INTERNATIONAL STANDARD

ISO 17090-4

First edition
2014-10-01

Health informatics — Public key infrastructure —

Part 4: Digital Signatures for healthcare documents

Informatique de la santé — Infrastructure clé publique —

Partie 4: Signatures numériques pour les documents des soins médicaux

Reference number
ISO 17090-4:2014(E)

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

Published in Switzerland

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

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

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

— *Part 1: Overview of digital certificate services*

— *Part 2: Certificate profile*

— *Part 3: Policy management of certification authority*

— *Part 4: Digital Signatures for healthcare documents*

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 be 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 International Standard seeks to address the need for guidance to support these rapid international developments.

This International Standard describes the common technical, operational, and policy requirements that need to be addressed to enable digital certificates to be used in protecting the exchange of healthcare information within a single domain, between domains, and across jurisdictional boundaries. Its purpose is to create a platform for global interoperability. It specifically supports digital-certificate-enabled communication across borders but could also provide guidance for 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 International Standard can be approached as a whole, with the four parts all making a contribution to defining how digital certificates can be used to provide security services in the healthcare industry, including authentication, confidentiality, data integrity, and the technical capacity to support the quality of digital signature.

ISO 17090-4 provides healthcare-specific profiles of digital signature based on the ETSI Standard and the profile of the ETSI Standard specified in CAdES and XAdES.

Health informatics — Public key infrastructure —

Part 4:
Digital Signatures for healthcare documents

1 Scope

This part of ISO 17090 supports interchangeability of digital signatures and the prevention of incorrect or illegal digital signatures by providing minimum requirements and formats for generating and verifying digital signatures and related certificates.

Furthermore, it defines the provable compliance with a PKI policy necessary in the domain of healthcare. This part of ISO 17090 adopts long-term signature formats to ensure integrity and non-repudiation in long-term electronic preservation of healthcare information.

This part of ISO 17090 conforms to ISO/ETSI standards for long-term signature formats to improve and guarantee interoperability in the healthcare field.

There is no limitation regarding the data format and the subject for which the signature is created.

2 Normative references

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

ISO 17090-1:2008, *Health informatics — Public key infrastructure — Part 1: Overview of digital certificate services*

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

3 Terms and definition

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

3.1
certification path
connection of a series of certificates binding the certificate which is to be validated to a trusted root trust anchor

3.2
certification path validation
path to be validated to a trusted root trust anchor including revocation checking

3.3
hash function
computation method used to generate a random value of fixed length from the data of any optional length

Note 1 to entry: The generated value is called a “hash value”, which has the properties of being uni-directional (the original data cannot be back calculated from it) and of having a low probability of having been generated from two different data (collision).