@dministración electrónica

eni
Esquema Nacional de Interoperabilidad

TECHNICAL INTEROPERABILITY STANDARD

For the Spanish Public Administration E-Signature and Certificate Policy

GOBIERNO
DE ESPAÑA

MINISTERIO
DE HACIENDA
Y ADMINISTRACIONES PÚBLICAS

SECRETARÍA DE ESTADO DE
ADMINISTRACIONES PÚBLICAS

DIRECCIÓN GENERAL DE MODERNIZACIÓN
ADMINISTRATIVA, PROCEDIMIENTOS E IMPULSO
DE LA ADMINISTRACIÓN ELECTRÓNICA

TÍTULO/TÍTLE: Technical Interoperability Standard for the Spanish Public Administration E-Signature and Certificate Policy

Elaboración y coordinación de contenidos/Content elaboration and coordination:
Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica/
General Directorate for Administrative Modernization, Procedures and Promotion of Electronic Administration

Características/Characteristics: Adobe Acrobat 5.0
Responsable edición digital: Subdirección General de Información, Documentación y Publicaciones/
Responsible for digital edition: Deputy directore for Information, Documentation and Publications
(Jesús González Barroso)

Así mismo, se puede encontrar esta publicación en el Portal de Administración Electrónica (PAe):/
Publication available at:
http://administracionelectronica.gob.es/

Para ver estas Guías de aplicación..... publicadas en 2011 ver :/
Technical Interoperability Standars 2011 available at:
http://www.seap.minhap.gob.es/es/publicaciones/centro_de_publicaciones_de_la_sgt/Guias_NTI.html

Edita:
© Ministerio de Hacienda y Administraciones Públicas
Secretaría General Técnica
Subdirección General de Información,
Documentación y Publicaciones
Centro de Publicaciones

Edit:
© Ministry of Finance and Public Administration
Technical Secretariat,
Directorate General for Information,
Documentation and Publications
Publication Center

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
CENTRO DE PUBLICACIONES

NIPO: 630-12-091-3

III. OTHER PROVISIONS

MINISTRY OF TERRITORIAL POLICY AND PUBLIC ADMINISTRATION

13171 *Resolution of the Secretary of State for Public Service, of 19 July 2011, giving approval to the Technical Interoperability Standard for the Spanish Public Administration E-Signature and Certificate Policy.*

The National Interoperability Framework, established in Article 42, Section 1, of Law 11/2007, of 22 June, on Citizens' E-Access to Public Services, is aimed at creating the conditions necessary to guarantee an adequate level of technical, semantic and organisational interoperability of the systems and applications used in the Public Administration, allowing the exercise of rights and the fulfilment of obligations through e-access to public services, while acting in the interest of effectiveness and efficiency.

Royal Decree 4/2010, of 8 January, regulating the National Interoperability Framework for E-Government, establishes in Additional Provision 1 the development of a series of Technical Interoperability Standards, which must be complied with in the Public Administration.

The Technical Interoperability Standards describe specific aspects of a wide range of topics such as e-documents, digitisation, e-files, authentic copy and conversion, signature policy, standards, data brokerage, data models, e-document management, connection to the communication network of the Spanish Public Administration, and data models for the exchange of registry entries and declarations of conformity, all of which are necessary to guarantee the more practical and operational aspects of interoperability between Public Administration agencies and citizens. The Technical Interoperability Standards shall be further developed and improved over time, parallel to the progress of e-government services, their supporting infrastructure, and the evolution of technology, in order to meet the provision in Article 42.3 of Law 11/2007, of 22 June.

Within the Technical Interoperability Standards, the Technical Interoperability Standard for e-signature policies is in accordance with the provisions in Article 18 of the aforementioned Royal Decree 4/2010, of 8 January, on the interoperability of e-signature and certificate policies.

In particular, the Technical Interoperability Standard for the Spanish Public Administration E-Signature and Certificate Policy sets forth the criteria for the development or incorporation of certificate-based e-signature policies by the agencies in the Public Administration. For this purpose, it describes the contents of certificate-based e-signature policies, determining the characteristics of common rules like formats, use of algorithms, or signature creation and validation for e-documents, as well as the trust rules for e-certificates, timestamps, and long-term signatures.

The conditions established in this Standard are aimed at the creation of a framework for the development of certificate-based e-signature policies in line with the latest European trends, such as the European Commission Decision 2011/130/EU, of February 25, 2011, establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market, which is in turn in accordance with already implemented e-signature systems.

