

Regelung der Signatur des Amtsblatts

Fassung 4

(1.3.171.4.1.1.4)

In Kraft ab dem 1. Oktober 2023

Inhalt

1	EINFÜHRUNG	4
1.1	ÜBERSICHT	4
1.2	GESCHÄFTSBEREICH	5
1.2.1	<i>Anwendungsbereich und Grenzen der Signaturregelung</i>	5
1.2.2	<i>Anwendungsbereich</i>	5
1.2.3	<i>Transaktionskontext</i>	5
1.3	NAME DER SIGNATURREGELUNG, KENNUNG UND KONFORMITÄTSREGELN	5
1.3.1	<i>Name der Regelung</i>	5
1.3.2	<i>Kennung der Regelung</i>	5
1.3.3	<i>Regeln für die Konformität der Regelung</i>	5
1.3.4	<i>Verbreitung der Regelung</i>	5
1.3.5	<i>Gültigkeit der Regelung</i>	5
1.3.6	<i>Anwendungsbereich der Regelung</i>	6
1.4	VERWALTUNG DES DOKUMENTS ÜBER DIE SIGNATURREGELUNG	6
1.4.1	<i>Zuständige Stelle</i>	6
1.4.2	<i>Kontaktperson</i>	6
1.4.3	<i>Genehmigungsverfahren</i>	7
1.4.4	<i>Fassungen der Regelung</i>	7
1.5	BEGRIFFSBESTIMMUNGEN UND ABKÜRZUNGEN	7
2	ERKLÄRUNGEN ZU DEN VERFAHREN DER SIGNATURANWENDUNG	8
2.1	MIT DER REGELUNG VERBUNDENE ANFORDERUNGEN	8
2.2	VERBUNDENE RECHTLICHE ANFORDERUNGEN	9
2.3	TECHNISCHE SICHERHEIT	10
2.4	RECHTLICHE AUSSAGEN	10
3	PARAMETER DER GESCHÄFTLICHEN ANWENDUNG	11
3.1	PARAMETER DER GESCHÄFTLICHEN ANWENDUNG, DIE SICH HAUPTSÄCHLICH AUF DIE BETREFFENDE ANWENDUNG/DEN BETREFFENDEN GESCHÄFTSPROZESS BEZIEHEN	11
3.1.1	<i>Parameter der geschäftlichen Anwendung (a): Arbeitsablauf (Abfolge und Zeitplan) der Signaturen</i>	11
3.1.2	<i>Parameter der geschäftlichen Anwendung (b): Zu signierende Daten</i>	15
3.1.3	<i>Parameter der geschäftlichen Anwendung (c): Beziehung zwischen signierten Daten und Signatur(en) und Siegel(n)</i>	15
3.1.4	<i>Parameter der geschäftlichen Anwendung (d): Zielgruppe</i>	16
3.1.5	<i>Parameter der geschäftlichen Anwendung (e): Zuweisung der Verantwortlichkeit für die Validierung und Ergänzung von Signaturen</i>	16
3.2	PARAMETER DER GESCHÄFTLICHEN ANWENDUNG, DIE HAUPTSÄCHLICH VON DEN RECHTS- UND VERWALTUNGSVORSCHRIFTEN IM ZUSAMMENHANG MIT DER BETREFFENDEN ANWENDUNG/DEM BETREFFENDEN GESCHÄFTSPROZESS BEEINFLUSST WERDEN	17
3.2.1	<i>Parameter der geschäftlichen Anwendung (f): Rechtsform der Signaturen</i>	17
3.2.2	<i>Parameter der geschäftlichen Anwendung (g): Vom Unterzeichner übernommene Verpflichtung</i>	18
3.2.3	<i>Parameter der geschäftlichen Anwendung (h): Grad der Zuverlässigkeit von Zeitnachweisen</i>	18
3.2.4	<i>Parameter der geschäftlichen Anwendung (i): Formalitäten der Signierung</i>	19
3.2.5	<i>Parameter der geschäftlichen Anwendung (j): Langlebigkeit und Widerstandsfähigkeit gegenüber Veränderungen</i>	19
3.2.6	<i>Parameter der geschäftlichen Anwendung (k): Archivierung</i>	19
3.3	PARAMETER DER GESCHÄFTLICHEN ANWENDUNG, DIE SICH HAUPTSÄCHLICH AUF DIE AN DER SIGNATURERSTELLUNG/ERGÄNZUNG/-VALIDIERUNG BETEILIGTEN AKTEURE BEZIEHEN	20
3.3.1	<i>Parameter der geschäftlichen Anwendung (l): Identität (und Zuständigkeiten/Attribute) der Unterzeichner</i>	20
3.3.2	<i>Parameter der geschäftlichen Anwendung (m): Für die Authentifizierung des Unterzeichners erforderliches Sicherheitsniveau</i>	20
3.4	SONSTIGE PARAMETER DER GESCHÄFTLICHEN ANWENDUNG	21
3.4.1	<i>Parameter der geschäftlichen Anwendung (o): Sonstige Angaben, die der Signatur oder dem Siegel beizufügen sind</i>	21
3.4.2	<i>Parameter der geschäftlichen Anwendung (p): Verschlüsselungssoftware</i>	22

4	ANFORDERUNGEN/ERKLÄRUNGEN ZU DEN TECHNISCHEN MECHANISMEN UND DER UMSETZUNG VON NORMEN	23
4.1	REGELN FÜR VERTRAUENSWÜRDIGE ZEITSTEMPEL	23
4.2	REGELN FÜR DIE LANGFRISTIGE GÜLTIGKEIT	23
4.3	SONSTIGE GESCHÄFTLICHE UND RECHTLICHE ASPEKTE	23
5	ANHANG	24

1 Einführung

In diesem Dokument wird die Signaturregelung im Zusammenhang mit der Signatur des Amtsblatts (OJ, Official Journal – Amtsblatt) und des Amtsblattsiegels beschrieben, die zur Authentifizierung der elektronischen Fassung des Amtsblatts der Europäischen Union gemäß der Verordnung (EU) Nr. 216/2013 des Rates über die elektronische Veröffentlichung des Amtsblatts der Europäischen Union¹ dienen.

Als Signaturregelung wird ein Katalog von Regeln zur Erstellung, Validierung und Ergänzung einzelner oder mehrerer miteinander in Zusammenhang stehender elektronischer Signaturen und/oder Siegel bezeichnet, in dem die technischen und verfahrensbezogenen Voraussetzungen für die Erstellung, Validierung und langfristige Verwaltung dieser Signaturen definiert werden. Außerdem sollen Signaturregelungen sämtliche Aspekte eines bestehenden Signier- oder Siegelungsworkflows für alle Beteiligten (d. h. für die Unterzeichner, die Empfänger und die vertrauenswürdigen Dritten („arbitrators“)) transparent machen, um die Vertrauenswürdigkeit und die Akzeptanz entsprechend konformer elektronischer Signaturen und Siegel zu erhöhen.

Die Konzepte einer Signaturregelung werden in [ETSI 2015] eingehend erläutert; außerdem werden dort der Aufbau dieses Dokuments und die in diesem Dokument behandelten Leitlinien beschrieben. Die Schlüsselwörter „MUSS“/„MÜSSEN“, „DARF NICHT“/„DÜRFEN NICHT“, „ERFORDERLICH“, „SOLLTE(N)“, „SOLLTE(N) NICHT“, „EMPFOHLEN“, „KANN“/„KÖNNEN“ und „OPTIONAL“ in diesem Dokument sind wie in RFC 2911 [Bradner 1997] beschrieben zu verstehen.

Das Amtsblatt wird vom Amt für Veröffentlichungen der Europäischen Union (Office des Publications – OP) auf der EUR-Lex-Website (siehe: 1.2.4) veröffentlicht und ist die einzige authentische Quelle des EU-Rechts. Das Amtsblatt wird von Montag bis Freitag und gegebenenfalls am Wochenende in allen Amtssprachen der Europäischen Union (EU) veröffentlicht. *Im Folgenden wird mit „Amtsblatt“ der hier beschriebene besondere Anwendungsbereich bezeichnet.*

1.1 Übersicht

In der Signaturregelung für das Amtsblatt werden wesentliche Elemente für die Erstellung, die Validierung und die langfristige Erhaltung elektronischer Signaturen und Siegel als Mittel zur Authentifizierung von Amtsblattausgaben des Amtes für Veröffentlichungen formal beschrieben.

Die Signaturregelung umfasst die folgenden Elemente:

- eine Einleitung mit dem Titel/der Kennung der Regelung, Angaben zum Herausgeber der Regelung, Informationen zur Verwaltung der Regelung, Begriffsbestimmungen und Akronyme usw.;
- die Erklärung zu den Verfahren der Signaturanwendung, in der die damit verbundenen Bestimmungen und Rechtsvorschriften festgelegt sind, sowie die geltenden Sicherheitserwägungen;
- die Parameter der geschäftlichen Anwendung, in denen die Arbeitsabläufe im Zusammenhang mit der Generierung elektronischer Signaturen und Siegel, die die Authentizität der vom Amt für Veröffentlichungen veröffentlichten Amtsblattausgaben belegen, ausführlich dargelegt sind;
- die Anforderungen und Erklärungen zu technischen Mechanismen und der Umsetzung von Normen sowie Anhänge.

