Signature applicability rules for electronic signatures and seals received by the European Commission

DIGIT.B.3

19.12.2023

EUROPEAN COMMISSION

Directorate-General for Digital Services (DIGIT)
Directorate B — Digital Enablers and Innovation
Unit B.3 — Digital Trust

Office: DRB A2/050

E-mail: EC-TL-Service@ec.europa.eu

European Commission
L-2920

EUROPEAN COMMISSION

Signature applicability rules for electronic signatures and seals received by the European Commission

Directorate-General for Digital Services (DIGIT)

2023

EUR EN

Manuscript completed in 19.12.2023

Revised edition

Contents

Document History

Version	Date	Modified Pages
1.0	2021-12-09	First version.
1.1	2022-03-11	Integration of SG.C1 comments.
1.2	2023-07-11	Integration of the EUIBA TL
1.3	2023-12-19	Generalization of the context: decorrelation from the use of a specific validation tool

References

When the version is not indicated in the description, the latest version of the document applies.

Ref	Description
[CID 2015/1506]	Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognized by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance).
[eIDAS Regulation]	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
[ETSI TS 119 101]	ETSI TS 119 101 V1.1.1: “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation”
[ETSI TS 119 172-1]	ETSI TS 119 172-1 V1.1.1: “Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents”
[ETSI TS 119 172-4]	Draft ETSI TS 119 172-4 V0.0.7: “Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists”
[ETSI TS 119 431-2]	ETSI TS 119 431-2 V1.1.1: “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for

Ref	Description
	trust service providers; Part 2: TSP service components supporting AdES digital signature creation”
[ETSI TS 119 441]	ETSI TS 119 441 V1.1.1: “Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services”
[ETSI TS 119 615]	Draft ETSI TS 119 615 V0.0.9: “Electronic Signatures and Infrastructures (ESI); Trusted Lists; Procedures for using and interpreting European Union Member States national trusted lists”
[ETSI TS 119 312]	ETSI TS 119 312: “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites”
[ETSI TS 102 176-1]	ETSI TS 102 176-1: “Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms”
[ETSI EN 319 102-1]	ETSI EN 319 102-1 V1.1.1: “Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation”
[ETSI EN 319 122-1]	ETSI EN 319 122-1 V1.1.1: “Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures”
[ETSI EN 319 132-1]	ETSI EN 319 132-1 V1.1.1: “Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures”
[ETSI EN 319 142-1]	ETSI EN 319 142-1 V1.1.1: “Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures”
[ETSI EN 319 162-1]	ETSI EN 319 162-1 V1.1.1: “Electronic Signatures and Infrastructures (ESI); Associated Signature Containers

Ref	Description
	(ASiC); Part 1: Building blocks and ASiC baseline containers”
[ETSI EN 319 411-1]	ETSI EN 319 411-1 V1.2.2: “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements”
[ETSI TS 103 171]	ETSI TS 103 171 v.2.1.1: "XAdES Baseline Profile"
[ETSI TS 103 172]	ETSI TS 103 172 v.2.2.2: "PAdES Baseline Profile"
[ETSI TS 103 173]	ETSI TS 103 173 v.2.2.1: "CAdES Baseline Profile"
[ETSI TS 103 174]	ETSI TS 103 174 v.2.2.1: "ASiC Baseline Profile"
[EUIBA TL specifications and usage]	“EUIBA Trusted List; Specifications and usage”, version 1.0. Available on the eIDAS Dashboard at https://eidas.ec.europa.eu/efda/tl-browser/#/screen/euiba-tl/home
[ISO 32000-1]	ISO 32000-1:2008 “Document management — Portable document format — Part 1: PDF 1.7”

1. Introduction

1.1. Overview

When receiving electronically signed or sealed documents, the European Commission (hereafter "the Commission") needs to determine whether electronic signatures or seals are *fit for purpose* in its specific business and legal context.

To fulfil this need, rules for determining whether an electronic signature or seal is fit for the Commission's business and legal purpose must be laid down.

Such rules, commonly referred to as *signature applicability rules*, take the form of requirements, specific to the Commission, bearing on electronic signatures and seals that are derived from the Commission's business and legal context.

Those requirements are both legal and technical.

Addressing this need, the present document lays down a set of signature applicability rules defined by the Commission.

For the purpose of implementing a technical process for the determination of whether the electronic signatures and seals received by the Commission conform to those signature applicability rules, this document further defines a *technical applicability rules checking* (TARC) process.

Applications claiming conformance to the present document are expected to implement that TARC process.

In particular, the Commission implements the rules and process laid down hereafter.

Other EU Institutions, Bodies and Agencies (hereafter "EUIBAs") having similar business and legal contexts as the Commission with respect to the electronic signatures and seals they receive, may rely on the present document.

1.2. Business or Application Domain

1.2.1. Scope and boundaries of the signature policy

The present document specifies the rules to be used for the technical validation of digital signatures and the determination of their applicability to the specific context the Commission when the Commission is receiving electronically signed or sealed documents.

The main body of this document (i.e. sections 3 and 4) present a default set of rules aimed at supporting the validation of electronic signatures and seals by the Commission. This default set of rules is particularly appropriate when the signers are parties with whom no bilateral agreements for the recognition of

electronic signatures has been established. When such bilateral agreements have been established however, as is the case when the signers are from within the EUIBAs, and for other specific contexts, an overriding of those rules may be required. For that purpose, Annexes to the present document describe stricter or less strict rules amending the main body of the document for those particular contexts. Additional specific amendments may be applied for specific business cases.

Overriding the present signature applicability rules should be made with care for interoperability and compatibility reasons. In particular, overriding with less strict rules should be discouraged and shall only occur when no parties external to the EUIBAs are involved.

Other requirements bearing on the content of the electronic document not specific to the signature or seal itself are out of scope of the present document.

It is equally out of scope of the present document to define which types of documents are subject to the set of rules laid down hereafter. In particular, the present document does not define which types of documents require the use of qualified electronic signature or qualified electronic seals.

