INTERNATIONAL STANDARD

ISO 17090-4

Second edition
2020-10

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 17090-4:2020(E)

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

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 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 definitions.

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 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.

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.

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.

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.

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

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.

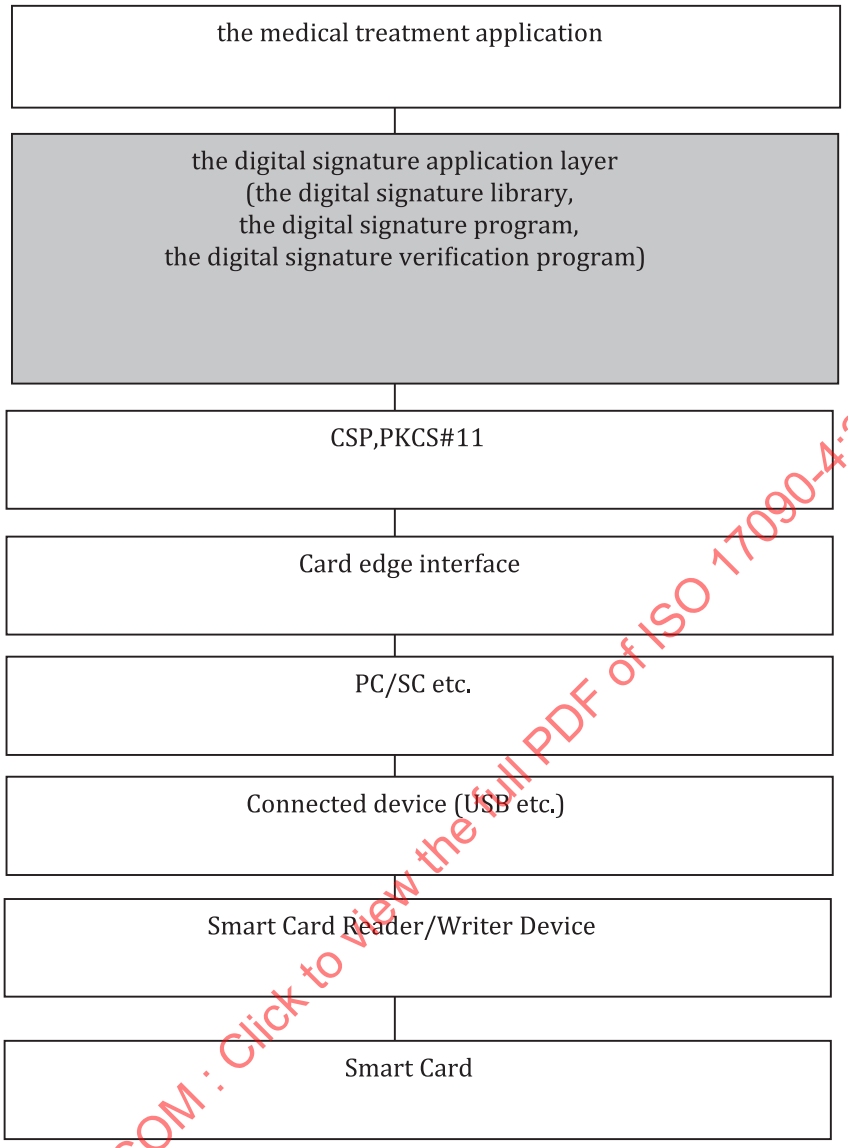

Figure 1 — Example of processing layer digital signature specification

4.2 Generation process

The digital signature format is based on ETSI advanced digital signatures, where CAdES (CMS Advanced Digital Signature)[8] and XAdES (XML Advanced Digital Signature)[9] 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.

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

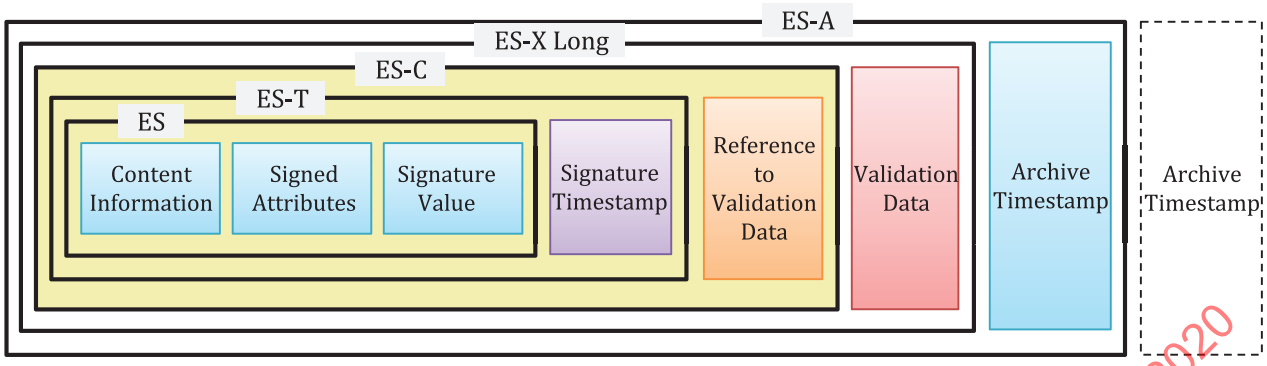

Figure 2 — Format types of digital signature

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[8] based on a CMS (Cryptographic Message Syntax) and XAdES[9] 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. Subclause 4.5 describes the XAdES profile of ES-T and ES-A.

