Politique de signature du Journal officiel

Version 4

(1.3.171.4.1.1.4)

Applicable à partir du 1er octobre 2023

Table des matières

1 Introduction

Le présent document décrit la politique applicable pour la signature du Journal officiel (signature du JO) et pour le cachet du Journal officiel (cachet du JO), lesquels sont utilisés en vue d'authentifier la version électronique du *Journal officiel de l'Union européenne* (JO) conformément au règlement (UE) nº 216/2013 du Conseil relatif à la publication électronique du *Journal officiel de l'Union européenne*[1].

Une politique de signature est un ensemble de règles relatives à la création, à la validation et à la prolongation d'une ou de plusieurs signatures et/ou d'un ou de plusieurs cachets électroniques liés entre eux, lesdites règles définissant les exigences techniques et procédurales applicables à leur création, à leur validation et à leur gestion à long terme en vue de satisfaire des besoins métier particuliers et de déterminer leurs conditions de validité. Une politique de signature sert aussi à rendre transparent pour toutes les parties concernées (signataires, destinataires et arbitres) l'ensemble des aspects d'un flux de travail donné pour la mise en œuvre de signatures ou cachets électroniques, de telle sorte que les signatures et cachets conformes aux exigences de cette politique puissent engendrer une confiance accrue dans leur applicabilité et leur acceptation.

Les concepts détaillés d'une politique de signature sont expliqués dans [ETSI 2015], où sont également définies les lignes directrices et la structure applicables au présent document. Le mot-clé «DOIT» et ses différentes formes grammaticales sont à comprendre dans le sens des termes «MUST», «REQUIRED» et «SHALL» tels que décrits dans le RFC 2119 [Bradner 1997]; le mot-clé «NE DOIT PAS» et ses différentes formes grammaticales sont à comprendre dans le sens des termes «MUST NOT» et «SHALL NOT» tels que décrits dans le RFC 2119 [Bradner 1997]; les mots-clés «DEVRAIT» et «RECOMMANDÉ» et leurs différentes formes grammaticales sont à comprendre dans le sens des termes «SHOULD» et «RECOMMENDED» tels que décrits dans le RFC 2119 [Bradner 1997]; le mot-clé «NE DEVRAIT PAS» et ses différentes formes grammaticales sont à comprendre dans le sens du terme «SHOULD NOT» tel que décrit dans le RFC 2119 [Bradner 1997]; les mots-clés «PEUT» et «OPTIONNEL» et leurs différentes formes grammaticales sont à comprendre dans le sens des termes «MAY» et «OPTIONAL» tels que décrits dans le RFC 2119 [Bradner 1997].

Le JO est publié par l'Office des publications de l'Union européenne (OP) sur le site web EUR-Lex (cf. point 1.2.4) afin de servir de seule source authentique du droit de l'Union européenne (UE). Il paraît du lundi au vendredi, et éventuellement le week-end, dans l'ensemble des langues officielles de l'UE. *Ci-après, l'acronyme «JO» est utilisé pour désigner globalement ce champ d'application particulier.*

1.1 Présentation générale

La politique de signature du JO formalise les éléments clés pour la mise en œuvre de la création, de la validation et de la conservation à long terme de la signature électronique et du cachet électronique appliqués au JO comme moyen d'authentification des numéros du JO publiés par l'OP.

Elle comprend les éléments suivants:

[1] Voir JO L 69 du 13.3.2013, p. 1.

- une introduction contenant l'intitulé/l'identification de la politique, des informations détaillées sur l'émetteur de la politique, des indications sur l'administration de la politique, des définitions et acronymes, etc.;
- les mentions relatives aux pratiques d'application de signature, qui définissent les exigences politiques et juridiques qui s'y rapportent, ainsi que les considérations applicables en matière de sécurité;
- les paramètres d'application métier, qui détaillent les flux de travail liés à la création des signatures et cachets électroniques comme moyen d'authentification des numéros du JO publiés par l'OP;
- les exigences et les déclarations relatives aux mécanismes techniques et à la mise en œuvre des normes, et les annexes.