Contexts requiring the application of the set of rules defined hereafter may reference the present document and/or its annexes to declare the technical rules against which the electronic signatures and seals will be validated for the purpose of verifying their applicability in said contexts.

1.2.2. Domain of applications

Not applicable.

1.2.3. Transactional context

Not applicable.

1.3. Document and policy names, identification and conformance rules

1.3.1. Signature policy document and signature policy name

The name of the present set signature applicability rules is “Baseline Signature Applicability Rules for electronic signatures and seals received by the European Commission” (SAR_EC_BASELINE).

1.3.2. Signature policy document and signature policy identifier

The reference for this set of signature applicability rules is SAR_EC_BASELINE_v1.0.

1.3.3. Conformance rules

This document does not claim conformance to any other normative document, however it is structured as per ETSI TS 119 172-1, the reader is advised to refer to that document for more information about the content of each section.

1.3.4. Distribution points

The latest version of the present signature applicability rules is available at the URL https://eidas.ec.europa.eu/efda/api/v1/file-center/download-center/download?file=VALIDATION_TOOL_SIGNATURE_APPLICABILITY_RULES

1.4. Signature policy document administration

1.4.1. Signature policy authority

DIGIT.B.3 is the authority responsible for the present signature applicability rules:

Address: 12, rue G. Kroll L-1882 (postal office Box: L-2920), Luxembourg, Luxembourg.

1.4.2. Contact person

Questions pertaining to the present signature applicability rules can be addressed to Apostolos Apladas via:

- The email address EC-TL-Service@ec.europa.eu

1.4.3. Approval procedures

Any modification made to this document is formally approved by DIGIT.B.3 during a meeting or through email exchanges. Formally approved documents

are sealed by the European Commission. Approved updates to the signature applicability rules currently in force are communicated and published prior to these new signature applicability rules becoming applicable. An amended signature applicability rules shall not take effect earlier than 90 days after publication.

1.5. Definitions and Acronyms

1.5.1. Definitions

For the purposes of the present document, the terms and definitions given in [ETSI TS 119 441] and the following apply:

- **Electronic signature**: data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.
- **Advanced electronic signature:** electronic signature which is
  - uniquely linked to the signatory;
  - capable of identifying the signatory;
  - is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
  - linked to the data signed therewith in such a way that any subsequent change in the data is detectable.
- **Qualified electronic signature:** advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.
- **Electronic seal:** data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;
- **Advanced electronic seal:** electronic seal which is
  - uniquely linked to the creator of the seal;
  - capable of identifying the creator of the seal;
  - is created using electronic seal creation data that the signatory can, with a high level of confidence, use under his sole control; and
  - linked to the data sealed therewith in such a way that any subsequent change in the data is detectable.
- **Qualified electronic seal:** advanced electronic seal that is created by a qualified electronic seal creation device, and which is based on a qualified certificate for electronic seal.
- **Signatory:** natural person who creates an electronic signature.
- **Creator of seal:** legal person who creates an electronic seal.
- **Signer:** Signatory or creator of seal.

- **Electronic signature creation device:** configured software or hardware used to create an electronic signature.
- **Qualified electronic signature creation device:** electronic signature creation device that has been certified as meeting the appropriates requirements laid down in the eIDAS Regulation by a certification body notified to the European Commission, and that has been published by the European Commission in the list of certified qualified electronic signature creation devices.

  NOTE: The list of certified qualified electronic signature/seal creation devices is published by the European Commission here: https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd
- **Electronic signature creation data:** unique data which is used by the signatory to create an electronic signature.
- **Electronic seal creation device:** configured software or hardware used to create an electronic seal.
- **Qualified electronic seal creation device:** electronic seal creation device that has been certified as meeting the appropriates requirements laid down in the eIDAS Regulation by a certification body notified to the European Commission, and that has been published by the European Commission in the list of certified qualified electronic seal creation devices.

  NOTE: The list of certified qualified electronic signature/seal creation devices is published by the European Commission here: https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd
- **Electronic seal creation data:** unique data which is used by the creator of seal to create an electronic seal.
- **Signature augmentation:** process of incorporating to a digital signature information aiming to maintain the validity of that signature over the long term.
- **Signature validation:** process of verifying and confirming that a digital signature is technically valid.
- **Conformity assessment body:** a body defined in eIDAS Art. 3(18).
- **Bulk signing:** the act of creating one signature that signs different data (e.g. through the implementation of signature on several document references consisting in hashes of the referenced documents).
- **Mass signing:** the act of creating more than one signature signing more than one document based on an authorization given once (e.g. credentials are only asked once to authorize the automated sealing or signing of all documents submitted to a server for one day).
- **Visible signature:** visual representation of the human act of signing placed within an electronic in a human understandable way as part of the human readable and printable content of the document.

  NOTE: A visible signature can represent an AdES digital signature. E.g. the PAdES format allows the creation of a visible signature linked to and representing an underlying digital signature.

1.5.2. Acronyms

For the purposes of the present document, the abbreviations given in [ETSI TS 119 441] and the following apply:

BSP	Business Scoping Parameter
EUIBA	EU Institution, Body or Agency
EUIBAs	EU Institutions, Bodies and Agencies
DTBS	Data to be signed
DA	Driving Application
SVA	Signature Validation Application

2. Signature application practices statements

2.1. Requirements for the Signature Validation Application

The SVA shall support the CAdES, XAdES and PAdES, as well as the ASiC container as referenced and/or defined in [CID 2015/1506], [ETSI EN 319 122-1], [ETSI EN 319 132-1], [ETSI EN 319 142-1] and [ETSI EN 319 162-1].

The SVA should support the format for PDF digital signatures defined in [ISO 32000-1].

> **NOTE**: The signature validation application (SVA) is specified in [ETSI EN 319 102-1].

2.2. Requirements for the Driving Application

Not applicable.