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.

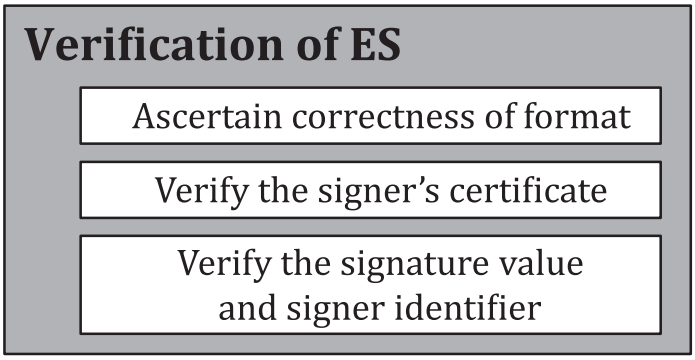

Figure 3 — Verification processes of ES

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 identifier.

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.

Verification process	Description
c) Verify the signature value and signer identifier.	1) Verify the signature value using the signer's public key. The following steps shall be performed. — Calculate the hash value of the content data and ascertain that it matches the value of the message digest contained in the signature. — Verify the signature value with signed attributes using the signer's public key.
	2) Verify the correspondence of the identifier information of the signer's certificate. — Ascertain that the signer identifier matches the signer's certificate attributes contained in the signature data.

4.3.3 Verification of ES-T

4.3.3.1 Verification process of ES-T

This section describes the process to verify a signature in ES-T format.

The verification processes of ES-T are described below, and the order of the processes should not be changed. See Figure 4.

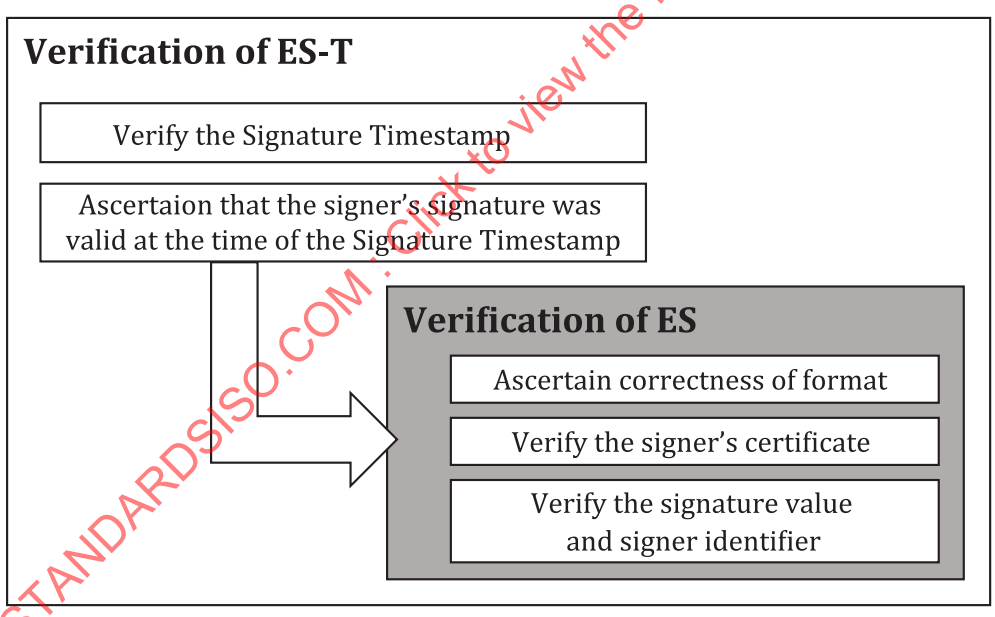

Figure 4 — Verification processes of ES-T

a) Verify the signature timestamp.

   1) Verify the certificate of the TSA that provides the signature timestamp.

   2) Verify the signature value of the TSA that provides the signature timestamp.

   3) Verify the message imprint of the timestamp token.

b) Verify the signer's signature at the time of the signature timestamp.

   1) Ascertain that the signer's signature was valid at the time of the signature timestamp.

2) Ascertain that the signer's trust anchor is appropriate.

The above processes are explained in Annex A.

4.3.3.2 Description of a verification process

Verification process	Description
a) Verify the signature timestamp.	1) Verify the certificate of the TSA that provides the signature timestamp. The following steps shall be performed for the TSA certificate. — Certification path validation as described in RFC5280. — Ascertain that the certificate contains extended key usage for TSA purpose.
	2) Verify the signature of the TSA that provides the signature timestamp. Verify the signature value of the timestamp token using the public key of a TSA certificate.
	3) Verify the message imprint of the timestamp token. — Calculate the hash value of the signer's signature value and ascertain that it matches the value of the message imprint within the timestamp token.
b) Verify the ES at the time of the signature timestamp.	1) Verify the ES at the time of the signature timestamp. — Verify that the certificate of the signer was valid at the time of the signature timestamp.
	2) Verify that the trust anchor is appropriate. — Verification could be performed in a long period of time after the ES-T data were created. The trust anchor that was valid at the time of signature might be expired or compromised at the time of verification. In this case, the verifier shall verify that the trust anchor is appropriate. — For example, the signer and the verifier specify an agreement about the trust anchor (for example, the signature policy) and manage it under protection against CA compromise, or the verifier refers to a trusted third party that manages the history of verification information of certificates. Specific methods are out of the scope of this document.