1.2 Domaine d'activité

1.2.1 Champ d'application et limites de la politique de signature

La politique de signature du JO s'applique aux signatures et cachets électroniques qui sont générés pour les numéros individuels du JO par des signataires autorisés du JO conformément au règlement du Conseil relatif à la publication électronique du *Journal officiel de l'Union européenne*, après validation positive de chaque numéro à signer.

1.2.2 Domaine d'application

La politique de signature du JO s'applique uniquement aux signatures et cachets électroniques décrits au point 3.1.

1.2.3 Contexte transactionnel

Sans objet.

1.3 Nom, identification et règles de conformité de la politique de signature

1.3.1 Nom de la politique

La politique de signature du JO est intitulée comme suit:

Politique de signature du Journal officiel

1.3.2 Identifiant de la politique

Dans la mesure où il n'existe qu'un seul *Journal officiel de l'Union européenne* et que sa publication est un processus bien connu de l'Union européenne, la politique de signature du JO peut être identifiée implicitement par toute partie concernée. Une description du flux de travail général métier figure au point 3.1.1.1.

Afin d'indiquer explicitement la politique, chaque signature et cachet du JO *PEUT* inclure une indication explicite de la politique de signature, comme défini au point 5.2.9 de [ETSI 2022-XAdES]. Si tel est le cas, l'indication explicite de la politique de signature DOIT mentionner l'identifiant d'objet 1.3.171.4.1.1.4, à l'aide des règles de codage spécifiées au point 5.2.9 de [ETSI 2022-XAdES] et dans [Mealling 2010].

L'identifiant d'objet 1.3.171.4.1.1.4, unique au niveau mondial, identifie sans ambiguïté la présente version de la politique. Le préfixe 1.3.171.4 a été enregistré comme OID de base pour les *politiques de signature et autres besoins de l'Office des publications de l'UE* (cf. http://www.oid-info.com/get/1.3.171.4). Le suffixe 1.1.4 identifie la présente version de la politique de signature du JO et sa notation de valeur ASN.1 avec les noms DOIT être {oj(1) politique de signature(1) version(4)}. Cette version rend obsolète la version 1.1.3 de cette politique.

1.3.3 Règles de conformité de la politique

La présente politique ne revendique aucune conformité avec une quelconque autre politique.

1.3.4 Points de diffusion de la politique

Le document relatif à la politique de signature du JO est publié sur le site web EUR-Lex. Il est accessible depuis le site web de l'Office des publications à l'adresse https://eur-lex.europa.eu/.

1.3.5 Période de validité de la politique

La version actuelle de la politique entre en vigueur à partir du 1er octobre 2023.

1.3.6 Champ d'application de la politique

La présente politique s'applique à tous les numéros du JO publiés et signés électroniquement depuis l'entrée en vigueur du règlement du Conseil relatif à la publication électronique du *Journal officiel de l'Union européenne*. Elle n'est pas applicable au Supplément au *Journal officiel de l'Union européenne* (série S, Journal officiel S ou JO S).

> AVERTISSEMENT: chaque version de la présente politique est valable pendant la période de validité définie dans chaque version. L'ensemble de toutes les versions couvre tous les numéros du JO.

1.4 Administration des documents de la politique de signature

L'émetteur de la politique de signature du JO est l'Office des publications de l'Union européenne, qui a adopté le présent document et l'a publié sur le site web EUR-Lex.

La politique de signature du JO, dans sa version publiée, DOIT automatiquement avoir valeur légale et DOIT s'appliquer à la création, à la vérification et à la gestion à long terme des signatures et cachets du JO.

