FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/FDIS
17090-4**

ISO/TC **215**

Secretariat: ANSI

Voting begins on:
2020-06-19

Voting terminates on:
2020-08-14

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/4a6e2708-140c-4a67-abdf-ff9382a19273/iso-fdis-17090-4

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/FDIS 17090-4:2020(E)

© ISO 2020

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/4a6e2708-140c-4a67-abdf-ff9382a19273/iso-fdis-17090-4

COPYRIGHT PROTECTED DOCUMENT

© ISO 2020

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

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO 2020 – All rights reserved

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/catalog/standards/sist/4a6e2708-1a9c-4a6e-abdf-ff9382a19273/so-fdis-17090-4

© ISO 2020 – All rights reserved

Foreword

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

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

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

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

For an explanation 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 second edition cancels and replaces the first edition (ISO 17090-4:2014), which has been technically revised. The main changes compared to the previous edition are as follows:

— update of the reference standard and addition of PAdES definition.

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/4a6e2708-145c-4a07-abdf-f9f82a1c273/iso-fdis-17090-4

 © ISO 2020 – All rights reserved

Introduction

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

Healthcare information concerning individual citizens is commonly interchanged by means of electronic mail, remote database access, electronic data interchange, and other applications. The Internet provides a highly cost-effective and accessible means of interchanging information but 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 that reliable information security services that minimize the risk of unauthorized access be available to the healthcare system.

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 seeks to address this challenge.

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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 might rely on the policies and practices and, by extension, on 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.

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.

The ISO 17090 series, contributes 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 2020 – All rights reserved

This document is in line with 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/4a6e2708-140c-4a67-abdf-ff9382a19273/iso-fdis-17090-4

© ISO 2020 – All rights reserved

Health informatics — Public key infrastructure —

Part 4:
Digital signatures for healthcare documents

1 Scope

This document 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.

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.

It defines the provable compliance with a PKI policy necessary in the domain of healthcare. This document specifies a method of adopting long-term signature formats to ensure integrity and non-repudiation in long-term electronic preservation of healthcare information.

This document provides Healthcare specific PKI (HPKI) profiles of digital signature based on the ETSI Standard and the profile of the ISO/ETSI Standard specified in CAdES, XAdES, and PAdES.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/4a6e2708-1d0d-4a67-abdf-ff9382a1/iso-fdis-17090-4

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 definition

For the purposes of this document, the terms and definitions given in ISO 17090-1 and the following 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
certification path
connection of a series of certificates binding the certificate that 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

© ISO 2020 – All rights reserved

3.3
hash value
value calculated by a hash function, which is a computation method used to generate a random value of fixed length from the data of any optional length

4 Target of application

4.1 Target system

The target systems of this document are as follows:

a) the digital signature library with the digital signature function and the digital signature verification function for the medical treatment application;

b) the digital signature program and the digital signature verification program as the stand-alone software or with the medical treatment application;

The following are out of the scope of application:

a) the medical treatment application that does not process the digital signature data directly;

