INTERNATIONAL STANDARD

ISO 17090-5

First edition
2017-07

Health informatics — Public key infrastructure —

Part 5: Authentication using Healthcare PKI credentials

Informatique de santé — Infrastructure de clé publique —
Partie 5: Authentification à l'aide des identifiants ICP de la santé

Reference number
ISO 17090-5:2017(E)

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

Contents

Page

Foreword

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

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

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

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

For an explanation on the 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 the following URL: www.iso.org/iso/foreword.html.

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

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

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 to support these rapid international developments. While underlying security standards address methods for verification, requirements for secure verification processes to support healthcare purposes are not defined.

This document describes the procedural requirements validating an entity credential based on Healthcare PKI defined in ISO 17090 series used in healthcare information systems. Although the cryptographic operations used at the authentication processes and the digital signature processes are the same, authentication and signature have different meanings. Systems and software prevent the users from misuse of the private keys and their certificates especially if both keys are on a secure token. This document describes the requirements to mitigate threats and vulnerabilities within the authentication processes with Healthcare PKI credentials.

Health informatics — Public key infrastructure —

Part 5:
Authentication using Healthcare PKI credentials

1 Scope

This document defines the procedural requirements for validating an entity credential based on Healthcare PKI defined in the ISO 17090 series used in healthcare information systems including accessing remote systems. Authorization procedures and protocols are out of scope of this document. The data format of digital signatures is also out of scope of this document.

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

3 Terms and definitions

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

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

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

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

4 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
HPKI	Healthcare Public Key Infrastructure
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PC/SC	Personal Computer/Smart Card
PKCS	Public-Key Cryptography Standards

5 Scope of application

5.1 General

The healthcare information system authenticates healthcare organizations or professionals for access control to healthcare information, such as EHR or PHR.

Inappropriate process in end entity authentication verification may increase the risk of spoofing, impersonation, and many other identity-based attacks. As result, that may cause security incidents leading to critical information leakage and system and data misuse.

This document describes target systems, methods of identification, threats, vulnerabilities and controls of health software which authenticate using PKI based on the ISO 17090 series.

These controls decrease risks of spoofing.

5.2 Target systems

The target systems of this document are as follows:

a) digital signature library with digital signature creation function and digital signature verification function for healthcare application;

b) digital signature creation program and digital signature verification program as stand-alone software or with healthcare application.

Examples of authentication technology to which healthcare PKI can be applied are shown in Annex A.

The following are out of scope:

— healthcare application that does not process digital signature data directly;

— healthcare application that processes digital signature and the result of signature verification with digital signature library, specific digital signature program or specific digital signature verification program;

— application interface and user interface within client environment;

— cryptographic library layer, e.g. CSP or PKCS#11, and any subsequent token access layers as depicted in Figure 1.

Figure 1 illustrates an example of software layers for web-based applications. A digital signature based application may have the same structure. According to ISO 17090-3, it is assumed that "Storage modules of the end entity subscriber private key shall conform to standards of levels equal to or higher than US FIPS 140-2 level 1." Therefore, in addition to the smart card, as illustrated in Figure 1, a system may use other tokens, such as a USB token or a software token, for the storage modules of the private key.

