Política de assinatura do Jornal Oficial

Versão 4

(1.3.171.4.1.1.4)

Em vigor a partir de 1 de outubro de 2023

Índice

1 INTRODUÇÃO 3

1.1 Apresentação geral 3
1.2 Âmbito operacional 4
1.2.1 Âmbito e limites da política de assinatura 4
1.2.2 Âmbito das aplicações 4
1.2.3 Contexto transacional 4
1.3 Nome da política de assinatura, identificação e regras de conformidade 4
1.3.1 Nome da política 4
1.3.2 Identificador da política 4
1.3.3 Regras de conformidade da política 4
1.3.4 Pontos de distribuição da política 4
1.3.5 Período de validade da política 4
1.3.6 Âmbito da política 5
1.4 Administração dos documentos relativos à política de assinatura 5
1.4.1 Entidade responsável pela política 5
1.4.2 Pessoa de contacto 5
1.4.3 Procedimentos de aprovação 5
1.4.4 Versões da política 6
1.5 Definições e siglas 6

2 DECLARAÇÕES DE PRÁTICAS DA APLICAÇÃO DA ASSINATURA 7

2.1 Requisitos políticos conexos 7
2.2 Requisitos jurídicos conexos 7
2.3 Considerações de segurança técnica 8
2.4 Declarações jurídicas 9

3 PARÂMETROS DE DELIMITAÇÃO DAS OPERAÇÕES (*BUSINESS SCOPING PARAMETERS* [BSP]) 10

3.1 BSP relacionados principalmente com a aplicação/o processo operacional em causa 10
3.1.1 BSP a): Sequência (sequenciação e calendário) das assinaturas 10
3.1.2 BSP b): Dados a assinar 13
3.1.3 BSP c): Relação entre os dados assinados e a(s) assinatura(s) e o(s) selo(s) 14
3.1.4 BSP d): Comunidade destinatária 14
3.1.5 BSP e): Atribuição da responsabilidade pela validação e pelo aumento da assinatura 14
3.2 BSP influenciados principalmente pelas disposições jurídicas/regulamentares associadas à aplicação/ao processo operacional em causa 16
3.2.1 BSP f): Forma jurídica das assinaturas 16
3.2.2 BSP g): Compromisso assumido pelo signatário 16
3.2.3 BSP h): Nível de garantia dos elementos temporais 16
3.2.4 BSP i): Formalidades da assinatura 17
3.2.5 BSP j): Conservação a longo prazo e resiliência à mudança 17
3.2.6 BSP k): Arquivo 17
3.3 BSP relativos sobretudo aos intervenientes envolvidos na criação/ampliação/validação das assinaturas 18
3.3.1 BSP l): Identidade (e funções/atributos) dos signatários 18
3.3.2 BSP m): Nível de garantia necessário para a autenticação do signatário 18
3.4 Outros BSP 18
3.4.1 BSP o): Outras informações a associar à assinatura ou ao selo 18
3.4.2 BSP p): Suites criptográficas 19

4 REQUISITOS/DECLARAÇÕES SOBRE OS MECANISMOS TÉCNICOS E A APLICAÇÃO DAS NORMAS 20

4.1 Regras relativas a marcas temporais de confiança 20
4.2 Regras relativas à validade a longo prazo 20
4.3 Diversos e questões jurídicas 20

5 APÊNDICE 21

1 Introdução

O presente documento estabelece a política de assinatura relativa à assinatura do Jornal Oficial (assinatura do JO) e ao selo do Jornal Oficial (selo do JO), utilizados para autenticar a versão eletrónica do Jornal Oficial da União Europeia (JO), em conformidade com o Regulamento (UE) n.º 216/2013 do Conselho relativo à publicação eletrónica do Jornal Oficial da União Europeia[1].

Uma política de assinatura é um conjunto de regras para criar, validar e ampliar uma ou mais assinaturas eletrónicas e/ou um ou mais selos eletrónicos inter-relacionados que define os requisitos técnicos e processuais para a sua criação, validação e gestão a longo prazo, a fim de satisfazer necessidades operacionais específicas e determinar quando são válidas. Uma política de assinatura serve igualmente para tornar todos os aspetos de uma dada sequência relativa à assinatura ou ao selo transparentes para todas as partes envolvidas, ou seja, signatários, destinatários e árbitros, de modo que as assinaturas eletrónicas e os selos eletrónicos que cumpram os requisitos dessa política possam gerar uma maior confiança na aplicabilidade e na aceitação das assinaturas e dos selos em causa.

Os conceitos específicos de uma política de assinatura são explicados em [ETSI 2015], que também define as orientações e a estrutura do presente documento. As palavras-chave «DEVE», «NÃO DEVE», «OBRIGATÓRIO», «DEVERÁ», «NÃO DEVERÁ», «DEVERIA», «NÃO DEVERIA», «RECOMENDADO», «PODE» e «FACULTATIVO» devem ser interpretadas tal como descritas em RFC 2911 [Bradner 1997].

O JO é publicado pelo Serviço das Publicações da União Europeia (OP) no sítio Web EUR-Lex (cf. 1.2.4) a fim de servir de única fonte autêntica do direito da UE. O JO é publicado de segunda a sexta-feira e, eventualmente, durante o fim de semana, em todas as línguas oficiais da União Europeia (UE). *Seguidamente, a sigla «JO» é utilizada para designar coletivamente este âmbito de aplicação específico.*

1.1 Apresentação geral

A política de assinatura do JO formaliza os elementos-chave da implementação da criação, validação e conservação a longo prazo da assinatura eletrónica e do selo eletrónico aplicada ao JO como forma de autenticação dos números do JO publicados pelo OP.

Consiste no seguinte:

- uma introdução que abrange o título/identificação da política, os dados sobre o emissor da política, a administração da política, as definições e as siglas, etc.;
- as declarações de práticas de aplicação da assinatura, que definem os requisitos políticos e jurídicos conexos, bem como as considerações de segurança aplicáveis;
- os parâmetros de delimitação das operações, que especificam as sequências envolvidas na geração de assinaturas eletrónicas e selos eletrónicos de autenticação dos números do JO publicados pelo OP;
- os requisitos e as declarações sobre os mecanismos técnicos e a aplicação das normas e os anexos.

[1] Ver JO L 69 de 13.3.2013, p. 1.

1.2 Âmbito operacional

1.2.1 Âmbito e limites da política de assinatura

A política de assinatura do JO abrange as assinaturas eletrónicas e os selos eletrónicos que são gerados para cada número do JO pelos signatários autorizados do JO em conformidade com o Regulamento do Conselho relativo à publicação eletrónica do Jornal Oficial da União Europeia após a validação de cada número a assinar.