L'émetteur de la politique de signature du JO est responsable des tâches suivantes:

- spécification et approbation de la politique de signature du JO;
- définition du processus de réexamen de la politique de signature du JO;
- définition des critères et du processus d'évaluation garantissant que la politique de signature du JO est conforme au règlement (UE) nº 216/2013 du Conseil du 7 mars 2013 relatif à la publication électronique du *Journal officiel de l'Union européenne* et au règlement (UE) 2018/2056 du Conseil du 6 décembre 2018 modifiant le règlement (UE) nº 216/2013 relatif à la publication électronique du *Journal officiel de l'Union européenne*;
- définition des critères et du processus d'évaluation garantissant que les applications déclarées conformes à la politique de signature du JO en respectent effectivement les règles en vigueur;
- publication, sur EUR-Lex, de la politique de signature du JO et de ses versions modifiées.

1.4.1 Autorité responsable de la politique

La politique de signature du JO est administrée par l'Office des publications de l'Union européenne.

1.4.2 Personne de contact

L'émetteur de la présente politique peut être contacté aux coordonnées suivantes:

Personne de contact:	Chef de l'unité «Journal officiel et jurisprudence»
Adresse postale:	2, rue Mercier, L-2985 Luxembourg
Nº de téléphone:	+352 29291
Nº de télécopieur:	+352 292944620
Adresse électronique:	OP-JO-AUTHENTIQUE-HELPDESK@publications.europa.eu

1.4.3 Procédures d'approbation

L'autorité responsable de l'approbation de la politique au sein de l'Office des publications de l'Union européenne est le directeur général de l'Office des publications de l'Union européenne.

1.4.4 Versions de la politique

Les versions initiales et modifiées de la politique *PEUVENT* spécifier une date minimale d'entrée en vigueur. Lorsqu'une version de la politique est publiée, elle DOIT entrer en vigueur, au plus tard, à l'une des trois dates suivantes:

1. la date minimale d'entrée en vigueur spécifiée, le cas échéant, par ladite version de la politique;
2. le jour suivant la date du premier horodatage de signature apposé sur la signature ou le cachet du numéro du JO dans lequel est mentionnée ladite version de la politique qui est publiée, selon l'heure locale à Luxembourg;
3. le jour suivant la date de publication de ladite version de la politique.

Toute version modifiée de la politique DOIT automatiquement expirer lorsque la version modifiée suivante entre en vigueur. La version modifiée suivante de la politique DEVRAIT, en outre, indiquer la version qu'elle rend obsolète.

Les règles susmentionnées sont destinées à garantir que la signature d'une version donnée de la politique n'est pas soumise, ni directement ni indirectement, à cette même version de la politique, de manière à éviter tout raisonnement circulaire. En outre, il est préférable de conserver par tous les moyens la version obsolète.

1.5 Définitions et acronymes

Les définitions et les acronymes utilisés dans le présent document figurent dans le tableau 1.

Acronyme	**Définition (FR)**
CA	Autorité de certification
DTBS	Données à signer
LTV	Validité à long terme
OID	Identifiant d'objet
JO	*Journal officiel de l'Union européenne*
PIN	Numéro d'identification personnel
OP	Office des publications de l'Union européenne
QC	Certificat qualifié
QESig	Signature électronique qualifiée
QESeal	Cachet électronique qualifié
QSCD	Dispositif de création de signature ou de cachet qualifié
SAA	Application d'extension de signature
SCA	Application de création de signature
SSCD	Dispositif sécurisé de création de signature
SVA	Application de validation de signature
TSP	Prestataire de service de confiance
QTSP	Prestataire de service de confiance qualifié
Wipiwis	Ce qui est présenté correspond à ce qui est signé

Tableau 1: Définitions et acronymes

2 Mentions des pratiques d'application de signature

2.1 Exigences politiques connexes

Les numéros du JO sont régis par les articles 1er et 2 du règlement du Conseil relatif à la publication électronique du *Journal officiel de l'Union européenne*, qui disposent, entre autres, que l'édition électronique du Journal officiel DOIT porter une signature électronique qualifiée définie conformément au règlement (UE) nº 910/2014 du Parlement européen et du Conseil, ou un cachet électronique qualifié défini conformément au règlement (UE) nº 910/2014.