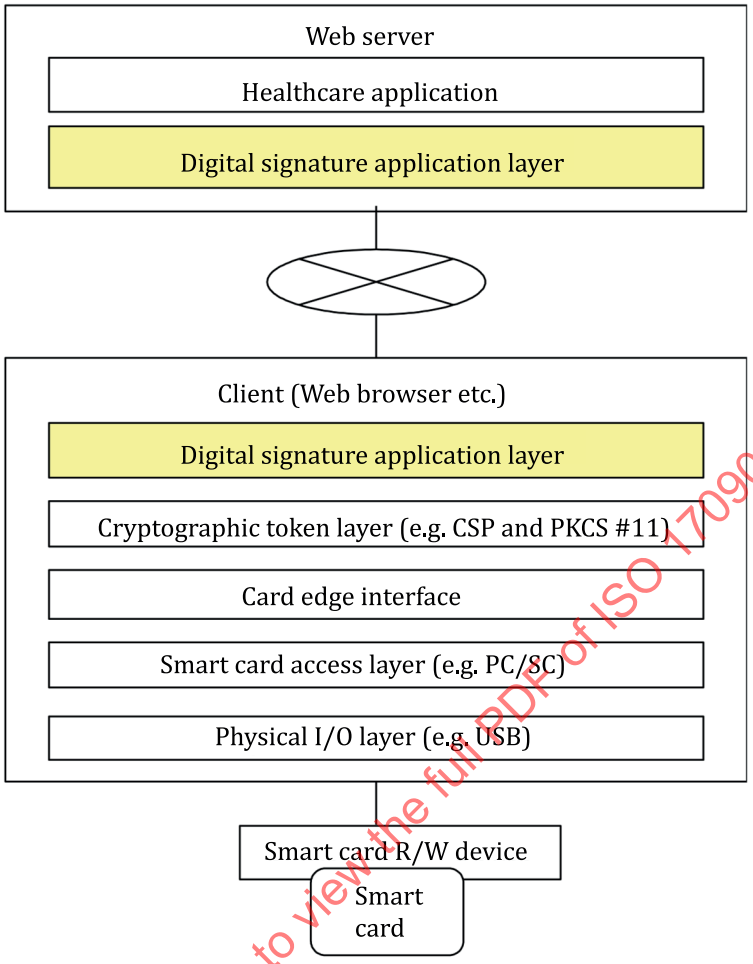

Figure 1 — Example of processing layer

5.3 Phases of method identification

The authentication process with Healthcare Public Key Infrastructure (HPKI) is composed of three phases as shown in Figure 2: (1) the preparation phase, (2) the configuration phase, (3) and the authentication phase.

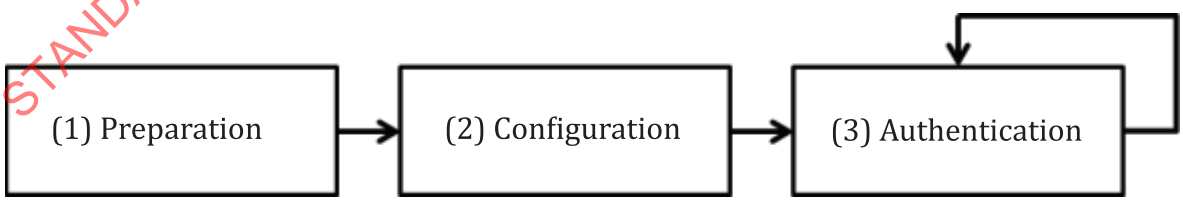

Figure 2 — Relationship between the three phases of an authentication process with HPKI

Following the preparation phase, go through the configuration phase and proceed to the authentication phase. After that, the authentication phase is repeated.

(1) Preparation phase

The preparation phase is composed of two steps (see Figure 3):

(1-1): Certificate Authority creates a certificate for public key corresponding with the subscriber's private key stored on the secure token (smart card, etc.) as credential. (Requirement for smart token that has to conform with FIPS 140-2 level 1 or more and that requirement is possible for mobile devices. Detail of that is written in ISO 17090-3.).

(1-2): Certificate Authority issues the certificate to the subscriber.