1.2.2 Âmbito das aplicações

As assinaturas eletrónicas e os selos eletrónicos abrangidos pela política de assinatura do JO são apenas os que são descritos na secção 3.1.

1.2.3 Contexto transacional

Não aplicável.

1.3 Nome da política de assinatura, identificação e regras de conformidade

1.3.1 Nome da política

A política de assinatura do JO tem o seguinte título:

Política de assinatura do Jornal Oficial

1.3.2 Identificador da política

Dado que existe apenas um Jornal Oficial da União Europeia e a sua publicação é um processo bem conhecido da União Europeia, a política de assinatura do JO pode ser identificada de forma implícita por qualquer uma das partes. A secção 3.1.1.1 contém uma descrição das sequências operacionais gerais.

Para indicar a política de forma explícita, cada assinatura e selo do JO *PODE* incluir uma indicação explícita da política de assinatura tal como definido na secção 5.2.9 de [ETSI 2022-XAdES]. Se incluída, a indicação explícita da política de assinatura DEVE indicar o identificador do objeto 1.3.171.4.1.1.4 utilizando as regras de codificação especificadas na secção 5.2.9 de [ETSI 2022-XAdES] e em [Mealling 2010].

O código 1.3.171.4.1.1.4 é um identificador de objeto único à escala mundial e identifica univocamente a presente versão desta política. O prefixo 1.3.171.4 foi registado como OID de base para as *Políticas de assinatura e outros fins do Serviço das Publicações da UE* (cf. http://www.oid-info.com/get/1.3.171.4). O sufixo 1.1.4 identifica a presente versão da política de assinatura do JO, e o seu valor em notação ASN.1 com identificadores É {oj(1) signature-policy(1) version(4)}. Esta versão substitui a versão 1.1.3 da presente política.

1.3.3 Regras de conformidade da política

A presente política não pretende ser conforme a qualquer outra política.

1.3.4 Pontos de distribuição da política

O documento relativo à política de assinatura do JO está publicado no sítio Web EUR-Lex. É possível aceder-lhe a partir do sítio Web do Serviço das Publicações no endereço https://eur-lex.europa.eu/.

1.3.5 Período de validade da política

A atual versão política entra em vigor a partir de 1 de outubro de 2023.

1.3.6 Âmbito da política

A presente política aplica-se a todos os números do JO publicados e assinados de forma eletrónica a partir da data em que entrou em vigor o Regulamento do Conselho relativo à publicação eletrónica do Jornal Oficial da União Europeia. A presente política não é aplicável ao Suplemento do Jornal Oficial da União Europeia (série S, Jornal Oficial S ou JO S).

NOTA: Cada versão da presente política é válida dentro do prazo de validade definido em cada versão. O conjunto de todas as versões abrange todos os números do JO.

1.4 Administração dos documentos relativos à política de assinatura

O emissor da política de assinatura do JO é o Serviço das Publicações da União Europeia, que adotou e publicou o presente documento no sítio Web EUR-Lex.

A política de assinatura do JO tal como publicada POSSUI automaticamente valor jurídico e APLICA-SE à criação, à verificação e à gestão a longo prazo das assinaturas e dos selos do JO.

O emissor da política de assinatura do JO é responsável por:

- especificar e aprovar a política de assinatura do JO;
- definir o processo de revisão da política de assinatura do JO;
- definir os critérios e o processo de avaliação que assegurem que a política de assinatura do JO seja conforme com o Regulamento (UE) n.º 216/2013 do Conselho, de 7 de março de 2013, relativo à publicação eletrónica do Jornal Oficial da União Europeia e com o Regulamento (UE) 2018/2056 do Conselho, de 6 de dezembro de 2018, que altera o Regulamento (UE) n.º 216/2013 relativo à publicação eletrónica do Jornal Oficial da União Europeia;
- definir os critérios e o processo de avaliação que assegurem que as aplicações que declarem ser conformes à política de assinatura do JO cumpram efetivamente as regras vigentes dessa política;
- publicar a política de assinatura do JO e as respetivas versões alteradas no EUR-Lex.

1.4.1 Entidade responsável pela política

A política de assinatura do JO é gerida pelo Serviço das Publicações da União Europeia.

1.4.2 Pessoa de contacto

O emissor da atual política pode ser contactado utilizando as seguintes coordenadas:

Pessoa de contacto:	Chefe da Unidade «Jornal Oficial e Jurisprudência»
Endereço postal:	2, rue Mercier, L-2985 Luxemburgo
N.º de telefone:	+352 29291
Número de fax:	+352 292944620
Endereço eletrónico:	OP-JO-AUTHENTIQUE-HELPDESK@publications.europa.eu

1.4.3 Procedimentos de aprovação

A entidade responsável pela aprovação da política no Serviço das Publicações da União Europeia é o Diretor-Geral do Serviço das Publicações da União Europeia.

1.4.4 Versões da política

A versão inicial e as versões alteradas da política *PODEM* especificar uma data de efeito mínima. Quando uma versão da política é publicada, DEVE entrar em vigor impreterivelmente a partir das seguintes três datas:

1. A data de efeito mínima especificada pela versão da política, se existir;
2. O dia seguinte à data da primeira marca temporal da assinatura ou do selo do JO do número do JO em que a versão da política é publicada, de acordo com a hora local no Luxemburgo;
3. O dia seguinte à data de publicação da versão da política.

Qualquer versão alterada da política CADUCA automaticamente quando a versão alterada seguinte entra em vigor. Uma versão alterada da política DEVE, além disso, indicar a versão que substitui.

Estas regras são concebidas para garantir que a assinatura de uma determinada versão da política não está sujeita, direta ou indiretamente, à mesma versão da política, de forma a evitar um raciocínio circular. Além disso, é preferível manter, por qualquer meio, a versão obsoleta.

1.5 Definições e siglas

O Table 1 contém as definições e as siglas utilizadas no presente documento.