La signature et le cachet électroniques des numéros du JO relèvent de la mise en œuvre d'une signature en tant que formalité substantielle, comme indiqué au point III.2.1 des MODALITÉS D'APPLICATION DE LA DÉCISION 2002/47/CE, CECA, EURATOM CONCERNANT L'ADMINISTRATION DES DOCUMENTS ET DE LA DÉCISION 2004/563/CE, EURATOM CONCERNANT LES DOCUMENTS ÉLECTRONIQUES ET NUMÉRISÉS adoptées par la Commission européenne le 30 novembre 2009[2]; cette disposition prévoit, en outre, que la signature électronique appliquée au JO requiert une signature électronique qualifiée, telle que définie dans le [règlement eIDAS].

Conformément au point III.2.3 des MODALITÉS D'APPLICATION DE LA DÉCISION 2002/47/CE ET DE LA DÉCISION 2004/563/CE[2], la vérification de l'habilitation à signer est de la responsabilité de la SCA du JO lorsqu'il s'agit de permettre à un fonctionnaire de l'OP de signer électroniquement des numéros du JO, ou lorsqu'il s'agit de permettre à l'OP, en tant que personne morale, d'apposer un cachet électronique sur les numéros du JO.

Bien que les numéros du JO publiés en format électronique ne puissent pas produire d'effets juridiques sans avoir été signés ou cachetés, la politique de signature du JO prévoit également que la SCA du JO DOIT garantir que seuls les signataires autorisés du JO sont capables de rejeter des numéros du JO, afin de prévenir efficacement les attaques contre le processus de publication du JO.

Étant donné que les signataires autorisés du JO agissent au nom de l'OP, il est de la responsabilité du directeur général de l'OP de garantir (par délégation) une autorisation en bonne et due forme des différents QC utilisés pour signer le JO. À cette fin, l'autorisation des QC pour la signature du JO:

- *DOIT* être correctement configurée dans la fonction de gestion des utilisateurs de la SCA du JO;
- *DEVRAIT* être limitée aux certificats (professionnels) internes, qui garantissent l'appartenance du porteur à l'OP[3];
- *DOIT* être rendue transparente par la publication des QC autorisés sur le site web EUR-Lex, conformément à l'article 2 du règlement du Conseil relatif à la publication électronique du *Journal officiel de l'Union européenne*.

2.2 Exigences juridiques connexes

La mise en œuvre des signatures et cachets électroniques relevant du champ d'application de la politique de signature du JO DOIT être régie par les dispositions juridiques suivantes:

[2] Voir SEC(2009) 1643.

[3] Les certificats internes garantissent l'appartenance du porteur à une organisation spécifique. La sécurité est renforcée, car le QTSP émetteur impose au détenteur du certificat d'apporter la preuve de son habilitation.

- règlement (UE) nº 216/2013 du Conseil du 7 mars 2013 relatif à la publication électronique du *Journal officiel de l'Union européenne*;
- règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE[4];
- décision 2009/767/CE de la Commission du 16 octobre 2009 établissant des mesures destinées à faciliter l'exécution de procédures par voie électronique par l'intermédiaire des guichets uniques conformément à la directive 2006/123/CE du Parlement européen et du Conseil relative aux services dans le marché intérieur[5];
- règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)[6];
- directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)[7];
- directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) nº 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs[8];
- décision 2010/425/UE de la Commission du 28 juillet 2010 modifiant les dispositions de la décision 2009/767/CE relatives à l'établissement, la mise à jour et la publication de listes de confiance de prestataires de services de certification contrôlés ou accrédités par les États membres[9];
- décision 2009/496/CE, EURATOM du Parlement européen, du Conseil, de la Commission, de la Cour de justice, de la Cour des comptes, du Comité économique et social européen et du Comité des régions du 26 juin 2009 relative à l'organisation et au fonctionnement de l'Office des publications de l'Union européenne[10];
- décision 2011/130/UE de la Commission du 25 février 2011 établissant des exigences minimales pour le traitement transfrontalier des documents signés électroniquement par les autorités compétentes conformément à la directive 2006/123/CE du Parlement européen et du Conseil relative aux services dans le marché intérieur[3].