4.3.4 Verification of ES-A

4.3.4.1 Verification process of ES-A

The verification processes of ES-A are described below, and the order of the processes should not be changed. See Figure 5.

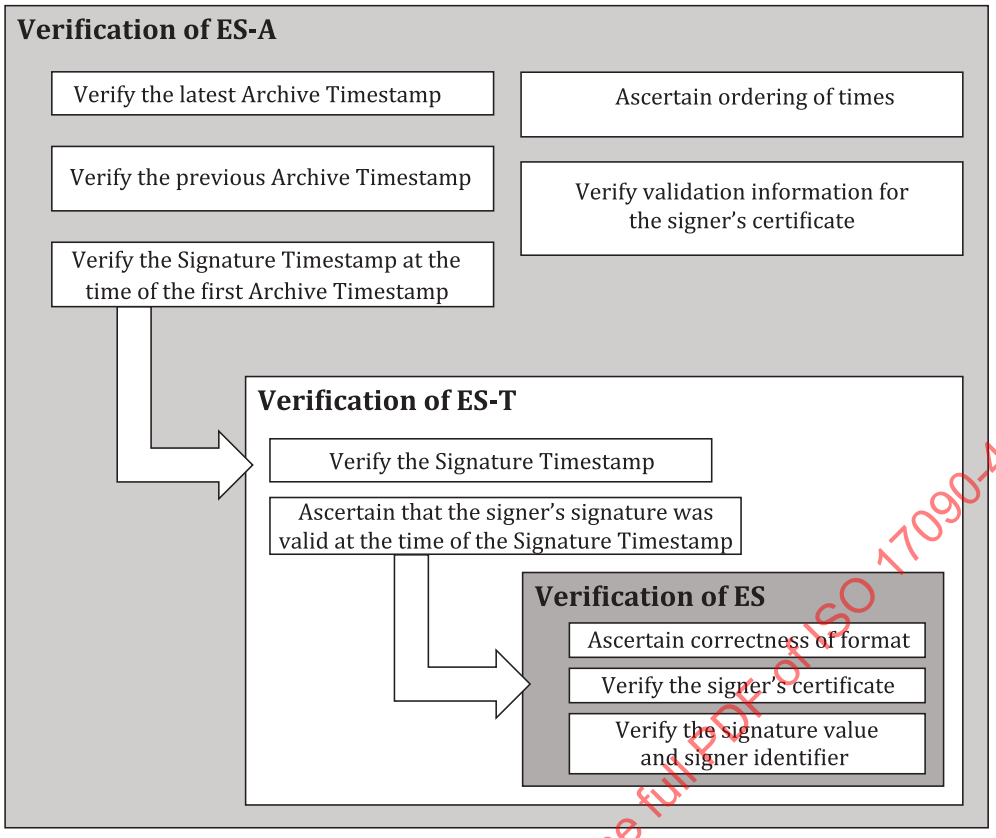

Figure 5 — Verification processes of ES-A

a) Verify the latest archive timestamp.

Verify that the latest archive timestamp is valid at the time of verification.

1) Verify the certificate of the TSA that provides the latest archive timestamp.
2) Verify the signature of the TSA that provides the latest archive timestamp.
3) Verify the correspondence of the latest archive timestamp and the target data of the timestamp.

b) Verify the previous archive timestamps, if present.

Verify that the timestamp was valid at the time when the data was archived.

1) Verify the certificate of the TSA that provides the archive timestamp.
2) Verify the signature of the TSA that provides archive timestamp
3) Verify the correspondence of the archive timestamp and the target data of the timestamp.
4) Verify that the trust anchor of the archive timestamp is appropriate.

c) Verify the validation data of the signer's certificate.

1) Verify the validity of the certificate chain archived in the validation data.
2) Verify that the trust anchor is appropriate.
3) Verify the validity of revoke information archived in the validation data.

4) Verify that the trust anchor of revoke information is appropriate.

d) Verify the signature timestamp.

Verify that the timestamp is appropriate.

1) Verify that the signature timestamp was valid at the time it was archived.

2) Verify that the trust anchor of the signature timestamp is appropriate.

e) Verify the ES at the time of the signature timestamp.

1) Verify that the ES was valid at the time of the signature timestamp.

2) Verify that the trust anchor is appropriate.

f) Verify the ordering of the times of timestamps and the issued time of validation data.

The above processes are explained in Annex A.

4.3.4.2 Description of verification process

Verification process	Description
a) Verify the latest archive timestamp	1) Verify the certificate of the TSA that provided the latest archive timestamp. The following steps shall be performed for the TSA certificate. — Verify the validity of the certificate at the time of verification. — Ascertain that the purpose of the key usage of the TSA certificate is appropriate.
	2) Verify the signature of the TSA that provides the latest signature timestamp. — Verify the signature value of the timestamp token using the public key of the TSA certificate.
	3) Verify the message imprint of the timestamp token. — Calculate the hash value of the target fields for the archive and verify that it matches the value of the message imprint within the timestamp token.