¹ Siehe ABl. L 69 vom 13.3.2013, S. 1.

1.2 Geschäftsbereich

1.2.1 Anwendungsbereich und Grenzen der Signaturregelung

Gegenstand der Amtsblattsignaturregelung sind elektronische Signaturen und Siegel, die für einzelne Amtsblattausgaben nach erfolgreicher Validierung der jeweils zu signierenden Ausgabe von autorisierten Amtsblattunterzeichnern gemäß der Verordnung des Rates über die elektronische Veröffentlichung des Amtsblatts der Europäischen Union erstellt werden.

1.2.2 Anwendungsbereich

Unter die Amtsblattsignaturregelung fallen nur die in Abschnitt 3.1 beschriebenen elektronischen Signaturen und Siegel.

1.2.3 Transaktionskontext

Entfällt.

1.3 Name der Signaturregelung, Kennung und Konformitätsregeln

1.3.1 Name der Regelung

Der Name der Amtsblattsignaturregelung lautet:

Regelung der Signatur des Amtsblatts

1.3.2 Kennung der Regelung

Da es nur ein Amtsblatt der Europäischen Union gibt und seine Veröffentlichung ein hinlänglich bekannter Prozess der Europäischen Union ist, kann die Amtsblattsignaturregelung implizit von jedem Dritten zugeordnet werden. Eine Beschreibung des allgemeinen Geschäftsablaufs ist in Abschnitt 3.1.1.1 enthalten.

Wenn die Regelung ausdrücklich genannt werden soll, *KANN* in jede einzelne Amtsblattsignatur und jedes Amtsblattsiegel ein ausdrücklicher Hinweis auf die Signaturregelung gemäß [ETSI 2022-XAdES] Abschnitt 5.2.9 aufgenommen werden. Wird der ausdrückliche Hinweis auf die Signaturregelung aufgenommen, *MUSS* er die Objektkennung (Objekt-ID oder OID) 1.3.171.4.1.1.4 enthalten. Bei der Eingabe sind die Verschlüsselungsregeln gemäß [ETSI 2022-XAdES] Abschnitt 5.2.9 sowie gemäß [Mealling 2010] zu berücksichtigen.

Die aktuelle Fassung dieser Regelung ist weltweit eindeutig mit der Objekt-ID 1.3.171.4.1.1.4 gekennzeichnet. Das Präfix 1.3.171.4 wurde als Ausgangs-OID für „*Signature policies and other purposes of the Publications Office of the EU*“ (Signaturregelungen und sonstige Belange des Amts für Veröffentlichungen der Europäischen Union) registriert (siehe <http://www.oid-info.com/get/1.3.171.4>). Das Suffix 1.1.4 bezeichnet die aktuelle Fassung der Amtsblattsignaturregelung. Die entsprechende ASN.1-Bezeichnung *MUSS* {oj(1) signature-policy(1) version(4)} lauten: Durch diese Fassung verliert die Fassung 1.1.3 dieser Regelung ihre Gültigkeit.

1.3.3 Regeln für die Konformität der Regelung

Die derzeitige Regelung beansprucht keinerlei Konformität mit einer sonstigen Regelung.

1.3.4 Verbreitung der Regelung

Das Dokument zur Erläuterung der Amtsblattsignaturregelung wird auf der EUR-Lex-Website veröffentlicht. Es ist über die Website des Amts für Veröffentlichungen (<https://eur-lex.europa.eu/>) aufzufinden.

1.3.5 Gültigkeit der Regelung

Die vorliegende Fassung der Regelung gilt ab dem 1. Oktober 2023.

1.3.6 Anwendungsbereich der Regelung

Die vorliegende Regelung gilt für sämtliche Ausgaben des Amtsblatts, die ab dem Zeitpunkt des Inkrafttretens der Verordnung des Rates über elektronische Veröffentlichungen des Amtsblatts der Europäischen Union veröffentlicht und elektronisch signiert wurden. Die vorliegende Regelung gilt nicht für die Beilage zum Amtsblatt der Europäischen Union (Reihe S, Amtsblatt S oder ABl. S).

ANMERKUNG: Jede Fassung der vorliegenden Regelung ist innerhalb der in jeder Fassung festgelegten Gültigkeitsdauer gültig. Die Reihe aller Fassungen deckt alle ABl.-Themen ab.

1.4 Verwaltung des Dokuments über die Signaturregelung

Herausgeber der Amtsblattsignaturregelung ist das Amt für Veröffentlichungen der Europäischen Union, das dieses Dokument angenommen und auf der EUR-Lex-Website veröffentlicht hat.

Die Amtsblattsignaturregelung ist in der veröffentlichten Form RECHTSKRÄFTIG und GILT für die Erstellung, Prüfung und langfristige Verwaltung von Amtsblattsignaturen und -siegeln.

Die folgenden Aufgaben fallen in die Zuständigkeit des Herausgebers der Amtsblattsignaturregelung:

- Spezifizierung und Genehmigung der Amtsblattsignaturregelung,
- Beschreibung des Vorgangs zur Überarbeitung der Amtsblattsignaturregelung,
- Festlegung der Bewertungskriterien und Beschreibung des Verfahrens zur Gewährleistung der Konformität der Amtsblattsignaturregelung mit der Verordnung (EU) Nr. 216/2013 des Rates vom 7. März 2013 über die elektronische Veröffentlichung des Amtsblatts der Europäischen Union und mit der Verordnung (EU) 2018/2056 des Rates vom 6. Dezember 2018 zur Änderung der Verordnung (EU) Nr. 216/2013 über die elektronische Veröffentlichung des Amtsblatts der Europäischen Union,
- Festlegung der Bewertungskriterien und Beschreibung des Verfahrens, mit dem gewährleistet wird, dass Anwendungen, die als konform mit der Amtsblattsignaturregelung dargestellt werden, in der jeweiligen Fassung tatsächlich die geltenden Anforderungen der Amtsblattsignaturregelung erfüllen,
- Veröffentlichung der Amtsblattsignaturregelung in der aktuellen Fassung auf EUR-Lex.

1.4.1 Zuständige Stelle

Die Amtsblattsignaturregelung wird vom Amt für Veröffentlichungen der Europäischen Union verwaltet.

1.4.2 Kontaktperson

Der Herausgeber der gegenwärtigen Regelung ist über die folgenden Kontaktdaten zu erreichen:

Kontaktperson:	Referatsleiter Amtsblatt und Rechtsprechung
Postanschrift:	2, rue Mercier, L-2985 Luxemburg
Telefonnummer:	+352 29291
Fax-Nr.:	+352 292944620
E-Mail-Adresse:	OP-JO-AUTHENTIQUE-HELPDESK@publications.europa.eu

1.4.3 Genehmigungsverfahren

Die Stelle für die Genehmigung von Regelungen des Amts für Veröffentlichungen der Europäischen Union ist der Generaldirektor des Amts für Veröffentlichungen der Europäischen Union.

1.4.4 Fassungen der Regelung

In der Ausgangsfassung und den geänderten Fassungen der Regelung *KANN* der späteste Zeitpunkt des Inkrafttretens vorgesehen sein. Eine veröffentlichte Fassung der Regelung wird spätestens zu den drei folgenden Zeitpunkten *WIRKSAM*:

1. gegebenenfalls zu dem in der Fassung der Regelung festgelegten spätesten Zeitpunkt des Inkrafttretens;
2. am Tag nach dem Datum des frühesten Signatur-Zeitstempels (Ortszeit Luxemburg) auf der Amtsblattsignatur oder dem Siegel der Amtsblattausgabe unter Angabe der veröffentlichten Fassung der Regelung;
3. am Tag nach der Veröffentlichung der betreffenden Fassung der Signaturregelung.

Geänderte Fassungen der Regelung werden automatisch *UNGÜLTIG*, wenn die jeweils folgende geänderte Fassung in Kraft tritt. In einer anschließenden geänderten Fassung der Regelung *SOLLTE* auch die Fassung genannt werden, die mit Inkrafttreten dieser Version ihre Gültigkeit verliert.

Mit den vorstehenden Bestimmungen soll ausgeschlossen werden, dass eine aufgrund einer beliebigen Fassung der Signaturregelung erstellte Signatur mittelbar oder unmittelbar einer zweiten (gleich bezeichneten) Fassung der Signaturregelung unterliegt. Dadurch sollen irreführende Zirkelschlüsse verhindert werden. Außerdem sollte die ungültig gewordene Fassung auf jeden Fall aufbewahrt werden.

1.5 Begriffsbestimmungen und Abkürzungen

Die in diesem Dokument verwendeten Begriffsbestimmungen und Abkürzungen sind in Table 1 aufgeführt.

