INTERNATIONAL STANDARD

ISO
17090-1

Third edition
2021-02

Health informatics — Public key infrastructure —

Part 1:
Overview of digital certificate services

Informatique de santé — Infrastructure de clé publique —

Partie 1: Vue d'ensemble des services de certificat numérique

Reference number
ISO 17090-1:2021(E)

© ISO 2021

COPYRIGHT PROTECTED DOCUMENT

Contents

Page

Foreword

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

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 of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 215, *Health informatics*.

This third edition cancels and replaces the second edition (ISO 17090-1:2013), of which it constitutes a minor revision. The changes compared to the previous edition are as follows:

— update to references;

— editorial update.

A list of all parts in the ISO 17090 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

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

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

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

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

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

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

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

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

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

This document 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.

This document 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[14] and the profile of this specified in IETF/RFC 3280 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. ISO 17090-3 is based on the recommendations of the informational IETF/RFC 3647 and identifies the principles needed in a healthcare security policy for cross border communication. It also defines the minimum levels of security required, concentrating on the aspects unique to healthcare.

Health informatics — Public key infrastructure —

Part 1:
Overview of digital certificate services

1 Scope

This document defines the basic concepts underlying the use of digital certificates in healthcare and provides a scheme of interoperability requirements to establish a digital certificate-enabled secure communication of health information. It also identifies the major stakeholders who are communicating health-related information, as well as the main security services required for health communication where digital certificates can be required.

This document gives a brief introduction to public key cryptography and the basic components needed to deploy digital certificates in healthcare. It further introduces different types of digital certificates — identity certificates and associated attribute certificates for relying parties, self-signed certification authority (CA) certificates, and CA hierarchies and bridging structures.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1 Healthcare context terms

3.1.1
application
identifiable computer running software process that is the holder of a private encipherment key

Note 1 to entry: Application, in this context, can be any software process used in healthcare information systems, including those without any direct role in treatment or diagnosis.

Note 2 to entry: In some jurisdictions, including software, processes can be regulated medical devices.

3.1.2
device
identifiable computer-controlled apparatus or instrument that is the holder of a private encipherment key

Note 1 to entry: This includes the class of regulated medical devices that meet the above definition.

Note 2 to entry: Device, in this context, is any device used in healthcare information systems, including those without any direct role in treatment or diagnosis.

3.1.3
healthcare actor
actor
regulated health professional, non-regulated health professional, sponsored healthcare provider, supporting organization employee, patient/consumer, healthcare organization, device, or application that acts in a health-related communication and requires a certificate for a digital certificate-enabled security service

3.1.4
healthcare organization
officially registered organization that has a main activity related to healthcare services or health promotion

EXAMPLE   Hospitals, Internet healthcare website providers, and healthcare research institutions.

Note 1 to entry: The organization is recognized to be legally liable for its activities but need not be registered for its specific role in health.

Note 2 to entry: An internal part of an organization is called here an organizational unit, as in X.501.

3.1.5
non-regulated health professional
person employed by a healthcare organization who is not a regulated health professional

EXAMPLE   Medical receptionist who organizes appointments or nurses aid who assists with patient care.

Note 1 to entry: The fact that the employee is not authorized by a body independent of the employer in his/her professional capacity does, of course, not imply that the employee is not professional in conducting his/her services.

3.1.6
organization employee
person employed by a healthcare organization or a supporting organization

EXAMPLE   Medical records transcriptionists, healthcare insurance claims adjudicators, and pharmaceutical order entry clerks.

3.1.7
patient
consumer
person who is the receiver of health-related services and who 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

[SOURCE: ISO/IEC 2382:2015, 2126263]

3.1.9
regulated health professional
person who is authorized by a nationally recognized body to be qualified to perform certain health services

EXAMPLE   Physicians, registered nurses, and pharmacists.

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

Note 2 to entry: A nationally recognized 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 for one nationwide directory of recognized health professional registration bodies to exist.

3.1.10
sponsored healthcare provider
health services provider who is not a regulated professional in the jurisdiction of his/her practice, but who is active in his/her healthcare community and sponsored by a regulated healthcare organization

EXAMPLE   A drug and alcohol education officer who is working with a particular ethnic group, or a healthcare aid worker in a developing country.

3.1.11
supporting organization
officially registered organization which is providing services to a healthcare organization, but which is not providing healthcare services

EXAMPLE 1   EXAMPLE

EXAMPLE 2   Healthcare financing bodies such as insurance institutions, suppliers of pharmaceuticals and other goods.

3.2   Security services terms

3.2.1
access control
means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways

[SOURCE: ISO/IEC 2382:2015, 2126294, modified — Notes to entry removed.]

3.2.2
accountability
property that ensures that the actions of an entity may be traced uniquely to the entity

[SOURCE: ISO 7498-2:1989, 3.3.3]

3.2.3
asymmetric cryptographic algorithm
algorithm for performing encipherment or the corresponding decipherment in which the keys used for encipherment and decipherment differ

[SOURCE: ISO/IEC 10181-1:1996, 3.3.1, modified — Note to entry removed.]

3.2.4
authentication
process of reliably identifying security subjects by securely associating an identifier and its authenticator

[SOURCE: ISO 7498-2:1989]

Note 1 to entry: See also data origin authentication and peer entity authentication.

3.2.5
authorization
granting of rights, which includes the granting of access based on access rights

[SOURCE: ISO 7498-2:1989, 3.3.10]

3.2.6
availability
property of being accessible and useable upon demand by an authorized entity

[SOURCE: ISO 7498-2:1989, 3.3.11]

3.2.7
ciphertext
data produced through the use of encipherment, the semantic content of which is not available

[SOURCE: ISO 7498-2:1989, 3.3.14, modified — Note to entry removed.]

3.2.8
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO 7498-2:1989, 3.3.16]

3.2.9
cryptography
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 unauthorized use

[SOURCE: ISO 7498-2:1989, 3.3.20, modified — Note to entry removed.]

3.2.10
cryptographic algorithm
cipher
method for the transformation of data in order to hide its information content, prevent its undetected modification, and/or prevent its unauthorized use

[SOURCE: ISO 7498-2:1989]

3.2.11
data integrity
property that data have not been altered or destroyed in an unauthorized manner

[SOURCE: ISO 7498-2:1989, 3.3.21]

3.2.12
data origin authentication
corroboration that the source of data received is as claimed

[SOURCE: ISO 7498-2:1989, 3.3.22]

**3.2.13
decipherment
decryption**
process of obtaining, from a ciphertext, the original corresponding data

[SOURCE: ISO/IEC 2382:2015, 2126281, modified — Notes 2 and 3 to entry removed.]

Note 1 to entry: A ciphertext may be enciphered a second time, in which case a single decipherment does not produce the original plaintext.

**3.2.14
digital signature**
data appended to, or a cryptographic transformation (see cryptography) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient

[SOURCE: ISO 7498-2:1989, 3.3.26]

**3.2.15
encipherment
encryption**
cryptographic transformation of data (see cryptography) to produce ciphertext

[SOURCE: ISO 7498-2:1989, 3.3.27]

**3.2.16
identifier**
piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator

[SOURCE: ENV 13608-1]

**3.2.17
integrity**
proof that the message content has not been altered, deliberately or accidentally, in any way during transmission

Note 1 to entry: Adapted from ISO 7498-2:1989.

**3.2.18
key**
sequence of symbols that controls the operations of encipherment and decipherment

[SOURCE: ISO 7498-2:1989, 3.3.32]

**3.2.19
key management**
generation, storage, distribution, deletion, archiving, and application of keys in accordance with a security policy

[SOURCE: ISO 7498-2:1989, 3.3.33]

**3.2.20
non-repudiation**
service providing proof of the integrity and origin of data (both in an unforgeable relationship), which can be verified by any party

Note 1 to entry: Adapted from Reference [18].