[4] Voir JO L 257 du 28.8.2014, p. 73.

[5] Voir JO L 274 du 20.10.2009, p. 36.

[6] Voir JO L 119 du 4.5.2016, p. 1.

[7] Voir JO L 201 du 31.7.2002, p. 37.

[8] Voir JO L 337 du 18.12.2009, p. 11.

[9] Voir JO L 199 du 31.7.2010, p. 30.

[10] Voir JO L 168 du 30.6.2009, p. 41.

2.3 Considérations de sécurité technique

Les outils cryptographiques susceptibles d'être utilisés pour la mise en œuvre des signatures et cachets du JO DOIVENT satisfaire aux exigences des signatures électroniques qualifiées, telles que définies dans le [règlement eIDAS], dans [ETSI 2016], et correspondre aux pratiques pertinentes les plus avancées.

2.4 Mentions légales

Les signatures et cachets électroniques apposés sur les numéros du JO doivent être créés au nom de l'OP sur la base du règlement du Conseil relatif à la publication électronique du *Journal officiel de l'Union européenne*.

3 Paramètres d'application métier (BSP)

3.1 BSP principalement liés à l'application/au processus métier en question

3.1.1 BSP a): flux de travail (séquence et délais) des signatures

3.1.1.1 Description générale du flux de travail métier

L'OP publie le JO du lundi au vendredi, et éventuellement le week-end. Cette publication du JO peut être un numéro du JO ou un numéro du JO-Act. Tout numéro du JO représente une publication multilingue d'un ou plusieurs documents. Chaque version linguistique d'un numéro se compose du texte complet de chaque document dans un dossier unique. Tout numéro du JO-Act représente une publication multilingue d'un seul document publié séparément. Chaque version linguistique d'un numéro du JO-Act se compose du texte complet de chaque document dans un dossier unique.

Les différents numéros du JO et numéros du JO-Act sont classés par catégorie en fonction de la série à laquelle ils appartiennent et chaque catégorie est un élément d'identification du JO. Deux séries sont pertinentes pour le présent champ d'application, à savoir la série L (législation) et la série C (communications et informations). Une série peut, à titre optionnel, comporter des sous-séries et des systèmes de classification (cf. http://publications.europa.eu/code/fr/fr-10000.htm pour des explications plus détaillées sur le champ d'application et sur la structure des documents, ainsi que pour des informations générales complémentaires).

Outre les séries L et C du JO, des éditions spéciales contenant le droit dérivé de l'UE sont également publiées dans la langue d'un pays en voie d'adhésion ou d'un nouvel État membre. Ces éditions spéciales font également partie du champ d'application.

Dès lors qu'un numéro du JO ou JO-Act est complet (c'est-à-dire que toutes les versions linguistiques du numéro du JO ou JO-Act sont disponibles en PDF/A) et prêt à être publié, le flux de travail se poursuivra avec un processus d'apposition de cachet électronique (cf. point 3.1.1.2) ou un processus de signature électronique (cf. point 3.1.1.3). Lorsqu'il s'agit d'apposer un cachet électronique, un cachet électronique qualifié est automatiquement généré à l'aide d'un certificat de cachet électronique qualifié délivré à l'OP en tant qu'entité de la Commission européenne. Lorsqu'il s'agit d'apposer une signature électronique, une signature électronique qualifiée est générée par une personne autorisée à l'aide d'un certificat de signature électronique qualifiée.

L'apposition d'un cachet électronique est le flux sélectionné par défaut par la SCA, c'est-à-dire que les numéros du JO ou du JO-Act qui sont complets passeront par le processus d'apposition de cachet automatisé à moins que ce processus ne soit pas disponible. Dans ce cas, c'est le processus de signature qui sera utilisé.