Abkürzung	Begriffsbestimmung
CA	Zertifizierungsstelle
DTBS	Zu signierende Daten
LTV	Langfristige Gültigkeit
OID	Objektkennung
ABl.	Amtsblatt der Europäischen Union
PIN	Persönliche Identifikationsnummer
OP	Amt für Veröffentlichungen der Europäischen Union
QC	Qualifiziertes Zertifikat
QESig	Qualifizierte elektronische Signatur
QESeal	Qualifiziertes elektronisches Siegel
QSCD	Qualifizierte Signatur-/Siegelerstellungseinheit
SAA	Anwendung zur Signaturergänzung
SCA	Anwendung zur Signaturerstellung
SSCD	Sichere Signaturerstellungseinheit
SVA	Anwendung zur Validierung von Signaturen
TSP	Anbieter von vertrauenswürdigen Diensten
QTSP	Qualifizierter Anbieter von vertrauenswürdigen Diensten
WIPIWIS	Was dargestellt wird, ist das, was signiert wird

Tabelle 1: Begriffsbestimmungen und Abkürzungen

2 Erklärungen zu den Verfahren der Signaturanwendung

2.1 Mit der Regelung verbundene Anforderungen

Amtsblattaussagen unterliegen den Bestimmungen der Artikel 1 und 2 der Verordnung des Rates über die elektronische Veröffentlichung des Amtsblatts der Europäischen Union; dort ist unter anderem vorgesehen, dass die elektronische Ausgabe des Amtsblatts eine qualifizierte elektronische Signatur gemäß Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates oder ein qualifiziertes elektronisches Siegel gemäß Verordnung (EU) Nr. 910/2014 tragen MUSS.

Die elektronische Signierung und Siegelung von Amtsblattaussagen fällt unter die Vorschriften für die Erstellung einer Signatur als wesentliche formale Anforderung gemäß Artikel III.2.1 der DURCHFÜHRUNGSBESTIMMUNGEN der Europäischen Kommission FÜR DEN BESCHLUSS 2002/47/EG, EGKS, EURATOM ZUR VERWALTUNG VON DOKUMENTEN UND FÜR DEN BESCHLUSS 2004/563/EG, EURATOM ÜBER ELEKTRONISCHE UND DIGITALISIERTE DOKUMENTE vom 30. November 2009²; gemäß dieser Vorschrift setzen elektronische Amtsblattsignaturen außerdem eine qualifizierte elektronische Signatur gemäß [eIDAS] voraus.

Gemäß Artikel III.2.3 der DURCHFÜHRUNGSBESTIMMUNGEN FÜR DEN BESCHLUSS 2002/47/EG UND FÜR DEN BESCHLUSS 2004/563/EG² obliegt die Prüfung der unterzeichnenden Behörde der Amtsblatt-SCA, wenn ein Beamter des Amts für Veröffentlichungen ermächtigt wird, Amtsblattaussagen elektronisch zu signieren, oder wenn das Amt für Veröffentlichungen als juristische Person ermächtigt wird, Amtsblattaussagen elektronisch zu siegeln.

Elektronische Amtsblattaussagen können ohne Signatur oder Siegel zwar keine Rechtskraft erlangen; gemäß der Amtsblattsignaturregelung MUSS die Amtsblatt-SCA jedoch gewährleisten, dass ausschließlich die autorisierten Amtsblatt-Unterzeichner in der Lage sind, Amtsblattaussagen zurückzuweisen. Auf diese Weise sollen Angriffe auf das Verfahren zur Veröffentlichung des Amtsblatts wirksam unterbunden werden.

Da autorisierte Amtsblatt-Unterzeichner für das Amt für Veröffentlichungen handeln, muss der Generaldirektor des Amts für Veröffentlichungen (im Wege der Befugnisübertragung) die ordnungsgemäße Autorisierung der jeweiligen Qualitätszertifikate (QC) für die Signierung des Amtsblatts gewährleisten. Dazu müssen QC-Autorisierungen im Zusammenhang mit der Signierung des Amtsblatts die folgenden Anforderungen erfüllen:

- In der Benutzerverwaltung der Amtsblatt-SCA *MÜSSEN* die Autorisierungen ordnungsgemäß konfiguriert sein.
- Die QC-Autorisierungen *SOLLTEN* auf einrichtungsspezifische (professionelle) Zertifikate beschränkt sein, welche die Zugehörigkeit der jeweiligen Person zum Amt für Veröffentlichungen gewährleisten³.
- Die Autorisierung *MUSS* transparent erfolgen; dazu sind die autorisierten QC gemäß Artikel 2 der Verordnung des Rates über die elektronische Veröffentlichung des Amtsblatts der Europäischen Union auf der EUR-Lex-Website zu veröffentlichen.

² Siehe SEC(2009) 1643.

³ Einrichtungsspezifische Zertifikate garantieren die Zugehörigkeit der betreffenden Person zu einer bestimmten Einrichtung. Die Sicherheit wird dadurch erhöht, dass der betreffende qualifizierte Anbieter von vertrauenswürdigen Diensten vom Inhaber des jeweiligen Zertifikates einen Berechtigungsnachweis verlangt.

2.2 Verbundene rechtliche Anforderungen

Die Einführung elektronischer Signaturen und elektronischer Siegel gemäß der Amtsblattsignaturregelung UNTERLIEGT den folgenden Rechtsvorschriften:

- Verordnung (EU) Nr. 216/2013 des Rates vom 7. März 2013 über die elektronische Veröffentlichung des Amtsblatts der Europäischen Union,
- Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG⁴,
- 2009/767/EG: Entscheidung der Kommission vom 16. Oktober 2009 über Maßnahmen zur Erleichterung der Nutzung elektronischer Verfahren über einheitliche Ansprechpartner gemäß der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates über Dienstleistungen im Binnenmarkt⁵,
- Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)⁶,
- Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)⁷,
- Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz⁸,
- 2010/425/EU: Beschluss der Kommission vom 28. Juli 2010 zur Änderung der Entscheidung 2009/767/EG in Bezug auf die Erstellung, Führung und Veröffentlichung von vertrauenswürdigen Listen der von den Mitgliedstaaten beaufsichtigten bzw. akkreditierten Zertifizierungsdiensteanbieter⁹,
- 2009/496/EG, EURATOM: Beschluss des Europäischen Parlaments, des Rates, der Kommission, des Gerichtshofs, des Rechnungshofs, des Europäischen Wirtschafts- und Sozialausschusses und des Ausschusses der Regionen vom 26. Juni 2009 über den Aufbau und die Arbeitsweise des Amts für Veröffentlichungen der Europäischen Union¹⁰,
- 2011/130/EU: Beschluss der Kommission vom 25. Februar 2011 über Mindestanforderungen für die grenzüberschreitende Verarbeitung von Dokumenten, die gemäß der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates über

⁴ Siehe ABl. L 257 vom 28.8.2014, S. 73.

⁵ Siehe ABl. L 274 vom 20.10.2009, S. 36.

⁶ Siehe ABl. L 119 vom 4.5.2016, S. 1.

⁷ Siehe ABl. L 201 vom 31.7.2002, S. 37.

⁸ Siehe ABl. L 337 vom 18.12.2009, S. 11.

⁹ Siehe ABl. L 199 vom 31.7.2010, S. 30.

¹⁰ Siehe ABl. L 168 vom 30.6.2009, S. 41.

Dienstleistungen im Binnenmarkt von zuständigen Behörden elektronisch signiert worden sind³.

2.3 Technische Sicherheit

Für die Erstellung von Amtsblattsignaturen und -siegel in Betracht kommende Verschlüsselungs-Tools MÜSSEN die Anforderungen an qualifizierte elektronische Signaturen gemäß [eIDAS], [ETSI 2016] und einschlägigen Verfahren gemäß dem Stand der Technik entsprechen.

2.4 Rechtliche Aussagen

Elektronische Signaturen und Siegel auf Amtsblattausgaben werden im Namen des Amtes für Veröffentlichungen gemäß der Verordnung des Rates über die elektronische Veröffentlichung des Amtsblatts der Europäischen Union erstellt.

3 Parameter der geschäftlichen Anwendung

3.1 Parameter der geschäftlichen Anwendung, die sich hauptsächlich auf die betreffende Anwendung/den betreffenden Geschäftsprozess beziehen

3.1.1 Parameter der geschäftlichen Anwendung (a): Arbeitsablauf (Abfolge und Zeitplan) der Signaturen

3.1.1.1 Beschreibung des allgemeinen Arbeitsablaufs

Das Amt für Veröffentlichungen veröffentlicht das Amtsblatt montags bis freitags und gelegentlich auch am Wochenende. Bei dieser Veröffentlichung kann es sich um eine Amtsblattausgabe oder um eine Ausgabe von Amtsblatt – Rechtsakte handeln. Eine Ausgabe des Amtsblatts ist die Veröffentlichung eines oder mehrerer Dokumente in mehreren Sprachen. Jede Sprachfassung einer Ausgabe enthält den Volltext jedes Dokuments in einer einzigen Datei. Eine Ausgabe von Amtsblatt – Rechtsakte stellt eine mehrsprachige Veröffentlichung eines einzigen Dokuments dar, das allein veröffentlicht wird. Jede Sprachfassung einer Ausgabe von Amtsblatt – Rechtsakte enthält den Volltext jedes Dokuments in einer einzigen Datei.