3.2.21
private key
key that is used with an asymmetric cryptographic algorithm and whose possession is restricted (usually to only one entity)

[SOURCE: ISO/IEC 10181-1:1996, 3.3.10]

3.2.22
public key
key that is used with an asymmetric cryptographic algorithm and that can be made publicly available

[SOURCE: ISO/IEC 10181-1:1996, 3.3.11]

3.2.23
role
set of behaviours that is associated with a task

3.2.24
security
combination of availability, confidentiality, integrity, and accountability

[SOURCE: ENV 13608-1]

3.2.25
security policy
plan or course of action adopted for providing computer security

[SOURCE: ISO/IEC 2382:2015, 2126246, modified — Notes to entry removed.]

3.2.26
security service
service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers

[SOURCE: ISO 7498-2:1989, 3.3.51]

3.3   Public key infrastructure related terms

3.3.1
attribute authority
AA
authority which assigns privileges by issuing attribute certificates

[SOURCE: RFC 5280]

3.3.2
attribute certificate
data structure, digitally signed by an attribute authority, that binds some attribute values with identification about its holder

[SOURCE: RFC 5280]

3.3.3
authority certificate
certificate issued to a certification authority or to an attribute authority

Note 1 to entry: Adapted from RFC 5280.

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 1 to entry: Certificate extensions may be either critical (i.e. a certificate-using system has to reject the certificate if it encounters a critical extension it does not recognize) or non-critical (i.e. it may be ignored if the extension is not recognized).

3.3.7
certificate generation
act of creating certificates

3.3.8
certificate profile
specification of the structure and permissible content of a certificate type

3.3.9
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, even though it is unexpired

3.3.10
certificate holder
entity that is named as the subject of a valid certificate

3.3.11
certification
procedure by which a third party gives assurance that all or part of a data processing system conforms to security requirements

[SOURCE: ISO/IEC 2382:2015, 2126258, modified — Notes to entry removed.]

3.3.12
certification authority
CA
certificate issuer
authority trusted by one or more relying parties to create and assign certificates and which may, optionally, create the relying parties' keys

Note 1 to entry: Adapted from ISO/IEC 9594-8:2021.

Note 2 to entry: Authority in the CA term does not imply any government authorization but only denotes that it is trusted.

Note 3 to entry: Certificate issuer may be a better term, but CA is very widely used.

3.3.13
certificate policy
CP
named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

[SOURCE: IETF/RFC 3647]

3.3.14
certification practices statement
CPS
statement of the practices which a certification authority employs in issuing certificates

[SOURCE: IETF/RFC 3647]

3.3.15
public key certificate
PKC
X.509 public key certificates (PKCs) which bind an identity and a public key

Note 1 to entry: 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.

Note 2 to entry: Adapted from IETF/RFC 3280.

3.3.16
public key infrastructure
PKI
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 and that 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

3.3.17
qualified certificate
certificate whose primary purpose is identifying a person with a high level of assurance in public non-repudiation services

Note 1 to entry: The actual mechanisms that will decide whether a certificate should or should not be considered to be a "qualified certificate" in regard to any legislation are outside the scope of this document.

3.3.18
registration authority
RA
entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e. an RA is delegated certain tasks on behalf of a CA)

[SOURCE: IETF/RFC 3647]

3.3.19
relying party
recipient of a certificate who acts in reliance on that certificate and/or digital signature verified using that certificate

[SOURCE: IETF/RFC 3647]

3.3.20
third party
party, other than data originator or data recipient, required to perform a security function as part of a communication protocol

3.3.21
trusted third party
TTP
third party which is considered trusted for purposes of a security protocol

[SOURCE: ENV 13608-1]

Note 1 to entry: This term is used in many ISO/IEC International Standards and other documents describing mainly the services of a CA. The concept is, however, broader and includes services such as time-stamping and possibly escrowing.

4   Abbreviations

ECG   electrocardiogram

EHR   electronic health record

5   Healthcare context

5.1   Certificate holders and relying parties in healthcare

For the purposes of facilitating the discussion on digital certificate requirements, the following classes of healthcare actors are introduced. This does not imply that other classes and definitions are not more appropriate in other contexts.

The focus here is on actors who are directly involved in a health-related communication and may require a certificate for a PKI-enabled security service. The following actors are defined in 3.1.

Persons: regulated health professional;

                  non-regulated health professional;

                  patient/consumer;

                  sponsored healthcare provider;

                  supporting organization employee.

Organizations: healthcare organization;

                  supporting organization.

Other entities: devices;

                  regulated medical devices;

                  applications.

In addition to these actors, the wide-scale deployment of digital certificates requires CAs and RAs to be part of the total system and these organizations become important certificate holders in their own right.

Some healthcare workers are associated with multiple healthcare organizations. There is a primary need in healthcare to avoid duplicate or redundant registration with its inherent costs and multiplicity of certificates.

Within the healthcare context, the role of RAs is to identify the actor as either a valid health professional performing a given role or to identify a consumer as the person with rights to his or her own information. There also needs to be a way of registering support staff for physicians in private practice (medical

receptionists, billing clerks, file clerks, etc.). Such individuals are not associated with institutions such as hospitals that are covered by national, state, or provincial health authorities.

5.2 Examples of actors

5.2.1 Regulated health professional

Examples of regulated health professionals are physicians, dentists, registered nurses, and pharmacists. There are many different classifications of officially regulated/accredited professions in healthcare in different countries. It is an important task to create a global mapping for this but, for the purposes of this document, it is assumed that only very broad classes can be recognized internationally. In ISO 17090-2, a data structure is presented that allows a broad international classification to be used in parallel with a more detailed defined classification that may be national or may follow other jurisdictions, since regulated health professionals are regulated in provinces or states in some countries.

5.2.2 Non-regulated health professional

Non-regulated health professionals are persons who are employed by a healthcare organization but who are not regulated health professionals, and include medical secretaries and record assistants, transcription clerks (i.e. those who type from a dictated voice recording), billing clerks, and assistant nurses. For the purpose of this document, it is important to include the relationship between the employing healthcare organization and the employee in a certificate for security services. For the healthcare professionals, it is important to include the relationship with the professional registration body in the structure of the digital certificate, but a possible employment or other affiliation of, for example, a physician may also be important.

There are many different types of roles or occupations of healthcare employees and this document makes no attempt to provide a classification scheme.

NOTE   The fact that the employee is not registered 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.

5.2.3 Patient/consumer

The person who receives health-related services is, in most cases, called the patient but, in some situations, it is more appropriate, in the case of a healthy person and when considering the contractual relations with the healthcare providers, to call such a person a consumer of health services. Only the patient/consumer who is also a direct user of a health information system is considered in this context.

5.2.4 Sponsored healthcare provider

There are some types of persons who are providers of health services that are not regulated in the jurisdiction but who are active in a community and where their professional role may be certified and sponsored by a registered healthcare organization. Examples are, in some countries, midwives (who may be sponsored by obstetricians or other physicians), physiotherapists of different types, and various persons active in community care for disabled and elderly (who may be sponsored by a general practitioner or a hospital).

5.2.5 Supporting organization employee

A supporting organization employee is a person who is working for a supporting organization and who is not a regulated or non-regulated health professional.

5.2.6 Healthcare organization

Examples of officially registered organizations that have a main activity related to healthcare services or health promotion are healthcare providers, healthcare financing bodies (insurance companies or administrators of governmental public health financing), and healthcare research institutions.