Sigla	**Definição (PT)**
CA	Certificate Authority (Autoridade de certificação)
DTBS	Data to Be Signed (Dados a assinar)
LTV	Long Term Validity (Validade a longo prazo)
OID	Object Identifier (Identificador de objeto)
JO	Jornal Oficial da União Europeia
PIN	Personal Identification Number (Número de identificação pessoal)
OP	Publications Office of the European Union (Serviço das Publicações da União Europeia)
QC	Qualified Certificate (Certificado qualificado)
QESig	Qualified Electronic Signature (Assinatura eletrónica qualificada)
QESeal	Qualified Electronic Seal (Selo eletrónico qualificado)
QSCD	Qualified Signature/Seal Creation Device (Dispositivo qualificado de criação de assinaturas/selos)
SAA	Signature Augmentation Application (Aplicação de ampliação da assinatura)
SCA	Signature Creation Application (Aplicação de criação da assinatura)
SSCD	Secure Signature Creation Device (Dispositivo seguro de criação da assinatura)
RWA	Signature Validation Application (Aplicação de validação da assinatura)
TSP	Trust Service Provider (Prestador de serviços de confiança)
QTSP	Qualified Trust Service Provider (Prestador qualificado de serviços de confiança)
WIPIWIS	What Is Presented Is What Is Signed (O que é apresentado é o que é assinado)

Quadro 1: Definições e siglas

2 Declarações de práticas da aplicação da assinatura

2.1 Requisitos políticos conexos

Os números do JO regem-se pelos artigos 1.º e 2.º do Regulamento do Conselho relativo à publicação eletrónica do Jornal Oficial da União Europeia, que estabelecem, nomeadamente, que a edição eletrónica do Jornal Oficial DEVE ostentar uma assinatura eletrónica qualificada, definida em conformidade com o Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, ou um selo eletrónico qualificado, definido nos termos do Regulamento (UE) n.º 910/2014.

A assinatura eletrónica e o selo eletrónico dos números do JO são abrangidos pela implementação de uma assinatura enquanto formalidade substancial, tal como referido no artigo III.2.1 das normas de execução da Comissão Europeia para a Decisão 2002/47/CE,CECA, Euratom relativa à gestão de documentos e para a Decisão 2004/563/CE, Euratom relativa aos documentos eletrónicos e digitalizados, de 30 de novembro de 2009[2], a qual prevê igualmente que as assinaturas eletrónicas aplicadas ao JO requerem uma assinatura eletrónica qualificada, tal como definida no [eIDAS].

Nos termos do artigo III.2.3 das normas de execução para a Decisão 2002/47/CE e para a Decisão 2004/563/CE[2], a responsabilidade pela verificação da entidade signatária recai sobre a SCA do JO quando confere a um funcionário do OP o poder de assinar eletronicamente os números do JO ou quando confere ao OP, enquanto pessoa coletiva, o poder de apor eletronicamente o selo nos números do JO.

Embora os números do JO em formato eletrónico não produzam efeitos jurídicos sem terem sido assinados ou selados, a política de assinatura do JO também estabelece que a SCA do JO DEVE garantir que apenas os signatários autorizados do JO possam rejeitar números do JO, a fim de evitar, de forma eficaz, ataques ao processo de publicação do JO.

Uma vez que os signatários autorizados do OJ agem em nome do OP, é da responsabilidade do Diretor-Geral do OP garantir (por delegação) a devida autorização do(s) respetivo(s) QC para a assinatura do OJ. Para este efeito, a autorização do(s) QC para a assinatura do OJ:

- *DEVE* ser corretamente configurada na gestão dos utilizadores da SCA do JO;
- *DEVE* ser limitada a certificados institucionais (profissionais) que garantam a pertença do agente ao OP[3];
- *DEVE* ser tornada transparente mediante a publicação dos QC autorizados no sítio Web EUR-Lex, em conformidade com o artigo 2.º do Regulamento do Conselho relativo à publicação eletrónica do Jornal Oficial da União Europeia.

2.2 Requisitos jurídicos conexos

A implementação de assinaturas eletrónicas e selos eletrónicos abrangidos pela política de assinatura do JO É regida pelas seguintes disposições legais:

- Regulamento (UE) n.º 216/2013 do Conselho, de 7 de março de 2013, relativo à publicação eletrónica do Jornal Oficial da União Europeia;

[2] Ver SEC(2009) 1643.

[3] Os certificados institucionais garantem a pertença do agente a uma organização específica. A segurança é aumentada porque o QTSP emissor estabelece a prova de habilitação do respetivo proprietário do certificado.

- Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE[4];
- 2009/767/CE: Decisão da Comissão, de 16 de outubro de 2009, que determina medidas destinadas a facilitar a utilização de procedimentos informatizados através de «balcões únicos», nos termos da Diretiva 2006/123/CE do Parlamento Europeu e do Conselho relativa aos serviços no mercado interno[5];
- Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)[6];
- Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas)[7];
- Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor[8];
- 2010/425/UE: Decisão da Comissão, de 28 de julho de 2010, que altera a Decisão 2009/767/CE no que respeita à elaboração, manutenção e publicação das listas aprovadas de prestadores de serviços de certificação controlados/acreditados pelos Estados-Membros[9];
- 2009/496/CE, EURATOM: Decisão do Parlamento Europeu, do Conselho, da Comissão, do Tribunal de Justiça, do Tribunal de Contas, do Comité Económico e Social Europeu e do Comité das Regiões, de 26 de junho de 2009, relativa à organização e ao funcionamento do Serviço das Publicações da União Europeia[10];
- 2011/130/UE: Decisão da Comissão, de 25 de fevereiro de 2011, que estabelece requisitos mínimos para o processamento transfronteiras de documentos assinados eletronicamente pelas autoridades competentes nos termos da Diretiva 2006/123/CE do Parlamento Europeu e do Conselho relativa aos serviços no mercado interno [3.]

2.3 Considerações de segurança técnica

As ferramentas criptográficas elegíveis para implementação das assinaturas e dos selos do JO DEVEM cumprir os requisitos de assinaturas eletrónicas qualificadas previstos no [eIDAS], em [ETSI 2016], e as práticas pertinentes mais avançadas.

4 Ver JO L 257 de 28.8.2014, p. 73.

5 Ver JO L 274 de 20.10.2009, p. 36.

6 Ver JO L 119 de 4.5.2016, p. 1.

7 Ver JO L 201 de 31.7.2002, p. 37.

8 Ver JO L 337 de 18.12.2009, p. 11.

9 Ver JO L 199 de 31.7.2010, p. 30.

10 Ver JO L 168 de 30.6.2009, p. 41.

2.4 Declarações jurídicas

As assinaturas eletrónicas e os selos eletrónicos apostos nos números do JO são gerados em nome do OP com base no Regulamento do Conselho relativo à publicação eletrónica do Jornal Oficial da União Europeia.

3 Parâmetros de delimitação das operações (*Business scoping parameters* [BSP])

3.1 BSP relacionados principalmente com a aplicação/o processo operacional em causa

3.1.1 BSP a): Sequência (sequenciação e calendário) das assinaturas

3.1.1.1 Descrição da sequência operacional geral

O OP publica o JO de segunda a sexta-feira e, eventualmente, durante o fim de semana. Esta publicação do JO pode ser um número convencional do JO ou um número dedicado a um só ato (JO-Ato). Um número do JO representa uma publicação multilingue de um ou mais documentos. Cada versão linguística de um número consiste no texto completo de cada documento num único ficheiro. Um número de um JO-Ato corresponde a uma publicação multilingue de um único documento que é publicado de modo autónomo. Cada versão linguística de um número do JO-Ato consiste no texto completo de cada documento num único ficheiro.