> **NOTE**: In a signature validation process, the driving application (DA) provides AdES digital signature and other input to a signature validation application (SVA). See [ETSI EN 319 102-1] for more information.

3. Business Scoping Parameters

3.1. BSPs mainly related to the concerned application/business process

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

There is no fixed workflow in which this “signature applicability rules” document takes place. The workflow is application dependent.

3.1.2. BSP (b): Data to be signed

The SVA shall make available to the DA an indication of whether the data content type attribute ([ETSI EN 319 102-1] clause 4.2.5.5), or any additional AdES attributes providing further information on the type of data content, is present in the signature, and the value thereof when it is present.

> **NOTE**: The data content type attribute is implemented under different names in the ETSI ESI AdES digital signature formats. E.g. In XAdES digital signatures, it corresponds to the DataObjectFormat qualifying property.

No requirements are made on the presence or the value of the data content type attribute.

Signature applicability rules further specifying the present document may impose additional requirements on the data content type attribute.

When signature applicability rules building on the present document impose additional requirements on the data content type attribute, the DA shall be responsible for verifying those requirements.

No requirements are made on the scope of the signatures (i.e. whether the signature signs part of or the whole data).

When signature applicability rules building on the present document impose additional requirements on the scope of the signatures, the DA shall be responsible for verifying those requirements.

3.1.3. BSP (c): The relationship between signed data and signatures

Bulk signing is allowed under the present signature applicability rules.

When one signature signs multiple data objects, the SVA shall make available to the DA an indication of the number of data objects the signature signs.

When signature applicability rules building on the present document impose additional requirements on bulk signing (such as prohibition, required use, or maximum number of data objects signed by one signature), the DA shall be responsible for verifying those requirements.

The signature formats shall be limited to:

- The formats referenced in the [CID 2015/1506]
- The CAdES format defined in [ETSI EN 319 122-1]
- The XAdES format defined in [ETSI EN 319 132-1]
- The PAdES format defined in [ETSI EN 319 142-1]

  The format for PDF digital signatures making use of PKCS#7 signatures defined in [ISO 32000-1].

When multiple signatures are included in a unique container, or when a signature signs different data objects, the container format shall be the ASiC container defined in [ETSI EN 319 162-1].

The SVA shall make available to the DA an indication on format and/or container of the signatures.

All signature levels defined in those standards are allowed under the present signature applicability rules.

The SVA shall make available to the DA an indication on level of the signatures.

When signature applicability rules building on the present document impose additional requirements on the format and level of the signatures (such as requiring that signatures be restricted to XAdES baseline signatures, or that the signatures be signatures with time at the minimum), the DA shall be responsible for verifying those requirements.

Signed data may only be detached from the signatures when both the detached signatures and the signed data are within an ASiC container.

When electronic documents contain more than one visible signature, there shall not be any overlapping of such signatures.

NOTE 1: Some signature formats (e.g. PAdES) allow users to embed in a signed document a visible signature representing the underlying digital signature they created. Because the position, placement and size of such visible signatures can be arbitrary, care must be taken to ensure that two visible signatures are not created at the same position in the document and that they do not overlap.

When electronic documents contain placeholders for visible signatures, the visible signatures should be placed in those placeholders, if applicable.

NOTE 2: Some document formats (e.g. PDF) allow users to create placeholders where a visible signature is expected to be placed.

3.1.4. BSP (d) Targeted community

The targeted community is the Commission as well as any other EUIBAs deciding to rely on the present document when validating electronic signatures and/or seals on electronic documents received from any third party. In that case, they may reference the present document as the Signature Applicability Rules they decided to follow.

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

The SVA is not responsible for augmenting the level of the signatures nor preserving them.

NOTE: Without proper preservation of the signatures, there is no guarantee that a signature validated as “valid” under the present applicability rules at a given time will continue to be validated with the same status at an ulterior time.

The DA is responsible for verifying that the signatures meet the appropriate requirements when this responsibility is delegated by the SVA to the DA under the present signature applicability rules, or documents further specifying them.

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

The electronic signature (respectively electronic seal) of the signers shall meet the requirements for qualified electronic signatures (respectively for qualified electronic seals) as defined in the [eIDAS Regulation].

> **NOTE 1**: Art. 32(1) (respectively Art. 40) of the [eIDAS Regulation] lays down the requirements for the validation of qualified electronic signatures (respectively qualified electronic seals).
>
> Those requirements are legal requirements bearing on the “signature validation” process.
>
> [ETSI TS 119 172-4] section 4.4 defines a *technical applicability rules checking* (TARC) process aiming to support the “validation” process referred to in Art. 32(1).
>
> The Commission has implemented that TARC process and makes use of it to determine the legal suitability of the received electronic signatures. See section 4.2.2 “Output constraints to be used when validating signatures in the context of the identified signature policy”.

> **NOTE 2**: This means, in particular, that electronic signatures and seals, whether advanced or not, that are not supported by a certificate, and advanced electronic signatures (respectively advanced electronic seals) supported by a qualified certificate that have not been created by means of a qualified electronic signature device (respectively qualified electronic seals creation device) do not meet the requirements laid down in the present signature applicability rules.

3.2.2. BSP (g): Commitment assumed by the signer

For electronic signatures, signatories acknowledge having duly read and approved its content, subsequently being bound by it.

An indication of that commitment should be present in the electronic signatures, using standard attributes and values intended for that purpose.

In PAdES signatures, the commitment-type-indication attribute defined in ETSI EN 319 122-1 clause 5.2.3 (whose presence is conditioned according to ETSI EN 319 142-1 clause 6.3) should be present, and should indicate either the commitment type “Proof of Origin” or “Proof of approval” identified by the OIDs 1.2.840.113549.1.9.16.6.1 and 1.2.840.113549.1.9.16.6.5 respectively, as defined in ETSI TS 119 172-1 Annex B.

No requirements are made on the commitment assumed by the creators of seal.

The SVA shall make available to the DA an indication on commitments assumed by the signers (i.e. both for signatories and creators of seal).