Verification process	Description
b) Verify the previous archive timestamp, if it is present.	1) Verify the certificate of the TSA that provides the archive timestamp. — Verify the validity of the TSA certificate of the archive timestamp at the time that is shown in the next generation archive timestamp. The relationship of time for verification is shown in the Figure 6.
	2) Verify the signature of the TSA that issued the archive timestamp.
	3) Verify the correspondence between the archive timestamp and the imprint data.
	4) Verify that the trust anchor of the TSA certificate is appropriate. — The validity of the certificate at the trust point could be expired at the time of verification of the TSA certificate for the archive timestamp. — In order to verify the trust anchor of b) 1), confirm that the certificate at the trust point is appropriate. Specific methods are out of the scope of this document.
c) Verify validation data for the signer's certificate.	1) Ascertain the validity of the certificate chain archived in the validation data.
	2) Ascertain that the trust anchor of the certificate is appropriate.
	3) Ascertain the validity of revoke information archived in the validation data. — Compare the issued time of revoke information with the time of archiving and confirm that the revoke information is appropriate.
	4) Ascertain that the trust point of the revoke information is valid. — Confirm that the trust point certificate is appropriate at the time of verification of validity of the certificate used for signing the revoke information.
d) Verify the signature timestamp at the time of the first archive timestamp.	1) Ascertain that the signature timestamp was valid at the time of the first archive timestamp. — Execute 4.3.4.2 assuming the time of the first archive timestamp. Verify that the TSA certificate was valid at the time of the first archive timestamp.
	2) Verify that the trust anchor of the signature timestamp was appropriate at the time of first archive timestamp. — The validity of the certificate at the trust point could be expired at the time of verification of the TSA certificate for the signature timestamp. — In order to verify the trust anchor of d) 1), confirm that the certificate at the trust point is appropriate. Specific methods are out of the scope of this document.

Verification process	Description
e) Verify the signer's signature at the time of the signature timestamp.	1) Verify the signer's signature based upon Annex A using validation data that is verified by process (c) and ascertain that the certificate was valid at the time of the signature timestamp.
	2) Ascertain that the trust anchor is appropriate. — The validity of the certificate at the trust point could be expired at the time of verification of the signer's certificate. — In order to verify the trust anchor of e) 1), confirm that the certificate at the trust point is appropriate. Specific methods are out of the scope of this document.
f) Verify the ordering of times. Confirm the correspondence of time.	Ascertain the correspondence of times that is not in the flow of the process above. — Ascertain the correspondence of signature timestamps and archive timestamps.