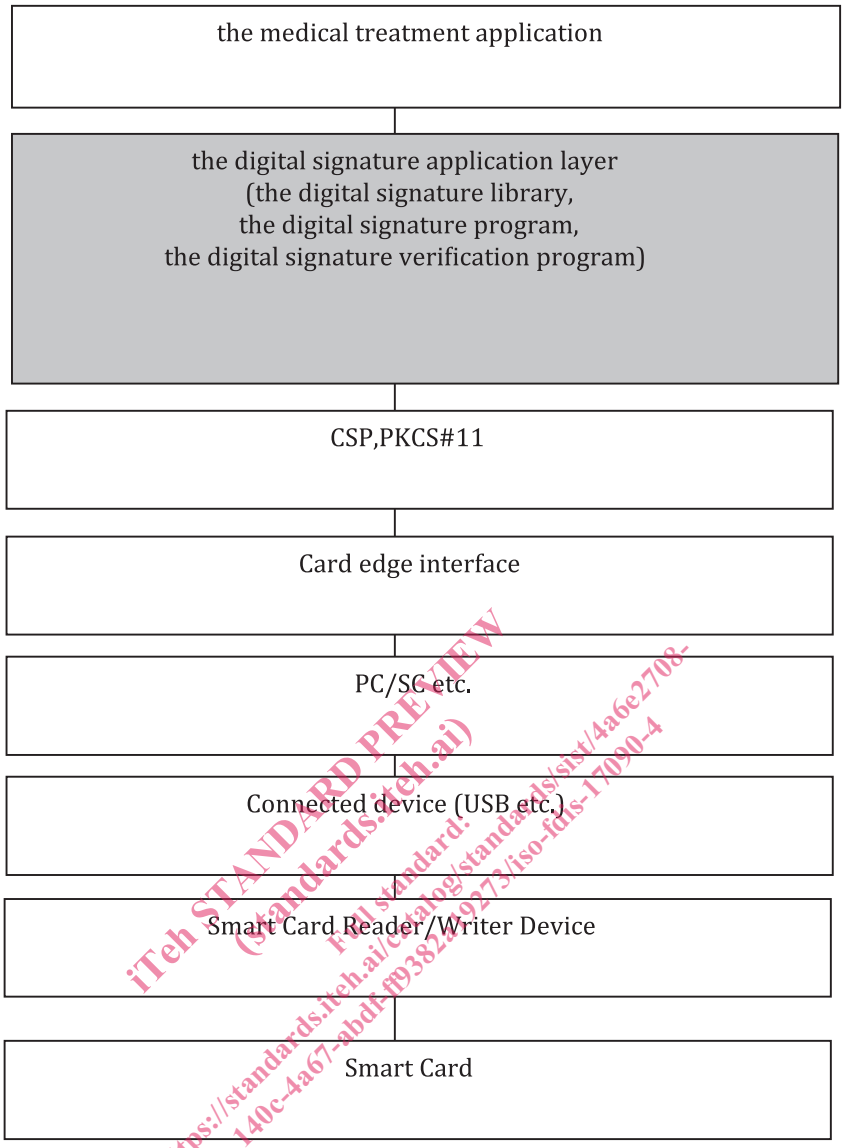
b) the medical treatment application that processes the digital signature and the result of signature verification with the digital signature library, the specific digital signature program, or the specific digital signature verification program;

c) the application interface and user interface; Figure 1 shows an example of the processing layer. The digital signature application layer (the digital signature library, the digital signature program, or the digital signature verification program) is the target scope of this example. Therefore, the following layer, CSP, and PKCS#11, is not within the targeted scope of this document.

In HPKI, it is assumed that storage modules of the end entity subscriber private key conform to standards of levels equal to or higher than US FIPS 140-2 level 1. Also, in addition to the smart card, as illustrated in Figure 1, a system could use a USB token, software token, etc. as the medium that stores the private key.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/4a6e3708-140c-4a67-add8-8982a1f27/iso-fdis-17090-4

 © ISO 2020 – All rights reserved



iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/4a6e2708-140c-4a67-abdf-ff9382a9273/iso-fdis-17090-4

Figure 1 — Example of processing layer digital signature specification

4.2 Generation process

The digital signature format is based on ETSI advanced digital signatures, where CAdES (CMS Advanced Digital Signature)[5] and XAdES (XML Advanced Digital Signature)[6] are described in this document.

These specifications define the various formats according to purpose of operation.

— ES: The format that has the digital signature value, data itself, and information about the signer.

— ES-T: The format that has the signature timestamp in addition to the ES format. Signature timestamp is a trusted timestamp provided by a timestamp authority to prove the existence of the signature.

— ES-C: The format that has validation data references in addition to the ES-T format.

— ES-X: The format that has ES-C timestamp to protect validation data references.

— ES-X Long: The format that has the ES-C format and revocation information for verification.

— ES-A: The format that has an archive timestamp to protect the signature, the timestamps, and the validation data.

© ISO 2020 – All rights reserved

See Figure 2 for the different format types of digital signature.