Drafted in collaboration with all the Public Administration agencies to which it applies, the present Technical Standard has received a favourable report from the Standing Committee of the High Council for E-Government, at the proposal of the E-Government Sector Committee.

In accordance with the provisions in Section 2 of Additional Provision 1 of Royal Decree 4/2010, of 8 January, the Secretary of State decides:

One

To approve the Technical Interoperability Standard for the Spanish Public Administration E-Signature and Certificate Policy whose text appears below.

Two

That the Technical Interoperability Standard for the Spanish Public Administration E-Signature and Certificate Policy that is being approved by virtue of this document shall come into force on the day following its publication in the Official State Gazette, irrespective of the clauses in Transitory Provision 1 of Royal Decree 4/2010, of 8 January, regulating the National Interoperability Framework for E-Government.

Madrid, 19 July, 2011. Secretary of State for Public Service María Consuelo Rumí Ibáñez.

TECHNICAL INTEROPERABILITY STANDARD FOR THE PUBLIC ADMINISTRATION E-SIGNATURE AND CERTIFICATE POLICY

CONTENTS

IV.3 Trust rules for long-standing signatures

Annex: E-signature creation and validation tags for accepted formats

I. *General considerations*

I.1 Purpose

1. The Technical Interoperability Standard for the Public Administration E-Signature and Certificate Policy is aimed at establishing common criteria for the Public Administration in relation to the authentication and the mutual recognition of electronic signatures based on electronic certificates , to be developed and strengthened by means - of e-signature policies based on electronic certificates.

2. The ultimate goal is to facilitate the use of secure and interoperable e-signature for the various agencies in the Public Administration.

I.2 Scope of application

The clauses of this Standard shall apply to the development or incorporation of certificate-based e-signature policies by any body in the Public Administration or public law entity associated or reporting to it (hereinafter referred to as "organisations"), as provided in Article 3 of Royal Decree 4/2010, of 8 January, regulating the National Interoperability Framework for E-Government.

II. *E-signature policy*

II.1 Definition and content

1. As defined in Royal Decree 4/2010, of 8 January, an e-signature policy is a "set of security, organisational, technical, and legal rules to decide when e-signatures should be created, verified, and managed, and the characteristics signature certificates should have."

2. An e-signature and certificate policy should define:

a) E-signature creation, validation, and preservation procedures.

b) Characteristics and requirements of e-signature systems, certificates, and timestamps.

3. A certificate-based e-signature policy should include:

a) A description of its own scope and field of application, specifying its relation to existing framework and special policies and identifying the agents involved and the uses of e-signature.

b) Identification data on documents and document management agents.

c) Common rules to signatories and e-signature verifiers, including:

i. Accepted e-signature formats and algorithm use rules.
ii. E-signature creation rules.
iii. E-signature validation rules.

d) Trust rules, including requirements for certificates, timestamps, and long-term signatures.

e) Additional rules to be decided by each organisation; e.g.:

i. Special commitment rules for each of the services provides, with specific requirements for signatures to be valid in each case.

ii. Attribute certificate rules for organisations to add information to e-certificates according to their needs and their environment.

f) E-signature filing and custody terms.

g) Policy management considerations.

II.2 Policy identification data

1. Signature policy documents should include the following information for policy identification:

a) Name of document.
b) Document version.
c) Policy identifier (OID-Object IDentifier).
d) Policy reference URI (Uniform Resource Identifier).
e) Issue date.
f) Scope of application.

2. Signature policies should include a description of their validity period and considerations on the relevant transition periods.

3. For management agent identification, certificate-based e-signature policies should include the following data:

a) Name of policy management agent.
b) Contact address.
c) OID of policy management agent.

II.3 Agents involved in e-signature use

The agent involved in e-signature creation and validation processes shall be:

a) Signatory: A person owning a signature creation device and acting on their own or on behalf of an individual or legal entity that they represent.

b) Verifier: An individual or legal entity validating or verifying an e-signature in accordance with the e-signature policy governing the e-relation platform being used or the service being provided. It can be a trust validation entity or a third party interested in the validity of the e-signature.

c) Certification service provider (CSP): An individual or legal entity issuing e-certificates or providing e-signature-related services.

d) E-signature policy issuer and management agent: The entity that has created and manages the signature policy document the signatory, the verifier, and the service provider must abide by in e-signature creation and validation processes.

