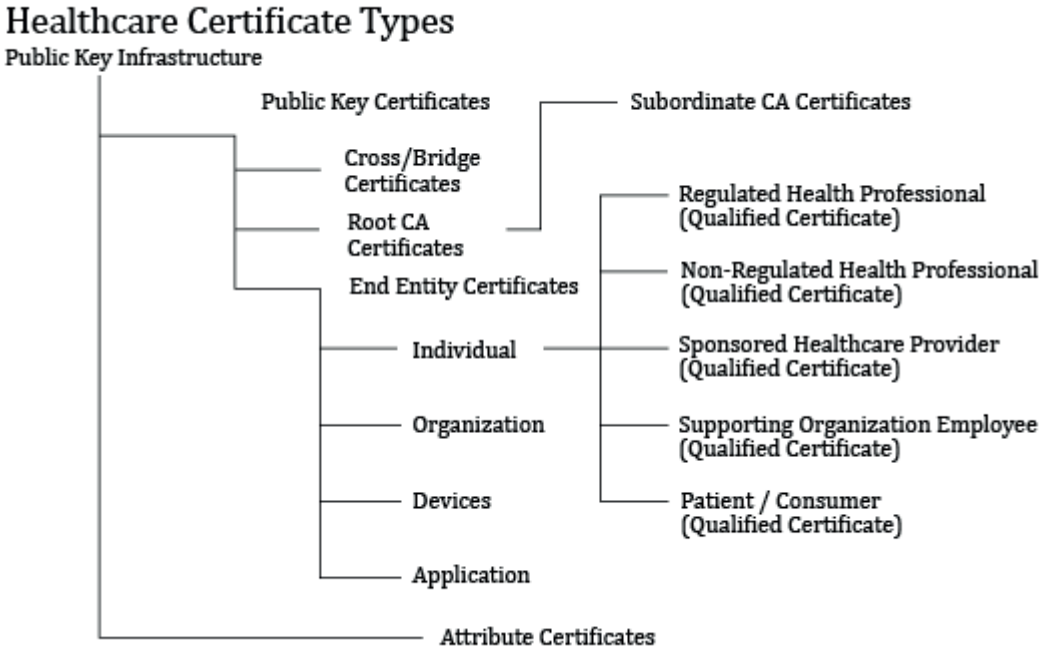

Figure 1 — Healthcare certificate types

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 (ISO 17090-1:2013, 5.1); these certificates may be qualified certificates (7.3 and ISO 17090-1:2013, 8.2);

© ISO 2015 – All rights reserved

b) non-regulated health professional:

— each certificate holder is a health professional who is not subject to registration or licensing from a government body (ISO 17090-1:2013, 5.1); 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 person employed by a healthcare organization or a supporting organization. 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 3647, provision is made in this part of ISO 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 17090 concentrates on the providers, but recognizes that patients/consumers will increasingly require the security services that digital certificates can provide 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 IETF/RFC 5755, An Internet Attribute Certificate Profile for Authorization.

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 specification still needs to be more widely implemented in the software industry.

The syntax of an AC is specified in IETF/RFC 3281, An Internet Attribute Certificate Profile for Authorization

© ISO 2015 – All rights reserved

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 ISO 17090-1:2013, 8.3.

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

© ISO 2015 – All rights reserved

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 17090.

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

b) Certificates shall be in accordance with IETF/RFC 5280. Deviations from IETF/RFC 5280 are only allowed if they are aligned with proposed solutions to known problems with IETF/RFC 5280.

c) For individual identity, certificates should be in accordance with the IETF/RFC 3739. 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 ISO 17090-3:2008, 7.6.1.5.

f) dataEncipherment key usage shall not be combined with either non-repudiation or digitalSignature key usage (see 7.2.3).

The common elements in all healthcare digital 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

© ISO 2015 – All rights reserved

a) **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).

b) **signature** contains the algorithm identifier for the algorithm used by the CA to sign the certificate.

c) **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.

d) **validity** is the time interval during which the CA warrants that information contained within the certificate is valid. For regulated health professionals, the CA shall ensure that the validity period of the certificate not exceed the validity period of the professional licence. To accomplish this, the CA shall either set the certificate validity so as not to exceed the period for the professional licence or else reliably confirm the renewal of the professional license prior to the license expiry date and revoke or suspend the certificate if the professional license has not been renewed.

