Authentic Official Journal Signature Policy

Version 2

(1.3.171.4.1.1.2)

Effective as of July 1st, 2013

Table of Contents

1 Introduction 1

1.1 Overview 1

1.2 Signature Policy Name, Identification and Conformance Rules 2

1.2.1 Signature Policy Name 2

1.2.2 Signature Policy Identifier 2

1.2.3 Signature Policy Conformance Rules 2

1.2.4 Signature Policy Distribution Points 2

1.2.5 Signature Policy Validity Period 2

1.3 Signature Policy Issuer 2

1.4 Signature Policy Administration 3

1.4.1 Organisation Administering the Document 3

1.4.2 Contact Person 3

1.4.3 Policy Versions 3

1.5 Definitions and Acronyms 4

2 Electronic Signature Flow Business Rules 4

2.1 Scope of Business Application 4

2.1.1 Scope and Boundaries of the AOJ Signature Policy 6

2.1.2 Scope of Application 6

2.1.3 Transactional Context 6

2.2 Associated Policy Requirements 6

2.3 Associated Legal Requirements 7

2.4 Business Scenario Use Cases and Electronic Signature Flow 8

2.4.1 AOJ Signature Creation 8

2.4.2 AOJ Signature Verification 10

2.5 Timing Constraints and Sequences 11

2.6 Data to Be Signed 11
2.7 Signer's Identification 12
2.7.1 Proposed Signer and Identification Rules 12
2.7.2 Signer Roles and Attributes 12
2.7.3 Associated Proof of Authority 12
2.8 Signature Commitment Type 13
2.9 Other Signature Attributes 13
2.10 Signing Formalities 13
2.11 Long-Term Validity Requirements 13
2.12 Risk Assessment 13
2.13 Technical Security Considerations 14
2.14 Legal Statements 14
2.15 Access Control Management 14
3 Electronic Signature Implementation Rules 14
3.1 Detailed Electronic Signature Arrangement Rules 14
3.2 Electronic Signature Types 15
3.3 Signer Identification Rules 16
3.4 Rules on Data to Be Signed 16
3.5 Electronic Signature Attributes, Scope and Purpose Rules 17
3.6 Trusted Time-Stamping Rules 17
3.7 Long-Term Validity Rules 17
3.8 Security Considerations 18
3.9 Electronic Signature Format Rules 18
3.10 Detailed Technical Creation and Verification Rules 18
3.11 Signature Creation and Verification Application Implementations Rules 18
3.11.1 Signature Creation Application 18
3.11.2 Signature Verification Application 19

3.12 Signature Policy Documents 19
4 Compliance Audit and Other Assessments 19
5 Other Business and Legal Matters 19
6 Annexes 20
6.1 Bibliographic References 20
6.2 Authorised OJ Signers and Time-stamping Authorities 21

1 Introduction

This document specifies the signature policy for the Authentic Official Journal Signature (AOJ signature), which is employed to authenticate the electronic version of the Official Journal of the European Union (OJ) in accordance with the Council Regulation Council Regulation (EU) No 216/2013 of 7 March 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 and validation of one or more interrelated electronic signatures 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 workflow transparent to all involved parties, i.e. signatories, recipients and arbitrators, so that electronic signatures complying with policy requirements may engender increased confidence in the applicability and acceptance of these signatures.

The detailed concepts of a signature policy are explained in [SEALED 2010 a], which also defines the guidelines and structure for the present document.

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 Tuesday to Saturday, and eventually on Monday, 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 AOJ signature policy formalises key elements of the implementation of electronic signature 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 signature policy, signature policy issuer details, policy administration, definitions and acronyms, etc.
- The Electronic Signature Flow Business Rules,
- The Electronic Signature Implementation Rules,
- Compliance Audit and Other Assessments,
- Other Business and Legal Matters and
- Annexes.

[1] OJ L 69, 13.3.2013, p. 1–3

1.2 Signature Policy Name, Identification and Conformance Rules

1.2.1 Signature Policy Name

The AOJ signature policy is entitled as follows:

Authentic Official Journal Signature Policy

1.2.2 Signature Policy Identifier

Since the publication of the OJ is a dedicated and well-known process of European Union legislation, the AOJ signature policy can be identified implicitly by any party.