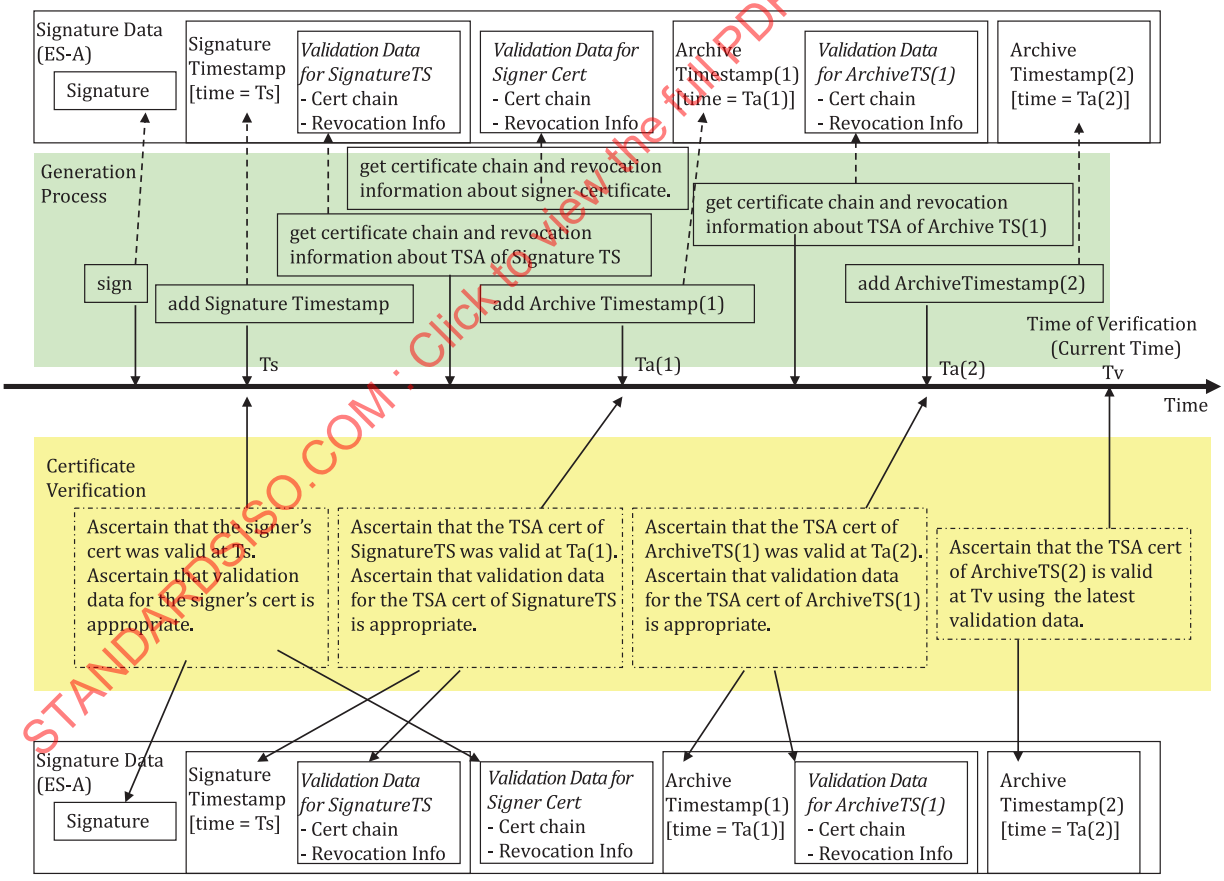

Figure 6 — The relationship of time for ES-A verification (the case of 2 archive timestamps)

4.4 CAdES specification

4.4.1 General

Subclause 4.4 describes requirements for the generation or validation of CAdES data.

Table 1 describes the relationships of profiles defined by this document and Table 2 describes the data structure of CAdES. Table 3, Table 4, and Table 5 describe profiles defined by this document, and Table 6 describes elements of the CAdES data.

4.4.2 Long term signature profile

In order to make digital signatures verifiable for the long term, signing time should be identifiable, any illegal alterations of information pertaining to signatures should be detectable, including the subject of information and validation data, and interoperability should be ensured. By defining the following two profiles, this document satisfies the previous requirements for CAdES.

a) CAdES-T profile

A profile pertaining to the generation and validation of CAdES-T data.

b) CAdES-A profile

A profile pertaining to the generation and validation of CAdES-A data.

Figure 7 shows the relationship between CAdES-T data and CAdES-A data.

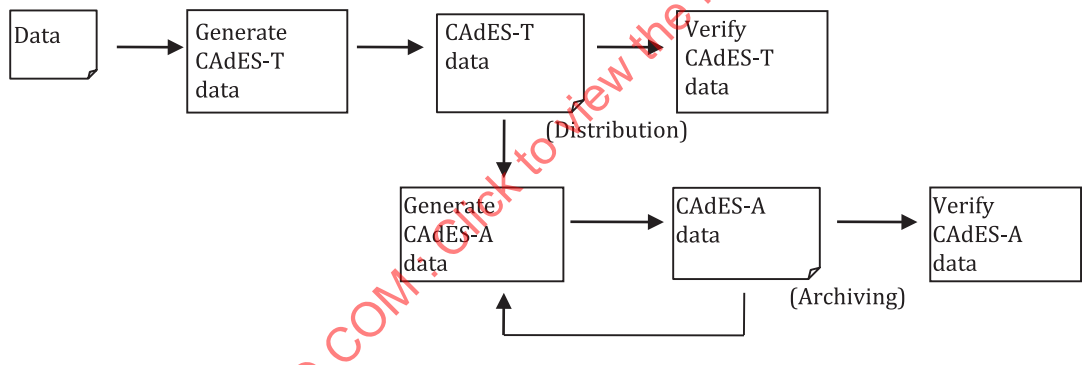

Figure 7 — Relationship between CAdES-T data and CAdES-A data

4.4.3 Representation of the required level

This document defines the following representation methods for the required level (as a profile) of each element constituting CAdES-T data and CAdES-A data.

a) Mandatory (M)

Elements whose required level is 'Mandatory' shall be implemented. If such an element has optional sub-elements, at least one sub-element shall be selected. Any element whose required level is 'Mandatory' and is one of the sub-elements of an optional element shall be selected whenever the optional element is selected.

b) Optional (O)

Elements whose required level is 'Optional' may be implemented at the discretion of the implementer.

c) Conditional (C)

Elements whose required level is 'Conditional' may be implemented at the discretion of the implementer. Detailed specifications pertaining to the processing of any element whose required level is 'Conditional' shall be provided. For example, the implementer provides the specifications for any 'Conditional' elements by disclosing a supplier's declaration of conformity and its attachment (see ISO 14533-1:2014, Annex A).

d) Prohibited (P)

Elements whose required level is 'Prohibited' shall not be in the data. The Prohibited element may be ignored in validation processes.

4.4.4 CAdES-T profile

Table 1 — ContentInfo

Element	Required level	Value
ContentType	M	Id-signedData
Content	M	SignedData

Table 2 — SignedData

Element	Required level	Value
CMSVersion	M	
DigestAlgorithmIdentifiers	M	
EncapsulatedContentInfo	M	
—eContentType	M	
—eContent	O	
CertificateSet (Certificates)	O	
—Certificate	O	
—AttributeCertificateV2	P	
—OtherCertificateFormat	P	
RevocationInfoChoices (crls)	O	
—CertificateList	O	
—OtherRevocationInfoFormat	C	
SignerInfos	M	
—single	O	
—parallel	O	

Table 3 — SignerInfo

Element	Required level	Value
CMSVersion	M	
SignerIdentifier	M	
—IssuerAndSerialNumber	O	
—SubjectKeyIdentifier	O	
DigestAlgorithmIdentifier	M	
SignedAttributes	M	
SignatureAlgorithm	M	
SignatureValue	M	

Table 3 *(continued)*

Element	Required level	Value
UnsignedAttributes	M	

The required level shall be 'Conditional' for any signed and unsigned attribute elements not listed in Table 4 and Table 5.