5.2.7 Supporting organization

Supporting organizations perform services for healthcare organizations but do not perform direct healthcare services.

5.2.8 Devices

Devices are equipment such as ECG machines, laboratory automation equipment, and different portable diagnostic aids that measure various physiological parameters of a patient; included also are computer devices such as electronic mail servers, web servers, and application servers.

5.2.9 Applications

Applications are computer software programs running on individual machines and/or networks. Within the healthcare context, applications relying upon digital certificates could include integrated clinical management systems, EHR applications, emergency department information systems, imaging systems, and prescribing, drug profiling, and medication management systems.

5.3 Applicability of digital certificates to healthcare

This document applies to the healthcare industry, both within and between jurisdictional boundaries. It is intended to cover public (government) health authorities and private healthcare providers across the entire range of settings including hospitals, community health, and general practice. It also applies to health insurance organizations, healthcare educational institutions, and health-related activities (such as home care).

While the primary aim is to develop a framework where health professionals, healthcare organizations, and insurers can securely exchange health information, this document is also intended to provide consumers with the ability to securely access their own healthcare information. Transactions can take place with CAs and RAs acting as trusted third parties to enable providers, insurers, and consumers to exchange information, safe in the knowledge that it is secure and protected, and that, if integrity is breached, it will quickly become known.

Suitable applications of digital certificates within healthcare are:

a) secure electronic mail;

b) access requests by applications used by community-based health professionals for patient information in hospital-based information systems;

c) access requests by applications used within hospital-based information systems (systems would include patient administration, clinical management, pathology, radiology, dietary, and other related information systems);

d) billing applications, which require non-repudiation, message integrity, confidentiality, and authentication of patients, health service providers, and health insurers, as well as (in some jurisdictions) fraud prevention;

e) tele-imaging applications, which require a reliable binding between an image and a patient identity, together with authentication of the health professional;

f) remote access control applications, which have a particular need to verify authenticity, confidentiality, and integrity;

g) electronic prescription applications, which require all the security services that digital certificates can offer to check that the prescription is verified as having originated from a particular health professional (origin authentication) and is being filled for the correct patient (ensuring there are no errors in transmission requires the integrity service that digital certificates can offer and ensuring auditability requires the service of non-repudiation);

h) digitally signed patient consent documents;

i) transcription services across national or jurisdictional boundaries;

j) other systems in accordance with local policies.

Local policies may exclude one or more of the above applications from relying upon or otherwise making use of digital certificates.

A set of scenarios where digital certificates could be applied is detailed in <u>Annex A</u>.

6 Requirements for security services in healthcare applications

6.1 Healthcare characteristics

The healthcare industry has particular security needs that require special interpretation, which is the reason why this document has been developed. Particular characteristics of healthcare are as follows.

a) Health information is reusable and can exist for as long as (and longer than) the person to whom it refers. This creates a special need for long-term preservation of digital signatures and a valuable role for the Time Stamp technology that can support this.

b) There are significant health consumer and health service provider concerns to ensure health information collected is used for health purposes and not for something else, unless the patient has given his/her explicit consent to use such information (e.g. anonymous patient data may be used for training and planning purposes).

c) There is a need to improve the health consumers' confidence in the ability of the health system to manage their information.

d) There is a need for health professionals and organizations to meet security obligations in the context of health strategies.

e) The need exists to ensure that health professionals, trading partners, and relying parties making use of digital certificates have confidence in measures to ensure privacy and security of patient information.

The security issue in healthcare becomes more visible as personal health information is being increasingly stored using electronic information systems instead of paper files. The first concern of the healthcare industry is to protect the privacy and safety of the patient. In particular, this concern extends to the need to comply with relevant privacy legislation, in respect of trans-border health information flows. If an information system is going to be used by both healthcare professionals and consumers/patients, it shall be trusted. For this reason, meeting the need for privacy and security is critical for healthcare information systems.

6.2 Digital certificate technical requirements in healthcare

6.2.1 General

Major security threats that need to be addressed in healthcare information and communication systems are unauthorized access gained through stealing the private key of a legitimate certificate holder and then masquerading as that certificate holder. Such unauthorized access can lead to the healthcare information itself being altered, lost, or replicated. Digital certificates used in combination with a security standard, such as ISO/IEC 27002, can significantly reduce the risk of unauthorized access.

Digital certificates provide the only combination of policy, procedures, and technology that offer all the services of authentication, integrity, confidentiality, and digital signature. Within the healthcare context, the use of digital certificates enables healthcare providers and consumers who may not know each other to communicate securely and with confidence, by electronic means, through a chain of trust.

Digital certificates can offer security services for which the health industry has a particular need. These services and their application to healthcare are described in more detail below.

6.2.2 Authentication

Healthcare is a multi-disciplinary endeavour and health professionals routinely rely upon the judgment of other healthcare providers when reviewing patient records, consultation reports and other documents containing personal health information. When these documents and records are accessed and updated electronically, it is essential that the information contained within be reliably attributable to its authors.

It is of paramount importance that health professionals be able to access sensitive personal health information from a variety of clinical settings and, at the same time, protect this information from access or alteration by unauthorized persons. Authentication is discussed further in 7.4.

6.2.3 Integrity

Maintaining the integrity of personal health information can literally become a life-or-death issue when such information is relied upon in the course of providing emergency healthcare. Moreover, strong incentives exist to corrupt the integrity of some forms of personal health information (for example, narcotics prescriptions).

6.2.4 Confidentiality

Personal health information is often regarded as the most confidential information in common use. Unlike information communicated electronically for the purposes of e-commerce, the confidentiality of personal health information cannot readily be assigned a monetary value, and a patient's right to privacy, once abrogated, cannot readily be restored.

6.2.5 Digital signature

Digital signatures used in healthcare, and the policies and practices to confirm their integrity, may ultimately be the subjects of considerable interest during inquest hearings, medical malpractice litigation, professional disciplinary hearings, and other legal or quasi-legal forums where electronically signed documents will be provided as evidence.

Digital signatures on healthcare documents should be verifiable even if the certificate has expired or been revoked. This may be accomplished using secure time stamp technology (see IETF/RFC 3161). IETF/RFC 3126 is recommended as a long-term signature format in such cases.

Digital certificates also support authorization and role-based access control services. These services are vital in healthcare as there are many specializations and many situations that require different levels of access to parts of a personal health information, depending on the situation and the role of the health professional involved.

6.2.6 Authorization

It is essential in healthcare to only grant rights for personal health information access to those entities requiring them for providing care to the patient/consumer, or to other entities where the explicit consent of the patient has been given.

6.2.7 Access control

In healthcare, it is essential that means are in place to ensure that the resources of a data processing system can only be accessed by authorized entities in authorized ways and for authorized purposes/functions, as the consequence of unauthorized access can be impossible to remedy.

When used in conjunction with an appropriate security standard, digital certificates can significantly reduce the risk of unauthorized disclosure of patient health information.

The purpose of this document is to define the common elements of a digital certificate issuance and use that will ensure the chain of trust for communicating health information extends as far as need be, even beyond jurisdictional or national boundaries.

6.3 Healthcare-specific needs and the separation of authentication from data encipherment

There is a particular health industry need to separate the signing from the encipherment function. The reason for this is that authorized health professionals may need to access a patient's record in emergency or special situations when the health professional for whom the message was intended is not physically present or contactable. It is common practice in healthcare security to have an individual identity certificate used for authentication and an organization unit certificate used for encipherment.