In order to indicate the policy explicitly, each AOJ signature *MAY* include an explicit signature policy indication as defined in section 7.2.3 of [ETSI 2010]. If included the explicit signature policy indication *SHALL* indicate the object identifier 1.3.171.4.1.1.2 using the encoding rules specified in section 7.1.2 of [ETSI 2010] and in [Mealling 2010].

The globally unique object identifier 1.3.171.4.1.1.2 unambiguously identifies the present version of this signature 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 1.1.2 identifies the present OJ signature policy version, and its ASN.1 value notation with names *SHALL* be {oj(1) signature-policy(1) version(2)}.

1.2.3 Signature Policy Conformance Rules

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

1.2.4 Signature Policy Distribution Points

The AOJ signature policy document is published on the EUR-Lex website. It can be accessed from the website of the Publications Office at http://publications.europa.eu .

1.2.5 Signature Policy Validity Period

The present signature policy *SHALL* apply to all OJ issues published on or after the date when the Council Regulation on the electronic publication of the Official Journal of the European Union enters into force. The present signature policy is not applicable to the Supplement to the Official Journal of the European Union (S series, Official Journal S or OJ S).

1.3 Signature Policy Issuer

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

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

The issuer of the AOJ signature policy is responsible for:

- specifying and approving the AOJ signature policy,

- defining the review process for the AOJ signature policy,
- defining the assessment criteria and process ensuring that the AOJ signature policy successfully complies with the European Commission's rules,
- defining the assessment criteria and process ensuring that applications claiming compliance with the AOJ signature policy successfully comply with its present rules in actuality,
- publication to the parties relying on the AOJ signature policy and amended versions thereof.

1.4 Signature Policy Administration

1.4.1 Organisation Administering the Document

The AOJ signature policy is administered by the Publications Office of the European Union (cf. section 1.3 for details).

1.4.2 Contact Person

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

Contact person:	The Head of Unit Official Journals 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@publications.europa.eu

1.4.3 Policy Versions

The initial and amended versions of the AOJ signature policy *MAY* specify a minimum effective date. When a version of the AOJ signature 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 time-stamp on the AOJ signature of the AOJ issue in which the policy version is published, according to Central European Time during the winter period (UTC+1:00) and Central European Summer Time during the daylight saving period (UTC+2:00).
3. The day following the date of publication of the policy version.

Any given amended version of the AOJ signature policy *SHALL* automatically expire when the respective subsequent amended version goes into effect. A subsequent amended version of the AOJ signature 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 AOJ signature policy is not subject, whether directly or indirectly, to the same version of the AOJ signature policy in order to prevent circular reasoning.

1.5 Definitions and Acronyms

Acronym	Definition
	EN
AOJ	Authentic Official Journal
CA	Certificate Authority
CSP	Certification Service Provider
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
QES	Qualified Electronic Signature
SCA	Signature Creation Application
SSCD	Secure Signature Creation Device
SVA	Signature Verification Application
WIPIWIS	What Is Presented Is What Is Signed

2 Electronic Signature Flow Business Rules

2.1 Scope of Business Application

The OP publishes the OJ from Tuesday to Saturday, and eventually on Monday. The documents to be published are grouped by individual issues. An OJ issue represents a multilingual publication of several legal texts. Each linguistic version of an issue consists of the entire text comprising all acts in a single document.

Individual OJ issues are categorised according to the series to which they belong, with the category as an identifying part of the OJ numbering scheme. 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 a candidate/new Member State containing EU secondary law. These special editions are also part of the scope.

Once an OJ issue is complete and ready for publication, it enters the signature creation workflow. During this process an authorised person of the OP verifies whether the set of PDF/A documents comprising this issue represent the correct result supplied by EU legislation. It is verified in particular that no obvious errors have been introduced due to the various document transformation processes required for successful publication.

Verification of an OJ issue is performed by an authorised OJ signer examining the content of the issue using a conformant PDF reader integrated in the signature creation application (SCA) that visualises the content. In doing so the content is examined on the basis of the signer's expert knowledge and complementary information.

