Official Journal Signature Policy

Version 4

(1.3.171.4.1.1.4)

Effective as of October 1, 2023

Table of Contents

1 Introduction

This document specifies the signature policy for the Official Journal Signature (OJ signature) and for the Official Journal Seal (OJ seal), which are employed to authenticate the electronic version of the Official Journal of the European Union (OJ) in accordance with Council Regulation (EU) No 216/2013 on the electronic publication of the Official Journal of the European Union[1].

A signature policy is a set of rules for the creation, validation and extension of one or more interrelated electronic signatures and/or seals, that defines the technical and procedural requirements for their creation, validation and long-term management in order to satisfy particular business needs and to determine when they are valid. A signature policy also serves to make all aspects of a given signature or seal workflow transparent to all involved parties, i.e. signers, recipients and arbitrators, so that electronic signatures and seals complying with policy requirements may engender increased confidence in the applicability and acceptance of these signatures and seals.

The detailed concepts of a signature policy are explained in [ETSI 2015], which also defines the guidelines and structure for the present document. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2911 [Bradner 1997].

The OJ is published by the Publications Office of the European Union (OP) on the EUR-Lex website (cf. 1.2.4) in order to serve as the only authentic source of EU law. The OJ is published from Monday to Friday, and possibly during the weekend, in all official languages of the European Union (EU). *Below, the acronym "OJ" is used to collectively denote this particular scope of application.*

1.1 Overview

The OJ signature policy formalises key elements of the implementation of electronic signature and electronic seal creation, validation and long-term preservation when applied to the OJ as a means of authentication of OJ issues published by the OP.
It consists of:

- an introduction covering the title/identification of the policy, policy issuer details, policy administration, definitions and acronyms, etc.;
- the signature application practices statements, which define the associated policy and legal requirements, as well as the applicable security considerations;
- the business scoping parameters, which detail the workflows involved in the generation of the electronic signatures and seals authenticating the OJ issues published by the OP;
- the requirements and statements on technical mechanisms and standards implementation, and annexes.

[1] See OJ L 69, 13.3.2013, p. 1.

1.2 Business domain

1.2.1 Scope and boundaries of signature policy

The OJ signature policy covers electronic signatures and seals that are generated for individual OJ issues by authorised OJ signers in accordance with the Council Regulation on the electronic publication of the Official Journal of the European Union upon successful validation of each issue to be signed.

1.2.2 Domain of applications

The electronic signatures and seals covered by the OJ signature policy are only those that are described in section 3.1.

1.2.3 Transactional context

Not applicable.

1.3 Signature policy name, identification and conformance rules

1.3.1 Policy name

The OJ signature policy is entitled as follows:

Official Journal Signature Policy

1.3.2 Policy identifier

Since there is only one Official Journal of the European Union and its publication is a well-known process of the European Union, the OJ signature policy can be identified implicitly by any party. A description of the General business workflow is provided in section 3.1.1.1.

In order to indicate the policy explicitly, each OJ signature and seal *MAY* include an explicit signature policy indication as defined in section 5.2.9 of [ETSI 2022-XAdES]. If included, the explicit signature policy indication SHALL indicate the object identifier 1.3.171.4.1.1.4 using the encoding rules specified in section 5.2.9 of [ETSI 2022-XAdES] and in [Mealling 2010].

The globally unique object identifier 1.3.171.4.1.1.4 unambiguously identifies the present version of this policy. The prefix 1.3.171.4 has been registered as the base OID for *Signature policies and other purposes of the Publications Office of the EU* (cf. http://www.oid-info.com/get/1.3.171.4). The suffix 1.1.4 identifies the present OJ signature policy version, and its ASN.1 value notation with names SHALL be {oj(1) signature-policy(1) version(4)}. This version obsoletes version 1.1.3 of this policy.

1.3.3 Policy conformance rules

The present policy does not claim any conformance to any other policy.

1.3.4 Policy distribution points

The OJ signature policy document is published on the EUR-Lex website. It can be accessed from the website of the Publications Office at https://eur-lex.europa.eu/.

1.3.5 Policy validity period

The present policy version is effective as of October 1, 2023.

1.3.6 Policy scope

The present policy is applicable to all OJ issues published and electronically signed since the Council Regulation on the electronic publication of the Official Journal of the European Union entered into force. The present policy is not applicable to the Supplement to the Official Journal of the European Union (S series, Official Journal S or OJ S).

NOTE: Each version of the present policy is valid within the validity period defined in each version. The set of all versions covers all OJ issues.

1.4 Signature policy document administration

The issuer of the OJ signature policy is the Publications Office of the European Union, having adopted the present document and published it on the EUR-Lex website.

The OJ signature policy as published SHALL automatically have legal value and SHALL apply to the creation, verification and long-term management of OJ signatures and seals.