II.4 Uses of e-signature

E-signature policies can establish the terms of application of certificate-based e-signatures for the following purposes:

a) Data transmission signature, as a tool to make exchanges secure, guaranteeing the authentication of the actors involved in the process, the integrity of the data message being sent, and the non-repudiation of messages in digital communications.

b) Content signature, as a tool to guarantee the authenticity, integrity, and non-repudiation of message contents, irrespective of whether they are part of data transmission processes or not.

II.5 Relations with other policies

1. Every organisation shall assess the need and convenience of developing a policy of its own instead of using an existing framework policy.

2. The scope and field of application of e-signature policies shall be defined taking into account their relations with other e-signatures policies and ensuring that:

a) Their development is interoperable with the framework policy in the case of special signature policies.

b) The terms of use and coexistence with special signature polices are defined in the case of framework policies.

3. An e-signature policy should ensure that:

a) The extensions or restrictions established for signature creation and validation rules comply with the signature format validation as established in this Standard and the relevant framework policy, so as to ensure interoperability between different organisations.

b) The reference to the e-signature framework policy it is part of is included, indicating the version.

c) The signatures created in compliance with framework or special policies include a field indicating the policy they comply with.

d) Special policies are available in XML format (eXtensible Markup Language) and ASN.1 (Abstract Syntax Notation One) for other applications to interpret their rules.

II.6 E-signature policy management

1. E-signature policies shall include a basic description of their management process, setting forth maintenance, update, and publication instructions and identifying the agent in charge of performing these tasks.

2. The policy managing agency shall keep it up to date in terms of:

a) Changes owing to internal needs of the organisation.

b) Changes in related policies.

c) Changes in e-certificates issued by the certification service providers mentioned in the signature policy.

3. In order to facilitate the validation of e-signatures created in accordance with earlier versions of a policy, a record can be kept containing the location of each version.

II.7 Archiving and custody

1. Depending on the specific needs and rules of their field of application, e-signature policies can include a description of e-signature archiving and custody terms and responsibilities in their various applications.

2. In order to guarantee signature reliability over time, the following methods can be used:

a) Long-term signatures adding information on associated certificate status, a timestamp, and the certificates that make the trust chain, applying the trust rules for long-term signatures described in Section IV.3.

b) Other technical methods preventing changes to signatures whose validity has been verified, in accordance with the relevant signature policy requirements, and which has been stored in a system at a given time.

All the changes made to the system in which the signature is stored can be audited to check that the signature has not been changed. System security requirements shall comply with the security levels established in Royal Decree 3/2010, of 8 January, regulating the National Security Framework for E-Government.

3. Each signature policy shall establish a maintenance service for long-term signature validity evidence and signature update management. This service shall specify the mechanisms and terms for the filing and custody of signatures themselves and the certificates or status information used in their validation.

4. Certificates and status information can be stored in the file resulting from e-signature creation or in a specific storage location.

a) If certificates and status information are stored in the signature file, they shall be sealed under AdES-X or AdES-A modes.

b) If certificates and status information are stored in a specific storage location, they shall be sealed independently.

5. In order to protect e-signatures from algorithm obsolescence and ensure their characteristics throughout their validity period, one of the following procedures shall be used:

a) Use of re-stamping procedures to add a filing date and time seal with a more robust algorithm when close to expiry date.

Signature policies can include re-stamping procedures to apply for e-signature preservation.

b) Storage of e-signatures in a secure location, guaranteeing protection against forgery and protecting the exact date of e-signature archiving.

Dating operations shall use date and time marks, without need of timestamps.

6. E-signature archiving and custody measures and procedures shall be in accordance with the uses of e-signature described in the policy’s scope and field of application.

7. The archiving and management of e-signed documents shall comply with the Technical Interoperability Standard for E-Document Management Policies.

III. *Common rules*

III.1 Common rules

1. Common rules enable for e-signature creation and verification responsibilities, defining the minimum requirements that should be met. Said requirements must be signed if they are signatory requirements and not signed if they are verifier requirements.

2. Common rules shall be defined according to accepted e-signature formats and taking into account the various uses of certificate-based e-signature, the use of algorithms, and signature creation and validation procedures.

III.2 Accepted e-signature formats

1. The e-certificate-based e-signature formats accepted by organisations are those specified in European e-signature format standards and the Technical Interoperability Standard for the Catalogue of Standards.

2. Accepted e-signature formats shall be:

a) Widely used open standards based on European signature standards.

b) Selected from those defined by the European Commission for the e-signature interoperability policy to be regulated through a EU decision.

c) Compatible with the signature creation and validation policy definition to facilitate interoperability and automation in the handling of e-signatures created by different organisations.

d) Such that they allow the development of advanced functions like the creation of long-term signatures for preservation purposes.

e) If necessary, interoperable with the framework policy they are based on.