When verification fails, the issue is rejected. Upon successful verification, the issue is signed by the authorised signer employing a qualified signature according to Directive 1999/93/ EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures[2]. This signature

- legally guarantees the integrity, authenticity and inalterability of the text of the issue,
- links the issue to its signatory,
- links the issue to the date and time when it was signed with a claimed signing time,
- links the issue to the trusted date and time with a trusted time-stamp immediately created after the issue was signed and
- is subsequently extended to a self-sustainable form in order to ensure long-term preservation of its validity

The signature *SHALL* be capable of being verified by a judge or any relying party, and *SHALL* not require the verifier's trust in the AOJ SCA.

Since a detached XAdES signature with a manifest (cf. [Bartel 2008], [ETSI 2010] 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[3]) is employed for signing each issue, when verifying an AOJ signature it is also necessary to perform a validation of the

[2] OJ L 13, 19.1.2000, p. 12–20
[3] OJ L 53, 26.2.2011, p. 66–72

manifest in addition to the XML signature core (cf. [Bartel 2008]) during [ETSI 2010] validation, for the purpose of verifying an AOJ signature.

2.1.1 Scope and Boundaries of the AOJ Signature Policy

The AOJ signature policy covers electronic signatures 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.

2.1.2 Scope of Application

The electronic signatures covered by the AOJ signature policy are only those that are described in this section (cf. section 2.1).

2.1.3 Transactional Context

Not applicable.

2.2 Associated Policy Requirements

Issues of the AOJ 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 an advanced electronic signature based on a QC and created with an SSCD in accordance with Directive 1999/93/EC of 13 December 1999[2].

Electronically signing OJ issues falls under the implementation of a signature as a substantial formality as stated in Article IV.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[4], which also mandates that electronic signatures applied to the AOJ require a qualified electronic signature as defined in Directive 1999/93/EC of 13 December 1999[2].

Pursuant to Article V.2 of IMPLEMENTING RULES FOR THE DECISION 2002/47/EC AND FOR THE DECISION 2004/563/EC [4], the verification of the signing authority is the responsibility of the AOJ SCA when enabling an official of the OP to electronically sign OJ issues.

Although OJ issues in electronic format cannot have legal effect without being signed, the AOJ signature policy also stipulates that the AOJ 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 AOJ SCA user management,

[4] SEC(2009)1643

- *SHOULD* be restricted to corporate certificates that guarantee the subject's affiliation to the OP,[5]

- *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.

2.3 Associated Legal Requirements

The implementation of electronic signatures as covered under the AOJ signature policy *SHALL* be governed by the following legal provisions:

- Council Regulation on the electronic publication of the Official Journal of the European Union

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures[2]

- 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 [6]

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[7]

- 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)[8]

- 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[9]

- 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[10]

[5] Corporate certificates guarantee the subject's affiliation to a specific organization. Security is augmented because the issuing CSP enforces the proof of entitlement of the respective certificate owner.
[6] OJ L 274, 20.10.2009, p. 36–37
[7] OJ L 281, 23.11.1995, p. 31–50
[8] OJ L 201, 31.7.2002, p. 37–47
[9] OJ L 337, 18.12.2009, p. 11–36
[10] OJ L 199, 31.7.2010, p. 30–35

- 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[11]

- 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]

2.4 Business Scenario Use Cases and Electronic Signature Flow

The following steps describe the high-level signature workflow as implemented in the AOJ SCA (cf. [CEN 2004 b]) and SVA (cf. [CEN 2004 c]).

2.4.1 AOJ Signature Creation

1. A complete OJ issue supplied by the CERES system – part of the OJ production chain – is detected.

2. A manifest with a reference to the whole issue in the individual EU languages is generated, with each issue 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 prepared 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 – integrated in the SCA – prior to being able to sign the issue. If the OJ edition has less than three linguistic versions, then the authorized 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.