This document advocates that separate certificates and associated keys be used for the purpose of authentication and encipherment (ensuring confidentiality). It also recognizes the need to have separate certificates to establish identity and others to manage access control that are bound to the subject's authentication key.

If keys are used for data encryption, a form of key management is necessary to prevent data loss if the decryption keys are not available.

6.4 Health industry security management framework for digital certificates

The digital certificate security infrastructure required to support the secure movement of healthcare-related information and access to data within and across national or jurisdictional boundaries needs to be supported by a framework of generic security management policies. To achieve some assurance that the infrastructure operates securely, there is a need to establish codes of practice for its management.

Standards giving the codes of practice for the management of information security already exist and are commonly accepted. ISO/IEC 27002 and the COBIT specification[15] establish practices for the identification of security risks, as well as for the application of the appropriate controls to manage those risks.

Such codes of practice place little or no constraint on the security services that can be offered by the deployment digital certificates and give the signer and the verifier a degree of assurance that the electronic signature is not weakened by poor security management.

Consequently, this document will refer to ISO/IEC 27002 to address the security issues presented in IETF/RFC 3647[10].

6.5 Policy requirements for digital certificate issuance and use in healthcare

The policy requirements and associated practices for issuing and using digital certificates in healthcare shall be in accordance with ISO 17090-3.

7 Public key cryptography

7.1 Symmetric vs. asymmetric cryptography

With symmetric cryptography, a secret key is used to encipher plain text into a cryptogram that is not readable. Such enciphered information can be deciphered with the same secret key by reversing the encipherment algorithm. This type of cryptosystem is widely used to ensure confidentiality and is called the symmetric or secret key.

Public key cryptography was first described by Whitfield Diffie and Martin Hellman in 1976. The approach uses two different keys, one public and the other private. Anyone with the public key can encipher a message but not decipher it. Only the person with the private key can decipher the message.

It is not possible to deduce the private key from knowledge of the public key alone and the public key can thus be made widely known without confidentiality concerns.

Such a cryptosystem is called asymmetric. The RSA asymmetric algorithm named after the three inventors (Rivest, Shamir, and Adelman) is widely used, either alone or in combination with symmetric cryptosystems. In such hybrid systems, the asymmetric algorithm is used to protect the secret key of the symmetric cryptosystem.

Asymmetric cryptosystems can add value to symmetric cryptosystems or virtual private networks by enabling relying parties to be authenticated by guaranteeing communication integrity and also by enabling authorization and access control.

Some public key algorithms such as RSA can be used to recover a message and are therefore suitable for confidentiality protection using encipherment as described above. This algorithm can also be used in the inverse direction where a text enciphered by the private key can be deciphered using the public key. This principle is not suitable for confidentiality protection but for authentication purposes. Only the holder of the private key could produce a cryptogram that can be deciphered using the corresponding private key. This quality can be used to authenticate the origin of messages to someone in possession of the private key.

7.2   Digital certificates

A digital certificate is a software data structure that binds an entity's public key and one or more attributes relating to that entity's identity, the public keys of an entity, together with other information, being rendered unforgeable by encipherment with the private key of the CA, which issued it in accordance with ISO/IEC 9594-8. Among the identity-related attributes is a distinguished name by which the entity can be identified.

The entity can be a person, an organizational unit, an application, a server, or a hardware device. The purpose of a digital certificate is to provide some level of confidence that the public key belongs to the identified entity and that the entity possesses the corresponding private key.

The level of confidence is provided by the CA signing the digital certificate with its own private key. By signing the digital certificate, the CA is taking responsibility for information contained in the digital certificate and providing the certificate holder with some level of authentication.

A CA publishes certificates, maintains a directory of certificates (together with its public keys), revokes any certificates that may become invalid, and ensures all relevant relying parties are promptly informed of any revocation of certificates. The process of managing certificates is specified in ISO 17090-3, which also specifies the role of the RA and restrictions on who can perform the role of an RA.

7.3   Digital signatures

A digital signature is appended data or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient, in accordance with ISO 7498-2[2].

The digital signature is generated by using the sender's private key to perform a mathematical operation on the message being sent. This operation uses the private key and a one-way mathematical function known as a hashing algorithm to produce a hash (a very large number) from the original message. The hash function has the property that it is computationally infeasible to produce the original message or private key from the hash. This hash is sent with the message. The recipient then uses the sender's public key to perform the same operation on the message and compare the resultant hash with the one sent with the message. If the two are identical, then the recipient can have a level of confidence that the message was sent by the source that claimed to have sent it. Since the private key is part of a key pair in which the public key is bound to an identity in a digital certificate, the identity of the sender can be verified to a level of confidence previously not possible. The level of confidence is provided by the CA signing the digital certificate with its own private key. By signing the digital certificate, the

CA is taking responsibility for information contained in the digital certificate and for providing the certificate holder with some level of authentication.

The level of confidence achieved is dependent upon the CA's policies and practices and the key management of the relying parties.

Besides providing a level of confidence about authentication of senders, the use of a digital signature can provide a level of confidence about the integrity of the communication, as identical hash results can only be obtained if the communication used to produce it is the same at the source and at the destination.

7.4 Protecting the private key

A certificate does not bind keys to identities; it only binds keys to the distinguished name of an entity. Special steps shall be taken to complete the binding of the private key to an entity ensuring that only the named entity can make use of the private key. Competent private key management is therefore critical to the successful deployment of digital certificates within the health industry. If the private key is compromised, the associated digital certificate is no longer effective in protecting information communicated and stored using that particular public/private key pair. Furthermore, if the private key of a CA is compromised, the security of that CA's domain may collapse.

Protecting the private key requires a combination of management processes and technical methods. Whatever technical option is used, key protection shall be managed within an overall information security management framework in accordance with ISO/IEC 27002.

A private key can be protected using a hardware token, where the private key is stored on a token which can perform cryptographic calculations and is accessed by the certificate holder through use of a password, a passphrase, or a biometric. This is a more secure method of protecting the private key as there is no electrical connection to the computer, it cannot be accessed through a network, and sophisticated authentication algorithms can be placed on the token. Certain types of smartcards can fulfil the role of such hardware tokens. It is also possible to use a USB (Universal Serial Bus) key or similar hardware token, which just stores the private key, with the cryptographic logic stored on a host computer.

To access the private key, the certificate holder, or another device or application, is required to be authenticated, most commonly by password, passphrase, or biometric. There are different types of authentication mostly based upon characteristics such as where you are, what you know, are, or have, e.g. requiring the use of a password (something you know) with use of a physical device such as a token (something you have). Using more than one type of authentication, known as two-factor authentication, greatly increases the security of the private key and is recommended.

This document identifies a need for multiple levels of security and states that higher levels of security will require a hardware token for private key protection. Managing the private key is specified in detail in ISO 17090-3:2021, 7.6.2 and 7.6.3.

Moving personal health information between jurisdictions, across national boundaries using an insecure medium such as the Internet, where sender and recipient may have had no previous contact and no personal contact, means that there need to be methods to authenticate the involved parties, to ensure that the information transmitted and stored remains confidential, to ensure that the information is not altered in transmission, and that none of the parties can later deny having sent or received the communication. This is the business requirement in the health industry for security services that digital certificates can address.

8 Deploying digital certificates

8.1 Necessary components

8.1.1 General

PKI is an infrastructure that consists of the components described below.

8.1.2 CP

A CP is a named set of rules that indicates the applicability of a certificate to a particular healthcare community and/or class of application with common security requirements. Certificates based on a CP, which is specifically designed to meet the needs of healthcare information, support services such as authorization, access control, and information integrity. The particular needs of the healthcare system as described in Clause 6, mean that digital certificates need to be specified especially for healthcare.