3. Every organisation shall decide on the specific signature formats and structures to be included in its policy, applying the criteria introduced in this Standard according to e-signature use and needs.

4. Every organisation shall identify the managing agency in charge of updating and publishing the list of accepted signature format specifications in its policy.

5. Signature policies shall include the requirements or update procedures for the inclusion of new versions of accepted formats.

III.3 Data transmission e-signature formats

1. Data transmission e-signatures shall be based on the standards contained in the Technical Interoperability Standard for the Catalogue of Standards. The policy development and management agent shall define the specific considerations to be applied in each organisation.

2. Each policy shall specify the versions of accepted formats and the changes in them that might lead to policy updates.

III.4 Content e-signature formats

1. Signature policies shall specify the accepted formats of content e-signatures.

2. In compliance with the Technical Interoperability Standard for the Catalogue of Standards, content e-signature formats shall be:

a) XAdES (XML Advanced Electronic Signatures), in accordance with technical specification ETSI TS 101 903, V1.2.2 and V1.3.2.

b) CAdES (CMS Advanced Electronic Signatures), in accordance with technical specification ETSI TS 101 733, V1.6.3 and V1.7.4.

c) PAdES (PDF Advanced Electronic Signatures), in accordance with technical specification ETSI TS 102 778-3.

3. The minimum format profile to be used for content e-signature creation within a policy shall be «-EPES», basic electronic signature (BES) plus information on signature policy. In any case, each organisation can include additional considerations in its signature policy for the interpretation and use of different format profiles and types in accordance with the provisions in this Standard.

4. Organisations shall apply particular considerations to content e-signatures at least in the following cases:

a) When the e-documents featuring a certificate-based signature for exchange purposes meet the format and structure requirements in the Technical Interoperability Standard for E-Documents.

The format of the certificate-based signature attached to an e-document shall be reflected in the minimum required metadata “Signature type” established in the Technical Interoperability Standard for E-Documents, which in this case can have one of the following values:

i. XAdES internally detached signature.
ii. XAdES enveloped signature.
iii. CAdES detached/explicit signature.
iv. CAdES attached/implicit signature.
v. PAdES.

b) With e-invoices signed under the format «Facturae» in accordance with Resolution PRE/2971/2007, of 5 October.

III.5 Algorithm use rules

1. Signature polices shall specify the rules for the use of algorithms for the various formats and the length of associated keys, according to e-signature use needs and in compliance with the provisions in the Technical Interoperability Standard for the Catalogue of Standards.

2. For general security environments, references to URN (Uniform Resource Name), where hash functions and signature algorithms for XAdES, CAdES and PAdES specifications are published, shall be considered as accepted signature formats, in accordance with technical specification ETSI TS 102 176-1, “Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash Functions and Asymmetric Algorithms” and the criteria established in compliance with Royal Decree 3/2010, of 8 January.

3. All the hash, base64 codification, signature, standardisation and transformation algorithms defined in XML-DSig (XML Digital Signature) and CMS (Cryptographic Message Syntax) standards shall be accepted as valid.

4. In high-security environments, following the National Cryptology Centre (CCN), the revised recommendations in CCN-STIC 405 and standard CCN-STIC 807 of the National Security Framework, concerning the use of cryptography, shall be applied.

5. The use of algorithms can be defined considering multiple possibilities according to specific needs.

III.6 E-signature creation rules

1. Signature policy must establish specific e-signature creation terms within their scope of application.

2. E-signature creation service platforms shall provide the necessary features to support signature creation processes based on the following points:

a) Signatory’s selection of file, form, or other binary objects to be signed. File formats shall be in accordance with the Technical Interoperability Standard for Standard the Catalogue of Standards.

Signatories must make sure that the file they want to sign does not contain dynamic contents affecting its validity or that change the signature over time.

b) Before signature creation, the e-signature service shall verify that:

i. The e-signature can be validated for the specific format of the file being signed.
ii. The certificates being used have been issued under a specific Certification Policy Statement and are valid under the applicable laws.
iii. The certificate is valid, has not been revoked or cancelled, has not expired, and the certificate chain has been validated, including the validation of each and every certificate in the chain.

If any of these verifications fails, the signature creation process shall be interrupted.

If these facts cannot be verified during the signature creation process, the relevant systems shall perform the validation before accepting the file, form, or binary object being signed.

c) The service shall create a file containing the signature according to the format being used.