The issuer of the OJ signature policy is responsible for:

- specifying and approving the OJ signature policy,
- defining the review process for the OJ signature policy,
- defining the assessment criteria and process ensuring that the OJ signature policy successfully complies with the Council Regulation (EU) No 216/2013 of 7 March 2013 on the electronic publication of the Official Journal of the European Union and the Council Regulation (EU) 2018/2056 of 6 December 2018 amending Regulation (EU) No 216/2013 on the electronic publication of the Official Journal of the European Union,
- defining the assessment criteria and process ensuring that applications claiming compliance with the OJ signature policy successfully comply with its present rules in actuality,
- publication on EUR-Lex of the OJ signature policy and amended versions thereof.

1.4.1 Policy authority

The OJ signature policy is administered by the Publications Office of the European Union.

1.4.2 Contact person

The issuer of the present policy can be contacted using the following coordinates:

Contact person:	The Head of Unit Official Journal and Case Law
Postal address:	2, rue Mercier, L-2985 Luxembourg
Telephone number:	+352 29291
Fax number:	+352 292944620
E-mail address:	OP-JO-AUTHENTIQUE-HELPDESK@publications.europa.eu

1.4.3 Approval procedures

The policy approval authority within the Publications Office of the European Union is the Director General of the Publications Office of the European Union.

1.4.4 Policy versions

The initial and amended versions of the policy *MAY* specify a minimum effective date. When a version of the policy is published, it SHALL go into effect as of the following three dates at the latest:

1. The minimum effective date specified by the policy version, if any;
2. The day following the date of the earliest signature timestamp on the OJ signature or seal of the OJ issue mentioning the policy version that is published, according to the local time in Luxembourg;
3. The day following the date of publication of the policy version.

Any given amended version of the policy SHALL automatically expire when the respective subsequent amended version goes into effect. A subsequent amended version of the policy SHOULD additionally indicate the version it makes obsolete.

The above rules are designed to ensure that the signature of any given version of the policy is not subject, whether directly or indirectly, to the same version of the policy in order to prevent circular reasoning. Furthermore, it is preferable to keep by any means the obsolete version.

1.5 Definitions and acronyms

The definitions and acronyms used throughout this document are listed in Table 1.

Acronym	**Definition (EN)**
CA	Certificate Authority
DTBS	Data to Be Signed
LTV	Long Term Validity
OID	Object Identifier
OJ	Official Journal of the European Union
PIN	Personal Identification Number
OP	Publications Office of the European Union
QC	Qualified Certificate
QESig	Qualified Electronic Signature
QESeal	Qualified Electronic Seal
QSCD	Qualified Signature/Seal Creation Device
SAA	Signature Augmentation Application
SCA	Signature Creation Application
SSCD	Secure Signature Creation Device
SVA	Signature Validation Application
TSP	Trust Service Provider
QTSP	Qualified Trust Service Provider
WIPIWIS	What Is Presented Is What Is Signed

Table 1: Definitions and acronyms

2 Signature application practices statements

2.1 Associated policy requirements

Issues of the OJ are governed by Articles 1 and 2 of the Council Regulation on the electronic publication of the Official Journal of the European Union, which stipulate, among other things, that the electronic edition of the Official Journal SHALL bear a qualified electronic signature defined in accordance with Regulation (EU) No 910/2014 of the European Parliament and of the Council, or a qualified electronic seal defined in accordance with Regulation (EU) No 910/2014.

Electronically signing and sealing OJ issues falls under the implementation of a signature as a substantial formality as stated in Article III.2.1 of the European Commission IMPLEMENTING RULES FOR THE DECISION 2002/47/EC, ECSC, EURATOM ON DOCUMENT MANAGEMENT AND FOR THE DECISION 2004/563/EC, EURATOM ON ELECTRONIC AND DIGITISED DOCUMENTS of 30 November 2009[2], which also mandates that electronic signatures applied to the OJ require a qualified electronic signature as defined in [eIDAS].

Pursuant to Article III.2.3 of IMPLEMENTING RULES FOR THE DECISION 2002/47/EC AND FOR THE DECISION 2004/563/EC[2] the verification of the signing authority is the responsibility of the OJ SCA when enabling an official of the OP to electronically sign OJ issues, or when enabling the OP as a legal person to electronically seal OJ issues.

Although OJ issues in electronic format cannot have legal effect without being signed or sealed, the OJ signature policy also stipulates that the OJ SCA SHALL guarantee that only the authorised OJ signers are able to reject OJ issues, in order to effectively prevent attacks on the OJ publication process.