Table 4 — SignedAttributes

Element	Required level	Value
ContentType	M	
MessageDigest	M	
SigningCertificateReference	M	
—ESSSigningCertificate	O[a]	
—ESSSigningCertificateV2	O[a]	
—OtherSigningCertificate	P	
SignatgureAlgorithmIdentifier	C	
SigningTime	O[b]	
ContentReference	C	
ContentIdentifier	C	
ContentHint	C	
CommitmentTypeIndicatio	C	
SignerLocation	C	
SignerAttribute	C	
ContentTimestamp	C	
[a] ESSSigningCertificate or ESSSigningCertificateV2 shall be selected.		
[b] When the element is not implemented, it may be ignored.		

Table 5 — Additional Unsigned Attributes

Element	Required level	Value
CounterSignature	O	
Signing time information	M	
—SignatureTimestamp	M	Timestamp defined in RFC3161
—time mark, etc.	P	

4.4.5 CAdES-A profile

The CAdES-A profile is defined as an extended form of the CAdES-T profile to which the unsigned attributes specified in Table 6 are added. The required level shall be 'Conditional' for any element not specified in Table 6.

Table 6 — Additional Unsigned Attributes

Element	Required level	Value
CompleteCertificateRefs	M (O for validation)	
CompleteRevocationRefs	M (O for validation)	
—CompleteRevRefs CRL	O	

Table 6 *(continued)*

Element	Required level	Value
—CompleteRevRefs OCSP	O	
—OtherRevRefs	P	
Attribute certificate references	P	
Attribute revocation references	P	
CertificateValues	M	
—CertificateValues	O	
—Certificates maintained by trusted service	P	
RevocationValues	M	
—CertificateList	O	
—BasicOCSPResponse	O	
—OtherRevVals	P	
—Revocation information maintained by trusted service	P	
CAdES-C-timestamp	P	
Time-stamped cert and crls reference	P	
Archiving	M	
—ArchiveTimestampV2 id-aa-48	O	Timestamp defined in RFC3161
—ArchiveTimestamp id-aa-27	O	Timestamp defined in RFC3161
—time mark etc.	P	

4.5 XAdES specification

4.5.1 General

Subclause 4.5 details the requirements for the generation and verification of XAdES.

Subclause 4.5.1 shows the outline of the profile defined in this document, and 4.5.2 shows the structure of XAdES. Subclauses 4.5.3, 4.5.4, and Table 11 show the requirements for a profile.

4.5.2 Defined long-term signature profiles

In order to make digital signatures verifiable for the long term, interoperability should be ensured, signing time should be identifiable, and any illegal alterations of information pertaining to signatures should be detectable, including the subject of information and validation data. By defining the following two profiles, this document satisfies these requirements for XAdES.

a) XAdES-T profile:

   A profile pertaining to the generation and validation of XAdES-T data.

b) XAdES-A profile:

   A profile pertaining to the generation and validation of XAdES-A data.

Figure 8 shows the relationship between XAdES-T data and XAdES-A data.

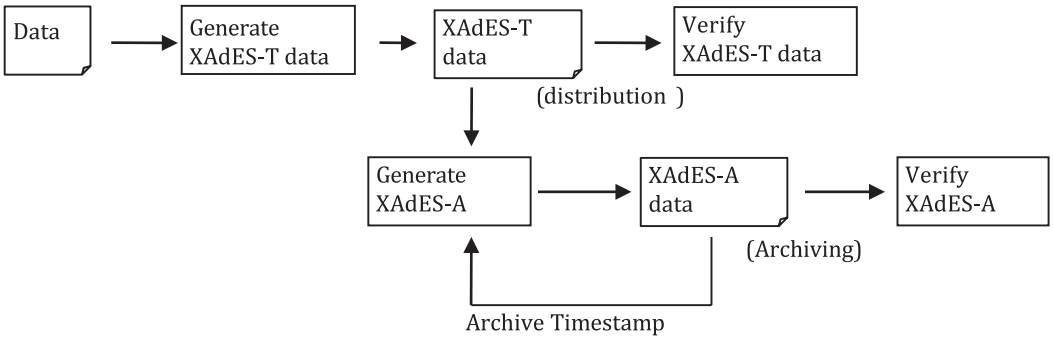

Figure 8 — Relationship between XAdES-T data and XAdES-A data

4.5.3 Representation of the required level

This document defines the following representation methods for the required level (as a profile) of each element constituting XAdES-T data and XAdES-A data

a) Mandatory (M)

Elements whose required level is 'Mandatory' shall be implemented without fail. If such an element has optional sub-elements, at least one sub-element shall be selected. Any element whose required level is 'Mandatory' and is one of the sub-elements of an optional element shall be selected whenever the optional element is selected.

b) Optional (O)

Elements whose required level is 'Optional' may be implemented at the discretion of the implementer.

c) Conditional (C)

Elements whose required level is 'Conditional' may be implemented at the discretion of the implementer. Detailed specifications pertaining to the processing of any element whose required level is 'Conditional' shall be provided. For example, the implementer provides the specifications for any 'Conditional' elements by disclosing a supplier's declaration of conformity and its attachment (see ISO 14533-1:2014, Annex A).

d) Prohibited (P)

Elements whose required level is 'Prohibited' shall not be implemented. The elements may be ignored in validation processes.