Os diferentes números do JO e do JO-Ato são classificados de acordo com a série a que pertencem, sendo a categoria uma parte identificadora do JO. Existem duas séries que são relevantes para o âmbito de aplicação atual, a saber L (Legislação) e C (Comunicações e Informações). Uma série pode facultativamente ter subséries e sistemas de classificação (cf. http://publications.europa.eu/code/pt/pt-10000.htm para uma explicação mais aprofundada sobre o âmbito de aplicação, a estrutura dos documentos e informação geral complementar).

Para além das séries L e C do JO, existem igualmente edições especiais publicadas na língua de um país aderente/novo Estado-Membro que contêm direito derivado da UE. Estas edições especiais também fazem parte do âmbito de aplicação.

Quando um número do JO ou do JO-Ato está completo (ou seja, quando estão disponíveis todas as versões linguísticas do número do JO ou do JO-Ato em formato PDF/A) e pronto para publicação, a sequência operacional prosseguirá com um processo de aposição de selo eletrónico (cf. secção 3.1.1.2) ou um processo de assinatura eletrónica (cf. secção 3.1.1.3). Em caso de aposição de selo eletrónico, um selo eletrónico qualificado é gerado automaticamente mediante um certificado qualificado de aposição de selos emitido para o OP enquanto entidade da Comissão Europeia. Em caso de assinatura eletrónica, uma assinatura eletrónica qualificada é gerada por uma pessoa autorizada que utiliza um certificado de assinatura eletrónica qualificada.

A aposição de selo eletrónico é a sequência predefinida selecionada pela SCA, ou seja, os números do JO ou do JO-Ato que estão completos passarão pelo processo automatizado de aposição de selo eletrónico, a menos que o processo de aposição de selo eletrónico não esteja disponível. Neste último caso, será utilizado o processo de assinatura.

Uma vez que é utilizada uma assinatura separada ou um selo separado XAdES com um manifesto (cf. [Bartel 2008], [ETSI 2022-XAdES] e a Decisão 2011/130/UE da Comissão, de 25 de fevereiro de 2011, que estabelece requisitos mínimos para o processamento transfronteiras de documentos assinados eletronicamente pelas autoridades competentes nos termos da Diretiva 2006/123/CE do Parlamento Europeu e do Conselho relativa aos serviços no mercado interno[11]) para assinar cada um dos números, ao verificar uma assinatura ou um selo do JO ou do JO-Ato é igualmente necessário efetuar uma validação do manifesto para além

[11] JO L 53 de 26.2.2011, p. 66.

do núcleo da assinatura XML (cf. [Bartel 2008]) durante a validação [ETSI 2022-XAdES], para efeitos de verificação de uma assinatura ou um selo do JO ou do JO-Ato.

As subsecções seguintes descrevem as sequências de aposição de selo eletrónico e assinatura de alto nível tal como implementadas na SCA, na SAA e na SVA do JO (cf. [ETSI 2016]).

3.1.1.2 Criação do selo do JO e do JO-Ato

1. É detetado um número completo do JO ou do JO-Ato para aposição do selo.
2. A SCA procede a controlos preliminares de verificação dos ficheiros fornecidos:
    a. verifica se existem incoerências de tamanho entre as versões linguísticas do número do JO/JO-Ato e se estas se encontram dentro dos limites de tamanho configuráveis;
    b. verifica se estava prevista a publicação de todas as versões linguísticas apresentadas.
3. Se a verificação fracassar, o processo de aposição do selo é interrompido. É necessária a intervenção manual do pessoal autorizado do OP para retomar o processo de aposição do selo.
4. Após uma validação bem-sucedida pela SCA, é gerado um manifesto que referencia cada versão linguística do número completo. Além disso, cada versão linguística corresponde a uma única língua da UE e é apresentada como um documento PDF/A que é tratado como um fluxo binário de octetos durante o cálculo do resumo da mensagem.
5. A SCA efetua a autenticação mediante confronto com o portal central de assinatura eletrónica da Comissão Europeia e transmite o manifesto gerado para aposição automatizada do selo.
6. O portal de assinatura eletrónica apõe o selo ao manifesto facultado através de um certificado qualificado de aposição de selos, emitido por um QTSP europeu acreditado (cf. [eIDAS]). A chave privada relativa a este certificado de aposição de selos é armazenada num QSCD com interface com o portal de assinatura eletrónica.
7. O selo XAdES (cf. [ETSI 2022-XAdES]) assim criado é então reenviado à SCA, que comprova, entre outras coisas, a validade dos algoritmos utilizados e verifica se o certificado de aposição de selos do respetivo selo está autorizado e é propriedade da mesma pessoa coletiva que foi autenticada como signatária autorizada.
8. Após uma verificação bem-sucedida, o selo eletrónico é ampliado com uma marca temporal de assinatura facultada por um QTSP acreditado (cf. [eIDAS]).
9. O selo eletrónico ampliado na fase de processamento anterior é transferido para publicação no sítio Web EUR-Lex. Ao mesmo tempo, a SCA conserva uma cópia idêntica do selo.
10. Uma vez cumprido o período de carência de 24 horas exigido para um selo resultante da etapa anterior do processo, volta a ser ampliado para uma forma autossustentável, a fim de prorrogar a validade da assinatura por um longo período de tempo recorrendo ao serviço de confiança de marcas temporais prestado por um QTSP europeu acreditado (cf. [eIDAS]).
11. O selo ampliado na etapa anterior do processo é transferido para publicação no sítio Web EUR-Lex, substituindo o selo da etapa 9 que ainda não tinha sido ampliado para uma forma autossustentável.

12. Para além da publicação no sítio Web EUR-Lex, são transferidas cópias idênticas dos documentos que constituem cada número do JO ou do JO-Ato, juntamente com o selo correspondente numa forma autossustentável, para o sistema de conservação digital a longo prazo, que é gerido pelo OP e conserva a longo prazo os documentos oficiais das instituições da UE. Os aspetos concretos da conservação a longo prazo NÃO são tratados na presente política de assinatura.

3.1.1.3 Criação da assinatura do JO ou do JO-Ato

1. É detetado um número completo do JO ou do JO-Ato para assinatura.
2. É gerado um manifesto que referencia cada versão linguística do número completo. Além disso, cada versão linguística corresponde a uma única língua da UE e é apresentada como um documento PDF/A que é tratado como um fluxo binário de octetos durante o cálculo do resumo da mensagem.