Die einzelnen Amtsblattausgaben und Ausgaben von Amtsblatt – Rechtsakte werden nach der Reihe klassifiziert, zu der sie gehören, wobei die Kategorie als kennzeichnender Teil des Amtsblatts dient. Für den hier relevanten Anwendungsbereich sind zwei Reihen maßgeblich: Reihe L (Gesetzgebung) und Reihe C (Informationen und Bekanntmachungen). Eine Reihe kann Unterreihen und Einordnungen enthalten (Nähere Erläuterungen zum Anwendungsbereich und zum Aufbau der Dokumente sowie Hintergrundinformationen: siehe <http://publications.europa.eu/code/de/de-10000.htm>).

Ergänzend zu den Amtsblatt-Reihen L und C werden gegebenenfalls Sonderausgaben mit EU-Sekundärrecht in der jeweiligen Landessprache eines beitretenden Staats/eines neuen Mitgliedstaats veröffentlicht. Diese Sonderausgaben sind ebenfalls Bestandteil des Anwendungsbereichs.

Sobald eine Ausgabe eines Amtsblatts oder eines Amtsblatts – Rechtsakte vollständig ist (d. h. alle Sprachfassungen des Amtsblatts oder des Amtsblatts – Rechtsakte in PDF/A verfügbar sind) und veröffentlicht werden kann, wird der Arbeitsablauf entweder mit einem elektronischen Siegelverfahren (siehe Abschnitt 3.1.1.2) oder einem elektronischen Signaturverfahren (siehe Abschnitt 3.1.1.3) fortgesetzt. Im Falle einer elektronischen Siegelung wird ein qualifiziertes elektronisches Siegel automatisch mithilfe eines qualifizierten Zertifikats für elektronische Siegel generiert, das dem Amt für Veröffentlichungen als einer Stelle der Europäischen Kommission ausgestellt wird. Im Falle einer elektronischen Signatur wird eine qualifizierte elektronische Signatur von einer autorisierten Person mit einem qualifizierten Zertifikat für elektronische Signaturen generiert.

Bei der elektronischen Siegelung handelt es sich um den von der SCA gewählten Standardarbeitsablauf, d. h. dass vollständige Ausgaben eines Amtsblatts oder eines Amtsblatts – Rechtsakte den automatisierten Siegelungsvorgang durchlaufen, es sei denn, dieser Vorgang ist nicht verfügbar. In letzterem Fall kommt das Signierverfahren zum Einsatz.

Da für die Signierung jeder einzelnen Ausgabe eine gesonderte XAdES-Signatur oder ein gesondertes XAdES-Siegel mit einem eigenen Manifest verwendet wird (siehe [Bartel 2008], [ETSI 2022-XAdES] und 2011/130/EU: Beschluss der Kommission vom 25. Februar 2011 über Mindestanforderungen für die grenzüberschreitende Verarbeitung von Dokumenten, die gemäß der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates über Dienstleistungen

im Binnenmarkt¹¹ von zuständigen Behörden elektronisch signiert worden sind), muss bei der Prüfung der Signatur oder des Siegels eines Amtsblatts oder eines Amtsblatts – Rechtsakte ergänzend zur Validierung der XML-Stammsignatur im Rahmen der Validierung gemäß [ETSI 2022-XAdES] (siehe [Bartel 2008]) auch das Manifest validiert werden.

In den folgenden Unterabschnitten werden die Arbeitsabläufe beschrieben, die in der Amtsblatt-SCA, SAA und SVA zur elektronischen Siegelung oder Signierung auf hoher Ebene umgesetzt werden (vgl. [ETSI 2016]).

3.1.1.2 Siegelerstellung für ein Amtsblatt und ein Amtsblatt – Rechtsakte

1. Es wird eine vollständige Ausgabe eines Amtsblatt oder eines Amtsblatts – Rechtsakte für die Siegelung ausgewählt.
2. Die SCA nimmt eine Vorabprüfung der vorgelegten Dateien vor:
 - a. Sie prüft, ob die Sprachfassungen der Ausgabe eines Amtsblatt/eines Amtsblatts – Rechtsakte größtmäßig übereinstimmen und innerhalb konfigurierbarer Größen liegen.
 - b. Sie prüft, ob alle vorgelegten Sprachfassungen zur Veröffentlichung vorgesehen waren.
3. Wird bei der Überprüfung etwas Gegenteiliges festgestellt, wird der Siegelungsvorgang unterbrochen. Damit der Vorgang fortgesetzt werden kann, müssen autorisierte Mitarbeiter des Amts für Veröffentlichungen manuell eingreifen.
4. Nach erfolgreicher Validierung durch die SCA wird ein Manifest erstellt, in dem jede Sprachfassung der vollständigen Ausgabe verzeichnet ist. Außerdem entspricht jede Sprachfassung einer einzelnen EU-Sprache und wird als PDF/A-Dokument erstellt, das bei der Berechnung des digitalen Fingerabdrucks („Message-Digest“) als binärer Oktett-Strom behandelt wird.
5. Die SCA führt eine Authentifizierung anhand des zentralen elektronischen Signaturportals der Europäischen Kommission durch und übermittelt das generierte Manifest zur automatischen Siegelung.
6. Das elektronische Signaturportal versieht das bereitgestellte Manifest mit einem qualifizierten Siegelzertifikat, das von einem akkreditierten europäischen QTSP ausgestellt wurde (siehe [eIDAS]). Der private Schlüssel für dieses Siegelzertifikat wird auf einer QSCD-Schnittstelle mit dem elektronischen Signaturportal gespeichert.
7. Das so erstellte XAdES-Siegel (vgl. [ETSI 2022-XAdES]) wird dann an die SCA zurückgesandt, die u. a. die Gültigkeit der verwendeten Algorithmen verifiziert und prüft, ob das Siegelzertifikat des jeweiligen Siegels autorisiert ist und von derselben juristischen Person, die als befugter Unterzeichner authentifiziert wurde, gehalten wird.
8. Nach erfolgreicher Überprüfung wird das elektronische Siegel durch einen von einem akkreditierten QTSP bereitgestellten Signaturzeitstempel ergänzt (siehe [eIDAS]).
9. Das im vorherigen Prozessschritt durch einen Zeitstempel ergänzte elektronische Siegel wird zur Veröffentlichung auf der EUR-Lex-Website weitergeleitet. Gleichzeitig wird in der SCA eine identische Kopie des Siegels gespeichert.
10. Wenn die erforderliche Karenzzeit von 24 Stunden für ein Siegel, das aus dem vorhergehenden Prozessschritt resultiert, verstrichen ist, wird seine Gültigkeit anhand des vertrauenswürdigen

¹¹ ABl. L 53 vom 26.2.2011, S. 66.

Zeitstempeldienstes eines akkreditierten europäischen QTSP zusätzlich ergänzt und nachhaltig verlängert, um der Signatur für einen langen Zeitraum Gültigkeit zu verleihen (siehe [eIDAS]).

11. Das Siegel, das im vorherigen Prozessschritt ergänzt wurde, wird dann zur Veröffentlichung auf der EUR-Lex-Website weitergeleitet und ersetzt dort das Siegel aus Schritt 9, dessen Gültigkeit noch nicht ergänzt und nachhaltig verlängert wurde.
12. Neben der Veröffentlichung auf der EUR-Lex-Website werden identische Kopien der Dokumente, die die Ausgabe eines Amtsblatts oder eines Amtsblatts – Rechtsakte sowie das entsprechende Siegel mit nachhaltiger Gültigkeit enthalten, in das System zur langfristigen digitalen Aufbewahrung übertragen, das vom Amt für Veröffentlichungen verwaltet wird und in dem die offiziellen Dokumente der EU-Organe langfristig aufbewahrt werden. Die praktische Ausgestaltung der langfristigen Aufbewahrung ist jedoch NICHT Gegenstand dieser Signaturregelung.

3.1.1.3 Signaturerstellung für das Amtsblatt oder das Amtsblatt – Rechtsakte

1. Es wird eine vollständige Ausgabe des Amtsblatts oder des Amtsblatts – Rechtsakte für die Signierung ausgewählt.
2. Es wird ein Manifest erstellt, in dem jede Sprachfassung der vollständigen Ausgabe verzeichnet ist. Außerdem entspricht jede Sprachfassung einer einzelnen EU-Sprache und wird als PDF/A-Dokument erstellt, das bei der Berechnung des digitalen Fingerabdrucks („Message-Digest“) als binärer Oktett-Strom behandelt wird.

Die vollständigen Ausgaben werden von der SCA bei der Erstellung des Manifests exklusiv verwaltet und gesperrt, um die für den gesamten Prozess entscheidende konsistente Digest-Berechnung zu gewährleisten.

3. Nach erfolgreicher Authentifizierung durch die SCA kann ein befugter Unterzeichner eine vollständige Ausgabe zum Signieren auswählen, wenn im vorherigen Schritt das betreffende Manifest erstellt wurde.
4. Nach erfolgreicher Auswahl einer zu signierenden Ausgabe tritt der befugte Unterzeichner in den Vorgang zur Signierung der betreffenden Ausgabe ein:
 - a. Um dem WIPIWIS-Grundsatz in angemessener Weise gerecht zu werden, muss der befugte Unterzeichner zumindest drei verschiedene Sprachfassungen der betreffenden Ausgabe mit einem konformen PDF/A-Viewer prüfen; erst nach dieser Prüfung kann die Ausgabe signiert werden. Umfasst eine Ausgabe des Amtsblatts oder des Amtsblatts – Rechtsakte weniger als drei Sprachfassungen, hat der befugte Unterzeichner alle verfügbaren Sprachfassungen zu prüfen.