Since authorised OJ signers act on behalf of the OP, it is the responsibility of the Director General of the OP to guarantee (by delegation) proper authorization of the respective QCs for OJ signing. To this purpose, authorization of QCs for OJ signing

- *SHALL* be correctly configured in the OJ SCA user management,
- *SHOULD* be restricted to corporate (professional) certificates that guarantee the subject's affiliation to the OP[3],
- *SHALL* be made transparent by publishing the authorized QCs on the EUR-Lex website, in line with Article 2 of the Council Regulation on the electronic publication of the Official Journal of the European Union.

2.2 Associated Legal Requirements

The implementation of electronic signatures and electronic seals as covered under the OJ signature policy SHALL be governed by the following legal provisions:

- Council Regulation (EU) No 216/2013 of 7 March 2013 on the electronic publication of the Official Journal of the European Union,

[2] See SEC(2009) 1643.

[3] Corporate certificates guarantee the subject's affiliation to a specific organization. Security is augmented because the issuing QTSP enforces the proof of entitlement of the respective certificate owner.

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC[4],
- 2009/767/EC: Commission Decision of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the points of single contact under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market[5],
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[6],
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)[7],
- Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws[8],
- 2010/425/EU: Commission Decision of 28 July 2010 amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States[9],
- 2009/496/EC, EURATOM: Decision of the European Parliament, the Council, the Commission, the Court of Justice, the Court of Auditors, the European Economic and Social Committee and the Committee of the Regions of 26 June 2009 on the organisation and operation of the Publications Office of the European Union[10],
- 2011/130/EU: Commission Decision of 25 February 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[3].

2.3 Technical security considerations

Cryptographic tools eligible for the implementation of OJ signatures and seals SHALL satisfy the requirements of qualified electronic signatures as defined in [eIDAS], in [ETSI 2016], and in relevant state-of-the-art practices.

[4] See OJ L 257, 28.08.2014, p. 73.

[5] See OJ L 274, 20.10.2009, p. 36.

[6] See OJ L 119, 4.5.2016, p. 1.

[7] See OJ L 201, 31.7.2002, p. 37.

[8] See OJ L 337, 18.12.2009, p. 11.

[9] See OJ L 199, 31.7.2010, p. 30.

[10] See OJ L 168, 30.06.2009, p. 41.

2.4 Legal statements

Electronic signatures and seals placed on OJ issues shall be generated on behalf of the OP on the basis of the Council Regulation on electronic publication of the Official Journal of the European Union.

3 Business scoping parameters (BSP)

3.1 BSPs mainly related to the concerned application/business process

3.1.1 BSP (a): Workflow (sequencing and timing) of signatures

3.1.1.1 General business workflow description

The OP publishes the OJ from Monday to Friday, and optionally during the weekend. This OJ publication can be an OJ issue or an OJ-Act issue. An OJ issue represents a multilingual publication of one or more documents. Each linguistic version of an issue consists of the entire text of each document in a single file. An OJ-Act issue represents a multilingual publication of one and only document that is published standalone. Each linguistic version of an OJ-Act issue consists of the entire text of each document in a single file.

Individual OJ and OJ-Act issues are categorised according to the series to which they belong, with the category as an identifying part of the OJ. There are two relevant series for the present scope of application, i.e. L (legislation) and C (information and notices). A series can optionally have sub-series and classification schemes (cf. http://publications.europa.eu/code/en/en-10000.htm for a more detailed explanation on the scope of application, document structure and complementary background information).

In addition to the OJ L and C series, there are also special editions published in the language of an acceding country/new Member State containing EU secondary law. These special editions are also part of the scope.

Once an OJ or OJ-Act issue is complete (i.e. all linguistic versions of the OJ or OJ-Act issue in PDF/A are available) and ready for publication, the workflow will continue with either an electronic sealing process (cf. section 3.1.1.2) or an electronic signing process (cf. section 3.1.1.3). In case of electronic sealing, a qualified electronic seal is automatically generated using a qualified electronic sealing certificate issued to the OP as an entity of the European Commission. In case of electronic signing, a qualified electronic signature is generated by an authorised person using a qualified electronic signing certificate.

The electronic sealing is the default flow selected by the SCA, i.e. OJ or OJ-Act issues that are complete will go through the automated sealing process unless the sealing process is not available. In the latter case, the signing process will be used.

Since a detached XAdES signature or seal with a manifest (cf. [Bartel 2008], [ETSI 2022-XAdES] and 2011/130/EU: Commission Decision of 25 February 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[11]) is employed for signing each issue, when verifying an OJ or OJ-Act signature or seal it is also necessary to perform a validation of the manifest in addition to the XML signature core (cf. [Bartel 2008]) during [ETSI 2022-XAdES] validation, for the purpose of verifying an OJ or OJ-Act signature or seal.

The following sub-sections describe the high-level electronic sealing and signing flows as implemented in the OJ SCA, SAA and SVA (cf. [ETSI 2016]).