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 YYMMDDHHMMSSZ). 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).

e) **subject** identifies the name of the entity associated with the public key found in the subject public key field.

f) **subjectPublicKeyInfo** is used to carry the public key and identify the algorithm with which the key is used.

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

(In accordance with RFC 5280, this International Standard recommends that this field should not be used.)

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

(In agreement with RFC 5280, this International Standard recommends that this field should not be used.)

i) **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 5280 or IETF/RFC 3279, are as follows.

© ISO 2015 – All rights reserved

6.3.2 Signature

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

a) md5WithRSAEncryption (1.2.840.113549.1.1.4)

b) sha1WithRSAEncryption (1.2.840.113549.1.1.5)

c) dsa-with-sha1 (1.2.840.10040.4.3)

d) md2WithRSAEncryption (1.2.840.113549.1.1.2)

e) ecdsa-with-SHA1 (1.2.840.10045.4.1)

f) ecdsa-with-SHA224 (1.2.840.10045.4.3.1)

g) ecdsa-with-SHA256 (1.2.840.10045.4.3.2)

h) ecdsa-with-SHA384 (1.2.840.10045.4.3.3)

i) ecdsa-with-SHA512 (1.2.840.10045.4.3.4)

j) id-RSASSA-PSS (1.2.840.113549.1.1.10).

k) sha256WthRSAEncryption 1.2.840.113549.1.1.11

l) sha384WithRSAEncryption 1.2.840.113549.1.1.12

m) sha512WithRSAEncryption 1.2.840.113549.1.1.13

NOTE MD2, MD5 and SHA1 hash algorithms [list items a) through e)] are included for backward compatibility with legacy systems. These hashing algorithms have been superannuated by newer and more robust algorithms in contemporary systems [see list items f) to m)].

6.3.3 Validity

Validity dates shall be in accordance with IETF/RFC 5280. This part of ISO 17090 has adopted reasonable constraints for health certificate validity periods as specified in ISO 17090-3:2008, 7.6.3.2.

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.

a) *RSA*

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

rsadsi(113549) pkcs(1) 1 }

rsaEncryption OBJECT IDENTIFIER:: = { pkcs-1 1}

b) 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 }

© ISO 2015 – All rights reserved

c) *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 }

d) Elliptic Curve

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

Refer to ISO 17090-3:2008, 7.6.1.5 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.

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

EXAMPLE 1 *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.

b) ***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 country 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 2 *localityName* = "California"

c) ***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 of the organization.

EXAMPLE 3 *organizationName* = "California Hospital Authority"

d) ***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 4 *organizationalUnitName* = "Midtown Hospital Radiology"

e) ***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 5 *commonName* = "Patient Health Information Policy"

© ISO 2015 – All rights reserved

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. Additional advice and guidance can be found in ISO/TS 21091 *Health Informatics – Directory Services for security, communications, and identification of professionals and patients.*

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

EXAMPLE 1 *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.

b) ***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 country. 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 2 *localityName* = "California"

c) ***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 or its registered trademark.

EXAMPLE 3 *organizationName* = "Midtown General Hospital"

d) ***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.

In some local healthcare implementations — for example, in Japan —organizational unit is used to store a healthcare role. This may also be useful in Virtual Private Network implementations, as some vendor VPN routers/firewalls can access OU and use it to apply rules to grant or restrict access. It also makes it easy for a relying party to read role information directly from the certificate. The *organizationalUnitName* field may when present, be used to store a healthcare role.

EXAMPLE 4 *organizationalUnitName* = "Midtown Hospital Radiology"

EXAMPLE 5 *organizationalUnitName* = "Licensed Physician"

e) ***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 6 *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.

© ISO 2015 – All rights reserved

f) ***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 7 *commonName* = "Wayne"

g) **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 8 *givenName* = "Bruce"

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

EXAMPLE 9 *e-mail* = "jsmith@network.com.au"

Simultaneous inclusion of the EmailAddress attribute in the subject distinguished name to support legacy implementations is deprecated by IETF RFC 5280 but permitted. This International Standard recommends that email not be used in the subject name field, but rather in the subjectAltName field.

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.