Die SCA ermöglicht dem Unterzeichner die Prüfung beliebiger Sprachfassungen der zu signierenden Ausgabe. Der Unterzeichner KANN daher den gesamten zu signierenden Inhalt prüfen, wenn er dies möchte.
 - b. Der befugte Unterzeichner kann die Ausgabe nach eigenem Ermessen zurückweisen und damit den Signiervorgang abbrechen oder auf die Schaltfläche Sign klicken, um den Signiervorgang fortzusetzen.
 - c. Wenn der Unterzeichner auf die Schaltfläche Sign klickt,
 - i. beantragt die SCA beim zentralen elektronischen Signaturportal der Europäischen Kommission die Signierung, übermittelt das Manifest für die Signierung und leitet den befugten Unterzeichner auf das Portal weiter;

- ii. anschließend authentifiziert sich der befugte Unterzeichner auf dem elektronischen Signaturportal, wo ihm gemäß den WIPIWIS-Grundsätzen das Manifest für die Signierung vorgelegt wird;
 - iii. das elektronische Signaturportal verbindet sich mit der auf dem Arbeitsplatz des befugten Unterzeichners installierten Middleware und holt das von einem akkreditierten europäischen QTSP ausgestellte qualifizierte Signierzertifikat des Unterzeichners ein (vgl. [eIDAS]). Dieses Zertifikat wird dem befugten Unterzeichner vorgelegt, der wiederum aufgefordert wird, die entsprechende PIN zum Schutz der QSCD einzugeben, um die QSCD zu ermächtigen, die Signatur unter Verwendung des privaten Schlüssels für das ausgewählte Signierzertifikat zu erstellen und damit den Signiervorgang abzuschließen.
- d. Die Middleware sendet den generierten Signaturwert an das elektronische Signaturportal, das wiederum eine entsprechende XAdES-Signatur generiert (vgl. [ETSI 2022-XAdES]).
5. Diese XAdES-Signatur wird dann an die SCA zurückgesandt, die über das elektronische Signaturportal u. a. die Gültigkeit der verwendeten Algorithmen verifiziert und prüft, ob das Signierzertifikat der jeweiligen Signatur autorisiert ist und von derselben Person, die als befugter Unterzeichner authentifiziert wurde, gehalten wird.
 6. Nach erfolgreicher Prüfung erhält die Signatur über das elektronische Signaturportal zur Ergänzung einen von einem akkreditierten QTSP bereitgestellten Signaturzeitstempel (vgl. [eIDAS]).
 7. Die im vorherigen Prozessschritt erteilte Signatur wird zur Veröffentlichung auf der EUR-Lex-Website weitergeleitet. Gleichzeitig wird eine identische Kopie der Signatur in der SCA gespeichert.
 8. Wenn die erforderliche Karenzzeit von 24 Stunden für eine aus dem vorhergehenden Prozessschritt resultierende Signatur verstrichen ist, wird deren Gültigkeit anhand des vertrauenswürdigen Zeitstempeldienstes eines akkreditierten europäischen QTSP nachhaltig verlängert, um der Signatur für einen langen Zeitraum Gültigkeit zu verleihen (siehe [eIDAS]).
 9. Die Signatur, deren Gültigkeit im vorherigen Prozessschritt verlängert wurde, wird dann zur Veröffentlichung auf der EUR-Lex-Website weitergeleitet und ersetzt dort die Signatur aus Schritt 7, deren Gültigkeit noch nicht nachhaltig verlängert wurde.
 10. Neben der Veröffentlichung auf der EUR-Lex-Website werden identische Kopien der in einer Ausgabe enthaltenden Dokumente sowie die entsprechende Signatur mit nachhaltiger Gültigkeit in das System für die langfristige digitale Aufbewahrung übertragen, das vom Amt für Veröffentlichungen verwaltet wird und in dem die offiziellen Dokumente der EU-Organe langfristig aufbewahrt werden. Die praktische Ausgestaltung der langfristigen Aufbewahrung ist jedoch NICHT Gegenstand dieser Signaturregelung.

3.1.1.4 Krisensituation

Wenn es aufgrund einer unvorhergesehenen und außergewöhnlichen Nichtverfügbarkeit der Amtsblatt-SCA nicht möglich ist, das Siegel oder die Signatur des Amtsblatts oder des Amtsblatts – Rechtsakte wie in den Abschnitten 3.1.1.2 beziehungsweise 3.1.1.3 beschrieben zu erstellen, bringt das Amt für Veröffentlichungen auf jedem PDF/A-Dokument, das jeweils einer Sprachfassung der Ausgabe des Amtsblatts oder des Amtsblatts – Rechtsakte entspricht, ein QESeal oder eine QESig an. Alle gesiegelten/signierten PDF/A-Dokumente werden zur Veröffentlichung auf die EUR-Lex-Website weitergeleitet.

3.1.2 Parameter der geschäftlichen Anwendung (b): Zu signierende Daten

- Signaturen und Siegel im Amtsblatt beziehungsweise Amtsblatt – Rechtsakte stützen sich auf ein XML-Manifest (siehe [Bartel 2008] und [ETSI 2022-XAdES]), in dem alle in einer Ausgabe des Amtsblatts oder des Amtsblatt – Rechtsakte enthaltenen Sprachfassungen im PDF/A-Format mit einer einzigen Signatur zusammengefasst werden. Diese Signatur muss die nachstehenden Anforderungen erfüllen: Jede logisch mit einer Ausgabe des Amtsblatts beziehungsweise des Amtsblatt – Rechtsakte verknüpfte Sprachfassung MUSS ihren eigenen Digest-Wert aufweisen.
- Sämtliche logisch mit einer Ausgabe des Amtsblatts beziehungsweise des Amtsblatt – Rechtsakte verknüpften Sprachfassungen MÜSSEN dem Unterzeichner während der Erstellung der Signatur zur Überprüfung angezeigt werden, damit der Inhalt der Signatur nach Ermessen des Unterzeichners geprüft werden kann (siehe Abschnitt 3.1.1.3) und damit dem WIPIWIS-Prinzip Rechnung getragen wird.
- Durch Verwendung einer PDF/A-Lesesoftware MUSS eine ordnungsgemäße Visualisierung gewährleistet werden.
- Während des Signiervorgangs werden dem Unterzeichner NUR die Sprachfassungen der zu signierenden Ausgabe ANGEZEIGT.
- Die technischen Merkmale aller logisch mit einer Ausgabe des Amtsblatts beziehungsweise des Amtsblatt – Rechtsakte verknüpften Sprachfassungen MÜSSEN zur Gewährleistung der Kohärenz bei der Erstellung von Siegeln und Signaturen überprüft werden.

Im Falle einer Krisensituation im Sinne des Abschnitts 3.1.1.4 gelten folgende Anforderungen:

- Jede Sprachfassung eines Amtsblatts oder eines Amtsblatt – Rechtsakte MUSS mit einem eigenen QESal oder einer eigenen QESig versehen sein.
- Alle logisch mit einem Amtsblatt oder einem Amtsblatt – Rechtsakte verbundenen Sprachfassungen MÜSSEN vom Unterzeichner bei der Signaturerstellung geprüft werden, damit der Signaturinhalt nach Ermessen des Unterzeichners überprüft werden kann, um dem WIPIWIS-Prinzip zu entsprechen.
- Eine ordnungsgemäße Visualisierung MUSS durch Verwendung einer PDF/A-Lesesoftware gewährleistet werden.

3.1.3 Parameter der geschäftlichen Anwendung (c): Beziehung zwischen signierten Daten und Signatur(en) und Siegel(n)

Eine Signatur oder ein Siegel des Amtsblatts oder des Amtsblatt – Rechtsakte gilt für alle Sprachfassungen einer Ausgabe des Amtsblatts oder des Amtsblatt – Rechtsakte, die jeweils als PDF/A-Dokument formatiert sind.

Bei der Erstellung einer Signatur oder eines Siegels des Amtsblatts oder des Amtsblatt – Rechtsakte wird der digitale Inhalt eines zu signierenden/siegelnden Dokuments als binärer Oktett-Strom in einem Digest zusammengefasst; dabei wird der stärkste mit den Anforderungen gemäß [ETSI 2022-Crypto] Abschnitt 7.3 kompatible Digest-Algorithmus verwendet.

Die Digest-Werte der einzelnen Dokumente werden mit den URIs der ursprünglichen Dateinamen in einem XML-Manifest kombiniert; weitere Umwandlungen werden nicht vorgenommen (siehe [Bartel 2008]).

Das Manifest wird zusammen mit den Signaturattributen im XAdES-Format (siehe [ETSI 2022-XAdES]) für das im Beschluss 2011/130/EU der Kommission vom 25. Februar 2013 spezifizierte Profil signiert oder gesiegelt.