The DA shall be responsible for verifying the requirements on the commitment assumed by the signers, including when additional requirements are made in documents further specifying the present applicability rules.

3.2.3. BSP (h): Level of assurance on timing evidences

The SVA shall only consider qualified timestamps as timing evidences.

The SVA shall make available to the DA the number of timing evidences found, which kind of timing evidences they are (e.g. content timestamp, signature timestamp, archival timestamp) and whether they are qualified or not.

3.2.4. BSP (i): Formalities of signing

Results of the validation against the present applicability rules should be presented to relying parties in a "what you see is what has been signed" environment.

The user environment should inform the relying parties of the maximum technical validity period of the signatures.

When the maximum validity period is less than a month, the user environment should inform the relying party of the need to further augment the signatures, or to appropriately preserve them.

The user environment should inform the relying party that for the augmentation of the signatures, only qualified timestamps shall be used as timing evidences.

The user environment should provide information to the relying party on the signature policy under which the signature claims to have been created, when that information is available.

3.2.5. BSP (j): Longevity and resilience to change

Notwithstanding possible revocation of supporting certificates or compromising cryptographic events (e.g. broken algorithm), the expected longevity for the signatures when they are validated as “valid” under the present applicability rules is:

- B-B level: The maximum guarantee provided by the signing certificate, taking into account the expiration date of the cryptographic suites associated with that certificate (including possible associated validation data and certificate chain).
- B-T level: If the signature timestamp is qualified and provides better guarantee than the underlying B-B level, then it is the maximum guarantee provided by the signature timestamp, taking into account the expiration date of the cryptographic suites associated with that timestamp (including possible associated validation data and certificate chain). If the timestamp is not qualified, it is the maximum guarantee of the underlying B-B level.
- B-LT level: Same as for the B-T level.
- B-LTA level: When there is only one archive timestamp, then if that archive timestamp is qualified and provides better guarantee than the underlying B-LT level, then it is the maximum guarantee provided by the archival timestamp, taking into account the expiration date of the cryptographic suites associated with that timestamp (including possible associated validation data and certificate chain). If the timestamp is not qualified, it is the maximum guarantee of the underlying B-LT level. When multiple -LTA augmentations have been performed, then it is defined recursively as follow: if the last archive timestamp is qualified and provides better guarantee than the underlying previous B-LTA level, then it is the maximum guarantee provided by that archival timestamp, taking into account the expiration date of the cryptographic suites associated with that timestamp (including possible associated validation data and certificate chain). If the last archival timestamp is not qualified, it is the maximum guarantee of the underlying previous B-LTA level.

3.2.6. BSP (k): Archival

Validation platforms implementing the current signature applicability rules are not responsible for archiving the documents submitted by relying parties.

Relying parties are responsible for properly archiving the signed or sealed documents, when applicable, and should archive the validation report they have been issued.

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

No requirements on the identity of the signers are specified in the present signature applicability rules.

Both signatories and creators of seals are allowed.

The SVA shall make available to the DA all signers' roles/attributes found in the signature.

When signature applicability rules building on the present document impose additional requirements on the identity of the signers (such as a specific certified attribute), the DA shall be responsible for verifying those requirements.

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

The identity of the signers shall be ensured by means of a qualified certificate for electronic signature or a qualified certificate for electronic seal.

3.3.3. BSP (n): Signature creation devices

All digital signatures received from third parties shall be created by means of a qualified signature creation device, or a qualified seal creation device.

> **NOTE**: Pursuant to Art. 31(2) and Art. 39(3) of the [eIDAS Regulation], the Commission publishes a list of certified qualified signature creation devices and certified qualified seal creation devices based on the information notified by the EU Member States. That list is available here: https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd

3.4. Other BSPs

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

All digital signatures received from third parties should contain a reference to the signature policy, or the signature policy document itself when it is embedded in the signature, with which they have been created.

The SVA shall make available to the DA the reference to the signature policy found in the signature, or the document itself, when it is available.

3.4.2. BSP (p): Cryptographic suites

All digital signatures received from third parties shall have been created (respectively augmented) using cryptographic algorithms and parameters that were compliant with the latest version of [ETSI TS 119 312] or [ETSI TS 102 176-1] that was applicable at the time of creation (respectively augmentation) of the signature.

The time stated by the timestamps required as timing evidence in clause “BSP (h): Level of assurance on timing evidences” will be the time of reference used for the determination of the suitability of the cryptographic algorithms and parameters used for creating and, when applicable, augmenting the signatures.

3.4.3. BSP (q): Technological environment

Not applicable.

4. Requirements / statements on technical mechanisms and standards implementation

4.1. Technical counterparts of BSPs – Statement summary

When the business statements are not strict requirements, no technical statement counterparts are expressed.

BSP	BSP title	Business statement summary	Technical statement counterpart
(a)	Workflow (sequencing & timing) of signatures	The workflow is application dependent.	Not applicable.
(b)	Data to be signed (DTBS)	No requirement.	Not applicable
(c)	Relationship between DTBS & signature(s)	The formats of electronic signatures and seals shall be one of the CAdES, XAdES, PAdES or PDF signature formats or they shall be embedded in an ASiC container. Any signature level may be used. Detached signatures may only be used when the format used is ASiC. There shall not be any overlapping of visible signatures.	Signature formats shall comply with the standards referenced in [CID 2015/1506] or with the standards [ETSI EN 319 122-1], [ETSI EN 319 132-1], [ETSI EN 319 142-1], [ETSI EN 319 162-1] and [ISO 32000-1]. [ISO 32000-1] PDF signatures and PAdES digital signatures shall not have their visual representation overlapping existing visual representation of other digital signatures.
(d)	Targeted community	The Commission and any other EUIBAs when validating electronic signatures and/or seals on electronic documents received from any third party.	Not applicable.