8.1.3 CPS

A CPS is a statement of the practices that a CA employs in issuing certificates to implement the CP. For example, it indicates the actions to be taken when a request from a health authority is received to issue a health professional with a certificate.

8.1.4 CA

A CA is a trusted entity that verifies the identity of a certificate holder and allocates a "distinguished name" to that certificate holder. A CA also verifies the correctness of information concerning the identified certificate holder by signing the data and, in so doing, verifying the binding between names or identities and public keys, which constitutes the digital signature for that certificate holder. Some of these functions may be delegated to an RA (see 8.1.5), e.g. verification of identity and allocation of a distinguished name, as these functions may be best performed at a local level.

The private key can then be stored on the subject's computer or on removable media such as a smart card. The key is generally accessed by the certificate holder entering a passphrase.

This document recognizes that health authorities may obtain certification services in different ways. Some may run their own; others may outsource the activity to accredited private organizations. There may also be multiple certifications depending on the purpose for which the certificates are issued. Certificate holders may also have multiple certificates.

Depending on how countries organize their own healthcare digital certificates, there may be up to several levels of CAs providing certificates for certificate holders within an organization, for the healthcare industry as a whole, or for anyone in that country.

The CA should be a recognized organization with suitable controls and procedures in place to provide the required degree of trust. At a minimum, the controls and procedures shall be in accordance with ISO/IEC 27002 (or its equivalent) and, where possible, should conform to a recognized digital certificate assurance scheme, appropriate to the jurisdiction(s) of operation.

8.1.5 RA

An RA is an entity that establishes the identities of certificate holders and registers their certification requirements with a CA. An RA may also verify a certificate holder's role, rank, or employment status for information that may be stored on an attribute certificate. In this situation, it is possible for the RA to verify that an attribute such as employment status (e.g. a government hospital authority) may be a different RA to an organization that verifies a health professional's qualification to practice (e.g. a health professional registration board).

The identification of the healthcare professional role may be performed by such bodies as

— national, state, or provincial health authorities (covering associated hospitals and health facilities),

— medical or health professional registration boards,

— medical or healthcare professional bodies, for example colleges of surgeons, psychiatrists, nurses,

— public or private health insurance organizations.

Users of digital certificates may rely on one or more of these bodies for the validation of a health professional's credentials. Procedures for registration are specified in 6.1, 7.2.1.2, 7.3.1.2, 7.3.2.2, 7.3.3.2, and 7.3.4.2 of ISO 17090-3:2021.

8.2 Establishing identity using qualified certificates

Qualified certificates are types of certificate whose primary purpose is to identify a person with a high level of assurance in digital signature services. Qualified certificates are particularly relevant in relation to the legal recognition of electronic signatures. This document makes provision for the use of qualified certificates in response to increasing numbers of countries legislating requirements to be met by health and other service providers supporting electronic signatures and requirements for signers and verifiers so that an electronic signature can be legally recognized.

The need for qualified certificates has been recognized by the Internet Engineering Task Force (IETF), which has produced IETF/RFC 3739[11]. This RFC forms a certificate profile for qualified certificates and aims to define a general syntax independent of local legal requirements. The qualified certificate profile is used by the IETF to describe the format for a certificate whose primary purpose is to reliably identify an individual person. The IETF qualified certificates profile is used in this document as the framework to support qualified certificates. The qualified certificates profile shall be in accordance with ISO 17090-2.

Within the healthcare context, a qualified certificate could be used to reliably identify an individual healthcare provider or consumer to a level of confidence necessary to validate that person's electronic signature. It is recommended to use of qualified certificates for regulated health professionals and non-regulated health professionals.

8.3 Establishing speciality and roles using identity certificates

This document recognizes that not all physicians are the same in the eyes of a patient/consumer. Patients/consumers may use different physicians for different health issues. HIV/AIDS, communicable diseases, and mental health are just some of the health issues where people manage separate relationships. As a result, a decision to grant a health professional access to particular parts of a patient/consumer's health record is usually based on that health professional's speciality, e.g. surgeon, and role, e.g. duty surgeon at Midtown General Hospital Emergency Department.

It is important to note that authorization information does not have the same lifetime as the binding of an entity identity to a public key, much less a primary medical qualification. For example, someone may have been a qualified physician for 40 years but may only be contracted to work as a consultant psychiatrist at a particular hospital for several months. When authorization information is codified in a PKC extension, the general result is the shortening of the PKC's useful lifetime. Secondly, the PKC issuer is not usually authoritative for the authorization information. In this case, the PKC issuer may be able to verify that the person concerned is a particular medical doctor but is less likely to be able to verify that person's role as the consulting psychiatrist in a particular hospital. This results in additional steps for the PKC issuer to obtain authorization information from the authoritative source. It may also result in a shortening of the life span of a PKC because some of the information it contains is no longer valid, causing an increase in administrative effort to revoke that PKC and issue a replacement. For these reasons, it is often better to separate this authorization information from the PKC. The detailed specification for the attribute certificates still needs to be more widely implemented in the software industry (see IETF/RFC 3281[15]).

While the IETF attribute certificate specification describes how the public key is used to validate digital signatures or cryptographic key management operations, it states that not all request and disclosure decisions are identity-based. Such access control decisions can also be rule-based, role-based, and rank-based and, therefore, require additional information. For example, information about a health professional being a particular type of specialist may be more important in deciding access than his/her identity. In these situations, authorization information to support such decisions may be codified in a PKC extension or codified in a separate attribute certificate, in accordance with IETF/RFC 3281[15], as well as with item 5 in ISO 17090-2: 2015, 6.3.6 and with ISO 17090-2:2015, 7.3.1.

The PKC should have proving identity as its main purpose. Information provided on X.509[14] certificates about a certificate holder's identity can be used as the basis for making decisions on whether to disclose information in response to a request made on a server for a certain purpose. X.509[14] PKCs bind a client identity and a public key. The identity may be used to support identity-based decisions which manage requests and disclosure of information after the certificate holder proves that he/she has the private key that corresponds to the public key contained in the PKC (see IETF/RFC 3281[15]).

As an alternative model to the inclusion of various attributes regarding professional roles in the primary identity certificate issued, other organizations responsible for those role assignments may, on the approval of the primary CA, issue a secondary key certificate that uses the same key as a primary identity certificate but includes one or several additional attributes.

Once identity is proved, attribute certificates can also be used to more appropriately manage information in situations where some of the information bound to a PKC is more volatile or ephemeral than other information. For this reason, provision is made in this document for attribute certificates. However, there are difficulties with this approach. The use of attribute certificates is still evolving and needs to be more widely implemented in the software industry. Furthermore, information about a health professional's specialization, e.g. psychiatry, paediatrics, urology, does have some longevity. In addition, there needs to be some capacity to record information about a patient/consumer role. For these reasons, provision for this is made by specifying an extension called HCRole to the PKC identity certificate types in ISO 17090-2:2015, 5.1.

Finally, digital certificates can also be used to sign security assertions using a standard such as SAML (Security Assertion Markup Language). Such security assertions can include assertions about the speciality and role of a healthcare professional.

8.4   Using attribute certificates for authorization and access control

The IETF attribute certificate specification concludes that the placement of authorization information in the PKC is not desirable. This document recognizes the desirability of multi-useability and the need to minimize the information to be kept on identity certificates. Secondary roles, group membership, and security clearance should be placed on accompanying attribute certificates.

It is noted that 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 these are not necessarily authorization information in themselves. This document makes provision for the use of attribute certificates to support the transmission of role-based information regarding healthcare providers.