3.1.1.2 OJ and OJ-Act Seal Creation

1. A complete OJ or OJ-Act issue is detected for sealing
2. The SCA performs preliminary verification checks on the supplied files:

[11] OJ L 53, 26.2.2011, p. 66

a. It verifies whether there are size inconsistencies between the linguistic versions of the OJ/OJ-Act issue, and whether they stand within configurable size limits;

b. It verifies whether all provided linguistic versions were forecast for publication.

3. In the case of verification failure, the sealing process is interrupted. Manual intervention from authorised OP personnel is required to resume the sealing process.
4. Upon successful validation by the SCA, a manifest referencing each linguistic version of the complete issue is generated. Furthermore, each linguistic version corresponds to one individual EU language and is represented as a PDF/A document that is treated as a binary octet stream during message digest calculation.
5. The SCA authenticates against the central electronic signature portal of the European Commission and transmits the generated manifest for automated sealing.
6. The electronic signature portal seals the provided manifest using a qualified sealing certificate, issued by an accredited European QTSP (cf. [eIDAS]). The private key related to this sealing certificate is stored on a QSCD interfaced with the electronic signature portal.
7. The XAdES seal (cf. [ETSI 2022-XAdES]) created in this manner is then sent back to the SCA, which checks the validity of algorithms used among other things and verifies that the sealing certificate of the respective seal is authorised and owned by the same legal person who has been authenticated as an authorised signer.
8. Upon successful verification, the electronic seal is augmented with a signature timestamp provided by an accredited QTSP (cf. [eIDAS]).
9. The electronic seal augmented at the previous processing step is transferred for publication on the EUR-Lex website. An identical copy of the seal is retained by the SCA at the same time.
10. When the required grace period of 24 hours for a seal resulting from the previous processing step has elapsed, it is further augmented to a self-sustainable form, in order to make the signature valid for a long period of time, using the trusted timestamp service of an accredited European QTSP (cfr. [eIDAS]).
11. The seal augmented at the previous processing step is transferred for publication on the EUR-Lex website, replacing the seal from step 9 that had not yet been augmented to a self-sustainable form.
12. Apart from publication on the EUR-Lex website, identical copies of the documents comprising an OJ or OJ-Act issue, along with the corresponding seal in a self-sustainable form, are transferred to the long-term digital preservation system, which is managed by OP, and preserves in the long-term the official documents of the EU Institutions. Implementation aspects concerning long-term preservation are NOT addressed by the present signature policy.

3.1.1.3 OJ or OJ-Act Signature Creation

1. A complete OJ or OJ-Act issue is detected for signature.
2. A manifest referencing each linguistic version of the complete issue is generated. Furthermore, each linguistic version corresponds to one individual EU language and is represented as a PDF/A document that is treated as a binary octet stream during message digest calculation.

Note that complete issues are exclusively managed and locked by the SCA during manifest generation in order to guarantee consistent digest calculation, which is critical for the process.

3. Upon successful authentication by the SCA, an authorised signer can select a complete issue for signing, provided that the corresponding manifest has been generated during the previous step.
4. Upon successfully selecting an issue to be signed, the authorised signer enters the signing process for this particular issue:
    a. In order to duly honour the WIPIWIS principle, the authorised signer is compelled to examine at least three different linguistic versions, using a conformant PDF/A viewer prior to being able to sign the issue. If the OJ or OJ-Act edition has less than three linguistic versions, then the authorised signer is compelled to examine all the available linguistic versions.

        Note that the SCA allows the signer to examine any linguistic version of the issue to be signed. The signer MAY therefore examine the entire content to be signed if he or she so wishes.

    b. The authorised signer can deliberately choose to either reject the issue, which aborts the signing process, or to proceed with signing by pressing the Sign button.
    c. Upon pressing the Sign button:
        i. The SCA generates a signing request towards the central electronic signature portal of the European Commission, transmitting the manifest to sign and redirecting the authorised signer to the portal;
        ii. The authorised signer authenticates to the electronic signature portal, and is presented with the manifest to sign, according to WIPIWIS principles;
        iii. The electronic signature portal connects to the middleware installed on the authorised signer's workstation and retrieves the qualified signing certificate of the signer, issued by an accredited European QTSP (cf. [eIDAS]). This certificate is presented to the authorised signer, who in turn is prompted to enter the corresponding PIN protecting the QSCD in order to authorize the QSCD to create the signature using the private key corresponding to the selected signing certificate, thus completing the signing process.
    d. The middleware sends the signature value that was generated to the electronic signature portal, which in turn generates a corresponding XAdES signature (cf. [ETSI 2022-XAdES]).
5. This XAdES signature is then sent back to the SCA, which checks – via the electronic signature portal - the validity of algorithms used among other things and verifies that the signing certificate of the respective signature is authorised and owned by the same person who has been authenticated as an authorised signer.
6. Upon successful verification, the signature is augmented – via the electronic signature portal - with a signature timestamp provided by an accredited QTSP (cf. [eIDAS]).
7. The signature extended at the previous processing step is transferred for publication on the EUR-Lex website. An identical copy of the signature is retained by the SCA at the same time.