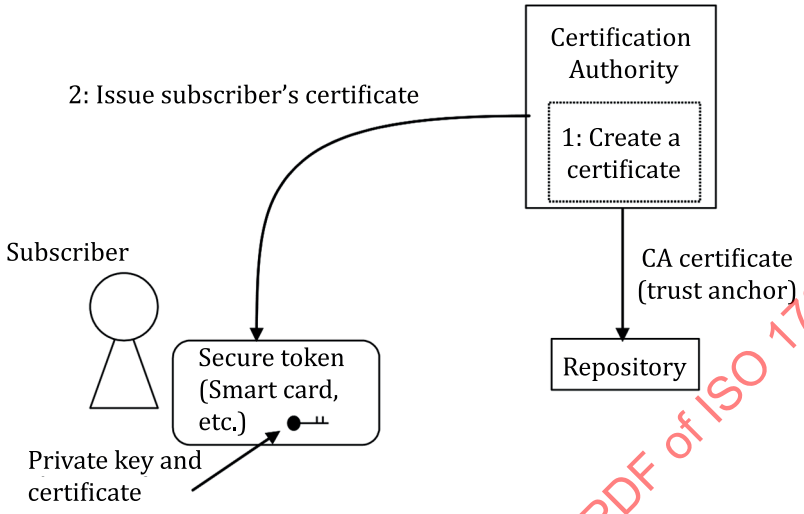

Figure 3 — Preparation phase

The trust anchor of the certificate authority is stored on repository beforehand.

(2) Configuration phase

The configuration phase is composed of two steps (see Figure 4):

(2-1): Server retrieves certificate authority's certificate from trustworthy repository.

(2-2): Server stores the certificate to certificate store as trust anchor.

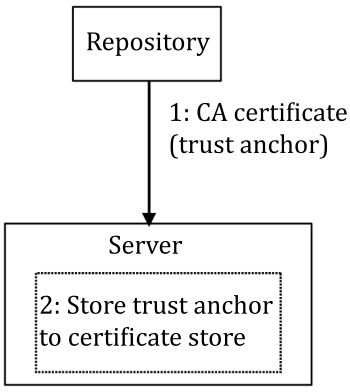

Figure 4 — Configuration phase

(3) Authentication phase

The authentication phase is composed of seven steps (see Figure 5):

(3-1): Client application sends the access request to server.

(3-2): Server generates a random number and sends it to client.

(3-3): Client application signs the random number with subscriber's private key.

(3-4): Client application returns the signed random number (signature) and subscriber's certificate to the server.

(3-5): Server sends a CRL request to repository of Certificate Authority.

(3-6): Repository returns the CRL to server.

(3-7): Server verifies subscriber's certificate and signature with public key in the certificate.

If the authentication process has completed successfully, the certificate is trusted and the user who accesses the server from the client is considered the owner of the certificate. After that, the user is identified by data stored on the certificate.

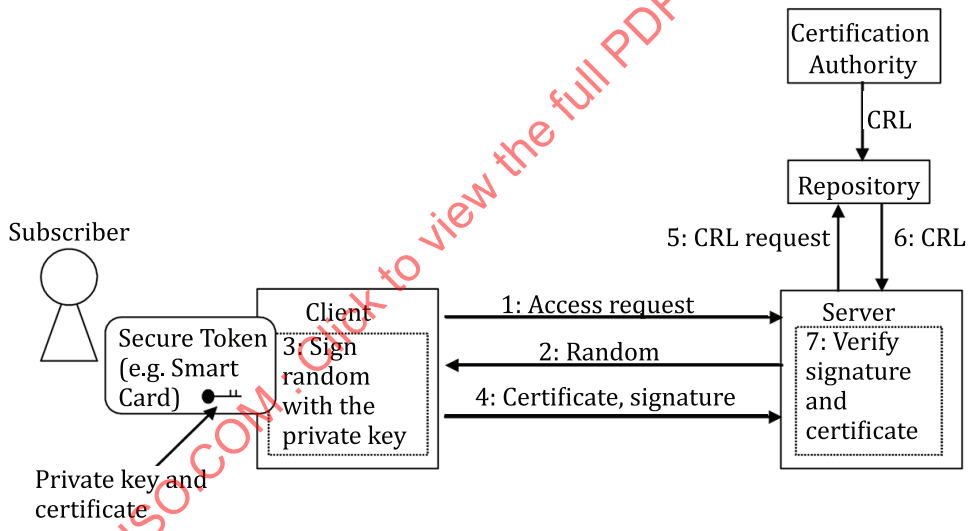

Figure 5 — Authentication phase

5.4 Threats and vulnerabilities

Table 1 shows threats and vulnerabilities assumed in the authentication process with HPKI credentials. Bracketed terms are threats and vulnerabilities. Other sentences are explanation of bracketed terms.