Im Falle einer Krisensituation im Sinne des Abschnitts 3.1.1.4 wird jedes PDF/A-Dokument, das jeweils einer Sprachfassung der Ausgabe des Amtsblatts oder des Amtsblatts – Rechtsakte entspricht, unter Verwendung von PAdES unterzeichnet oder versiegelt (vgl. [ETSI 2016-PAdES] [eIDAS]).

3.1.4 Parameter der geschäftlichen Anwendung (d): Zielgruppe

Die Zielgruppe ist jede Partei, die sich auf das Amtsblatt stützt und die Authentizität des Amtsblatts überprüfen muss, sowie alle für die Umsetzung der SCA und der SAA verantwortlichen Parteien, die für die Erstellung elektronischer Signaturen oder elektronischer Siegel sowie deren Erweiterung für Ausgaben des Amtsblatts oder des Amtsblatts – Rechtsakte zuständig sind.

3.1.5 Parameter der geschäftlichen Anwendung (e): Zuweisung der Verantwortlichkeit für die Validierung und Ergänzung von Signaturen

3.1.5.1 Überprüfung von Signaturen oder Siegeln für das Amtsblatt oder das Amtsblatt – Rechtsakte

Jede vertrauende Partei (insbesondere jeder europäische Bürger) kann eine auf der EUR-Lex-Website veröffentlichte Ausgabe eines Amtsblatt oder eines Amtsblatts – Rechtsakte und die entsprechende gesonderte XAdES-Signatur oder das entsprechende gesonderte XAdES-Siegel (cf. [ETSI 2022-XAdES]) zur Prüfung herunterladen.

Da bei der Erstellung von Signaturen und Siegeln ein interoperabler europäischer Signaturstandard zugrunde gelegt wird und die Dienste eines akkreditierten europäischen QTSP in Anspruch genommen werden (siehe [eIDAS]), kann die Prüfung mit einer beliebigen Prüf-Utility eines Fremdanbieters vorgenommen werden, welche die zugrunde gelegten Normen erfüllt, sofern das betreffende Manifest auf der Grundlage der Amtsblattsignaturregelung validiert werden kann.

Im Falle einer Krisensituation im Sinne des Abschnitts 3.1.1.4 wird jedes PDF/A-Dokument, das jeweils einer Sprachfassung der Ausgabe des Amtsblatts oder des Amtsblatts – Rechtsakte entspricht, unter Verwendung von PAdES unterzeichnet oder versiegelt (vgl. [ETSI 2016-PAdES]). Die Prüfung kann mit einer beliebigen Prüf-Utility eines Fremdanbieters vorgenommen werden, welche die zugrunde gelegte Norm erfüllt.

3.1.5.1.1 Server-seitige Prüfung

Um die Prüfung von Signaturen und Siegeln zu erleichtern, KANN das Amt für Veröffentlichungen eine kostenlose Amtsblatt-SVA auf dem Server bereitstellen, die gemäß dem im Folgenden beschriebenen Prüfungsarbeitsablauf strukturiert ist:

1. Der Prüfende lädt die zu prüfende PDF/A-Datei mit der damit verbundenen Signatur oder dem damit verbundenen Siegel anhand der in der SVA zum Hochladen von Dateien vorgesehenen Funktion hoch.
2. Die SVA berechnet den Digest der hochgeladenen PDF/A-Datei und prüft, ob der berechnete Digest in dem Teil der hochgeladenen Signatur enthalten ist, der sich auf das Manifest bezieht.
3. Nach erfolgreicher Prüfung des Digest wird eine XAdES-Standardprüfung der hochgeladenen Kandidatensignatur oder des hochgeladenen Kandidatensiegels durchgeführt. Voraussetzung ist allerdings, dass im Signier- oder im Siegelzertifikat ein für den durch den Zeitstempel der Signatur festgelegten Zeitraum befugter Amtsblattunterzeichner genannt wird. Ferner überprüft die SVA, ob der Unterzeichner zu dem Zeitpunkt, zu dem die Signatur laut ihrem Zeitstempel erstellt wurde, zur Unterzeichnung befugt war.

4. Die Prüfung ist bestanden, wenn alle vorherigen Schritte erfolgreich absolviert wurden. Ansonsten ist die Prüfung nicht bestanden. In jedem Fall wird dem Prüfenden ein verständlicher Bericht über den Prüfungsvorgang angezeigt.

3.1.5.1.2 Client-seitige Prüfung

Um die Prüfung von Signaturen und Siegeln zu erleichtern, KANN das Amt für Veröffentlichungen eine kostenlose Amtsblatt-SVA beim Client bereitstellen; die Amtsblatt-SVA ist gemäß dem im Folgenden beschriebenen Prüfungsarbeitsablauf strukturiert:

1. Der Prüfende startet die heruntergeladene SVA. Anschließend wird die Code-Signatur automatisch von der Laufzeitumgebung geprüft. Nach erfolgreicher Prüfung der Code-Signatur autorisiert der Prüfende die Ausführung des Programms.
2. Im Dateiauswahl-Fenster der SVA wählt der Prüfende aus dem lokalen Dateisystem des jeweiligen PCs eine PDF/A-Datei in einer bestimmten Sprachfassung aus, die anhand der damit verbundenen Kandidatensignatur oder dem damit verbundenen Kandidatensiegel geprüft werden soll.
3. Die SVA berechnet den Digest des hochgeladenen Dokuments und prüft, ob der berechnete Digest im Manifest der ausgewählten Kandidatensignatur oder des ausgewählten Kandidatensiegels enthalten ist.
4. Nach erfolgreicher Prüfung des Digest erfolgt die XAdES-Standardprüfung der ausgewählten Kandidatensignatur oder des ausgewählten Kandidatensiegels.
5. Der Prüfungsvorgang ist erfolgreich, wenn alle vorherigen Schritte erfolgreich durchgeführt wurden und wenn im Signier- oder Siegelzertifikat ein Amtsblattunterzeichner genannt wird, der für den durch den Zeitstempel der Signatur festgelegten Zeitraum befugt war.

Die Informationen über den befugten Unterzeichner sind der SVA UNTER UMSTÄNDEN aus einer (voreingestellten) Konfiguration bekannt. Außerdem wird der Zertifikat-Digest des Signier- oder Siegelzertifikats im SVA-Ergebnis angezeigt, damit der Prüfende die Informationen selbst mit den veröffentlichten Informationen zu dem rechtlich befugten Unterzeichner im Zeitraum der Signatur- oder Siegelerstellung vergleichen kann; auch dieser Zeitraum wird im SVA-Ergebnis angezeigt.

3.2 Parameter der geschäftlichen Anwendung, die hauptsächlich von den Rechts- und Verwaltungsvorschriften im Zusammenhang mit der betreffenden Anwendung/dem betreffenden Geschäftsprozess beeinflusst werden

3.2.1 Parameter der geschäftlichen Anwendung (f): Rechtsform der Signaturen

Elektronische Signaturen und Siegel im Amtsblatt oder im Amtsblatt – Rechtsakte MÜSSEN QESig und QESeal im Sinne von [eIDAS] sein.

Diese Anforderungen sind insbesondere in der Verordnung des Rates über die elektronische Veröffentlichung des Amtsblatts der Europäischen Union festgelegt (siehe Abschnitt 2.2).

Voraussetzung für die Nutzung des Signatursystems ist, dass der jeweilige Unterzeichner ein QC erhalten hat.

Die spezifischen Elemente der erforderlichen QESig und QESeal MÜSSEN die folgenden Qualitätsanforderungen erfüllen:

- Signier- und Siegelungseinheit: QSCDs entsprechen den Anforderungen gemäß [eIDAS] Anhang II;
- Bereitstellung des Zertifikats: QC entspricht den Anforderungen gemäß [eIDAS] Anhang I;

- Unabhängige Gewähr für die Bereitstellung von Zertifikaten: Das QC muss von einem QTSP-Zertifizierungsdienst ausgestellt worden sein, der beaufsichtigt wird oder in einem Land, in dem [eIDAS] gilt, akkreditiert ist;
- Signaturverschlüsselungs-Software: Es darf nur in [ETSI 2022-Crypto] Abschnitt 7.3 aufgeführte Signatursoftware verwendet werden;
- LTV-Lösungen: Signier- und Siegelungsformulare für das Amtsblatt oder das Amtsblatt – Rechtsakte im XAdES-Format (siehe [ETSI 2022-XAdES]) MÜSSEN auf das Signierformular im LTA-Format hochgestuft werden; die Hochstufung beinhaltet die Verlängerung der Archivzeitstempel oder sonstiger Archivierungssysteme. (Alternativ KÖNNEN statt der Verlängerung der mit dem Archivzeitstempel definierten Frist sichere Fremdarchivierungsmechanismen zum Einsatz kommen, die dem internen System mindestens gleichwertig sein müssen.);
- Anwendung zur Signaturerstellung (SCA): Die Qualität der Amtsblatt-SCA MUSS die Qualitätsanforderungen der maßgeblichen EU-Regelungen sowie die Anforderungen der Verordnung des Rates über die elektronische Veröffentlichung des Amtsblatts der Europäischen Union erfüllen.