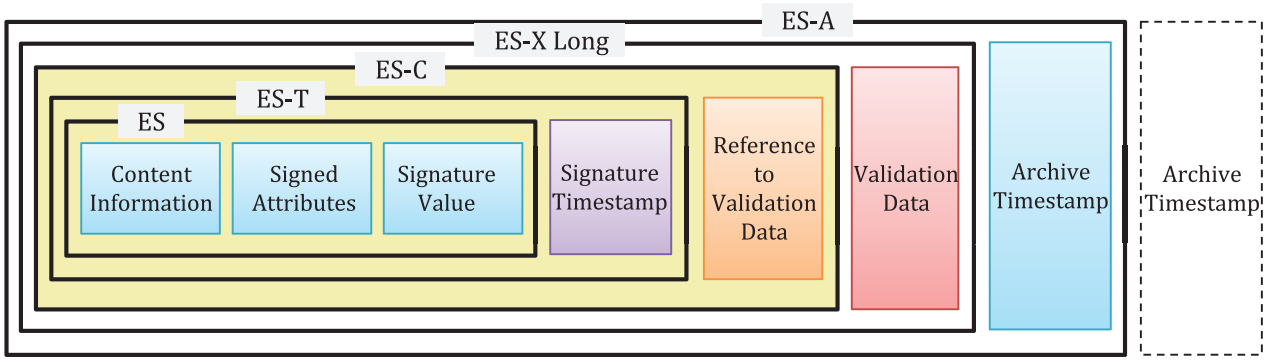


Figure 2 — Format types of digital signature

These specifications only define the profile of ES-T and ES-A. The other formats (ES-C, ES-X, ES-X Long) are considered to be intermediate formats to generate ES-T or ES-A. So they are not included in this document.

The digital signature format is based on ETSI advanced digital signatures, where CAdES[5] based on a CMS (Cryptographic Message Syntax) and XAdES[6] based on an XML Advanced Digital signature are described in this document.

Subclause 4.4 describes the CAdES profile that specifies elements required/allowed to generate ES-T and ES-A. Clause 4.5 describes the XAdES profile of ES-T and ES-A.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/4a6e2...-1406...-ffp382a19273/iso-fdis-17090-4

4.3 Verification process

4.3.1 General

Subclause 4.3 describes an overview of the basic verification processes. This document does not provide verification methods for optional attributes. If the signature data contains any optional attributes, the optional attributes should be correctly verified in accordance with other specifications, policies, or guidelines.

4.3.2 Verification of ES

4.3.2.1 Verification processes of ES

The verification processes of ES are described below, and the order of the processes should not be changed. See Figure 3.

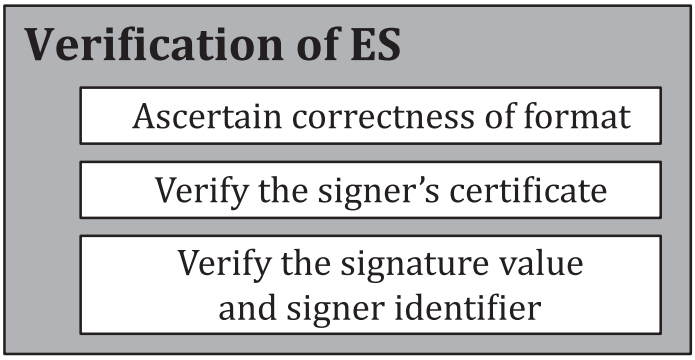


Figure 3 — Verification processes of ES

© ISO 2020 – All rights reserved

a) Verify the format of the signing data.

Verify if the digital signature format is correct.

b) Verify the signer's certificate.

The following steps are performed to ascertain the validity of the signer's certificate.

1) Certification path validation described in RFC5280[10].

2) Verify signer's certificate extensions regarding HPKI as stated in ISO 17090-1

c) Verify the signature value of the signer.

The following steps are performed.

1) Verify the signature value using the signer's public key.

2) Verify the identifier of the signer's certificate.

The above processes are explained in Annex A.

4.3.2.2 Description of verification processes

Verification process	Description
a) Ascertain correctness of format.	The following conditions shall be checked. — If the structure of the signature data conforms to the defined format. — If the signature data contains all elements required in the profile. — If the version number of the signature data are correct.
b) Verify the signer's certificate.	1) Certification path validation described in RFC5280. — Build and verify the certification path for the signer's certificate.
	2) Ascertain extensions regarding HPKI contained in the signer's certificate. — Implementations are required to support functions to check the following elements. — HPKI certificate policy identifier. — The value of the hcRole attribute in the signer's certificate. — The ascertainment method not covered by this document. It is possible to choose suitable methods for applications.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/4a6e2708-140c-4a67-abdf-f3824b9273/iso-fdis-17090-4

© ISO 2020 – All rights reserved