   Note-se que os números completos são geridos e bloqueados exclusivamente pela SCA durante a geração do manifesto, a fim de garantir a coerência do cálculo do resumo, o que é essencial para o processo.
3. Uma vez efetuada a autenticação pela SCA, um signatário autorizado pode selecionar um número completo para assinatura desde que o manifesto correspondente tenha sido gerado durante a fase anterior.
4. Uma vez efetuada a seleção de um número para assinar, o signatário autorizado inicia o processo de assinatura desse número específico:
   a. Com vista a respeitar devidamente o princípio WIPIWIS, o signatário autorizado é obrigado a examinar pelo menos três versões linguísticas diferentes com recurso a um visualizador PDF/A conforme antes de poder assinar o número. Se o número do JO ou do JO-Ato tiver menos de três versões linguísticas, o signatário autorizado é obrigado a examinar todas as versões linguísticas disponíveis.

      Note-se que a SCA permite ao signatário examinar qualquer versão linguística do número a assinar. O signatário PODE, por conseguinte, examinar todo o conteúdo a assinar se assim o entender.
   b. O signatário autorizado pode deliberadamente escolher entre rejeitar o número, interrompendo o processo de assinatura, e prosseguir com a assinatura premindo o botão «Assinar».
   c. Após ter sido premido o botão «Assinar»:
      i. a SCA gera um pedido de assinatura dirigido ao portal central de assinatura eletrónica da Comissão Europeia, transmitindo o manifesto para assinatura e redirecionando o signatário autorizado para o portal;
      ii. o signatário autorizado autentica-se no portal de assinatura eletrónica e recebe o manifesto para assinar, em conformidade com os princípios WPIWIS;
      iii. o portal de assinatura eletrónica estabelece a ligação com o software intermédio instalado no posto de trabalho do signatário autorizado e extrai o certificado de assinatura qualificado do signatário, emitido por um QTSP europeu acreditado (cf. [eIDAS]). O certificado é apresentado ao signatário autorizado que, por sua vez, é instado a inserir o PIN correspondente que protege o QSCD a fim de autorizar o QSCD a criar

a assinatura utilizando a chave privada correspondente ao certificado de assinatura selecionado, completando, assim, o processo de assinatura.

d. O software intermédio envia o valor da assinatura gerada ao portal de assinatura eletrónica, que, por sua vez, gera uma assinatura XAdES correspondente (cf. [ETSI 2022-XAdES]).

5. Esta assinatura XAdES é então reenviada à SCA, que comprova, entre outras coisas, — através do portal de assinatura eletrónica — a validade dos algoritmos utilizados e verifica se o certificado da respetiva assinatura está autorizado e é propriedade da mesma pessoa que foi autenticada como signatária autorizada.

6. Após uma verificação bem-sucedida, a assinatura é ampliada — através do portal de assinatura eletrónica — com uma marca temporal de assinatura facultada por um QTSP acreditado (cf. [eIDAS]).

7. A assinatura ampliada na fase de processamento anterior é transferida para publicação no sítio Web EUR-Lex. Ao mesmo tempo, a SCA conserva uma cópia idêntica da assinatura.

8. Uma vez cumprido o período de carência de 24 horas exigido para uma assinatura resultante da etapa anterior do processo, volta a ser ampliada para uma forma autossustentável, a fim de prorrogar a validade da assinatura por um longo período de tempo recorrendo ao serviço de confiança de marcas temporais prestado por um QTSP europeu acreditado (cf. [eIDAS]).

9. A assinatura ampliada na etapa anterior do processo é transferida para publicação no sítio Web EUR-Lex, substituindo a assinatura da etapa 7 que ainda não tinha sido ampliada para uma forma autossustentável.

10. Para além da publicação no sítio Web EUR-Lex, são transferidas cópias idênticas dos documentos que constituem cada número do JO ou do Ato do JO, juntamente com a assinatura correspondente numa forma autossustentável, para o sistema de conservação digital a longo prazo, que é gerido pelo OP e conserva a longo prazo os documentos oficiais das instituições da UE. Os aspetos concretos da conservação a longo prazo NÃO são tratados na presente política de assinatura.

3.1.1.4 Situação de emergência

Se não for possível criar o selo ou a assinatura do JO ou do JO-Ato, tal como descrito na secção 3.1.1.2 ou 3.1.1.3, devido a uma indisponibilidade imprevista e excecional da SCA do JO, o Serviço das Publicações aplicará um QESeal ou uma QESig em cada documento PDF/A correspondente a cada versão linguística do JO ou do JO-Ato. Todos os documentos PDF/A selados/assinados serão transferidos para publicação no sítio Web EUR-Lex.

3.1.2 BSP b): Dados a assinar

- as assinaturas e os selos do JO ou do JO-Ato têm por base um manifesto XML (cf. [Bartel 2008] e [ETSI 2022-XAdES]), que combina todas as versões linguísticas disponíveis no formato PDF/A pertencentes a um número do JO ou do JO-Ato numa assinatura única, que deve cumprir os requisitos seguintes: cada versão linguística associada logicamente a um número do JO ou do JO-Ato *DEVE* ter o seu próprio valor de resumo;

- todas as versões linguísticas associadas logicamente a um número do JO ou do JO-Ato *DEVEM* ser apresentadas ao signatário durante a criação da assinatura para que este as examine e possa verificar livremente o conteúdo da assinatura, tal como descrito na secção 3.1.1.3, a fim de observar o princípio WIPIWIS;

- DEVE ser garantida uma visualização adequada através de um leitor de PDF/A conforme;
- durante o processo de assinatura de um número, DEVEM ser apresentadas ao signatário unicamente as versões linguísticas pertencentes a esse número;
- as características técnicas de todas as versões linguísticas associadas logicamente a um número do JO ou do JO-Ato *DEVEM* ser verificadas durante a criação do selo e da assinatura, a fim de assegurar a coerência.

Em caso de situação de emergência descrita na secção 3.1.1.4 *supra*, são aplicáveis os seguintes requisitos:

- cada versão linguística de um número do JO ou do JO-Ato *DEVE* ter o seu próprio QESig ou QESeal;
- todas as versões linguísticas associadas logicamente a um número do JO ou do JO-Ato *DEVEM* ser examinadas pelo signatário durante a criação da assinatura para que este possa verificar livremente o conteúdo da assinatura, a fim de observar o princípio WIPIWIS;
- *DEVE* ser garantida uma visualização adequada através de um leitor de PDF/A conforme.

3.1.3 BSP c): Relação entre os dados assinados e a(s) assinatura(s) e o(s) selo(s)

Uma assinatura ou um selo do JO ou do JO-Ato aplica-se a todas as versões linguísticas de um número do JO ou do JO-Ato, cada uma formatada como documento PDF/A.

Durante a criação de uma assinatura ou de um selo do JO ou do JO-Ato, o conteúdo digital do documento a assinar/selar é resumido sob a forma de uma sequência binária de octetos, utilizando o algoritmo de resumo mais robusto suportado em conformidade com a secção 7.3 de [ETSI 2022-Crypto].