When the signature is created, the reference shall be included to the unique identifier of the version of the e-signature policy document the signature creation process is based on.

3. The link to the signatory will be made through tags which, included under the signature and defined in accordance with the corresponding standards (XAdES, CAdES y/o PAdES), shall provide the following complementary information:

a) Date and time of signature (depending on signature creation processes, it could be an indication only).

b) Signatory's certificate.

c) E-signature policy document that signature creation is based on.

d) Original object format.

4. E-signatures can include the following additional information:

a) Geographic location of document signature.
b) Role of e-signature holder.
c) Task performed by signatory (approval, information, reception, certification, etc.).
d) Timestamp for some or all signature objects.

5. The information in Paragraphs 3 and 4 in this Section shall be included in each signature format according to the tags in the Annex.

6. In the case of e-signature by multiple signatories for a single object, where the second signatory ratifies the first signature, the corresponding CounterSignature tag shall be used to count them.

7. In the case of multiple signatures at the same level, each of them shall be represented separately.

III.7 E-signature validation rules

1. E-signature policies shall establish the special terms under which it shall be possible to validate document e-signatures.

2. In the case of e-documents, in order to access signature display, the user can submit the document containing metadata and signature(s) at a virtual office or in a general system providing tools for document display, e.g. VALIDe at 060.

3. The minimum conditions for signature validation shall be:

a) A guarantee that the signature is valid for the specific file being signed.

b) Validity of certificates.

i. The time to be taken as reference for validation shall be:

1) The time when the signature was made in the following cases:

a) When provider services make certificate status records available and the signature bears a valid period stamp at the time of verification.

b) When long-term signatures include evidence of e-signature validity at the time of signature creation or first validation and the evidence bears a valid period stamp.

2) The time of validation in other cases.

ii. It shall be checked that the certificates have not been revoked or cancelled, or that they have not expired.

iii. The validity of the whole certificate chain shall be checked, including each and every certificate in it, irrespective of whether they are included in the signature or not.

iv. It shall be checked that the certificate has been issued by a trusted certification service provider under a specific Certification Policy Statement complying with the regulations in force and included in the applicable signature policy.

v. If existing and required by the e-listing platform or a service in it, the timestamps of the implemented formats and their validity periods shall be verified.

4. The following information shall be taken into account for e-signature validation:

a) Date and time of signature: When there are timestamps, the oldest timestamp in the signature structure shall be used to determine the date of signature. Otherwise, the date and time of signature shall be an indication only and shall not be used to determine the time when the signature was made. If the signature bears no timestamps, certificate validation shall be performed at the time of signature validation.

b) Signatory's certificate: This field shall be used to verify certificate and, if relevant, certificate chain status on the date of signature creation.

c) Signature policy the e-signature creation process is based on: It shall be used to identify by means of the hash and the identifier (OID) that the signature policy used for signature creation matches the policy being used for the service being provided.

Signature policy validation means that the verification agent has the means to check the terms and conditions of the policy being validated. The availability of signature policies in a format that can be interpreted by automated means (XML or ASN.1), in compliance with European signature policy representation standards as indicated in Paragraph 3.d of Section II.5 of this Standard, shall facilitate the work of e-signature receiving applications in applying said signature policies.

5. If a document bears several signatures, all signatures shall undergo the same verification process as the first one, checking each signature or CounterSignature tag in the field of unsigned properties, containing information on the countersignatures created.

6. The signature verification agent can define its own validation and filing processes in accordance with the signature policy requirements relevant to the service and the provisions in the Technical Interoperability Standard for E-document Management Policies.

7. For certificate status verification in the case of long-term signature formats, signature validity shall be determined by the validity of the timestamp for validity evidence included in the signature. In those cases, signature validity over time shall be renewed by re-stamping the signature before the certificate issued by the Time-Stamping Authority (TSA) that made the previous stamp has expired, so that it can at any time be checked that, at the time when the signature was made, the certificate was valid.

IV. *Trust rules*

IV.1 Trust rules for e-certificates

1. Framework or special policies may impose limits or restrictions on the e-certificates accepted for each of the relevant services, in accordance with the relevant regulations in force.

2. Valid content e-signature certificates shall be:

a) Any e-certificate accepted under Law 59/2003, of December 19, or Directive 1999/93/EC, of 13 December, 1999.

b) New certificate types as defined in Law 11/2007, of 22 June.