[11] OJ L 168, 30.6.2009, p. 41–47

c. Upon pressing the Sign button

   i. The SCA signer applet is downloaded and its code signature is verified by the client-side runtime environment prior to executing the applet.

   ii. The manifest pertaining to the AOJ issue to be signed is downloaded by the applet and then transferred to the SSCD attached to the signer PC to be signed together with other attributes (cf. section 3.5).

   iii. For this purpose, the qualified signing certificate of the signatory, issued by an accredited European CSP (cf. Commission Decision 2010/425/EU of 28 July 2010[10]) is automatically and unambiguously selected on the SSCD and presented to the authorised signer, who in turn is prompted to enter the corresponding PIN in order to authorise the SSCD to create the signature using the private key corresponding to selected signing certificate, thus completing the signing process.

5. The XAdES signature (cf. [ETSI 2010]) created in this manner is uploaded to the server-side part of the SCA, which checks the validity of algorithms used among other things and verifies

   a. that the signed manifest is the manifest that was previously downloaded for signing and

   b. 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 extended with a signature time-stamp provided by an accredited European CSP (cf. Commission Decision 2010/425/EU of 28 July 2010[10]).

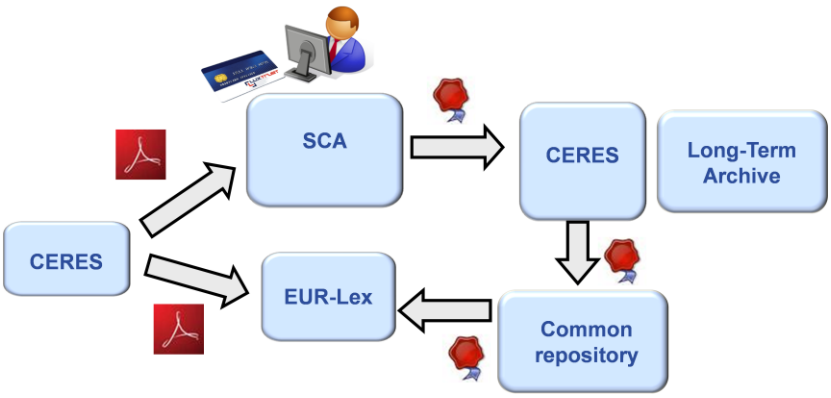
7. It is verified that the signed and time-stamp-extended issue has not been updated during signature creation so as to comply with the WIPIWIS principle (cf. section 3.1).

8. The signature extended during the previous processing step is transferred to the CERES system for publication on the EUR-Lex website. An identical copy of the signature is retained by the SCA at the same time.

9. When the required grace period for a signature resulting from the previous processing step has lapsed, it is further extended to a self-sustainable form using the trusted time-stamp service of an accredited European CSP (cf. Commission Decision 2010/425/EU of 28 July 2010[10]).

10. The signature extended during the previous processing step is transferred to the CERES system for publication on the EUR-Lex website, replacing the signature from step 8 that had not yet been extended to a self-sustainable form.

    Apart from publication on the EUR-Lex website, identical copies of the documents comprising an issue, along with the corresponding signature in a self-sustainable form, are handed over to the electronic archive system for official documents of the EU Institutions, which is managed by OP, for long-term preservation. However, implementation aspects concerning long-term preservation are NOT addressed by the present signature policy.



2.4.2 AOJ Signature Verification

Any relying party, in particular any European citizen, can download an AOJ issue published on the EUR-Lex website and the corresponding detached XAdES signature (cf. [ETSI 2010]) for verification.

Since an interoperable European signature standard and services of an accredited European CSP (cf. Commission Decision 2010/425/EU of 28 July 2010[10]) are used during signature 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 AOJ signature policy.

2.4.2.1 Server-Side Verification

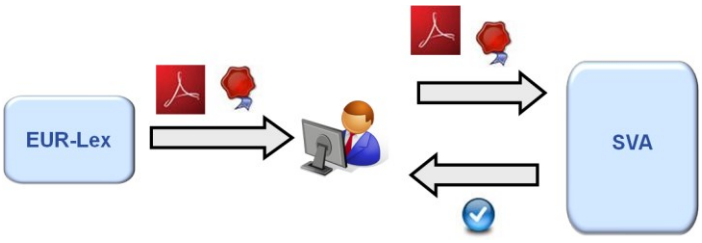
In order to facilitate signature verification, the OP *MAY OPTIONALLY* offer a free AOJ server-side SVA (cf. section 5) that operates according to the verification workflow specified below:

1. The verifier uploads the PDF/A file to be verified with the associated signature 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 uploaded signature.