While an identity certificate issued by a PKC may imply a role, it does not contain sufficient information in many situations to make the access control decision. For example, while a PKC issued for a physician on behalf of an RA such as the College of Surgeons does imply that the physician is a surgeon, this does not usually constitute sufficient information to authorize that physician, while employed as a locum in a particular hospital emergency department, to admit a patient to the hospital.

Such detailed authorization information is more appropriately supplied by using an attribute certificate that is bound to the health professional's public key. A health professional may have many attribute certificates that reflect multiple roles. Such attribute certificates are typically more short-lived than an identity certificate.

The IETF attribute certificate RFC also states that authorization information needs to be protected in a fashion similar to a PKC and an attribute certificate provides this protection. It is simply a digitally signed (or certified) set of attributes. An attribute certificate is a structure similar to a PKC; the main difference being that it contains no public key. It may contain attributes that specify group membership, role, security clearance, and other access control information associated with the attribute certificate owner.

A specification of the data elements in an attribute certificate in accordance with IETF/RFC 3281[15] is provided in ISO 17090-2. As the specification for attribute certificates is still evolving, healthcare attribute certificate types will be specified in more detail in later editions of this document.

Refer to A.4.16 for scenarios involving signing of healthcare documents.

9 Interoperability requirements

9.1 Overview

This document seeks to adopt and add to the IETF and other existing security standards to support the secure electronic transfer of healthcare information across national or jurisdictional boundaries. The Internet is becoming increasingly used as the vehicle of choice to support this transfer.

Since one of the purposes of this document is to support the secure transmission of healthcare information across national, regional, and organizational boundaries, this document must be Internet-based to maximize its global effectiveness. For this reason, it uses the informational IETF/RFC 3647[10] as an organising framework for this document and references other relevant IETF/RFCs as required.

The secure transfer of health information across national boundaries could be achieved by participating countries mutually recognizing the mechanisms each country puts in place to review the policies, practices, and procedures to accredit CAs.

Governance of the issuance and use of digital certificates in healthcare needs further development and is outside the scope of this document. This document suggests that interoperability across national boundaries be achieved by a series of bilateral and multilateral agreements between countries, based upon minimum requirements as specified in ISO 17090-3. Ultimately, the relying party needs CAs to establish procedures as required to enable the infrastructure to be used with the level of assurance required.

9.2 Options for deploying healthcare digital certificates across jurisdictions

9.2.1 General

The main issue to address for any deployment of digital certificates that aims to span jurisdictions, including national boundaries, is trust. Trust is the practice of many parties relying on the policies and practices and, by extension, the validity of digital certificates issued to a certificate holder by an established authority. The options for deploying a healthcare digital certificate architecture are summarized below.

9.2.2 Option 1 — Single hierarchy of CAs

This is, from a technical viewpoint, the easiest option. It is not feasible however to establish a world spanning deployment of digital certificates in healthcare with one centralized CA. Although registration could be devolved in this scenario, the management arrangements might still be unworkable.

9.2.3 Option 2 — Relying party management of trust

In this option, it is the responsibility of the relying party to decide whether to trust the issuing CA concerned. This option has inherent difficulties as it requires the trust decision to fall on the relying party and, in some situations, this may place inappropriate responsibility upon the relying party who may not be in a position to make an informed decision.

9.2.4 Option 3 — Cross-recognition

Cross-recognition refers to an interoperability arrangement in which a relying party in one digital certificate domain can use authority information in another digital certificate domain to authenticate a subject in the other domain, and vice versa. Typically, such authority information either results from a formal licensing or accreditation process in the jurisdiction of the other domain, or results from a formal audit process performed by or on behalf of a representative CA of the relying party's domain. Technically, the information can be stored as the value of a certificate field accessible by the relying party.

Compared to cross-certification, the onus of whether to trust a foreign digital certificate domain lies with the relying party or the owner of the application or service, rather than a CA that the relying party directly trusts. It does not necessarily involve a contract or an agreement between two domains.

In a cross-recognition arrangement, detailed mapping of CPs and CPSs is not necessary. Instead, the relying party (via the application at hand) decides whether to accept a foreign certificate for the purpose depending on whether the certificate has been issued by a trustworthy foreign CA.

The CA is regarded as trustworthy if it has been licensed/accredited by a formal licensing/accreditation body or has been audited by a trusted independent party. Also, the relying party shall be able to unilaterally make an informed judgement based on the policies stipulated in the CP or CPS in the foreign domain. Hence, the process is comparatively less complicated than cross-certification, especially in respect of policy and legal harmonization. The process is also inherently scalable.

However, it is procedurally less rigorous than cross-certification and places a potential burden on the relying party, who may not be aware of the full consequences of accepting a certificate (see Reference [11]).

To summarize, in cross-recognition, the decision of whether to trust a foreign certificate lies with the relying party and not with the CA.

9.2.5 Option 4 — Cross-certification

Cross-certification moves trust decisions to agreements between certification authorities. Technical protocols then enforce these agreements and provide interoperability. This model is more difficult to achieve than options 1, 2, or 3, but is more transparent to the user and, hence, easier to support from the end user's perspective. It also means the end user may not need to assume the responsibility for making the trust decision, as it can be left to the CA for that end-user's CA domain.

Cross-certification results in a bilateral approach, with two domains (in whole or in part) being merged into one larger domain through an elaborate process carried out by two representative CAs. For hierarchical CAs, the representative CA is usually the root CA. However, cross-certification can also be implemented between any two CAs. In the latter case, each domain constitutes only one CA and its subscribers. For cross-certification to be possible, there shall be compatibility at the application level, the policy level, and the technical level. When this occurs, for the relying party in the CA domains covered by cross-certification, the movement of information is transparent and the CAs are responsible for decisions about trust.

The process of cross-certification requires detailed mapping of the respective policies of each CA and the effort in doing this will increase geometrically with each CA domain that is to be included in the collective domain. This raises issues of scalability. There is also a risk that a third CA may cross-certify with the second CA but find the first CA's policy inappropriate. In a situation like that, CA-3 cannot exclude CA-1. As a result, cross-certification is more relevant for relatively closed healthcare models and, at best, open but bounded systems. It is most suitable if the two domains belong to two work contexts that share a close working relationship with each other. For example, both work domains may share the set of applications and services, e.g. electronic mail and financial applications (see Reference [11]).

To summarize, in cross-certification, the decision of whether to trust a foreign certificate lies with the CA.

9.2.6 Option 5 — Bridge CA

The bridge CA model depends upon all the CAs within the potential community of CA domains agreeing to a common set of minimum standards. These minimum standards are then incorporated into their own CP and CPSs. The difference between this and the cross-certification model is that individual CAs may have their own local requirements in addition to the shared minimum standards. These local requirements are not required for bridge certificates from relying parties who are not in that local CA domain. This model works best where CAs have a considerable common interest and are prepared to allow some local variations, for example in the case of cross-certification between state or provincial health authorities within a country.

In this model, organizations can build their own CAs and decide later whether to join a bridge CA or not.

To summarize, in the bridge CA model, the decision of whether to trust a foreign certificate lies with the CA and not with the relying party.

9.3 Option usage

This document recognizes that differences in administrative arrangements and policies exist between jurisdictions. As a result, any of the above options may be acceptable. Whatever option is chosen, the use of this document in its application will be beneficial.

To enable maximum flexibility, ISO 17090-2 specifies profiles for bridge certificates and fields in CA certificates for the CA's audit status and auditor's accreditation, which will support cross-recognition.

Annex A
(informative)

Scenarios for the use of digital certificates in healthcare

A.1   Introduction

The following series of high-level business cases or "scenarios" represents core business and technical requirements for digital certificate solutions that will support a broad cross-section of the healthcare industry.