4.5.4 Requirement for XAdES-T

The required level shall be 'Conditional' for any elements not listed in Table 7, Table 8, Table 9, and Table 10.

Table 7 — Signature element

Element or attribute	Required level	Condition
ID attribute of ds:Signature	M (See Note 1)	
ds:SignedInfo	M	
Either ds:KeyInfo or SigningCertificate (Table 9) is required. If ds:KeyInfo is selected (Mandatory in XAdES v1,1,1), an X,509 data element defined in the XML signature shall be included as a subelement. NOTE 'Optional' in an XML signature but 'Mandatory' in XAdES.		

Table 7 *(continued)*

Element or attribute	Required level	Condition
—ds:CanonicalizationMethod	M	C14n
—ds:SignatureMethod	M	
—ds:Reference	M	
—ds:Transforms	O	
—ds:DigestMethod	M	
—ds:DigestValue	M	
ds:SignatureValue	M	
ds:KeyInfo	O (See Note 2)	
ds:Object	M	
Either ds:KeyInfo or SigningCertificate (Table 9) is required. If ds:KeyInfo is selected (Mandatory in XAdES v1,1,1), an X,509 data element defined in the XML signature shall be included as a subelement. NOTE 'Optional' in an XML signature but 'Mandatory' in XAdES.		

Table 8 — Object element

Element	Required level	Condition
QualifyingProperties	M	The ID attribute value of the signature element shall be entered in the target attribute.
—SignedProperties	M	
—UnsignedProperties	O	
QualifyingPropertiesRefernece	C	

Table 9 — Signed Properties element

Element	Required level	Condition
SignedSignatureProperties	M	
—SigningTime	O (See Note 1)	
—SigningCertificate	O (See Note 1,2)	
—SignaturePolicyIdentifier	C	
—SignatureProductionPlace	C	
—SignerRole	C	
SignedDataObjectProperties	C	
—DataObjectFormat	C	
—CommitmentTypeIndication	C	
—AllDataObjectsTimeStamp	C	
—IndividualDataObjectTimeStamp	C	
Either SigningCertificate or ds: KeyInfo (Table 7) is required. NOTE Mandatory in XAdES v1,1,1.		

Table 10 — Unsigned Properties element

Element	Required level	Condition
UnsignedSignatureProperties	M	
—CounterSignature	O	
—Trusted signing time	M	
—SignatureTimeStamp	M	Timestamp defined as RFC3161[a]
—time mark or other method	P	
UnsignedDataObjectProperties	C	

[a] Timestamp is defined as RFC3161 because the method of acquiring a Timestamp and storing it in XAdES data and the method of verifying the Timestamp are clearly shown by standards.

4.5.5 Requirement for XAdES-A

The XAdES-A profile is defined as an extended form of the XAdES-T data. The required level of each element of the UnsignedSignatureProperties defined as XAdES shall be as specified in Table 11. The required level shall be 'Conditional' for any element not specified in Table 11.

Table 11 — Unsigned Signature Properties element

Element or Processing method	Required level	Condition
CompleteCertificateRefs	O (See Note 1)	
CompleteRevocationRefs	O (See Note 1)	
—CRLRef	O	
—OCSPRef	O	
—OtherRef	P	
AttributeCetrificateRefs	P	
AttributeRevocationRefs	P	
SigAndRefsTimeStamp	P	
—not distributed case	P	
—distributed case	P	
RefsOnlyTimeStamp	P	
—not distributed case	P	
—distributed case	P	
CertificateValues	M	
—EncapsulatedX509Certificate	O	
—OtherCertificate	P	
—Certificates maintained by trusted service	P	
RevocationValues	M	
—CRLValues	O	

[a] Timestamp is defined as RFC3161 because the method of acquiring a Timestamp and storing it in XAdES data and the method of verifying the Timestamp are clearly shown by standards.

NOTE 1 Mandatory in XAdES v1,1,1.

NOTE 2 Italic type describes the processing method.

NOTE 3 AttrAuthoritiesCertValues, AttributeRevocationValues, not distributed cases and distributed cases are not defined in XAdES v1,1,1 and v1,2,1. AttributeCetrificateRefs and AttributeRevocationRefs are also not defined in v1,1,1.

Table 11 *(continued)*

Element or Processing method	Required level	Condition
—OCSPValues	O	
—OtherValues	P	
—Revocation information maintained by trusted service	P	
AttrAuthoritiesCertValues	P	
AttributeRevocationValues	P	
Archiving	M	
—ArchiveTimeStamp	M	
—not distributed case	M	Timestamp defined as RFC3161[a]
—distributed case	P	
—time mark or other method	P	
Any unsigned signature property defined in any other version of XAdES	C	

[a] Timestamp is defined as RFC3161 because the method of acquiring a Timestamp and storing it in XAdES data and the method of verifying the Timestamp are clearly shown by standards.

NOTE 1 Mandatory in XAdES v1,1,1.

NOTE 2 Italic type describes the processing method.

NOTE 3 AttrAuthoritiesCertValues, AttributeRevocationValues, not distributed cases and distributed cases are not defined in XAdES v1,1,1 and v1,2,1. AttributeCetrificateRefs and AttributeRevocationRefs are also not defined in v1,1,1.