8. When the required grace period of 24 hours for a signature resulting from the previous processing step has elapsed, it is further augmented to a self-sustainable form, in order to make the signature valid for a long period of time, using the trusted timestamp service of an accredited European QTSP (cfr. [eIDAS]).
9. The signature extended at the previous processing step is transferred for publication on the EUR-Lex website, replacing the signature from step 7 that had not yet been augmented to a self-sustainable form.
10. Apart from publication on the EUR-Lex website, identical copies of the documents comprising an OJ or OJ-Act issue, along with the corresponding signature in a self-sustainable form, are transferred to the long-term digital preservation system, which is managed by OP, and preserves in the long-term the official documents of the EU Institutions. Implementation aspects concerning long-term preservation are NOT addressed by the present signature policy.

3.1.1.4 Emergency situation

Where it is not possible to create the OJ or OJ-Act seal or signature as described in sections 3.1.1.2 or 3.1.1.3 due to an unforeseen and exceptional unavailability of the OJ SCA, the Publications Office will apply a QESeal or QESig on each PDF/A document corresponding to each linguistic version of the OJ or OJ-Act issue. All sealed/signed PDF/A documents will be transferred for publication on the EUR-Lex website.

3.1.2 BSP (b): Data to be signed

- OJ or OJ-Act signatures and seals rely on an XML manifest (cf. [Bartel 2008] and [ETSI 2022-XAdES]) which combines all the linguistic versions available in PDF/A format pertaining to an OJ or OJ-Act issue in a single signature that must comply with the following requirements: each linguistic version logically associated with an OJ or OJ-Act issue *MUST* have its own digest value;
- All linguistic versions logically associated with an OJ or OJ-Act issue *MUST* be presented to the signer during signature creation for examination by him or her so that the signature content can be verified at the signer's discretion as described in section 3.1.1.3, in order to comply with the WIPIWIS principle;
- Proper visualisation *MUST* be guaranteed by using a PDF/A conformant reader;
- Only the linguistic versions pertaining to the particular issue being signed SHALL be presented to the signer during the signing process;
- The technical characteristics of all linguistic versions logically associated with an OJ or OJ-Act issue *MUST* be verified during seal and signature creation, to ensure consistency.

In case of an emergency situation as described in section 3.1.1.4 above, the following requirements will apply:

- Each linguistic version of an OJ or OJ-Act issue *MUST* have its own QESeal or QESig;
- All linguistic versions logically associated with an OJ or OJ-Act issue *MUST* be examined by the signer during signature creation so that the signature content can be verified at the signer's discretion in order to comply with the WIPIWIS principle;
- Proper visualisation *MUST* be guaranteed by using a PDF/A conformant reader.

3.1.3 BSP (c): The relationship between signed data and signature(s) and seal(s)

An OJ or OJ-Act signature or seal applies to all linguistic versions of an OJ or OJ-Act issue, each formatted as a PDF/A document.

During the creation of an OJ or OJ-Act signature or seal, the digital content of a document to be signed/sealed is digested as a binary octet string using the strongest supported digest algorithm compliant with section 7.3 of [ETSI 2022-Crypto].

The individual document digest values are combined together with the URIs of the original file names in an XML manifest with no additional transformations applied (cf. [Bartel 2008]).

The manifest, including the signed attributes, is signed or sealed employing XAdES (cf. [ETSI 2022-XAdES]) with respect to the profile specified in Commission Decision 2011/130/EU of 25 February 2013.

In case of an emergency situation as described in section 3.1.1.4 above, each PDF/A document representing each one linguistic version of the OJ or OJ-Act issue will be signed or sealed employing PAdES (cf. [ETSI 2016-PAdES] [eIDAS]).

3.1.4 BSP (d): Targeted community

The targeted community is any party that relies on and needs to verify the authenticity of the OJ as well as all parties responsible for the implementation of the SCA and SAA used to create e-signatures or e-seals as well as augmenting them for the OJ or OJ-Act issues.

3.1.5 BSP (e): Allocation of responsibility for signature validation and augmentation

3.1.5.1 OJ or OJ-Act signature and seal verification

Any relying party, in particular any European citizen, can download an OJ or OJ-Act issue published on the EUR-Lex website and the corresponding detached XAdES signature or seal (cf. [ETSI 2022-XAdES]) for verification.