(e)	Allocation of responsibility for signature validation and augmentation	No responsibility for augmenting the level of the signatures nor preserving them is allocated to the validator.	Not applicable
(f)	Legal type of signature	The electronic signature (respectively electronic seal) of the signers shall meet the requirements for qualified electronic signatures (respectively for qualified electronic seals) as defined in the [eIDAS Regulation].	The determination of the qualified status shall comply with [ETSI TS 119 172-4], except for the revocation freshness constraint, to allow validation of basic signatures.
(g)	Commitment assumed by the signer	Electronic signatures should contain the “Proof of Origin” or “Proof of approval” commitment-type.	The OIDs 1.2.840.113549.1.9.16.6.1 and 1.2.840.113549.1.9.16.6.5 should be present as commitment-type indication.
(h)	Level of assurance on timing evidences	Only qualified timestamps are considered as timing evidences.	The determination of the qualified status shall comply with [ETSI TS 119 615].
(i)	Formalities of signing	A "what you see is what has been signed" environment is recommended. Informing the relying parties of: - the maximum technical validity period of the signatures; - the need to augment or preserve signature with expected maximum validity period of less than a month - the fact that for the augmentation of the signatures, only qualified timestamps shall be used as timing evidences;	Not applicable.

		- the signature policy under which the signature claims to have been created is recommended	
(j)	Longevity & resilience to change	The maximum guarantee provided by the signing certificate or the timing evidences, whichever is the highest, taking into account expiry of the cryptographic suites used at best-signing time.	Idem.
(k)	Archival	Relying parties are responsible for properly archiving any suitable documents.	Not applicable
(l)	Identity of signers	No requirements on identity attributes.	Not applicable
(m)	Level of assurance required for the authentication of the signer	The identity of the signers shall be ensured by means of a qualified certificate for electronic signature or a qualified certificate for electronic seal.	The determination of the qualified status shall comply with [ETSI TS 119 615].
(n)	Signature creation devices	All digital signatures received from third parties shall be created by means of a qualified signature creation device, or a qualified seal creation device.	The determination of the qualified status shall comply with [ETSI TS 119 615].
(o)	Other information to be associated with the signature	Referencing the signature creation policy in the signature itself is recommended.	Not applicable.
(p)	Cryptographic suites	The cryptographic suites defined in [ETSI TS 119 312] and [ETSI TS 102 176-1] are used. Compliance against the latest version applicable at best signing time is required.	Compliance against the latest version of [ETSI TS 119 312] or [ETSI TS 102 176-1] applicable at best signing time is required.

(q)	Technological environment	No requirements.	Not applicable.
Signature creation/validation application practices statements		-	-

Table 1

4.2. Input and output constraints for signature creation, augmentation and validation procedures

4.2.1. Input constraints to be used when generating, augmenting and/or validating signatures in the context of the identified signature policy

The input constraints are expressed using the recommendation of [ETSI TS 119 172-1].

NOTE: The below validation input constraints are initialized according to the validation constraints specified in [ETSI TS 119 172-4], except for the revocation freshness constraint: Verification of the freshness of the revocation data is skipped to allow validation of basic signatures.

Name and identifier of the signature policy: SAR_EC_BASELINE_v1.0					
BSP	**BSP title**	**Business statement summary**	**Technical counterpart statement**	**Constraint(s)**	**Constraint value at signature validation (SVA or DA)**
(a)	Workflow (sequencing & timing)	The workflow is application dependent.	Not applicable.	**MassSigningAcceptable:** **ForESig:** **ForESeal:**	 **yes** **yes**

Name and identifier of the signature policy: SAR_EC_BASELINE_v1.0					
BSP	**BSP title**	**Business statement summary**	**Technical counterpart statement**	**Constraint(s)**	**Constraint value at signature validation (SVA or DA)**
(b)	DTBS	No requirement.	Not applicable	**None**	
(c)	Relationship between DTBS and Signature	The formats of electronic signatures and seals shall be one of the CAdES, XAdES, PAdES, or ISO PDF signature formats or they shall be embedded in an ASiC container. Any signature level may be used.	Signature formats shall comply with the standards referenced in [CID 2015/1506] or with the standards [ETSI EN 319 122-1], [ETSI EN 319 132-1], [ETSI EN 319 142-1], [ETSI EN 319 162-1] and [ISO 32000-1].	**MandatedSignatureFormat:**	**CAdES-B-*** **XAdES-B-*** **PAdES-B-*** **ASiC-S** **ASiC-E** **ISOPDFSig** *Note: "-*" means that all levels are permitted.*
		There shall not be any overlapping of visible signatures.	[ISO 32000-1] PDF signatures and PAdES digital signatures shall not have their visual representation overlapping existing visual representation of other digital signatures.	**SignatureVisualElementsConstraints:**	**OverlappingProhibited**
(d)	Targeted community	The Commission and the EUIBAs making use of the validation service provided by the Commission and receiving electronic documents containing electronic signatures and/or seals from any third party.	Not applicable.	**TargetedCommunityConstraints:**	**EUIBA**

Name and identifier of the signature policy: SAR_EC_BASELINE_v1.0					
BSP	**BSP title**	**Business statement summary**	**Technical counterpart statement**	**Constraint(s)**	**Constraint value at signature validation (SVA or DA)**
(e)	Allocation of responsibility for validation & augmentation	No responsibility for augmenting the level of the signatures nor preserving them is allocated to the validator.	Not applicable	**None**	
(f)	Legal type	The electronic signature (respectively electronic seal) of the signers shall meet the requirements for qualified electronic signatures (respectively for qualified electronic seals) as defined in the [eIDAS Regulation].	The determination of the qualified status shall comply with [ETSI TS 119 172-4].	**ConstraintsOnCertificateMetadata:** **LegalPersonSignerAllowed:** **EUQualifiedCertificateRequired:** **EUSSCDRequired:**	**yes** **yes** **yes**
(g)	Commitment type	Electronic signatures should contain the “Proof of Origin” or “Proof of approval” commitment-type.	The OIDs 1.2.840.113549.1.9.16.6.1 and 1.2.840.113549.1.9.16.6.5 should be present as commitment-type indication.	**None**	
(h)	LoA on timing evidences	Only qualified timestamps are considered as timing evidences.	The determination of the qualified status shall comply with [ETSI TS 119 615].	**LoAOnTimingEvidences:** **LoA-on-content-time-stamp:** **LoA-on-signature-time-stamp:** **LoA-on-archival-time-stamp:**	**EUQTST** **EUQTST** **EUQTST**