Os valores de síntese de cada documento são combinados com os URI dos nomes de ficheiros originais num manifesto XML sem que sejam aplicadas transformações adicionais (cf. [Bartel 2008]).

O manifesto, incluindo os atributos assinados, é assinado ou selado com recurso a XAdES (cf. [ETSI 2022-XAdES]) no que respeita ao perfil indicado na Decisão 2011/130/UE da Comissão, de 25 de fevereiro de 2013.

Em caso de situação de emergência descrita na secção 3.1.1.4 *supra*, cada documento PDF/A que representa cada versão linguística do JO ou do JO-Ato será assinado ou selado utilizando PAdES (cf. [ETSI 2016-PAdES] [eIDAS]).

3.1.4 BSP d): Comunidade destinatária

A comunidade destinatária é constituída por qualquer parte que se baseie na autenticidade do JO e necessite da sua verificação, bem como por todas as partes responsáveis pela implementação da SCA e da SAA utilizadas para criar e ampliar assinaturas eletrónicas ou selos eletrónicos para os números do JO ou do JO-Ato.

3.1.5 BSP e): Atribuição da responsabilidade pela validação e pelo aumento da assinatura

3.1.5.1 Verificação da assinatura e do selo do JO ou do JO-Ato

Qualquer parte utilizadora, em especial qualquer cidadão europeu, pode descarregar um número do JO ou do JO-Ato publicado no sítio Web EUR-Lex e a assinatura ou selo XAdES separada/o correspondente (cf. [ETSI 2022-XAdES]) para verificação.

Uma vez que na criação da assinatura e do selo se recorre a uma norma europeia interoperável e aos serviços de um QTSP europeu acreditado (cf. [eIDAS]), a verificação pode ser efetuada recorrendo a uma aplicação de verificação de terceiros que seja conforme às normas utilizadas, desde que se possa efetuar a validação do manifesto com base na política de assinatura do JO.

Em caso de situação de emergência descrita na secção 3.1.1.4 *supra*, cada documento PDF/A que representa cada versão linguística do JO ou do JO-Ato será assinado ou selado utilizando PAdES (cf. [ETSI 2016-PAdES]). A respetiva verificação pode ser efetuada recorrendo a uma aplicação de verificação de terceiros que seja conforme à norma utilizada.

3.1.5.1.1 Verificação no servidor

A fim de facilitar a verificação da assinatura e do selo, o OP PODE oferecer uma SVA do JO gratuita no servidor funcionando de acordo com a sequência de verificação indicada a seguir:

1. O verificador carrega o ficheiro PDF/A a verificar juntamente com o ficheiro da assinatura ou do selo associado através da função de carregamento oferecida pela SVA.
2. A SVA calcula o resumo do ficheiro PDF/A carregado e verifica se o resumo calculado está contido na parte do manifesto da assinatura carregada.
3. Se a verificação do resumo é positiva, a norma de verificação XAdES da assinatura ou do selo candidato carregado é executada, desde que o certificado da assinatura ou do selo identifique um signatário autorizado do JO para o período determinado pela marca temporal da assinatura. A SVA também verifica se o signatário estava autorizado a assinar quando, de acordo com a marca temporal da assinatura, a assinatura foi criada.
4. O processo de verificação considera-se realizado quando todas as etapas anteriores são bem-sucedidas. Caso contrário, a verificação fracassa. Em qualquer caso, o verificador recebe um relatório compreensível do processo de verificação.

3.1.5.1.2 Verificação no cliente

A fim de facilitar a verificação da assinatura e do selo, o OP PODE oferecer uma SVA do JO gratuita para o cliente funcionando de acordo com a sequência de verificação indicada a seguir:

1. O verificador lança a SVA descarregada, a assinatura do código é automaticamente verificada pelo ambiente de execução e a execução é autorizada pelo verificador após a verificação bem-sucedida da assinatura do código;
2. O verificador seleciona um ficheiro PDF/A numa dada versão linguística a verificar juntamente com o ficheiro da assinatura ou do selo candidato associado no sistema de ficheiros do PC local, utilizando o sistema de diálogo de seleção de ficheiros oferecido pela SVA;
3. A SVA calcula o resumo do documento selecionado e verifica se o resumo calculado está contido no manifesto da assinatura ou do selo candidata/o selecionada/o;
4. Se a verificação do resumo for positiva, é efetuada a verificação XAdES normal da assinatura ou do selo candidata/o selecionada/o.
5. O processo de verificação considera-se realizado quando todas as etapas anteriores são bem-sucedidas e o certificado da assinatura ou do selo identifica um signatário autorizado do JO para o período determinado pela marca temporal da assinatura.

   Note-se que a informação sobre o signatário autorizado PODE ser conhecida da SVA com base numa configuração (por omissão). No entanto, o resumo do certificado da assinatura ou do selo é, além disso, indicado no resultado da SVA, a fim de que o verificador o possa comparar manualmente com a informação jurídica do signatário

publicada respeitante ao período de criação da assinatura ou do selo, a qual é igualmente indicada no resultado da SVA.

3.2 BSP influenciados principalmente pelas disposições jurídicas/regulamentares associadas à aplicação/ao processo operacional em causa

3.2.1 BSP f): Forma jurídica das assinaturas

As assinaturas eletrónicas e os selos eletrónicos apostos no JO ou no JO-Ato DEVEM ser respetivamente em forma QESig e QESeal, nos termos do [eIDAS].

O requisito acima referido é imposto, especificamente, pelo Regulamento do Conselho relativo à publicação eletrónica do Jornal Oficial da União Europeia (cf. secção 2.2).

Cada signatário deve obter um QC como pré-requisito para a utilização do sistema de assinatura.

A qualidade dos elementos específicos da QESig e do QESeal exigidos DEVE satisfazer os seguintes requisitos de qualidade:

- dispositivo de assinatura e de aposição de selo: QSCD que cumpram o disposto no anexo II do [eIDAS];
- fornecimento de certificados: QC que cumpra o disposto no anexo I do [eIDAS];
- garantia independente de fornecimento de certificados: QC emitido por um serviço de certificação QTSP controlado ou acreditado em qualquer país em que se aplique o [eIDAS];
- suite criptográfica da assinatura: apenas devem ser utilizadas as suites de assinatura enumeradas na secção 7.3 de [ETSI 2022-Crypto];
- soluções LTV: os formatos da assinatura e do selo XAdES do JO ou do JO-Ato (cf. [ETSI 2022-XAdES]) DEVEM ser ampliados para o formato da assinatura LTA, incluindo a renovação das marcas temporais de arquivo ou outras (PODEM-SE considerar mecanismos externos de arquivo seguro como alternativa à renovação das marcas temporais de arquivo sempre que tenham uma qualidade equivalente ou superior);
- aplicação de criação da assinatura: a qualidade da SCA do JO DEVE satisfazer as exigências de qualidade impostas pelas políticas da CE e cumprir os requisitos do Regulamento do Conselho relativo à publicação eletrónica do Jornal Oficial da União Europeia.