Table 1 — Threats and vulnerabilities related to HPKI credentials

Threats and vulnerabilities	Risk source (Process of 5.3)	Validation type in Table 2
[Identity fraud] By sending a false signature value at authentication, a person who has a false private key accesses a system.	(3) Authentication phase Step (3–3)	Signature value
[Spoofing attack of users] Unauthorized user accesses systems with illegal certificate issued from illegal CA.	(3) Authentication phase Step (3–3)	Trust anchor
[Unauthorized use of revoked key] a) By using own revoked key, a person who has already lost an access right accesses a system. or b) By using another user's revoked key, a person accesses a system as the other user.	(3) Authentication phase Step (3–3)	Revocation status
[Unauthorized use of expired key] a) By using own expired key, a person who has already lost an access right accesses a system. or b) By using another user's expired key, a person accesses a system as the other user.	(3) Authentication phase Step (3–3)	Validity date
[Malicious usage of certificates for tests (ex. demonstration, or system test)] A legitimate certificate may be distinguished from a certificate for tests in certificate policy.	(3) Authentication phase Step (3–3)	Key usage extension

6 Validation procedures for HPKI credentials

The server shall prevent users holding invalid credentials from accessing sensitive health data. For this reason, a HPKI credential shall be correctly verified. The validation procedure for HPKI credentials is composed of five validation elements, which are verification of signature value, trust anchor, revocation status, validity period, and key usage extension. Table 2 shows validation elements and their requirements.

The validation elements may not work correctly. For example, the CRL may not be updated because of communication failures. The administrator of the server should prepare alternative rules for irregular cases.

Table 2 — Requirements for validation procedures

Validation element	Threat	Validation requirement	Step in 0
Signature value	Identity fraud By sending a false signature value at authentication, a person who has a false private key accesses a system.	A signature value shall be verified by using a public key included in a user's certificate.	(3) Authentication Phase Step (3–7)
Trust anchor	Spoofing attack of users Unauthorized user accesses systems with illegal certificate issued from illegal CA.	The trust anchors shall be verified in certification path-building processes. Without using the trust anchor set installed in OS or applications beforehand, only a necessary trust anchor should be set.	(3) Authentication Phase Step (3–7) (2) Configuration Phase Step (2–2)
Revocation status	Unauthorized use of revoked key a) By using own revoked key, a person who has already lost an access right accesses a system. b) By using another user's revoked key, a person accesses a system as the other user.	Revocation status of user's certificate shall be confirmed by revocation information obtained from a certification authority or a related authority (ex. CRL distribution point, OCSP responder) It shall be verified that revocation information is signed by a certification authority (or a related authority) The latest revocation information shall be used. If an authentication system uses a cached copy of revocation information, it is desirable to keep cached revocation information fresh by using "nextUpdate" of revocation information, etc.	(3) Authentication Phase Step (3–7) (3) Authentication Phase Step (3–7) (3) Authentication Phase Step (3–7)

Table 2 *(continued)*

Validation element	Threat	Validation requirement	Step in 0
Validity date	Unauthorized use of expired key a) By using own expired key, a person who has already lost an access right accesses a system. b) By using another user's expired key, a person accesses a system as the other user.	Validity date of a user's certificate shall be confirmed. Time on a system validating a user's certificate shall be maintained by trusted time source (ex. NTP server, etc.)	(3) Authentication Phase Step (3–7) (3) Authentication Phase Step (3–7)
Key usage extension	None NOTE There is no threat on the server side. But there is a possibility that users may misuse his/her certificate for digital signatures in authentication process (see Annex B).	None	(3) Authentication Phase Step (3–7)
Certificate policy	Malicious usage of certificates for tests (ex. demonstration, or system test) A legitimate certificate may be distinguished from a certificate for tests in certificate policy.	Certificate policy OID shall be checked, besides trust anchor check.	(3) Authentication Phase Step (3–7)

Annex A
(informative)

Examples of authentication technology with available X.509 certification as credentials

A.1 TLS

TLS (transport layer security) protocol is used to provide communication security over a computer network. It implements functions such as authentication, encryption and tamper detection, between transport layer and application layer of a network. TLS 1.2 is defined in IETF RFC 5246. A typical usage of TLS which provides secure communication is HTTPS. Based on the TLS handshake protocol, the server requests a X.509 certificate and signed data to the client. The server verifies the returned certificate and signed data in order to make sure of the legitimateness of the client. Then, the server establishes a connection to the client. It can be used as a client authentication method of website.