3.2.2 Parameter der geschäftlichen Anwendung (g): Vom Unterzeichner übernommene Verpflichtung

Elektronische Signaturen und Siegel auf Ausgaben des Amtsblatts oder des Amtsblatts – Rechtsakte werden im Namen des Amtes für Veröffentlichungen gemäß der Verordnung des Rates über die elektronische Veröffentlichung des Amtsblatts der Europäischen Union ERSTELLT.

Aufgrund seiner entsprechend eingegangenen Verpflichtung bestätigt der Amtsblattunterzeichner, dass die signierten Daten eine authentische Ausgabe des Amtsblatts oder des Amtsblatts – Rechtsakte darstellen, die unter Berücksichtigung der Regeln für die geschäftliche Anwendung (siehe Abschnitt 3.1.1) ordnungsgemäß validiert und vom Amt für Veröffentlichungen gemäß der Verordnung des Rates über die elektronische Veröffentlichung des Amtsblatts der Europäischen Union als authentische Quelle des EU-Rechts veröffentlicht wurde.

In einer Amtsblattsignatur ist KEINE ausdrückliche Angabe zum Verpflichtungstyp enthalten (siehe [ETSI 2022-XAdES] Abschnitt 5.2.3).

3.2.3 Parameter der geschäftlichen Anwendung (h): Grad der Zuverlässigkeit von Zeitnachweisen

Signaturen oder Siegel des Amtsblatts oder des Amtsblatts – Rechtsakte, die gemäß den Abschnitten 3.1.1.2 oder 3.1.1.3 erstellt werden, MÜSSEN an dem Tag mit einem Signaturzeitstempel (Ortszeit Luxemburg) versehen werden, der dem Datum auf der Signatur oder dem Siegel der Ausgabe des Amtsblatts oder des Amtsblatts – Rechtsakte entspricht; nur so ist sichergestellt, dass die Signatur oder das Siegel nicht nach dem Datum der Veröffentlichung erstellt wurde. Dadurch wird gewährleistet, dass die zum Zeitpunkt der Veröffentlichung befugten Unterzeichner für die Signaturen oder Siegel autorisiert sind.

Die Amtsblatt-SCA MUSS sicherstellen, dass alle erstellten XAdES-B-T-Signaturen diese Anforderung erfüllen.

Die Zeitstempel für die Erstellung von Signaturzeitstempeln in XAdES-B-T-Signaturen MÜSSEN qualifizierte Zeitstempel sein.

PAdES-Signaturen, die im Falle einer Krisensituation gemäß Abschnitt 3.1.1.4 erstellt wurden, KÖNNEN ohne Signaturzeitstempel erstellt werden.

Wenn PAdES-Signaturen, die im Falle einer Krisensituation gemäß Abschnitt 3.1.1.4 erstellt wurden, mit einem Signaturzeitstempel erstellt werden, SOLLTE der Signaturzeitstempel ein qualifizierter Zeitstempel sein und am selben Tag (Ortszeit in Luxemburg) wie das Datum der Signatur oder des Siegels der Ausgabe des Amtsblatts oder des Amtsblatts – Rechtsakte verwendet, um zu bestätigen, dass die Signatur oder das Siegel nicht nach dem Datum der Veröffentlichung erstellt wurde.

ANMERKUNG: Dies bedeutet, dass im Falle einer Krisensituation, wenn in der Signatur ein Signaturzeitstempel enthalten ist, ein nichtqualifizierter Zeitstempel verwendet werden kann.

Alle anderen Zeitstempel, einschließlich Archivzeitstempel und ggf. inhaltlicher Zeitstempel, SOLLTEN qualifizierte Zeitstempel sein.

3.2.4 Parameter der geschäftlichen Anwendung (i): Formalitäten der Signierung

Es ist Aufgabe der Amtsblatt-SCA, eine Signaturschnittstelle bereitzustellen, die so weit wie möglich eine gültige rechtliche Signatur- und Siegelumgebung gewährleistet. Die Schnittstelle muss folgende Anforderungen erfüllen:

- Sie muss angemessene Hinweise und Informationen zum Signier- und Siegelungsverfahren der Anwendung bereitstellen;
- sie muss die Kohärenz zwischen der Nutzung der betreffenden Daten zur Erstellung und zur Verifizierung von Signaturen und Siegeln, den Signatur- und Siegelerstellungseinheiten, den zu signierenden Daten sowie dem erwarteten Umfang und dem Zweck der Signatur und des Siegels (bzw. des Signier- und Siegelungsvorgangs) gewährleisten;
- sie muss dem Unterzeichner die Möglichkeit bieten, klar seinen Willen zur Signierung zum Ausdruck zu bringen, und sie muss dem Nutzer die Möglichkeit bieten, klar zum Ausdruck zu bringen, dass er beabsichtigt, die mit der Signatur oder dem Siegel verbundene Verpflichtung einzugehen;
- sie muss eine informierte Zustimmung ermöglichen und zum Ausdruck bringen.

Die Amtsblatt-SVA MUSS vertrauenden Parteien (einschließlich des Unterzeichners) die richtigen Verfahren für die Prüfung und die Archivierung der elektronischen Signatur oder des elektronischen Siegels und der Prüfungsdaten bereitstellen.

3.2.5 Parameter der geschäftlichen Anwendung (j): Langlebigkeit und Widerstandsfähigkeit gegenüber Veränderungen

Die signierten Ausgaben des Amtsblatts oder des Amtsblatts – Rechtsakte und die jeweiligen Signaturen MÜSSEN unbefristet archiviert werden. Die Erhaltung der Gültigkeit der Signaturen des Amtsblatts oder des Amtsblatts – Rechtsakte MUSS unbefristet sichergestellt werden (siehe Artikel 2 der Verordnung des Rates über die elektronische Veröffentlichung des Amtsblatts der Europäischen Union).

3.2.6 Parameter der geschäftlichen Anwendung (k): Archivierung

Entfällt.

3.3 Parameter der geschäftlichen Anwendung, die sich hauptsächlich auf die an der Signaturerstellung/-ergänzung/-validierung beteiligten Akteure beziehen

3.3.1 Parameter der geschäftlichen Anwendung (l): Identität (und Zuständigkeiten/Attribute) der Unterzeichner

3.3.1.1 Vorgeschlagene Regeln bezüglich der Identifikation der Unterzeichner

Signaturen des Amtsblatts oder des Amtsblatts – Rechtsakte MÜSSEN von befugten Unterzeichnern angebracht werden, bei denen es sich ausdrücklich um Beamte des Amts für Veröffentlichungen handeln MUSS, die über die für die Validierung von Signaturen des Amtsblatts oder des Amtsblatts – Rechtsakte gemäß den Regeln für die geschäftliche Anwendung erforderliche Erfahrung verfügen (siehe Abschnitt 3.1.1.3). Im Falle von Siegeln des Amtsblatts oder des Amtsblatts – Rechtsakte MUSS es sich bei dem befugten Unterzeichner um das Amt für Veröffentlichungen als eine Stelle der Europäischen Kommission handeln.

Autorisierte Unterzeichner sind sich ferner ihrer Verantwortung bewusst und MÜSSEN bei der Authentifizierung von Rechtstexten, die EU-Recht wiedergeben, nach bestem Wissen und Gewissen handeln.

Die Verknüpfung zwischen diesen Unterzeichnern als natürliche Personen und den Daten zur Prüfung der jeweiligen Signatur MUSS durch ein QC gemäß [eIDAS] bescheinigt sein, in dem ihre Identität und ihre Zugehörigkeit zum Amt für Veröffentlichungen belegt ist.

Die Autorisierung eines Amtsblattunterzeichners MUSS durch den Generaldirektor des Amts für Veröffentlichungen (ggf. im Wege der Befugnisübertragung) erfolgen.

3.3.1.2 Rollen und Attribute des Unterzeichners

Abgesehen von der Bestätigung der Zugehörigkeit des Unterzeichners zum Amt für Veröffentlichungen müssen QCs KEINERLEI sonstige Zuständigkeiten, Funktionen oder Qualifikationsattribute des Unterzeichners bescheinigen.

Es liegt in der VERANTWORTUNG der Amtsblatt-SCA, eine angemessene Zugangskontrolle und eine ordnungsgemäße Autorisierung des Unterzeichners zu gewährleisten, bevor Unterzeichnern Zugang zu den Signatureinrichtungen des Amtsblatts gewährt wird.

Zugangskontrolle und Autorisierung der Unterzeichner MÜSSEN auf der Grundlage eines in der SCA eingebetteten leistungsfähigen Authentifizierungsmechanismus sowie ausgehend von den Genehmigungen erfolgen, die zusammen mit den Public-Key-Zertifikaten der jeweils befugten Unterzeichner in der SCA-Nutzerverwaltungsdatenbank erfasst sind.

Vertrauende Parteien KÖNNEN die veröffentlichten Zertifikate der Amtsblattunterzeichner heranziehen, um deren rechtliche Befugnis zu prüfen.

3.3.1.3 Verbundener Autorisierungsnachweis

Keine über Abschnitt 3.3.1.2 hinausgehenden Bestimmungen.