Name and identifier of the signature policy: SAR_EC_BASELINE_v1.0					
BSP	**BSP title**	**Business statement summary**	**Technical counterpart statement**	**Constraint(s)**	**Constraint value at signature validation (SVA or DA)**
(i)	Formalities of signing	A "what you see is what has been signed" environment is recommended. Informing the relying parties of: - the maximum technical validity period of the signatures; - the need to augment or preserve signature with expected maximum validity period of less than a month - the fact that for the augmentation of the signatures, only qualified timestamps shall be used as timing evidences; - the signature policy under which the signature claims to have been created is recommended	Not applicable	**None**	
(j)	Longevity & resilience	The maximum guarantee provided by the signing certificate or the timing evidences, whichever is the highest, taking into account expiry of the cryptographic suites used at best-signing time.	Idem.	**None**	
(k)	Archival	Relying parties are responsible for properly archiving any suitable documents.	Not applicable	**None**	
(l)	Identity and role attributes of the signer	No requirements on identity attributes.	Not applicable	**None**	
(m)	LoA on signer authentication	The identity of the signers shall be ensured by means of a qualified certificate for electronic signature or a qualified certificate for electronic seal.	The determination of the qualified status shall comply with [ETSI TS 119 615].	**X509CertificateValidationConstraints: SetOfTrustAnchors:**	Set according to REQ-4.2-03 of [ETSI TS 119 172-4]

Name and identifier of the signature policy: SAR_EC_BASELINE_v1.0					
BSP	**BSP title**	**Business statement summary**	**Technical counterpart statement**	**Constraint(s)**	**Constraint value at signature validation (SVA or DA)**
				RevocationConstraints: **RevocationCheckingConstraints:** **RevocationFreshnessConstraints**	**eitherCheck** **IGNORE**
(n)	Signature Creation Devices	All digital signatures received from third parties shall be created by means of a qualified signature creation device, or a qualified seal creation device.	The determination of the qualified status shall comply with [ETSI TS 119 615].	**LoAOnSCD:** **EUSSCDRequired:**	**yes**
(o)	Other information to be associated with signatures	Referencing the signature creation policy in the signature itself is recommended.	Not applicable.	**None**	
(p)	Cryptographic suites	The cryptographic suites defined in [ETSI TS 119 312] and [ETSI TS 102 176-1] are used. Compliance against the latest version applicable at best signing time is required.	Compliance against the latest version of [ETSI TS 119 312] or [ETSI TS 102 176-1] applicable at best signing time is required.	**CryptographicSuitesConstraints:**	Set according to [ETSI TS 119 312], using historical values of previous version of the standard and values of the historical standard [ETSI TS 102 176-1].
(q)	Technological environment	No requirements.	Not applicable.	**None**	

Table 2

4.2.2. Output constraints to be used when validating signatures in the context of the identified signature policy

The determination of whether a digital signature meets the requirement on the legal type of the signature (See BSP (f): Legal type of the signatures) shall comply with the requirements on the TARC process specified in section 4.4 of [ETSI TS 119 172-4]. Checking the revocation freshness is skipped to allow the validation of basic signatures.

5. Other business and legal matters

Not applicable.

6. Compliance audit and other assessments

Not applicable.

7. Check lists for parties submitting electronically signed and or sealed documents to an EUIBA.

The below table provides a summary of the points to which third parties that are submitting electronically signed or sealed documents, shall pay particular attention to. References to the corresponding sections of the signature applicability rules are provided:

Name and identifier of the signature policy: SAR_EC_BASELINE_v1.0		
BSP	BSP title	Business statement summary
(c)	Relationship between DTBS & signature(s)	The formats of electronic signatures and seals shall be one of the CAdES, XAdES, PAdES, or PDF signature formats or they shall be embedded in an ASiC container, as referenced and/or defined in [CID 2015/1506], [ETSI EN 319 122-1], [ETSI EN 319 132-1], [ETSI EN 319 142-1], [ETSI EN 319 162-1] and [ISO 32000-1]. Detached signatures not within an ASiC may not be used. Any signature level may be used. There shall not be any overlapping of visible signatures.
(f)	Legal type of signature	Electronic signatures (respectively seal) shall be qualified electronic signatures (respectively qualified electronic seals).
(g)	Commitment assumed by the signer	Electronic signatures should contain the “Proof of Origin” or “Proof of approval” commitment-type.
(h)	Level of assurance on timing evidences	Only qualified timestamps are considered as timing evidences
(p)	Cryptographic suites	Signature and seals shall have been created using cryptographic algorithms and parameters that were compliant with the latest version of [ETSI TS 119 312] or [ETSI TS 102 176-1] that was applicable at the best signing time of the signature.

ANNEX I: SIGNATURE APPLICABILITY RULES FOR ELECTRONIC SIGNATURES AND SEALS IN THE CONTEXT OF ELECTRONIC DOCUMENTS TO BE SIGNED BY AN EUIBA

When not otherwise explicitly specified, all requirements from the baseline signature applicability rules “SAR_EC_BASELINE” apply. To improve readability, all sections for which there is no override are not present.

1. Introduction

1.1 Overview

Electronic documents received by the Commission may need to be subsequently signed, however the formats associated with those documents might make it possible for users to specify permissions that prevent the creation of new electronic signatures or electronic seals in those documents.

Therefore, there is a need for defining specific signature applicability rules to be used to determine whether the electronic signature or electronic seal present in those electronic documents are fit for purpose.