A.2 SAML

SAML (security assertion markup language), defined by the Security Services Technical Committee of the Organization for the Advancement of Structured Information Standards (OASIS), is an XML-based framework for the secure exchange of authentication information. By sending and receiving the message for sharing SAML Assertion (XML-based authentication information), via HTTP or SOAP, it is possible to implement SSO (single sign-on) to transmit authorization, authentication and attribute information, between the authentication server and application. Because SAML does not specify the authentication method, it can use any authentication method such as using an ID and password, biometrics or a X.509 certificate.

A.3 Kerberos

Kerberos, defined in IETF RFC 4120/4121, provides the functions of user authentication and network route encryption using common key cryptography. It is possible to implement SSO, by using the ticket issued by a KDC (key distribution center) which contains information of the authentication server and ticket-granting service. Because Kerberos does not specify the authentication method, it can use any authentication method such as using an ID and password, biometrics or a X.509 certificate.

A.4 WS-Security

WS-Security (web service security), published by OASIS, defines how to store the authentication and authorization information and tokens in SOAP message header. The message receiver is capable of performing authentication and authorization. Because the WS-Security does not specify the authentication method, it is possible to use a X.509 certificate as credentials.

A.5 OpenID

OpenID is a decentralized authentication service that has been developed by the OpenID Foundation working group. It allows users to easily use multiple websites after the user is authenticated by any OpenID service. Because the OpenID does not specify the authentication method, it is possible to use a X.509 certificate as a credentials.

Annex B
(informative)

Appropriate use of authentication certificates

B.1 General

Although the cryptographic operations used at the authentication process and the digital signature process, which is the calculation with a private key, are the same, authentication and signature have different meanings, and even the certificates and their contents are different if issued to an entity. Systems and software shall prevent the users from misuse of the private keys and their certificates especially if both keys are on a secure token or smart card. This annex shows why two private keys should not be used in wrong contexts and how to prevent misuse.

B.2 Necessity for proper use

Authentication and signature have quite different meanings. In the authentication process, PKI is used for confirming that the accessing person is the right person for accessing the system by the signed value. On the other hand, PKI is used for confirming whether the subscriber is responsible for the signed medical record or document by the signed value in the signature process or not. If the user uses his/her signature key and certificate at authentication, he/she may have following risks.

Generally speaking, a challenge and response mechanism is used at authentication processing. In a simple challenge and response mechanism, the client software signs to the given challenge (random number) that is an authentication subject and returns the signed value and certificate to the server. The server verifies the authentication subject and determines his/her identity and authenticity. Figure B.1 illustrates this procedure.

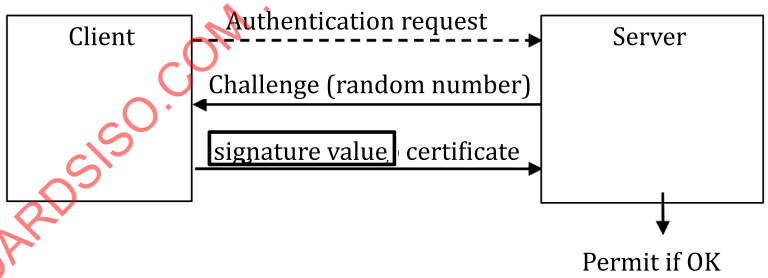

Figure B.1 — Authentication procedure in a simple challenge and response mechanism

Think about the case, a malicious server sends to the client a hash value of a document. The client application does not distinguish a random number for challenge and a hash value of a document, and may return the signed value and the certificate. If the certificate is for digital signature, the malicious server will easily get the digital signature in the document. As the result, the user is responsible with the document, which may be IOU. Figure B.2 illustrates the process.