3.2.2 BSP g): Compromisso assumido pelo signatário

As assinaturas eletrónicas e os selos eletrónicos apostos nos números do JO ou do Ato do JO SÃO gerados em nome do OP em conformidade com o Regulamento do Conselho relativo à publicação eletrónica do Jornal Oficial da União Europeia.

O compromisso assumido por um signatário autorizado do JO expressa que os dados assinados representam um número autêntico do JO ou do Ato do JO devidamente validado com respeito às regras do âmbito de aplicação operacional (cf. secção 3.1.1) e publicado pelo OP em conformidade com o Regulamento do Conselho relativo à publicação eletrónica do Jornal Oficial da União Europeia com vista a servir de fonte autêntica de direito da UE.

Não DEVE figurar qualquer indicação explícita do tipo de compromisso numa assinatura do JO (cf. secção 5.2.3 de [ETSI 2022-XAdES]).

3.2.3 BSP h): Nível de garantia dos elementos temporais

DEVE ser adicionada uma marca temporal às assinaturas ou aos selos do JO ou do JO-Ato que são criados conforme a descrição na secção 3.1.1.2 ou 3.1.1.3 no mesmo dia (hora local do Luxemburgo) da data da assinatura ou do selo do número do JO ou do JO-Ato, a fim de certificar que a assinatura ou o selo não foram criados após a data de publicação. Isto garante que o

conjunto de signatários autorizados aplicável na data de publicação é aplicável à assinatura ou ao selo.

A SCA do JO DEVE garantir que todas as assinaturas XAdES-B-T geradas cumprem este requisito.

As marcas temporais utilizadas para criar marcas temporais em assinaturas XAdES-B-T DEVEM ser marcas temporais qualificadas.

As assinaturas PAdES criadas em caso de situação de emergência, tal como descrito na secção 3.1.1.4, PODEM ser criadas sem uma marca temporal da assinatura.

Se as assinaturas PAdES criadas em caso de situação de emergência, tal como descrito na secção 3.1.1.4, tiverem sido criadas com uma marca temporal da assinatura, essa marca temporal DEVE ser uma marca temporal qualificada, aplicada no mesmo dia (hora local no Luxemburgo) da data da assinatura ou do selo do número do JO ou do JO-Ato, a fim de certificar que a assinatura ou o selo não foram criados após a data de publicação.

NOTA: Isto significa que, em caso de situação de emergência, se a assinatura incluir uma marca temporal da assinatura, esta pode ser uma marca temporal não qualificada.

Todos as outras marcas temporais, incluindo as marcas temporais de arquivo e, caso se aplique, as de conteúdo, DEVEM ser marcas temporais qualificadas.

3.2.4 BSP i): Formalidades da assinatura

Cabe à SCA do JO proporcionar uma interface ao signatário que garanta, na medida do possível, um ambiente de assinatura ou selo juridicamente válido. A interface deve:

- incluir a prestação de assessoria e de informações adequadas sobre o processo de assinatura e aposição do selo da aplicação;
- assegurar a coerência entre a utilização dos dados adequados de criação e verificação da assinatura e do selo, os dispositivos de criação da assinatura e do selo, os dados a assinar e o âmbito e a finalidade previstos da assinatura e do selo (ou do ato de assinatura ou de aposição do selo);
- permitir e mostrar uma manifestação clara da vontade de assinar e a intenção do utilizador de ficar vinculado pela assinatura ou pelo selo;
- permitir e manifestar um consentimento informado.

A SVA do JO DEVE oferecer às partes utilizadoras (incluindo o signatário) procedimentos corretos para verificar e arquivar a assinatura eletrónica ou o selo eletrónico e os dados de verificação.

3.2.5 BSP j): Conservação a longo prazo e resiliência à mudança

Os números do JO ou do JO-Ato assinados e as respetivas assinaturas DEVEM ser conservados por um período de tempo indefinido. A conservação da validade das assinaturas do JO ou do Ato do JO DEVE ser garantida pelo mesmo período de tempo (cf. artigo 2.º do Regulamento do Conselho relativo à publicação eletrónica do Jornal Oficial da União Europeia).

3.2.6 BSP k): Arquivo

Não aplicável.

3.3 BSP relativos sobretudo aos intervenientes envolvidos na criação/ampliação/validação das assinaturas

3.3.1 BSP l): Identidade (e funções/atributos) dos signatários

3.3.1.1 Signatário proposto e regras de identificação

As assinaturas do JO ou do JO-Ato DEVEM ser aplicadas por signatários autorizados, que DEVEM ser obrigatoriamente funcionários do OP com a experiência necessária para validar números do JO ou do JO-Ato em conformidade com as regras relativas ao âmbito de aplicação operacional (cf. secção 3.1.1.3). No caso dos selos do JO ou do JO-Ato, o signatário autorizado DEVE ser o próprio OP enquanto entidade da Comissão Europeia.

Os signatários autorizados DEVEM também estar cientes da sua responsabilidade e DEVEM agir de boa-fé ao autenticar os textos jurídicos do direito da UE.

O vínculo entre estas pessoas singulares signatárias e os dados de verificação das suas assinaturas DEVE ser atestado por um QC nos termos do [eIDAS] que confirme a sua identidade e pertença ao OP.

A autorização de um signatário do JO DEVE ser concedida pelo Diretor-Geral do OP (com possibilidade de delegação):

3.3.1.2 Funções e atributos do signatário

Para além da pertença ao OP, NÃO DEVE exigir-se no QC do signatário certificação de quaisquer outras funções ou qualificações.

COMPETE à SCA do JO assegurar um controlo do acesso e uma autorização do signatário adequados antes de conceder aos signatários acesso aos mecanismos de assinatura do JOA.

O controlo do acesso e a autorização dos signatários DEVEM ser realizados com base num mecanismo de autenticação robusto implementado na SCA e nas permissões registadas nos certificados de chave pública correspondentes aos signatários autorizados na base de dados da SCA.

As partes utilizadoras *PODEM* utilizar os certificados publicados dos signatários do JO para verificar a sua habilitação legal.

3.3.1.3 Provas de habilitação conexas

Nada para além do disposto na secção 3.3.1.2.

3.3.2 BSP m): Nível de garantia necessário para a autenticação do signatário

O nível de garantia exigido para a autenticação do signatário é assegurado pelo seu certificado qualificado e pelos seus meios de criação da assinatura que DEVEM ser um dispositivo qualificado de criação de assinaturas/selos, tal como definido no [eIDAS].