© ISO 2015 – All rights reserved

Table 1 — Issuer field requirements for each healthcare certificate type

Certificate elements	CA certificates		Identity certificates						Attribute certificate
	Certification authority certificate[b]	Cross/ Bridge certificate	Regulated health professional certificate	Non-regulated healthcare professional certificate[c]	Consumer certificate	Organization certificate	Devices certificate	Applications certificate	
Issuer fields[a]									
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_Unit Name	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional
CommonName	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Not applicable

[a] This table refers to issuer ID elements that may vary between certificate types.

[b] Certification authority certificates refer to those issuing certificates to end-entities.

[c] The values for non-regulated health professional certificates also apply to sponsored healthcare provider certificates and supporting healthcare employee certificates.

© ISO 2015 – All rights reserved

Table 2 — Subject field requirements for each healthcare certificate type

Certificate elements	CA certificates		Identity certificates						Attribute certificate
	Certification authority certificate[b]	Cross/ Bridge certificate	Regulated health professional certificate	Non-regulated healthcare professional certificate[c]	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_UnitName	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] Certification authority certificates refer to those issuing certificates to end-entities.

[c] The values for non-regulated health professional certificate also apply to sponsored healthcare provider certificates and supporting healthcare employee certificates.

© ISO 2015 – All rights reserved

7 Use of certificate extensions

7.1 General

Requirements that implementations shall have of certificate extensions in X.509 version 3 certificates for healthcare are given below. More detailed information about these extensions is given in IETF/RFC 5280 and IETF/RFC 3739.

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. If used, it is recommended that the extension be configured as mandatory.

7.2.2 subjectKeyIdentifier

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

IETF/RFC 5280 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 a single key pair for both encipherment and digital signature is discouraged and dataEncipherment key usage shall not be combined with either non-repudiation or digitalSignature key usage (see 6.1).

This extension shall be mandatory. It is recommended (as in IETF/RFC 5280) 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 17090-3.

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 this extension contain an RFC 822 e-mail address for the subscriber. If directoryName is included, it should be set to a UTF8String for the purpose of providing international character set support for a subject distinguished name.

This is an optional and non-critical extension.

© ISO 2015 – All rights reserved

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**.

See Table 3 regarding whether this extension is critical or non-critical, and optional or non-optional.

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 have this extension set to TRUE.

7.2.8 CRLDistributionPoints

IETF/RFC 5280 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 digital certificate 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 issuing CA certificate and OCSP Responders. The location of CRLs is not specified in this extension. The extension comprises 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.

7.2.11 Subject information access

The subjectInfoAccess indicates how to access access subject CA certificate and services such as time stamping.

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 ISO 17090-1:2013, 8.4.

© ISO 2015 – All rights reserved

This part of ISO 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 International Standard:

```
{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

id-hcpki-is OBJECT IDENTIFIER :: = {id-hcpki 2}
id-hcpki-is OBJECT IDENTIFIER :: = 1.0.17090.2
```

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 or national registration.
-- The ISO coding scheme OID is id-hcpki-is (defined above).
-- At least ONE of the following SHALL be present:
codeDataValue [1] UTF8String OPTIONAL,
codeDataFreeText [2] DirectoryString OPTIONAL }

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

Definition of REGIONALDATA object class:

```
REGIONALDATA     :: = CLASS {
&Type,
          &id     OBJECT 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}
```