3.3.2 Parameter der geschäftlichen Anwendung (m): Für die Authentifizierung des Unterzeichners erforderliches Sicherheitsniveau

Das für die Authentifizierung des Unterzeichners erforderliche Sicherheitsniveau wird durch sein qualifiziertes Zertifikat und seine Signaturerstellungsmittel gewährleistet, bei denen es sich um eine qualifizierte Signatur-/Siegelerstellungseinheit gemäß Definition in [eIDAS] handeln MUSS.

3.4 Sonstige Parameter der geschäftlichen Anwendung

3.4.1 Parameter der geschäftlichen Anwendung (o): Sonstige Angaben, die der Signatur oder dem Siegel beizufügen sind

3.4.1.1 Autorisierte Amtsblattunterzeichner und Stellen zur Vergabe von Zeitstempeln

Die Prüfung der Autorisierung von Unterzeichnern ist ein wesentliches vertrauensbildendes Element im Zusammenhang mit dem Amtsblatt.

Die Genehmigung MUSS explizit erfolgen, indem die elektronischen Zertifikate aller befugten Unterzeichner in einem vertrauenswürdigen Medium veröffentlicht werden, bei dem es sich nicht um die SCA/SVA handelt.

Aus der Veröffentlichung der befugten Amtsblattunterzeichner MUSS hervorgehen, dass der Beaufachtungsstatus der Unterzeichner-Zertifikate für den jeweils aktuellen Signaturzeitraum des Amtsblatts oder des Amtsblatts – Rechtsakte garantiert ist.

Befugte Amtsblattunterzeichner und Stellen zur Vergabe von Zeitstempeln DÜRFEN NICHT im Amtsblatt veröffentlicht werden, weil ansonsten Probleme aufgrund von Zirkelschlüssen entstehen würden, insbesondere in Bezug auf langfristige Validierungen.

Kommt es im Laufe der Zeit zu einem Wechsel bei den befugten Amtsblattunterzeichnern, MUSS die jeweils vorhergehende Gruppe von Unterzeichnern als historische vertrauenswürdige Information veröffentlicht werden. Die Veröffentlichung dieser Informationen ist erforderlich, damit die von den betreffenden Unterzeichnern signierten Ausgaben des Amtsblatts oder des Amtsblatts – Rechtsakte geprüft werden können.

Bei der Veröffentlichung befugter Unterzeichner MUSS der Zeitraum angegeben werden, für den die aufgeführten Unterzeichner zugelassen waren oder sind, damit diese Vorschrift den Zeitvorgaben der vorliegenden Fassung der Regelung gerecht wird.

3.4.1.2 Elektronische Signatur- und Siegelattribute, Anwendungsbereich und Zweck

Die Signatur- und Siegelerstellungsverfahren STÜTZEN SICH in angemessener Weise auf Signaturattribute. Dies gilt insbesondere für Signaturattribute mit Informationselementen, welche die elektronische Signatur/das elektronische Siegel unterstützen und auf die sich die Signatur/das Siegel bezieht, sowie für die DTBS. Dabei müssen die folgenden Anforderungen erfüllt sein:

- Die Signierungszertifikat-Kennung MUSS verwendet werden. Sie ist die Kennung des Zertifikates bzw. verweist auf das Zertifikat mit den Signatur-Prüfdaten der betreffenden Signatur- oder Siegelerstellungsdaten, die der Unterzeichner zur Erstellung der elektronischen Signatur oder des elektronischen Siegels verwendet hat.
- Angaben zur Signaturregelung sind MÖGLICH (siehe Abschnitt 1.2.2).
- Die Zeitangabe für den angeblichen Zeitpunkt der Signierung MUSS verwendet (ausgefüllt) werden. Als Zeitpunkt der Signierung wird der Zeitpunkt bezeichnet, den der Unterzeichner für die Erstellung einer Signatur oder eines Siegels angibt.

Dieser Zeitpunkt entspricht der aktuellen Systemzeit des vom Unterzeichner verwendeten PCs. Diese ist NICHT als vertrauenswürdige Zeitangabe zu verstehen.

Der Inhaber der Amtsblatt-SCA MUSS (nach Befugnisübertragung durch den Generaldirektor des Amts für Veröffentlichungen) gewährleisten, dass die aktuelle Systemzeit der PCs sämtlicher Unterzeichner genau eingestellt ist.

Dazu kann ein NTP (Netzzeitprotokoll) mit einer geeigneten Zeitquelle verwendet werden (siehe [Mills 2010]).

- Eine Angabe zum Verpflichtungstyp DARF NICHT erfolgen.
- Es KÖNNEN auch sonstige Signaturattribute verwendet werden,

Signaturattribute MÜSSEN gemäß [ETSI 2010] sowie gemäß Beschluss 2011/130/EU der Kommission vom 25. Februar 2013 verwendet werden.

3.4.2 Parameter der geschäftlichen Anwendung (p): Verschlüsselungssoftware

Siehe Abschnitt 3.2.1.

4 Anforderungen/Erklärungen zu den technischen Mechanismen und der Umsetzung von Normen

4.1 Regeln für vertrauenswürdige Zeitstempel

Das XAdES-B-LTA-Signaturformular (siehe [ETSI 2022-XAdES]) sieht mehrere Zeitstempel vor, die von einem in einem Mitgliedstaat oder in einem EWR-Land akkreditierten Zeitstempeldienst bezogen werden MÜSSEN.

Der Inhaber der Amtsblatt-SCA MUSS (nach Befugnisübertragung durch den Generaldirektor des Amts für Veröffentlichungen) dafür sorgen, dass die SCA für die Verwendung geeigneter Verschlüsselungsalgorithmen konfiguriert ist.

4.2 Regeln für die langfristige Gültigkeit

Die Erhaltung der Gültigkeit der Signaturen des Amtsblatts oder des Amtsblatts – Rechtsakte während des für die Gültigkeit der Signatur anzunehmenden Zeitraums wird durch die Verwendung des XAdES-B-LTA-Formulars (siehe [ETSI 2022-XAdES]) sowie anschließend dadurch sichergestellt, dass die Signatur mit einem zusätzlichen qualifizierten Archivzeitstempel versehen wird, um ihre Gültigkeit nach Bedarf zu verlängern, oder dass eine geeignete Archivierungslösung genutzt wird, die die Erhaltung der Gültigkeit der Signatur gewährleistet.

4.3 Sonstige geschäftliche und rechtliche Aspekte

Da das Amtsblatt montags bis freitags und gelegentlich auch am Wochenende erscheint, MUSS der Inhaber der Amtsblatt-SCA (nach Befugnisübertragung durch den Generaldirektor des Amts für Veröffentlichungen) dafür sorgen, dass die SCA ständig funktionsfähig ist.

Daher SOLLTEN geeignete Dienstleistungsvereinbarungen getroffen werden.

Wenngleich Signaturen und Siegel im Amtsblatt beziehungsweise Amtsblatt – Rechtsakte von jeder SVA geprüft werden können, die die Normen und Regeln der Amtsblattsignaturregelung erfüllt (u. a. die Validierung von Manifesten), KANN das Amt für Veröffentlichungen eine öffentlich zugängliche SVA auf der EUR-Lex-Website bereitstellen, damit vertrauende Parteien (insbesondere europäische Bürgerinnen und Bürger) Signaturen und Siegel im Amtsblatt beziehungsweise Amtsblatt – Rechtsakte prüfen können, ohne auf die Prüf-Utility eines Fremdanbieters zurückgreifen zu müssen.

Alternativ KANN das Amt für Veröffentlichungen auch eine SVA als öffentlich herunterladbare Utility bereitstellen, welche die Benutzer selbstständig auf ihrem Desktop-PC ausführen können. In diesem Fall wird nur vorausgesetzt, dass der Prüfende, dem das Ergebnis der Prüfung angezeigt wird, auf die betreffende Software vertraut.

5 Anhang

[Bartel 2008]	Bartel M., Boyer J., Fox B., LaMacchia B., Simon E. <i>XML Signature Syntax and Processing (2. Auflage)</i> W3C Recommendation, 2008
[Bradner 1997]	Bradner S. <i>Key words for use in RFCs to indicate requirement levels</i> RFC 2119, Network Working Group, 1997
[Mealling 2010]	Mealling M. <i>A URN Namespace of Object Identifiers</i> RFC 3061, Network Working Group, 2001
[Mills 2010]	Mills D., Delaware U., Martin J., ISC Ed., Burbank J., Kasch W. <i>Network Time Protocol Version 4: Protocol and Algorithms Specification</i> RFC 5905, IETF, 2010
[eIDAS]	<i>Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG</i> Amtsblatt L 257
[ETSI 2015]	ETSI-ESI <i>Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents</i> TS 119 172-1, v1.1.1, ETSI, 2015
[ETSI 2016]	ETSI-ESI <i>Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation</i> TS 119 101, v1.1.1, ETSI, 2016
[ETSI 2016-PAdES]	ETSI-ESI PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures ETSI EN 319 142-1 V1.1.1 (2016-04)
[ETSI 2022-XAdES]	ETSI-ESI XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures ETSI EN 319 132-1 V1.2.1 (2022-02)
[ETSI 2022-Crypto]	ETSI-ESI Cryptographic Suites ETSI TS 119 312 V1.4.2 (2022-02)