Since an interoperable European signature standard and services of an accredited European QTSP (cf. [eIDAS]) are used during signature and seal creation, verification can be performed by using any third-party verification utility that complies with the employed standards, provided that manifest validation can be performed on the basis of the OJ signature policy.

In case of an emergency situation as described in section 3.1.1.4 above, each PDF/A document representing each one linguistic version of the OJ or OJ-Act issue will be signed or sealed employing PAdES (cf. [ETSI 2016-PAdES]). Verification of these can be performed by using any third-party verification utility that complies with the employed standard.

3.1.5.1.1 Server-side verification

In order to facilitate signature and seal verification, the OP MAY offer a free OJ server-side SVA that operates according to the verification workflow specified below:

1. The verifier uploads the PDF/A file to be verified with the associated signature or seal file using the file upload functionality provided by the SVA;
2. The SVA calculates the digest of the uploaded PDF/A file and verifies whether the calculated digest is contained in the manifest part of the uploaded signature;
3. Upon successful digest verification, standard XAdES verification of the uploaded signature or seal candidate is performed, provided that the signing or sealing certificate identifies an authorised OJ signer for the period determined by the signature timestamp. The SVA also verifies that the signer was authorised to sign when, according to the signature timestamp, the signature was created;
4. The verification succeeds when all previous steps terminate successfully. Otherwise, the verification fails. In any event, a comprehensible report of the verification process is presented to the verifier.

3.1.5.1.2 Client-side verification

In order to facilitate signature and seal verification, the OP MAY offer a free OJ client-side SVA which operates according to the verification workflow specified below:

1. The verifier starts the downloaded SVA, its code signature is automatically verified by the runtime environment and execution is authorised by the verifier upon successful code signature verification;
2. The verifier selects a PDF/A file in a certain linguistic version to be verified with the associated candidate signature or seal file on the local PC file system using the file selection dialogue provided by the SVA;
3. The SVA calculates the digest of the selected document and verifies whether the calculated digest is contained in the manifest of the selected signature or seal candidate;
4. Upon successful digest verification, standard XAdES verification of the selected signature or seal candidate is performed.
5. The verification process succeeds when all previous steps terminate successfully and when the signing or sealing certificate identifies an authorised OJ signer for the period determined by the signature timestamp.

   Note that the authorised signer information MAY be known to the SVA on the basis of a (default) configuration. However, the certificate digest of the signing or sealing certificate is additionally indicated in the SVA result, so that the verifier can manually compare it with the published legal signer information pertaining to the signature or seal creation period, which is also indicated in the SVA result.

3.2 BSPs mainly influenced by the legal/regulatory provisions associated to the concerned application/business process

3.2.1 BSP (f): Legal type of the signatures

Electronic signatures and seals placed on OJ or OJ-Act SHALL be QESig and QESeal in the sense of [eIDAS].

The above requirement is mandated in particular by the Council Regulation on electronic publication of the Official Journal of the European Union (cf. section 2.2).

A QC is to be obtained by each signer as a prerequisite for using the signature system.

The quality of specific elements of the requisite QESig and QESeal SHALL satisfy the following quality requirements:

- signing and sealing device: QSCDs compliant with Annex II of [eIDAS];
- certificate provision: QC compliant with Annex I of [eIDAS];
- independent assurance on certificate provision: QC issued by a supervised or accredited QTSP certification service accredited from any country to which [eIDAS] applies;
- signature cryptographic suite: only signature suites listed in section 7.3 of [ETSI 2022-Crypto] shall be used;
- LTV solutions: OJ or OJ-Act XAdES (cf. [ETSI 2022-XAdES]) signature and seal forms SHALL be augmented to the -LTA form including the renewal of the archival timestamps or other (external secure archival mechanisms MAY be considered as an alternative to archive timestamp renewal provided they are of equivalent or higher quality);

- signature creation application: the quality of the OJ SCA SHALL satisfy the quality requirements imposed by EC policies and comply with the requirements of the Council Regulation on the electronic publication of the Official Journal of the European Union.

3.2.2 BSP (g): Commitment assumed by the signer

Electronic signatures and seals placed on OJ or OJ-Act issues SHALL be generated on behalf of the OP in accordance with the Council Regulation on electronic publication of the Official Journal of the European Union.

The commitment made by an authorised OJ signer expresses that the signed data represents an authentic OJ or OJ-Act issue that has been properly validated with respect to the rules on the scope of business application (cf. section 3.1.1) and published by the OP in line with the Council Regulation on electronic publication of the Official Journal of the European Union so as to serve as an authentic source of EU law.

No explicit commitment type indication SHALL be contained in an OJ signature (cf. section 5.2.3 of [ETSI 2022-XAdES]).