3. Upon successful digest verification, standard XAdES verification of the uploaded signature candidate is performed, provided that the signing certificate identifies an authorised AOJ signer for the period determined by the signature time-stamp. And the SVA verifies that the signer was authorised to sign when, according to the signature time-stamp, the signature was created.

4. Signature verification succeeds when all previous steps terminate successfully. Otherwise signature verification fails. In any event, a comprehensible report of the verification process is presented to the verifier.



2.4.2.2 Client-Side Verification

In order to facilitate signature verification, the OP *MAY OPTIONALLY* offer a free AOJ client-side SVA (cf. section 5) 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 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 candidate.

4. Upon successful digest verification, standard XAdES verification of the selected signature candidate is performed.

5. Signature verification succeeds when all previous steps terminate successfully and when the signing certificate identifies an authorised AOJ signer for the period determined by the signature time-stamp.

   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 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 creation period, which is also indicated in the SVA result.

2.5 Timing Constraints and Sequences

A signature time-stamp *MUST* be added to an AOJ signature (cf. step 6 in section 2.4.1) on the same day (according to Central European Time during the winter period (UTC+1:00) and Central European Summer Time during the daylight saving period (UTC+2:00) as the date of publication of the AOJ issue, in order to certify that the signature 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.

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

2.6 Data to Be Signed

An AOJ signature is an XML manifest signature (cf. [Bartel 2008] and [ETSI 2010]) which combines all the linguistic versions available in PDF/A format pertaining to an OJ issue in a single signature that must comply with the following requirements:

- Each linguistic version logically associated with an OJ issue *MUST* have its own digest value.

  All linguistic version logically associated with an OJ 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 2.1, in order to honour the WIPIWIS principle.

- Proper visualisation *MUST* be guaranteed by using a PDF/A conformant reader (cf. [CEN 2004 b] and [CEN 2004 c]).
- Only the linguistic versions pertaining to the particular issue being signed *SHALL* be presented to the signer during the signing process.

2.7 Signer's Identification

2.7.1 Proposed Signer and Identification Rules

AOJ signatures *SHALL* be applied by authorised signers, who specifically *SHALL* be officials of the OP having the requisite expertise for validating OJ issues in accordance with the rules pertaining to the scope of business application (cf. section 2.1).

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 signatories and their signature verification data *SHALL* be attested in a QC in terms of Directive 1999/93/EC of 13 December 1999[2] confirming their identity and their affiliation with the OP.

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

- during certificate procurement and
- certificate publication (cf. section 2.2) and
- when linking the procured certificates to SCA permissions in the SCA user management database.

2.7.2 Signer Roles and Attributes

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

It *SHALL* be the responsibility of the AOJ SCA to ensure proper access control and signer authorisation prior to granting access to signatories 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 AOJ signers for verifying their legal entitlement (cf. section 6.2)

2.7.3 Associated Proof of Authority

No further stipulation apart from section 2.7.2.

2.8 Signature Commitment Type

Electronic signatures placed on AOJ 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 AOJ signer expresses that the signed data represents an authentic OJ issue that has been properly validated with respect to the rules on the scope of business application (cf. section 2.1) 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 a authentic source of EU law.

No explicit commitment type indication *SHALL* be contained in an AOJ signature (cf. section 7.2.6 of [ETSI 2010]).

2.9 Other Signature Attributes

No further stipulations apart from the requirements mandated by Commission Decision 2011/130/EU of 25 February 2011[3].

2.10 Signing Formalities

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

- include the provision of proper advice and information on the application's signature process,
- ensure consistency between the use of the appropriate signature creation and verification data, the signature creation device, the data to be signed and the expected scope and purpose of the signature (or act of signing);
- allow and demonstrate a clear expression of will to sign and the user's intention to be bound by the signature;
- allow and exhibit informed consent.

The AOJ SVA *SHALL* provide relying parties (including the signatory) with correct procedures for verification and archival of the electronic signature and verification data.