© ISO 2015 – All rights reserved

Definition of coded information object:

```
coded      :: = REGIONAL-DATA {
     WITH SYNTAX      CodedRegionalData
                    ID      id-hcpki-cd}

CodedRegionalData      :: = SEQUENCE {
country      [0] PrintableString (SIZE (2)),
- ISO 3166 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 **HcActor** be taken from the appropriate national coding scheme.

For regulated health professional certificates and non-regulated professional certificates, this extension is mandatory and non-critical. In all other cases, 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 International Standard.

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 qcStatement attribute. The detailed specification is given in IETF/RFC 3739.

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.

© ISO 2015 – All rights reserved

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

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

[a] It is recommended that this field be mandatory.

[b] The values for non-regulated health professional certificate also apply to sponsored healthcare provider certificates and supporting healthcare employee certificates.

[c] Mandatory in those jurisdictions where the use of qualified certificates is supported by legislation.

© ISO 2015 – All rights reserved

Annex A
(informative)

Certificate profile examples

A.1 General

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 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.

BillSmith,NHSnumber368964278,Dateofcertificateissuance:1August2001,Dateofcertificateexpiration: 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)

© ISO 2015 – All rights reserved

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:: = *Policy-OID-for-Patient-Certificate-v1*

cRLDistributionPoints (http://crl.location.nhs.uk)

authorityInformationAccess (http:ocspserver.nhs.uk/OCSP_SERVER:5555)

subjectDirectoryAttributes

hcRole OBJECT IDENTIFIER:: = *id-hcpki-at-healthcareactor*

hcActorData SET OF {

codedData CodedData:: = {

codingSchemeReference OBJECT IDENTIFIER:: = *id-hcpki*,

codeDataValue UTF8String:: = *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 UTF8String:: = Type-OID-for-patient,

codeDataFreeText UTF8String:: = "patient ID 368964278"} } }

© ISO 2015 – All rights reserved

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:: = id-hcpki-at-healthcareactor

hcActorData SET OF {

codedData CodedData:: = {

© ISO 2015 – All rights reserved

codingSchemeReference OBJECT IDENTIFIER:: = *id-hcpki*,

codeDataValue UTF8String:: = *the-code-for-transcriptionist-role*,

codeDataFreeText DirectoryString:: = *optional-data}*

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 UTF8String:: = 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 (validity period coded as UTCTime)

Subject

countryName (US = United States of America)

localityName (California)

organizationName (CertHolderOrganization)

commonName (Woolley, Tink)

© ISO 2015 – All rights reserved

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 UTF8String:: = *the-code-for-physician-role*,

codeDataFreeText DirectoryString:: = *optional-data}*

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, 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 UTF8String:: = ASTM-Type-OID-for-physician}

codeDataFreeText UTF8String:: = "license number 20A4073"}

hcMinorClassCode CodedData:: = {

codingSchemeReference OBJECT IDENTIFIER:: =

ASTM-Coding-Scheme-for-License-Status-OID,

codeDataValue UTF8String:: = "*unrestricted",*

codeDataFreeText UTF8String:: = "unrestricted"} })

© ISO 2015 – All rights reserved

Note that, in this example, a license number and license status have been encoded as regional data. Such regional data are 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 (validity period coded as UTCTime)

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

© ISO 2015 – All rights reserved

hcActorData SET OF {

codedData CodedData:: = {

codingSchemeReference OBJECT IDENTIFIER:: = *id-hcpki*,

codeDataValue UTF8String:: = *the-code-for-midwife-role*,

codeDataFreeText DirectoryString:: = *optional-data}*

regionalHCData Sequence of RegionalData:: = {

type OBJECT IDENTIFIER:: = OID-for-this-regional-encoding,

country PrintableString (SIZE (2):: = ISO-country-code-for-Canada,

issuingAuthority DirectoryString:: = (C = CA, OU = Name-of-CA-for-Ontario-Health-Care),

hcMajorClassCode CodedData:: = {

codingSchemeReference OBJECT IDENTIFIER:: = *ISO-Role-Coding-Scheme*,

codeDataValue UTF8String:: = *the-code-for-midwife-role* }

codeDataFreeText UTF8String:: = "*optional printable data*"} })

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})

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 (validity period coded as UTCTime)

Subject

countryName (US = United States of America)

localityName (California)

organizationName (American Health Systems)

commonName (Jones, Sally R.)

surname (Jones)

© ISO 2015 – All rights reserved

givenName (Sally R.)

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 UTF8String:: = *the-code-for-file-clerk-role*,

codeDataFreeText DirectoryString:: = CN = Sally R. Jones*}*

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 Health Systems),

hcMajorClassCode CodedData:: = {

codingSchemeReference OBJECT IDENTIFIER:: = ASTM-Coding-Scheme-for-Type,

codeDataValue UTF8String:: = ASTM-Type-OID-for-file-clerk} } })