3.2.3 BSP (h): Level of assurance on timing evidence

A signature timestamp SHALL be added to OJ or OJ-Act signatures or seals that are created as described in sections 3.1.1.2 or 3.1.1.3, on the same day (local time in Luxembourg) as the date of the signature or seal of the OJ or OJ-Act issue, in order to certify that the signature or seal was not created after the date of publication. This ensures that the set of authorised signers applicable on the publication date are applicable for the signature or seal.

The OJ SCA SHALL ensure that all XAdES-B-T signatures that are generated fulfil this requirement.

The timestamp used for the purpose of creating signature timestamps in XAdES-B-T signatures SHALL be qualified timestamps.

PAdES signatures created in case of an emergency situation as described in section 3.1.1.4 MAY be created without a signature timestamp.

If PAdES signatures created in case of an emergency situation as described in section 3.1.1.4 are created with a signature timestamp, the signature timestamp SHOULD be a qualified timestamp and applied on the same day (local time in Luxembourg) as the date of the signature or seal of the OJ or OJ-Act issue, in order to certify that the signature or seal was not created after the date of publication.

NOTE: This means that in case of an emergency situation, if a signature timestamp is included in the signature, it can be a non-qualified timestamp.

All other timestamps, including archival timestamps and content timestamps if any, SHOULD be qualified timestamps.

3.2.4 BSP (i): Formalities of signing

It is the responsibility of the OJ SCA to provide a signer interface in such a manner so as to guarantee, to the extent possible, a valid legal signature and seal environment. The interface must:

- include the provision of proper advice and information on the application's signature and seal process;
- ensure consistency between the use of the appropriate signature and seal creation and verification data, the signature and seal creation devices, the data to be signed and the expected scope and purpose of the signature and seal (or act of signing or sealing);

- allow and demonstrate a clear expression of will to sign and the user's intention to be bound by the signature or seal;
- allow and exhibit informed consent.

The OJ SVA SHALL provide relying parties (including the signer) with correct procedures for verification and archival of the electronic signature or seal, and verification data.

3.2.5 BSP (j): Longevity and resilience to change

The signed OJ or OJ-Act issues and their signatures MUST be retained for an indefinite period of time. The preservation of the validity of the OJ or OJ-Act signatures MUST be ensured for such a time period (cf. Article 2 of the Council Regulation on electronic publication of the Official Journal of the European Union).

3.2.6 BSP (k): Archival

Not Applicable.

3.3 BSPs mainly related to the actors involved in creating/augmenting/ validating signatures

3.3.1 BSP (l): Identity (and roles/attributes) of the signers

3.3.1.1 Proposed Signer and Identification Rules

OJ or OJ-Act signatures SHALL be applied by authorised signers, who specifically SHALL be officials of the OP having the requisite expertise for validating OJ or OJ-Act issues in accordance with the rules pertaining to the scope of business application (cf. section 3.1.1.3). In the case of OJ or OJ-Act seals, the authorised signer SHALL be the OP itself as an entity of the European Commission.

Authorised signers SHALL also be conscious of their responsibility and SHALL act faithfully in authenticating legal texts representing EU law.

The link between these natural person signers and their signature verification data SHALL be attested in a QC in terms of [eIDAS] confirming their identity and their affiliation with the OP.

Authorisation of an OJ signer SHALL be performed by the Director General of the OP (possibly by delegation).

3.3.1.2 Signer's roles and attributes

No further role, function or qualification attribute SHALL require certification in the signer's QC apart from the signer's affiliation with the OP.

It SHALL be the responsibility of the OJ SCA to ensure proper access control and signer authorisation prior to granting access to signers to the signature facilities of the AOJ.

Access control and signer authorisation SHALL be performed on the basis of a strong authentication mechanism implemented in the SCA and the permissions registered with the public key certificates corresponding to the authorised signers in the SCA user management database.

Relying parties *MAY* use the published certificates of OJ signers for verifying their legal entitlement.

3.3.1.3 Associated proof of authority

No further stipulation apart from section 3.3.1.2.

3.3.2 BSP (m): Level of assurance required for the authentication of the signer

The level of assurance required for the authentication of the signer is ensured by its qualified certificate and its signature creation means which SHALL be a qualified signature/seal creation device as defined in [eIDAS].

3.4 Other BSPs

3.4.1 BSP (o): Other information to be associated with the signature or seal

3.4.1.1 Authorised OJ signers and timestamping authorities

Verifying the authorisation of signers is a key trust element of the AOJ.

Authorisation SHALL be made explicit by publishing the electronic certificates of all authorised signers via a trusted medium external from the SCA/SVA.

The publication of authorised OJ signers SHALL indicate that the supervision status of the signer certificates is guaranteed for the current OJ or OJ-Act signing period.