2.11 Long-Term Validity Requirements

The signed AOJ issues and their signatures *MUST* be retained for an indefinite period of time. The preservation of the validity of the AOJ 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).

2.12 Risk Assessment

A risk assessment on the implementation of electronic signatures in the context of the AOJ SCA for the purpose of electronically signing OJ issues governed by the Council Regulation on electronic publication of the Official Journal of the European Union *SHALL* be performed by the AOJ SCA owner (by delegation of the Director General of the OP) and made available on request for audit purposes where applicable.

This requirement *SHALL* also apply to an AOJ SVA.

2.13 Technical Security Considerations

Cryptographic tools eligible for the implementation of AOJ signatures *SHALL* satisfy the requirements of qualified electronic signatures as defined by Directive 1999/93/EC of 13 December 1999[2] and relevant state-of-the-art practices.

2.14 Legal Statements

Electronic signatures placed on AOJ 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.

2.15 Access Control Management

No further stipulations.

3 Electronic Signature Implementation Rules

3.1 Detailed Electronic Signature Arrangement Rules

The following remarks are in reference to the signature workflow of the AOJ SCA specified in section 2.4.1 of the present document.

Steps 1 and 2 relate to the preparation of the DTBS:

- The OJ issue is prepared for signing. This is the beginning of the signing process.
- All involved resources, i.e. all the linguistic versions representing the issue, are locked against further changes or substitution. The manifest is generated.

Note that complete resource locking is critical for the consistency of the entire signature process.

Step 3 describes the selection of the DTBS, which is necessary because multiple instances of a DTBS may be available for signing.

Steps 4 and 5 detail how the signatory signs the issue – with his or her smart card and reader attached to the local PC – via a signer applet to create a basic XAdES signature with an optional policy indication (cf. [ETSI 2010] and section 1.2.2).

Showing the PDF/A content to be signed to the signatory is part of the signature process (cf. step 4.a) for the purpose of complying with the WIPIWIS principle.

At the end of the signing process a validation is performed to determine whether the signer is authorised. This is necessary because signature creation is a client-side operation and can not be directly controlled by the server-part of the SCA (cf. step 5).

Step 7 guarantees that the signed data has not been asynchronously updated during signing, which is critical for the process. The chosen approach represents an optimistic locking strategy, i.e. if data to be signed was modified during signing, this would be detected during this particular step and signature creation would be aborted.

Step 9 guarantees that the signature contains the necessary validation data in order to enable long-term validation even if online services used for validating the signature at the present time are no longer available or can no longer provide the necessary validation data with respect to the point of time when the signature or time-stamps contained in the signature were created.

Note that this latter step does not replace an electronic archive because it can only provide a first set of validation data. It is, however, necessary to add additional validation data for also validating validation data already collected when the risk is posed that online validation of collected validation data is no longer feasible.

The grace period *MUST* be respected in order to guarantee that correct timing constraints for validation data are evident. For example, revocation status information for a given signature can not be evident unless it is provable that the status information was not generated prior to the point in time when the given signature was created.

A*n SVA workflow has no impact on the legal value of a signed OJ issue.*

3.2 Electronic Signature Types

Electronic signatures placed on AOJ *SHALL* be QES in the sense of Directive 1999/93/EC of 13 December 1999[2], i.e. advanced electronic signatures that are based on a QC compliant with Annex I of Directive 1999/93/EC of 13 December 1999[2], issued by a CSP compliant with its Annex II and that are created by an SSCD compliant with its Annex III.

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 signatory as a prerequisite for using the signature system. The QC should be purchased from an accredited CSP.

The quality of specific elements of the requisite QES *SHALL* satisfy the following quality requirements:

- Signing Device: SSCD compliant with Annex III of Directive 1999/93/EC of 13 December 1999[2].
- Certificate Provision: QC compliant with Annex I of Directive 1999/93/EC of 13 December 1999[2].
- Independent Assurance on Certificate Provision: QC issued by a supervised or accredited CSP certification service accredited in a Member State or EEA country.
- Signature Cryptographic Suite: The quality level *SHALL* be equal to 3 at minimum, as defined in [SEALED 2010 b] although a quality level equal to or higher than 4 is recommended.
- LTV solutions: AOJ XAdES (cf. [ETSI 2010]) signature forms *SHALL* be extended to the -A form including the renewal of the archival time-stamps or other (external secure archival mechanisms *MAY* be considered as an alternative to archive time-stamp renewal provided they are of equivalent or higher quality).