1.2 Business or Application Domain

1.2.1 Scope and boundaries of the signature policy

The present Annex specifies the rules to be used for the technical validation of digital signatures and the determination of their applicability to the specific context of the Commission validating the electronic signatures and/or electronic seals present in electronic received from third parties when there is the need for the Commission to subsequently sign and/or seal those documents.

1.3 Document and policy names, identification and conformance rules

1.3.1 Signature policy document and signature policy name

The name of the present annexed signature applicability rules is “Signature applicability rules for electronic signatures and seals in the context of electronic documents to be signed by the European Commission” (SAR_DOC_TBS).

1.3.2 Signature policy document and signature policy identifier

The reference for the present signature applicability rules is SAR_DOC_TBS_v1.0

See section 1.3.2 of the SAR_EC_BASELINE.

3. Business scoping parameters

3.1 BSPs mainly related to the concerned application/business process

3.1.2 BSP (b): Data to be signed

The following amendment is made to section 3.1.2 of the SAR_BASELINE:

Electronically signed and/or sealed documents shall not contain any attribute or element that may prevent the creation of any new electronic signature and/or seal.

NOTE: PDF files provide security and permission features that allow the creator to retain control of the document and associated rights. Those features, when used, can sometime prevent any ulterior modification of the file, including the creation of new digital signatures.

3.1.4 BSP (d) Targeted community

The targeted community is not only the Commission, but also the EUIBAs making use of the validation service provided by the Commission and receiving electronic documents from third parties that they need to subsequently sign and/or seal.

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

The following amendment is made to section 3.3.1 of the SAR_BASELINE:

The identity of the signers is defined by the business context in which they occur. There shall not be any signature or seal identifying a natural or legal person that is not related to the business, such as signing-platform specific technical seals.

4. Requirements / statements on technical mechanisms and standards implementation

4.1. Technical counterparts of BSPs – Statement summary

Row (c) of Table 1 of the SAR_EC_BASELINE is amended so that it reads:

(c)	Relationship between DTBS & signature(s)	The formats of electronic signatures and seals shall be one of the CAdES, XAdES, PAdES, or PDF signature formats or they shall be embedded in an ASiC container. Any signature level may be used. There shall not be any overlapping of visible signatures. Electronically signed and/or sealed documents shall not contain any attribute or element that may prevent the creation of any new electronic signature and/or seal.	Signature formats shall comply with the standards referenced in [CID 2015/1506] or with the standards [ETSI EN 319 122-1], [ETSI EN 319 132-1], [ETSI EN 319 142-1], [ETSI EN 319 162-1] and [ISO 32000-1]. [ISO 32000-1] PDF signatures and PAdES digital signatures shall not have their visual representation overlapping existing visual representation of other digital signatures. [ISO 32000-1] PDF signatures and PAdES digital signatures shall not contain any element prohibiting the creation of new digital signatures.

4.2. Input and output constraints for signature creation, augmentation and validation procedures

4.2.1. Input constraints to be used when generating, augmenting and/or validating signatures in the context of the identified signature policy

The following amendment is made to section 4.2.1 of the SAR_EC_BASELINE:

Row (c) of Table 2 is amended so to include constraint **DocPermissionAllowed** with value **no**.

7. Check lists for parties submitting electronically signed and or sealed documents to an EUIBA that needs to be subsequently signed

The below table provides a summary of the points to which third parties that are submitting electronically signed or sealed documents that needs to be subsequently signed, shall pay particular attention to. References to the corresponding sections of the signature applicability rules are provided:

Name and identifier of the signature policy: SAR_DOC_TBS_v1.0		
BSP	BSP title	Business statement summary
(c)	Relationship between DTBS & signature(s)	The formats of electronic signatures and seals shall be one of the CAdES, XAdES, or PAdES formats or they shall be embedded in an ASiC container, as referenced and/or defined in [CID 2015/1506], [ETSI EN 319 122-1], [ETSI EN 319 132-1], [ETSI EN 319 142-1] and [ETSI EN 319 162-1]. Detached signatures not within an ASiC may not be used. Any signature level may be used. There shall not be any overlapping of visible signatures. Electronically signed and/or sealed documents shall not contain any attribute or element that may prevent the creation of any new electronic signature and/or seal.
(f)	Legal type of signature	Electronic signatures (respectively seal) shall be qualified electronic signatures (respectively qualified electronic seals).
(g)	Commitment assumed by the signer	Electronic signatures should contain the “Proof of Origin” or “Proof of approval” commitment-type.
(h)	Level of assurance on timing evidences	Only qualified timestamps are considered as timing evidences
(l)	Identity of the signers	There shall not be any signature or seal identifying a natural or legal person that is not related to the business, such as signing-platform specific technical seals.
(p)	Cryptographic suites	Signature and seals shall have been created using cryptographic algorithms and parameters that were compliant with the latest version of [ETSI TS 119 312] or [ETSI TS 102 176-1] that was applicable at the best signing time of the signature.

ANNEX II: SIGNATURE APPLICABILITY RULES FOR ELECTRONIC SIGNATURES AND SEALS IN THE CONTEXT OF TRANSACTIONS INTERNAL TO THE EUIBAs

When not otherwise explicitly specified, all requirements from the baseline signature applicability rules “SAR_EC_BASELINE” apply with the amendment that all mention of “third parties” shall be replaced by “third parties external to the EUIBAs”. To improve readability, all sections for which there is no override are not present.

1. Introduction

1.1. Overview

Electronic documents transmitted from one EUIBA to another, that have been electronically signed or sealed by parties exclusively from within the EUIBAs, use procedures that require the definition of specific signature applicability rules to be used to determine whether the electronic signature or electronic seal present in those electronic documents are fit for purpose.

In particular, EUIBAs have established bilateral agreements recognising advanced electronic signatures and advanced electronic seals supported by a certificate issued by specific trust services provided by some EUIBAs. The EUIBA Trusted List references the internally recognised CAs, outside qualified TSPs.