Authorised OJ signers and timestamping authorities SHALL NOT be published in the OJ, because this approach would create circular reasoning issues, particularly with respect to long-term validation.

When authorised OJ signers change over time, the previous set of signers SHALL be published as historical trust information. This is required for verifying OJ or OJ-Act issues signed by these signers.

The publication of authorised signers SHALL specify the period for which the listed signers were or are authorised, this specification to be in line with the timing constraints of the present policy version.

3.4.1.2 Electronic signature and seal attributes, scope and purpose rules

The signature and seal creation processes SHALL make appropriate use of signature attributes, in particular the signed attributes which are pieces of information that support the electronic signature/seal and which are covered by the signature/seal together with the DTBS in accordance with the following:

- The signing certificate identifier SHALL be used. It is the identifier of, or a reference to, the certificate holding the signature verification data corresponding to the signature or seal creation data used by the signer to create the electronic signature or seal;
- A signature policy indication MAY be used (cf. section 1.2.2);
- The claimed signing time SHALL be used. It indicates the time when the signer claims to have created the signature or seal.

  Note that this time represents the current system time of the signer's workstation. It is NOT a trusted time.

  The OJ SCA owner SHALL (by delegation of the Director General of the OP) make provisions that the current system time of all signer workstations is accurate.

  This can be achieved by using NTP with a suitable time source (cf. [Mills 2010]).
- NO commitment type indication SHALL be used;
- Other signed attributes MAY be used.

The usage of signature attributes MUST be in accordance with [ETSI 2010] and Commission Decision 2011/130/EU of 25 February 2013.

3.4.2 BSP (p): Cryptographic suites

See section 3.2.1.

4 Requirements / statements on technical mechanisms and standards implementation

4.1 Trusted timestamping rules

The XAdES-B-LTA signature form (cf. [ETSI 2022-XAdES]) requires several timestamps that SHALL be obtained from a qualified timestamping service accredited in a Member State or EEA country.

The OJ SCA owner SHALL (by delegation of the Director General of the OP) make provisions that the SCA is configured to use suitable cryptographic algorithms.

4.2 Long-term validity rules

Preservation of the validity of OJ or OJ-Act signatures during the expected preservation period is ensured by virtue of the implementation of the XAdES-B-LTA form (cf. [ETSI 2022-XAdES]) and subsequently by augmenting the signature with an additional qualified archive timestamp to extend its validity as needed or a suitable archival solution providing preservation guarantees of the signature validity.

4.3 Other business and legal matters

Since the OJ is published from Monday to Friday, and possibly during the weekend, the OJ SCA owner MUST (by delegation of the Director General of the OP) make provisions that the SCA is continuously operable.

For this purpose, suitable service level agreements SHOULD be established.

Although OJ or OJ-Act signatures and seals can be verified by any SVA complying with the standards and rules defined by the OJ signature policy, which also requires manifest validation, the OP MAY expose a publicly accessible SVA on the EUR-Lex website in order to enable relying parties, in particular European citizens, to verify OJ or OJ-Act signatures without the need to procure a third-party utility.

The OP MAY, in the alternative, provide an SVA as a publicly downloadable utility that can run independently on the user’s desktop and requires only that a verifier trust the software when relying on the results produced by it.

5 Appendix

[Bartel 2008]	Bartel M., Boyer J., Fox B., LaMacchia B., Simon E. *XML Signature Syntax and Processing (Second Edition)* W3C Recommendation, 2008
[Bradner 1997]	Bradner S. *Key words for use in RFCs to indicate requirement levels* RFC 2119, Network Working Group, 1997
[Mealling 2010]	Mealling M. *A URN Namespace of Object Identifiers* RFC 3061, Network Working Group, 2001
[Mills 2010]	Mills D., Delaware U., Martin J., ISC Ed., Burbank J., Kasch W. *Network Time Protocol Version 4: Protocol and Algorithms Specification* RFC 5905, IETF, 2010
[eIDAS]	*Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC* Official Journal L 257
[ETSI 2015]	ETSI-ESI *Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents* TS 119 172-1, v1.1.1, ETSI, 2015
[ETSI 2016]	ETSI-ESI *Electronic Signatures and Infrastructures (ESI);* *Policy and security requirements for applications for signature creation and signature validation* TS 119 101, v1.1.1, ETSI, 2016
[ETSI 2016-PAdES]	ETSI-ESI PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures ETSI EN 319 142-1 V1.1.1 (2016-04)
[ETSI 2022-XAdES]	ETSI-ESI XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures ETSI EN 319 132-1 V1.2.1 (2022-02)
[ETSI 2022-Crypto]	ETSI-ESI Cryptographic Suites ETSI TS 119 312 V1.4.2 (2022-02)