- Signature Application: The quality of the AOJ 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.

3.3 Signer Identification Rules

A QC of the AOJ signer *SHALL* include confirmation of the signatory's first and last name, as well as his or her affiliation with the OP.

The AOJ SCA *SHALL* ensure proper access control and authorisation prior granting access to signatories to the signature facilities of the AOJ. This *SHOULD* be done by way of a strong authentication mechanism implemented in the SCA (cf. section 2.7.2).

The AOJ application owner *SHALL* (by way of delegation of the Director General of the OP) guarantee

- that access control and signer authorisation of the AOJ SCA is correctly configured in accordance with the AOJ signature policy version in effect at the time of signing,

- that the sets of authorised signers are correctly configured in the AOJ SVA in accordance with the AOJ signature policy versions in effect at the assumed signing time[12] of each OJ issue to be verified.

  Consequently, the AOJ SVA must maintain all sets of authorised signers, along with their respective validity periods, that were valid at any assumed signing time to be supported by the AOJ SVA for verification.

3.4 Rules on Data to Be Signed

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

During the creation of an AOJ signature the file content of a document to be signed is digested as a binary octet string using the strongest supported digest algorithm compliant with section 3.2.

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

The manifest, including the signed attributes (cf. section 3.5), is signed employing XAdES (cf. [ETSI 2010]) with respect to the profile specified in Commission Decision 2011/130/EU of 25 February 2011[3].

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

This obligation *SHALL* also apply to all digest algorithms and the signature algorithm used for AOJ signature creation.

[12] The *assumed signing time* is determined by the nearest verifiable trusted time-stamp that cryptographically covers the signature in question.

3.5 Electronic Signature Attributes, Scope and Purpose Rules

The signature creation process *SHALL* make appropriate use of signature attributes, in particular the signed attributes which are pieces of information that support the electronic signature and which are covered by the signature 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 creation data used by the signer to create the electronic signature.
- 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 signatory claims to have created the signature.

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

  The AOJ SCA owner *SHALL* (by delegation of the Director General of the OP) make provisions that the current system time of all signatory PCs is accurate.

  This can be achieved by using NTP with a suitable time source (cf. [Mills 2010*]).*
- NO commitment type indication *SHALL* be used (cf. section 2.8).

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 2011[3].

3.6 Trusted Time-Stamping Rules

The XAdES-A signature form (cf. [ETSI 2010]) requires several time-stamps that *SHALL* be obtained from a time-stamping service accredited in a Member State or EEA country.

The strongest supported digest and signature algorithms compliant with section 3.2 *SHALL* be used for generating time-stamp signatures.

The strongest supported digest algorithm compliant with section 3.2 *SHALL* be used for generating the message imprint of the data to be time-stamped.

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

3.7 Long-Term Validity Rules

Preservation of the validity of AOJ signatures during the expected preservation period is ensured by virtue of the implementation of the XAdES-A form (cf. [ETSI 2010]) and subsequently by applying time-stamp renewal as needed or a suitable archival solution providing preservation guarantees of the signature validity.

Note that signatures compliant with the present policy version are extended only once to the XAdES-A form. Specifying a subsequent archival solution to guarantee preservation of signature validity is not covered by the present signature policy.

The AOJ application owner *SHALL* (by way of delegation of the Director General of the OP) make provisions for a suitable archival solution providing preservation guarantees of signature validity.

The Publications Office chooses to use as an archival solution the *electronic archive system for official documents of the EU Institutions*.

3.8 Security Considerations

No further stipulations.

3.9 Electronic Signature Format Rules

The AOJ signature form *SHALL* be a detached XAdES manifest signature of an OJ issue in compliance with [ETSI 2010].

The signature *SHALL* be extended to the -T and after the grace period to -A form.

3.10 Detailed Technical Creation and Verification Rules

Qualified certificates and time-stamping authority certificates employed for the AOJ *SHALL* be issued by services accredited in a Member State or EEA country (cf. sections 3.2 and 3.6).