4.6 PAdES Specification

4.6.1 General

Subclause 4.6 shows the requirements about generation and verification of PAdES.

Subclause 4.6.1 shows the outline of the profile which this standard defines, and 4.6.2 shows the structure of PAdES. Subclauses 4.6.3 to 4.6.5 show the requirements for a profile, and the section Subclause 4.6.6 shows the outline of each constituent elements.

4.6.2 Defined long term signature profiles

In order to make digital signatures verifiable for a long term, interoperability should be ensured, signing time should be identifiable, and any illegal alterations of information pertaining to signatures should be detectable, including the subject of information and validation data. By defining the following two profiles, this document satisfies the previous requirements for PAdES.

a) PAdES-T profile:

   A profile pertaining to the generation and validation of PAdES-T data.

b) PAdES-A profile:

   A profile pertaining to the generation and validation of PAdES-A data.

Figure 9 shows the relation between PAdES-T data and PAdES-A data.

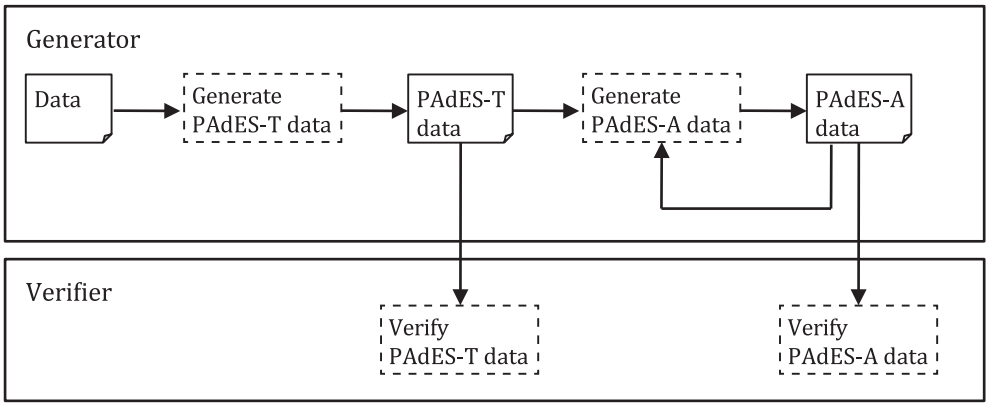

Figure 9 — Relation between PAdES-T data and PAdES-A data

4.6.3 Representation of the required level

This document defines the following representation methods for the required level (as a profile) of each element constituting PAdES-T data and PAdES-A data:

a) Mandatory (M)

Elements whose required level is 'Mandatory' shall be implemented without fail. If such an element has optional sub-elements, at least one sub-element shall be selected. Any element whose required level is 'Mandatory' and is one of the sub-elements of an optional element shall be selected whenever the optional element is selected.

b) Optional (O)

Elements whose required level is 'Optional' may be implemented at the discretion of the implementer.

c) Conditional (C)

Elements whose required level is "Conditional" may be implemented at the discretion of the implementer. Detailed specifications pertaining to the processing of any element whose required level is "Conditional" shall be provided. For example, the implementer provides the specifications for any elements "Conditional" by disclosing a supplier's declaration of conformity and its attachment (see References [1],[2],[3]).

d) Prohibited (P)

Elements whose required level is 'Prohibited' shall not be implemented. The elements may be ignored upon validation.

4.6.4 Requirement for PAdES-T

The required level shall be 'Conditional' for any elements not listed in Table 12 to Table 17

Table 12 — Signature dictionary

Entry	Required level	Value
Type	O	Sig
Filter	M	
[a] Even if a signature does not contain M Entry, a signature validation application shall not consider this signature invalid. Time of M Entry is not basically used to validate certificates. If this information is used for validation, it is necessary to define clearly a usage of this information. (e.g. describing a usage in a signature policy).		

Table 12 *(continued)*

Entry	Required level	Value
SubFilter	M	ETSI.CAdES.detached
Contents	M	See Table 13
ByteRange	M	
M	M[a]	
Cert	P	
Location	O	
Reason	O	
ContactInfo	O	

[a] Even if a signature does not contain M Entry, a signature validation application shall not consider this signature invalid. Time of M Entry is not basically used to validate certificates. If this information is used for validation, it is necessary to define clearly a usage of this information. (e.g. describing a usage in a signature policy).

Table 13 — ContentInfo in signature

Element	Required level	Value
ContentType	M	id-signedData
Content	M	See Table 14

Table 14 — SignedData in signature

Element	Required level
CMSVersion	M
DigestAlgorithmIdentifiers	M
EncapsulatedContentInfo	M
— eContentType	M
— eContent	O
CertificateSet (Certificates)	M
— certificate	M[a]
— v2AttrCert	P
— other	C
RevocationInfoChoices (crls)	O
— crl	O
— other	C
SignerInfos	M[b]
— signerInfo	M

[a] At least a signature generation application shall contain a signer certificate for interoperability. Even if a signature does not contain this element, a signature validation application shall not consider this signature invalid.

[b] Only a single signerInfo shall be present in PDF signature.

Table 15 — SignerInfo in signature

Element	Required level
CMSVersion	M
SignerIdentifier	M
— issuerAndSerialNumber	C
— subjectIdentifier	C