3.4 Outros BSP

3.4.1 BSP o): Outras informações a associar à assinatura ou ao selo

3.4.1.1 Signatários autorizados do JO e entidades responsáveis pela marca temporal

A verificação da autorização dos signatários é um elemento essencial da confiança no JO.

A autorização DEVE ser explicitada através da publicação dos certificados eletrónicos de todos os signatários autorizados num suporte externo da confiança da SCA/SVA.

Na publicação dos signatários autorizados do JO DEVE indicar-se que o estado de supervisão dos certificados do signatário está garantido para o período de assinatura do JO ou JO-Ato em curso.

NÃO DEVEM ser publicados no JO os signatários autorizados do JO nem as autoridades responsáveis pela marca temporal, dado que esta forma de proceder iria criar problemas de raciocínio circular, especialmente no que respeita à validação a longo prazo.

Se os signatários autorizados do JO mudarem ao longo do tempo, o conjunto dos anteriores signatários DEVE ser publicado como informação histórica sobre a confiança. Isto é necessário para verificar os números do JO ou do JO-Ato assinados por esses signatários.

Na publicação dos signatários autorizados DEVE ser especificado o período em que os signatários constantes da lista estavam ou estão autorizados, devendo essa especificação estar em consonância com as limitações temporais da versão atual da política.

3.4.1.2 Regras para os atributos, o âmbito de aplicação e a finalidade das assinaturas eletrónicas e dos selos eletrónicos

Os processos de criação da assinatura e do selo DEVEM fazer um uso adequado dos atributos da assinatura, em especial dos atributos assinados, que são os elementos de informação que suportam a assinatura eletrónica/o selo eletrónico e estão abrangidos pela assinatura/pelo selo em conjunto com os DTBS de acordo com o seguinte:

- DEVE usar-se o identificador do certificado de assinatura. Trata-se do identificador do certificado — ou de uma referência a esse identificador — que contém os dados de verificação da assinatura correspondentes aos dados de criação da assinatura ou do selo usados pelo signatário para criar a assinatura ou o selo eletrónico;
- PODE ser usada uma indicação da política de assinatura (cf. secção 1.2.2);
- DEVE usar-se a data e hora de assinatura alegadas. Esta informação indica a data e hora em que o signatário alega ter criado a assinatura ou o selo.

  Note-se que esta informação reflete a data e hora do sistema do posto de trabalho do signatário. NÃO é uma data e hora de confiança.

  O proprietário da SCA do JO (por delegação do Diretor-Geral do OP) DEVE tomar as medidas necessárias para que a data e hora do sistema dos postos de trabalho dos signatários sejam exatas.

Para o efeito, pode usar-se o protocolo NTP com uma fonte de informação temporal adequada (cf. [Mills 2010]).

- NÃO DEVE usar-se qualquer indicação do tipo de compromisso;
- PODEM ser utilizados outros atributos assinados.

A utilização de atributos de assinatura DEVE estar em conformidade com [ETSI 2010] e a Decisão 2011/130/UE da Comissão, de 25 de fevereiro de 2013.

3.4.2 BSP p): Suites criptográficas

Ver secção 3.2.1.

4 Requisitos/declarações sobre os mecanismos técnicos e a aplicação das normas

4.1 Regras relativas a marcas temporais de confiança

O formato de assinatura XAdES-LTA (cf. [ETSI 2022-XAdES]) requer várias marcas temporais que DEVEM ser obtidas de um serviço qualificado de marcas temporais acreditado num Estado-Membro ou num país do EEE.

O proprietário da SCA do JO DEVE (por delegação do Diretor-Geral do OP) tomar as medidas necessárias a fim de que a SCA seja configurada para utilizar algoritmos criptográficos adequados.

4.2 Regras relativas à validade a longo prazo

A conservação da validade das assinaturas do JO ou do JO-Ato durante o período de conservação previsto é garantida graças à implementação do formato XAdES-B-LTA (cf. [ETSI 2022-XAdES]) e, posteriormente, ampliando a assinatura com uma marca temporal qualificada adicional de arquivo para prorrogar a sua validade quando necessário, ou a uma solução de arquivo adequada que ofereça garantias de conservação da validade da assinatura.

4.3 Diversos e questões jurídicas

Uma vez que o JO é publicado de segunda a sexta-feira e, eventualmente, durante o fim de semana, o proprietário da SCA do JO DEVE (por delegação do Diretor-Geral do OP) tomar as medidas necessárias para que a SCA esteja sempre operacional.

Para este efeito, DEVEM ser estabelecidos acordos de nível de serviço adequados.

Embora as assinaturas e os selos do JO ou do JO-Ato possam ser verificados por qualquer SVA conforme às normas e regras definidas na política de assinatura do JO, as quais incluem obrigatoriamente a validação do manifesto, o OP PODE oferecer uma SVA de acesso público no sítio Web EUR-Lex para permitir às partes utilizadoras, em especial aos cidadãos europeus, verificar as assinaturas do JO ou do JO-Ato sem terem de recorrer a um utilitário de terceiros.

Alternativamente, o OP PODE oferecer uma SVA que consista num utilitário disponível publicamente para descarga que funcione de forma independente no computador do utilizador e que requeira unicamente que o verificador confie no software quando use os resultados por ele produzidos.

5 Apêndice

[Bartel 2008]	Bartel M., Boyer J., Fox B., LaMacchia B., Simon E. *XML Signature Syntax and Processing (Second Edition)* W3C Recommendation, 2008
[Bradner 1997]	Bradner S. *Key words for use in RFCs to indicate requirement levels* RFC 2119, Network Working Group, 1997
[Mealling 2010]	Mealling M. *A URN Namespace of Object Identifiers* RFC 3061, Network Working Group, 2001
[Mills 2010]	Mills D., Delaware U., Martin J., ISC Ed., Burbank J., Kasch W. *Network Time Protocol Version 4: Protocol and Algorithms Specification* RFC 5905, IETF, 2010
[eIDAS]	*Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE* Jornal Oficial L 257
[ETSI 2015]	ETSI-ESI *Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents* TS 119 172-1, v1.1.1, ETSI, 2015
[ETSI 2016]	ETSI-ESI *Electronic Signatures and Infrastructures (ESI);* *Policy and security requirements for applications for signature creation and signature validation* TS 119 101, v1.1.1, ETSI, 2016
[ETSI 2016-PAdES]	ETSI-ESI PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures ETSI EN 319 142-1 V1.1.1 (2016-04)
[ETSI 2022-XAdES]	ETSI-ESI XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures ETSI EN 319 132-1 V1.2.1 (2022-02)
[ETSI 2022-Crypto]	ETSI-ESI Cryptographic Suites ETSI TS 119 312 V1.4.2 (2022-02)