Note that, unlike EXAMPLE 3 (for regulated health professional), there is no license number or license status encoded. This is permissible because these regional data fields are optional, and decision to include or exclude such regional data is left up to the issuing CA.

A.7 EXAMPLE 6: Organization certificate profile

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

Version (2 – decimal code for version 3 certificates)

SerialNumber (unique number)

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

© ISO 2015 – All rights reserved

Issuer	
countryName	(US = United States of America)
localityName	(California)
organizationName	(California Hospital Authority)
commonName	(Health Digital Certificate policy v01)
Validity	(validity period coded as UTCTime)
Subject	
countryName	(US = United States of America)
localityName	(Region = California)
organizationName	(Midtown Hospital)
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)

A.8 EXAMPLE 7: AC 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.

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	(California)

© ISO 2015 – All rights reserved

organizationName	(California Hospital Authority)
commonName	(CA - / policy v01)
Validity	(validity period coded as UTCTime)
Subject	
countryName	(US = United States of America)
localityName	(Region = California)
organizationName	(Midtown Hospital)
commonName	(Midtown Secure Server 01)
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)

A.9 EXAMPLE 8: CA 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.

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	(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)

© ISO 2015 – All rights reserved

commonName	(Ex. CalifHA PKI US CT/ policy V.03)
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	(CRL and certificate signing)
certificatePolicies	(appropriate policy OID)
basicConstraints	(CA = true)
cRLDistributionPoints	(CRL X.500 entry location)

A.10 EXAMPLE 9: Bridge 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.

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	(Region California)
organizationName	(California Hospitals Authority)
commonName	(CA – Health PKI US-CT/ policy v01)
Validity	(validity period coded as UTCTime)
Subject	
countryName	(US = United States of America)
localityName	(Region Washington)
organizationName	(Washington Health Authority)
commonName	(CalifHA PKI US CT/ policy V.03)
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)

© ISO 2015 – All rights reserved

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

© ISO 2015 – All rights reserved

Bibliography

[1] ISO/IEC 2382-8:1998, *Information technology — Vocabulary — Part 8: Security*

[2] ISO/IEC 7498-2, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

[3] ISO/IEC 8824-1:1998, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1*

[4] ISO/IEC 9594-8:2001, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks — Part 8*

[5] ISO/IEC 10181-1:1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview — Part 1*

[6] ISO/IEC/TR 13335-1, *Information technology — Guidelines for the management of IT Security — Part 1: Concepts and models for IT security*

[7] ISO/IEC 14516, *Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services*

[8] ISO/IEC 15945, *Information technology — Security techniques — Specification of TTP services to support the application of digital signatures*

[9] ISO/IEC 27799:2008, *Information technology — Code of practice for information security management*

[10] IETF/RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

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

[12] IETF/RFC 3739, Internet X.509 Public Key Infrastructure Qualified Certificates Profile

[13] IETF/RFC 5755, An Internet Attribute Certificate Profile for Authorization

[14] ENV 13608-1, *Health informatics — Security for healthcare communication — Concepts and terminology*

[15] Ankney R. CertCo. Privilege Management Infrastructure, v0.4, August 24, 1999

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

[17] Draft Standard ASTM Standard Guide for Model Certification Practice Statement for Healthcare. January 2000

[18] Bernd B., & Roger-France F. A Systemic Approach for Secure Health Information Systems. *Int. J. Med. Inform*. 2001, ••• pp. 51–78

[19] Canadian Institute for Health Information. Model Digital Signature and Confidentiality Certificate Policies, June 30 2001. Drummond Group. The Healthkey Program, PKI in Healthcare: Recommendations and Guidelines for Community-based Testing, May 2000

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

[21] Feghhi J., & Williams P. *Digital Certificates — Applied Internet Security*. Addison-Wesley, 1998

© ISO 2015 – All rights reserved

[22] Government of Canada. Criteria for Cross Certification, 2000

[23] Klein G., Lindstrom V., Norr A., Ribbegard G., Torlof P. Technical Aspects of PKI, January 2000

[24] Klein G., Lindstrom V., Norr A., Ribbegard G., Sonnergren E., Torlof P. Infrastructure for Trust in Health Informatics, January 2000

[25] Standards Australia. Strategies for the Implementation of a Public Key Authentication Framework (PKAF) in Australia SAA MP75

[26] Wilson S. Audit Based Public Key Infrastructure, Price Waterhouse Coopers White Paper, November 2000

© ISO 2015 – All rights reserved

ICS 35.240.80
Price based on 32 pages

© ISO 2015 – All rights reserved