Note that such services are listed in EU Member States' Trusted Lists (cf. Commission Decision 2010/425/EU of 28 July 2010[10]).

Moreover, the AOJ SCA owner *SHALL* (by delegation of the Director General of the OP) make provisions by out-of-band means that the supervision status of the services issuing the certificates employed for signing and time-stamping the AOJ for a given period is properly verified and make this aspect transparent and verifiable by publishing AOJ signers and time-stamp authorities via a trusted medium (cf. section 6.2).

3.11 Signature Creation and Verification Application Implementations Rules

3.11.1 Signature Creation Application

The AOJ SCA that creates electronic signatures on OJ issues implements the WIPIWIS principle. This means that during the signing process, the signatory is put into a position to see what he signs and is guaranteed that the application prevents any change to the content of the document to be signed until his signature. Any collaborator of the signer supposed to help him decide during the ceremony must also be ensured of seeing that exact same inalterable version of the document(s).

In order to do so, the AOJ SCA *MUST* ensure that the data to be signed cannot be misrepresented to the user or altered once the signing process is engaged, and that the to be signed manifest is correctly supplied to the signer applet.

3.11.2 Signature Verification Application

The OP *MAY* be provide an SVA for AOJ signatures to any relying party.

When an SVA is provided it *SHALL* apply the rules defined by the present policy. In particular, it *SHALL* enable a relying party to verify whether an OJ signer was authorised with respect to the assumed signing time (cf. section 3.2).

3.12 Signature Policy Documents

The present signature policy is a formalised and standardised human-readable document providing the applicable set of rules for the creation, verification and preservation of electronic signatures on the AOJ defined and governed by the Council Regulation on the electronic publication of the Official Journal of the European Union.

4 Compliance Audit and Other Assessments

Compliance of the AOJ SCA and SVA with the AOJ signature policy *SHALL* be assessed on a regular basis by an EC internal audit team in accordance with EC internal audit processes.

5 Other Business and Legal Matters

Since the OJ is published from Tuesday to Saturday, and eventually on Monday, the AOJ 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 AOJ signatures can be verified by any SVA complying with the standards and rules defined by the AOJ 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 AOJ 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.

6 Annexes

6.1 Bibliographic References

[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

[CEN 2004 a] CEN
Workshop Agreement, Secure signature-creation devices "EAL 4+"
CWA 14169, European Committee for Standardization, 2004

[CEN 2004 b] CEN
Workshop Agreement, Security requirements for signature creation applications
CWA 14170, European Committee for Standardization, 2004

[CEN 2004 c] CEN
Workshop Agreement, General guidelines for electronic signature verification,
CWA 14171, European Committee for Standardization, 2004

[ETSI 2010] ETSI-ESI
Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)
TS 101 903, v1.4.2, ETSI, 2010

[SEALED 2010 a] SEALED, time.lex and Siemens
CROBIES Work Package 5-1, Guidelines and guidance for cross-border and interoperable implementation of electronic signatures
Final Report, 2010

[SEALED 2010 b] SEALED, time.lex and Siemens
CROBIES Work Package 5-2, Quality Classification Scheme for eSignature elements
Final Report, 2010

6.2 Authorised OJ Signers and Time-stamping Authorities

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

Authorisation *SHALL* be made explicit by publishing the hexadecimal sequence of the certificate hashes of all authorised signer certificates via a medium that is regarded as trusted by employing out-of-band means.

Publication of the hashes must also specify the digest algorithm used to produce the hashes, and this *SHALL* be the strongest algorithm supported at publication time (cf. [SEALED 2010 b]).

The publication of authorised AOJ signers *SHALL* indicate that the supervision status of the signer certificates is guaranteed for the current AOJ signing period, as specified in section 3.10 of the present policy version.

The hashes of the time-stamping authority certificates applicable to the current AOJ signing period shall be published in the same manner. The time-stamping certificate hashes *MUST* be distinguishable from signing certificate hashes, e.g. by grouping the two certificate types separately.

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

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

The publication of authorised signers and time-stamping authorities *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 (cf. section 2.5).