General requirements are presented first, relating to basic privacy and security principles, together with fundamental needs of the healthcare industry. Each scenario gives

— a description of the scenario or healthcare situation requiring secure, private electronic communications, and

— the business and technical requirements fulfilled by a digital certificate solution.

A.2   Scenario explanation

The care scenarios described in A.3 show how digital certificates can be used in healthcare. Each scenario is intended to:

— be policy driven: the scenarios are intended to show how digital certificates can meet the requirements of the healthcare industry to implement international, national, and local requirements to ensure that information which serves to provide healthcare to individuals and communities is used for the purposes for which it is intended;

— be applicable across healthcare: with the dispersed nature of healthcare across the world, together with the range of different persons and organizations that will need to actively cooperate to provide seamless healthcare, it is essential that any implementation of digital certificates be able to operate across different healthcare settings, including hospital and community-based care, and public and private sectors;

— be technology neutral: one of the essential purposes of developing a digital certificate standard for the healthcare industry is to ensure that information can be securely passed between providers, consumers, insurers, and other relevant parties, without regard to the vendor, hardware, operating system, or applications they are running;

— satisfy current and emerging privacy requirements: if electronic health applications are to become widely used, they need to be trusted by providers and patients. Privacy and security concerns need to be addressed to develop this trust;

— be user-friendly: the security services provided by digital certificates should not interfere with the authorized function of the healthcare organization or professional. If the daily operation of a security system becomes too onerous, clinicians will try to bypass it or will not adhere adequately enough to the management procedures. If this occurs, there will be significant risk of a security breach.

A.3   Services exemplified in healthcare scenarios

Healthcare services and scenarios are given in Table A.1.

Table A.1 — Healthcare services and scenarios

Service	Scenario number															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Authentication	X		X	X	X	X	X	X	X	X	X	X	X	X	X	
Confidentiality	X		X			X	X	X	X	X	X		X			
Integrity		X		X	X		X	X						X		
Digital signature		X		X	X			X			X	X	X	X	X	X

Key to scenarios

1 ER access to records

2 Temporary services (emergency aid)

3 Enrol new member

4 Tele-imaging

5 Automated results reporting

6 Results reporting/Practitioner messaging

7 Patient-physician treatment discussion

8 Patient care registry summary

9 Patient-pharmacist question

10 Patient-pharmacist messaging

11 Remote access to clinical info system

12 Emergency access

13 Remote transcription

14 Electronic transcription

15 Authenticate physician order

16 Potential uses of digital signatures in healthcare

A.4   Scenario descriptions

A.4.1   Emergency department access to records

Scenario description:	A patient, visiting from another country, is brought into an emergency department (ED). The patient is unable to answer questions coherently and a medical history cannot be reliably obtained. His/her health insurance provider membership card is in his/her wallet and positive identification is provided by his/her passport.
Without digital certificates:	From the information on the health insurance provider card, the attending ED physician attempts an international call to the health insurance provider. Because of time zone differences, the physician is asked to call back when the administrative office is open. The physician treats the patient's symptoms. The cause of the patient's incoherence is unknown.
With digital certificates:	From the information on the health insurance provider card, the attending ED physician accesses the patient's health insurance provider site over the Internet and presents his/her digital certificate identifying himself/herself in his/her current role as an ED physician. The health insurance provider web service validates the electronic credential by verifying the digital signature and checking that the certificate is not expired or revoked. Because this credential is validated and follows existing standards, it is accepted by the health insurance provider's web service and access to the patient's chart is granted. An audit record documenting access is created with date, time, attending physician's full name, and medical licence number, and identification of the ED facility. The physician learns from the medical history, allergies, and current medications that the patient has had a recent change in one of his/her prescriptions that may have produced an adverse reaction. After treating the patient, the ED physician sends a digitally signed and enciphered copy of the ED visit to the health insurance provider, which places it in the patient's electronic health record, indicating the symptoms, diagnosis, treatment, and disposition.

A.4.2   Temporary services (emergency aid)

Scenario description:	A major earthquake causes extensive damage in a large metropolitan area. Local hospitals and clinics are themselves damaged, and there are catastrophic numbers of deaths and injuries. National health resources are unable to deal with the conditions and international offers of aid are accepted.
Without digital certificates:	It is not possible to immediately verify the qualifications and practice licences of the health professionals offering help. It is also not possible to ensure that early offers of help are not later denied.
With digital certificates:	The offers of help from health professionals are immediately validated by reading their attached digital certificates. The messages of help are not able to be repudiated because they have been digitally signed by the private key of those offering help.

A.4.3 Member enrolment

Scenario description:	In preparing for a stay of six to 12 months in another country, a head of the household arranges for health insurance coverage.
	A prospective member, Mr. Charles, wishes to enrol in a health insurance plan. He accesses the insurance company's home page that contains membership enrolment forms. He completes the form and sends it to the enrolment department's mailbox. The form is validated and forwarded to medical review. Medical review makes an appointment for the prospective member to undergo a physical examination and notifies him by letter. The prospective member keeps the appointment and the physician determines that he is acceptable for membership. The physician notifies medical review and this information is transmitted back to membership enrolment. Membership enrolment sends Mr. Charles a contract under which he agrees to have his monthly dues deducted from a checking account. Membership enrolment accepts the new member and sends instructions for obtaining his photo identity health card. As part of the membership process, the prospective member has to show a driver's licence or other recognized photo identity. When Mr. Charles receives his new photo identity health card, he also receives instructions for downloading a digital certificate from the health insurance plan.
Without digital certificates:	It is not possible for the new member to reliably identify himself to the physician, nor for the physician to identify himself to the patient. Although there are other means of enciphering messages sent between the two, the combination of authenticity and confidentiality is not possible.
With digital certificates:	Using the newly issued digital certificate, Mr. Charles is able to access member services over the web, including some of his personal health data, and to exchange secure electronic mails with his physician. A digital signature certificate would also give Mr. Charles the ability to directly grant access to his patient records to other providers (a healthcare provider seen while travelling away from home, say).

A.4.4 Tele-imaging

Scenario description:

A physician tele-imaging specialist interprets an angiogram series by viewing it on a PC and creating a text version of the analysis. The specialist has a heavy workload (10 to 15 cases per day) and prefers to do some of it at home. At home, the physician accesses the imaging server over the Internet, using his/her digital certificate to authenticate himself/herself, and downloads the images. While viewing the images on his/her workstation, the physician also accesses the healthcare institution's clinical information system over the Internet to review other medical information on the patient. The physician is confident the image is correct because the application includes an integrity checking function, through use of a hashing algorithm, which verifies the integrity of the message. The physician enters the findings he/she sees on the images into an imaging report and has the option of electronically signing his/her reports remotely.

Without digital certificates:

The physician is not able to authenticate himself/herself to the hospital to the same level of confidence as with a digital certificate, which means the acceptance of an element of risk on the part of the hospital that they may be downloading images to an impostor. The physician's electronically transmitted opinions and findings are also open to the same risk. The physician can also not be sure that the downloaded image has not suffered some transmission error or intentional alteration.

With digital certificates:

The physician can authenticate himself/herself to the hospital to a level of confidence that will be acceptable to a court of law. The physician can be confident that the image downloaded to him/her is correct and he/she will not make his/her findings on an inaccurate image. The hospital can also rely on the physician's digital signature to verify that he/she did send the report.