1.2. Business or Application Domain

1.2.1. Scope and boundaries of the signature policy

The present Annex specifies the rules to be used for the technical validation of digital signatures and the determination of their applicability to the specific context of the Commission validating the electronic signatures and/or electronic seals present in electronic received from an EUIBA, and whose signers are exclusively from within the EUIBAs.

1.3. Document and policy names, identification and conformance rules

1.3.1. Signature policy document and signature policy name

The name of the present annexed signature applicability rules is “Signature applicability rules for electronic signatures and seals in the context of transactions internal to the EUIBAs” (SAR_EUIBA_INTERNAL).

1.3.2. Signature policy document and signature policy identifier

The reference for the present signature applicability rules is SAR_EUIBA_INTERNAL_v1.2

See section 1.3.2 of the SAR_EC_BASELINE.

3. Business scoping parameters

3.1. BSPs mainly related to the concerned application/business process

3.1.4. BSP (d) Targeted community

The targeted community is not only the Commission, but also the EUIBAs making use of the validation service provided by the Commission and receiving electronic documents from an EUIBA containing electronic signatures and/or seals whose signers are exclusively from within the EUIBAs.

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

All mentions “signers” in section 3.2.1 of the SAR_EC_BASELINE shall be replaced by “signers, when they are external to the EUIBAs,”.

In addition, the following amendment is made to section 3.1.4 of the SAR_EC_BASELINE:

The electronic signature (respectively electronic seal) from the signers, when they are from within the EUIBAs, shall meet the requirements for advanced electronic signatures or the requirements for advanced electronic seals as defined in the [eIDAS Regulation].

NOTE: Requirements on the issuers of the signing certificates for parties from within the EUIBAs are laid down in section “BSP (m): Level of assurance required for the authentication of the signer” of the present signature applicability rules.

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

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

All mentions of “signers” in section 3.3.2 of the SAR_EC_BASELINE shall be replaced by “signers, when they are external to the EUIBAs,”.

In addition, the following amendment is made to section 3.3.2 of the SAR_EC_BASELINE:

The identity of the signers, when they are from within the EUIBAs, shall be ensured by means of a qualified certificate for electronic signature or a qualified certificate for electronic seal, or by means of a certificate issued by trust service internally operated by an EUIBA that is referenced in the EUIBA trusted list.

NOTE: Currently, the EUIBA Trusted List references the internally recognised CAs, outside qualified TSPs.

3.3.3. BSP (n): Signature creation devices

No additional requirements.

NOTE: This means that no requirements are made on the signature creation devices for the signatures received from parties within the EUIBAs.

4. Requirements / statements on technical mechanisms and standards implementation

4.1. Technical counterparts of BSPs – Statement summary

Row (m) of Table 1 of the SAR_EC_BASELINE is amended to so that the set of trust anchors include the certificates of the EUIBA recognised CAs.

4.2. Input and output constraints for signature creation, augmentation and validation procedures

4.2.1. Input constraints to be used when generating, augmenting and/or validating signatures in the context of the identified signature policy

The following amendment is made to section 4.2.1 of the SAR_EC_BASELINE:

Row (m) of Table 2 is amended so that the set of trust anchors is augmented with the certificates of the bilaterally recognised CAs.

4.2.2. Output constraints to be used when validating signatures in the context of the identified signature policy

The following amendment is made to section 4.2.2 of the SAR_EC_BASELINE:

If the following conditions are met:

a) the signature has not been determined technically to be either an EU qualified electronic signature, or an EU qualified electronic seal under the TARC process specified in [ETSI TS 172-4];

b) the signing certificate is determined, at the best signature time, as an EUIBA certificate for electronic signatures (respectively for electronic seals) as a result of running the process specified in clause 4.3 of the [EUIBA TL specifications and usage]; and

c) the result of the process performed as specified in [ETSI EN 319 102-1] using the validation constraints defined in Table 1 rows (b), (m), and (p) is TOTAL-PASSED.

then the digital signature shall be determined as technically suitable to implement an electronic signature (respectively an electronic seal) recognised by the EUIBAs, otherwise the signature shall not be determined technically either as an electronic signature, or as an electronic seal recognised by the EUIBAs.

When a digital signature is determined as technically suitable to implement an electronic signature (respectively an electronic seal) recognised by the EUIBAs, the output shall be “AdESig_EUIBA” (respectively “AdESeal_EUIBA”).

7. Check lists for parties submitting electronically signed and or sealed documents to an euiba in the context of a transaction internal to the EUIBAs

The below table provides a summary of the points to which parties from within the EUIBAs that are submitting electronically signed or sealed documents, shall pay particular attention to. References to the corresponding sections of the signature applicability rules are provided:

Name and identifier of the signature policy: SAR_EUIBA_INTERNAL_v1.2		
BSP	BSP title	Business statement summary
(c)	Relationship between DTBS & signature(s)	The formats of electronic signatures and seals shall be one of the CAdES, XAdES, or PAdES formats or they shall be embedded in an ASiC container, as referenced and/or defined in [CID 2015/1506], [ETSI EN 319 122-1], [ETSI EN 319 132-1], [ETSI EN 319 142-1] and [ETSI EN 319 162-1]. Detached signatures not within an ASiC may not be used. Any signature level may be used. There shall not be any overlapping of visible signatures.
(f)	Legal type of signature	Electronic signatures (respectively seal) shall be advanced electronic signatures (respectively qualified electronic seals).
(h)	Level of assurance on timing evidences	Only qualified timestamps are considered as timing evidences
(m)	Level of assurance required for the authentication of the signer	The signature (respectively seal) shall be supported by either: - A qualified certificate for electronic signature (respectively seal); or - A certificate issued by an EUIBA TSP referenced in the EUIBA Trusted List.
(p)	Cryptographic suites	Signature and seals shall have been created using cryptographic algorithms and parameters that were compliant with the latest version of [ETSI TS 119 312] or [ETSI TS 102 176-1] that was applicable at the best signing time of the signature.