3. The technical, semantic, and organisational interoperability requirements to be complied with by certification service providers shall be those set forth in Article 21 of Law 11/2007, of 22 June, Article 19 of Royal Decree 4/2010, of 8 January, and the other applicable laws.

4. The list of certification service providers issuing accepted certificates shall be available at the Trusted List of Certification Service Providers (TSL) published at the virtual office of the Ministry of Industry, Tourism and Trade.

5. Each e-signature policy can determine a grace period for certificate validation. This period can span, from the time when the signature or timestamp is created, at least the maximum time allowed for the full refreshment of CRLs (Certificate Revocation Lists) or the maximum time for certificate status update on the OCSP (Online Certificate Status Protocol) service. It shall be considered that times may vary according to the Certification Service Provider.

6. The verification agent shall validate the e-certificates based on the validation and filing procedures described in the signature policy the service is governed by.

IV.2 Trust rules for timestamps

1. The basic elements of an e-timestamp shall be:

a) Information on the identity of the authority issuing the timestamp: legal status, public key used in timestamp verification, number of bits in the key, e-signature algorithm and hash function used.

b) Type of form submitted, including whether it is a summary value or a document, its value and reference data.

c) Summary values: “previous,” “current,” “next.”

d) UTC (Universal Time Coordinated) date and time.

e) E-signature of all of the above.

2. Timestamps and validation information can be added by the sender, the receiver, or a third party and included as unsigned properties in the corresponding fields according to the signature format being used.

3. Signature policies shall establish the conditions to determine the accepted timestamps according to specific needs and in compliance with the regulations and laws in force. This includes determining the maximum time allowed for time stamping, which in any case must be prior to certificate expiration.

4. Timestamps shall comply with the technical specifications in standard ETSI TS 102 023, “Electronic Signatures and Infrastructures (ESI); Policy Requirements for Time-Stamping Authorities.”

IV.3 Trust rules for long-term signatures

1. In the case of long-term signatures, the signatory or the signature verification agent shall include a timestamp to guarantee that the certificate was valid when the signature was made. If the timestamp is included by the signatory, it can be done after the grace period.

2. For e-signature conversion to long-standing e-signature:

a) The created or verified e-signature shall be verified, validating its integrity, compliance with standards XAdES, CAdES, or PAdES, and references.

b) An e-signature filling procedure shall be performed to obtain and store the references to:

i. Certificates, including signatory’s and certificate chain’s certificates.
ii. Certificate status information, CRLs, or OCSP responses.

c) Time-stamping shall be applied to the references to certificates and status information.

3. For the inclusion of full validation information in the signature, CRL or OCSP validation shall be used.

4. Signature policies may include use instructions or format descriptions for long-term signatures according to specific needs within their scope of application and in compliance with applicable laws.

ANNEX

E-signature creation and validation tags for accepted formats

Information	Mandatory/ optional	Field – Tag – Element[1]		
		XAdES	CAdES	PAdES
Date and time of signature	Mandatory	SigningTime (SignedProperties)	Signing-time (SignedData)	Indicated in the M field of the signature dictionary
Signatory's certificate	Mandatory	SigningCertificate (SignedProperties)	ESS signing-certificate ESS signing-certificate-v2	ESS signing-certificate ESS signing-certificate-v2
Signature policy	Mandatory	SignaturePolicyIdentifier – SigPolicyId	SignaturePolicyIdentifier – SigPolicyId	SignaturePolicyIdentifier
		SignaturePolicyIdentifier – SigPolicyHash	SignaturePolicyIdentifier – SigPolicyHash	
Format of original object	Mandatory	DataObjectFormat (SignedProperties)	Content-hints (SignedData)	Not allowed
Geographic location	Optional	SignatureProductionPlace (SignedProperties)	Signer-location (SignedData)	Indicated in the Location field of the signature dictionary
Role of signatory	Optional	SignerRole - ClaimedRoles (SignedProperties)	Signer-attributes (SignedData)	Signer-attributes
Task performed on document	Optional	CommitmentTypeIndication (SignedProperties)	Commitment-type-indication (SignedData)	Commitment-type-indication
Timestamp	Optional	AllDataObjectsTimeStamp (SignedProperties)	Content-time-stamp (SignedData)	Content-time-stamp
		IndividualDataObjectsTimeStamp (SignedProperties)		
E-signature counter	Optional	CounterSignature (UnsignedProperties)	CounterSignature (UnsignedProperties)	Not allowed

[1] Note that this table is not a full list of the tags defined by each standard but a reference guide to tags reflecting signature creation and validation information.