A.4.5 Automated results reporting to the physician

Scenario description:

On Tuesday, a patient goes to the laboratory and has some blood drawn. When the result is ready, the system automatically generates a message to the physician, telling him/her that his/her results are ready. On Thursday, the physician logs onto the healthcare delivery organization's website with his/her health worker ID and PIN, sees that there is a message waiting, and goes into his/her in-basket. There, he/she finds a message with the subject "Cholesterol Test." The message tells the physician that his/her patient's cholesterol level is 220 and this puts the patient in the moderate risk category. The physician discusses the result with the patient and suggests the patient contact the lipid management team to learn how to reduce his/her cholesterol through diet and exercise. The physician also recommends a follow-up repeat cholesterol test and office visit in six months' time. The patient requests the physician to add the result to the patient's Internet-based electronic medical record. The patient's website contains several links for additional information. One link leads to information about the cholesterol test itself, a second connects to the lipid management team appointment scheduling function, and another link leads to personal diet recommendations based on current clinical protocols, which have been drawn from a variety of data about the patient (e.g. age). The diet recommendations contain further links to a behaviour-change support application that helps him/her create and track his/her diet over the next six months.

Without digital certificates:

The laboratory cannot be sure that the physician has received the message. There is no guarantee that the message has not been read or altered.

With digital certificates:

A digital signature will ensure the physician that the message has indeed come from the laboratory and that the links given to the patient for managing the cholesterol issue are valid. A digitally signed acknowledgement of the message will provide proof that the physician has indeed received the message.

A.4.6 Results reporting with practitioner messaging

Scenario description:

During a routine doctor's surgery visit, a physician orders a cell blood count (CBC) for his/her patient. After asking the patient about his/her preference, the physician checks a box on the order screen, indicating that the results should be sent to the patient via the Internet after the physician has viewed them and had a chance to comment.

The results come back mostly normal, with one result slightly high. The physician knows that this is of no concern for the patient, so he/she types a quick note to that effect and attaches it to the result record.

Later that day, the patient gets a generic notice in her electronic mail box that a message from his/her doctor is waiting for him/her on the secure website. He/she clicks the embedded URL, enters his/her medical record number and password, and reads both the laboratory result and the message from his/her physician. The website has automatically determined that this is a CBC result and displays a link to the health encyclopaedia section that contains a lay person's description of the CBC and its results.

Without digital certificates:

Without the ability to confidently authenticate the electronic mail from the laboratory or the physician, or to ensure that it is transmitted in an enciphered secure form, the patient receives the result by post, notices the slightly high reading for one result, and telephones the physician for further information. The physician is with another patient and cannot be disturbed, while the patient with the blood test has an important meeting to attend. They finally connect, but not without a few days of anxiety on behalf of the patient and a number of unsuccessful telephone calls by the physician.

With digital certificates:

The results are rapidly conveyed to the patient in a verified, secure manner. The patient is able to read the physician's explanatory electronic mail and access the websites for more information and his/her anxiety is quickly eased, without requiring the telephone conversation.

A.4.7 Patient-physician treatment discussion

Scenario description:	A member covered by a health insurance plan has a question about his/her treatment plan. He/she logs onto his/her physician's website, using a trusted digital certificate for authentication, fills out a message form, and clicks "Send" to initiate the conversation:

Hi, Dr. C.

Yesterday you told me to change the dressing on my wound. But I can't remember how often you want me to change the dressing. You said something about not changing it as often as normal, but I don't remember if you said to change it once a week or what. Also, I forgot to ask you — how much of a scar do you think it will leave?

Within a couple of hours, an advice nurse at the call centre reviews the patient's message and determines that it is non-urgent and that it should be responded to by a member of his/her primary care team. Shortly thereafter, the message appears on the computer screen of the patient's primary care physician, who types in a response and digitally signs the message. The next morning, the patient logs onto his/her physician's website again and reads the message:

Hi, [Patient Name].

For the next couple of weeks, only change the dressing every 4 or 5 days, unless it becomes wet, in which case you should change it right away. After that, you'll be seeing me again and we can decide where to go from there. In terms of a scar, I think you'll always have a bit of a scar there, but it won't be very strong — just a little bit of a line.

Without digital certificates:	The absence of a reliable authentication technique means the healthcare organization the physician works for is unable to verify that [Patient Name] is the person sending the electronic mail, and it may be someone else seeking free advice. The patient can also not be certain that the reply from the physician did in fact come from him/her, nor can it be certain that the exchange has not been intercepted and read by a third party.
With digital certificates:	The health insurance organization and the physician can be confident that they are securely communicating with a known and valid member of one of their health insurance plans. The patient can be confident that his/her physician did address his/her inquiry and that it is in fact him/her who is replying to him/her.

A.4.8 Patient care registry summary

Scenario description:

The diabetes risk registry gathers clinical data from a variety of clinical information systems in the healthcare delivery organization about a patient with diabetes. Clinical guidelines built into the registry enable the generation of a personal report summarizing the patient's condition, history, risks, and the next steps. This summary report, after review by the physician, is presented to the patient via the organization's website. The patient authenticates to the website using a digital certificate issued by the healthcare delivery organization's CA. When the patient views the summary, hypertext links embedded in the report enable him/her to easily view relevant educational information (e.g. class schedules, descriptions of tests, patient education), to request a non-urgent appointment, or to send a message to a clinician. The system provides assurance that the patient has accessed the report.

Without digital certificates:

There cannot be a sufficient level of confidence for the patient that the website is really the website of the diabetes risk registry and that the communication with the registry is confidential. It is also not possible for the registry to be certain that the patient has accessed the site and received the information.

With digital certificates:

Digital certificates enable the patient and the registry to authenticate each other and to conduct confidential communication, and the registry can be certain that the patient has accessed the site and received the information.

A.4.9 Patient-pharmacist question

Scenario description:

A health insurance plan member's seven-year-old daughter has asthma. The paediatrician recently prescribed cromolyn for her, but the member cannot tell when the inhaler is empty and when it is full. He/she goes to his/her healthcare organization's website looking for information about this but is still confused, and so sends a question to the on-line pharmacist asking how to tell when an inhaler is empty.

The on-line pharmacist uses electronic mail with access to a healthcare digital certificate directory, where the member's digital certificate is stored, and sends an enciphered message, using a template designed for this question, adding a few personal lines and a phone number to call if there are still questions.

Without digital certificates:

It is not possible for the pharmacist to authenticate the health insurance plan member to the required level of confidence. It is possible to send a secure message but it cannot be authenticated.

With digital certificates:

It is possible to authenticate the member and send him/her an enciphered message. The member can be confident that it came from the pharmacist.

A.4.10 Patient-physician messaging, unstructured to specific clinician

Scenario description:

A patient has a rash and sees a dermatologist, who prescribes a cream. The dermatologist tells the patient that if the rash has not cleared up in three weeks, he/she should let him/her know so that he/she can prescribe a different medication.

Three weeks later, the rash still looks very much the same, so the patient logs onto the group practice website, using his/her healthcare digital certificate to authenticate himself/herself. The patient sends a secure, unstructured message to the physician:

I've been using that cream for 3 weeks now, and it hasn't gotten any better. What should I do now?

The physician writes a new prescription and tells the patient he/she can pick up the new cream either by coming into the pharmacy or by ordering it on-line.

When the patient reads the message from the dermatologist on the secure website, he/she simply clicks to the on-line pharmacy section and orders the cream to be shipped to his/her home.

Without digital certificates:

The physician is not able to authenticate the patient to a high enough level of confidence to give advice by electronic mail on treating the condition.

With digital certificates:

The physician and patient can authenticate themselves to each other and the pharmacist. Confidential messages can be exchanged and a new type of cream can be ordered with the pharmacist. All parties are confident that they did send the messages they claimed to have sent.