Étant donné qu'une signature ou un cachet XAdES détaché accompagné d'un manifeste (cf. [Bartel 2008], [ETSI 2022-XAdES] et décision 2011/130/UE de la Commission du 25 février 2011 établissant des exigences minimales pour le traitement transfrontalier des documents signés électroniquement par les autorités compétentes conformément à la directive 2006/123/CE du Parlement européen et du Conseil relative aux services dans le marché intérieur[11]) est employé pour signer chaque numéro, il est nécessaire, lors de la vérification d'une signature ou d'un cachet du JO ou du JO-Act, de valider non seulement le noyau de la signature XML, mais également le manifeste (cf. [Bartel 2008]) dans le cadre de la validation selon [ETSI 2022-XAdES].

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

Les sous-sections suivantes décrivent les flux d'apposition de cachet et de signature électroniques de haut niveau tels que mis en œuvre dans la SCA, la SAA et la SVA du JO (cf. [ETSI 2016]).

3.1.1.2 Création de cachet du JO et du JO-Act

1. Un numéro du JO ou du JO-Act qui est complet est détecté pour l'apposition du cachet
2. La SCA effectue des contrôles de vérification préliminaires sur les fichiers fournis:
    a. elle vérifie la présence ou non d'incohérences liées à la taille entre les versions linguistiques du numéro du JO/JO-Act, et si celles-ci se situent dans des limites de taille configurables;
    b. elle vérifie s'il était prévu que toutes les versions linguistiques fournies soient publiées.
3. En cas de vérification négative, le processus d'apposition de cachet est interrompu. L'intervention manuelle du personnel autorisé de l'OP est nécessaire pour reprendre le processus d'apposition de cachet.
4. En cas de validation positive par la SCA, un manifeste désignant chaque version linguistique du numéro complet est généré. En outre, chacune des versions linguistiques correspond à une seule langue de l'UE et a la forme d'un document PDF/A qui est traité comme un flux d'octets binaires lors du calcul des condensés de messages.
5. La SCA s'authentifie sur le portail central de signature électronique de la Commission européenne et transmet le manifeste créé pour apposer automatiquement un cachet.
6. Le manifeste qui est fourni est cacheté sur le portail de signature électronique à l'aide d'un certificat de cachet qualifié, délivré par un QTSP européen accrédité (cf. [règlement eIDAS]). La clé privée liée à ce certificat de cachet est stockée sur un QSCD relié au portail de signature électronique.
7. Le cachet XAdES (cf. [ETSI 2022-XAdES]) ainsi créé est ensuite renvoyé à la SCA, qui vérifie, entre autres, la validité des algorithmes utilisés et s'assure que le certificat de cachet du cachet en question est autorisé et appartient à la même personne morale qui a été authentifiée en tant que signataire autorisé.
8. Si la vérification est positive, le cachet électronique est complété par un horodatage de la signature fourni par un QTSP accrédité (cf. [règlement eIDAS]).
9. Le cachet électronique complété au cours de la précédente étape de traitement est transféré pour publication sur le site web EUR-Lex. En même temps, une copie identique du cachet est conservée par la SCA.
10. Lorsque le délai de latence de 24 heures requis pour un cachet résultant de la précédente étape de traitement est écoulé, le cachet est de nouveau complété à un format autodurable, afin de prolonger la validité de la signature pour une période plus longue, à l'aide du service d'horodatage de confiance d'un QTSP européen accrédité (cf. [règlement eIDAS]).
11. Le cachet complété au cours de la précédente étape de traitement est transféré pour publication sur le site web EUR-Lex et remplace le cachet de l'étape 9, qui n'avait pas encore été complété à un format autodurable.
12. Outre la publication sur le site web EUR-Lex, des copies identiques des documents composant un numéro du JO ou du JO-Act, avec le cachet correspondant sous un format autodurable, sont transférées au système de conservation numérique à long terme, qui est géré par l'OP et préserve à long terme les documents officiels des institutions de l'UE. Les aspects concernant la mise

en œuvre de la conservation à long terme ne font PAS l'objet de la présente politique de signature.

3.1.1.3 Création de signature du JO et du JO-Act

1. Un numéro du JO ou du JO-Act qui est complet est détecté pour signature.
2. Un manifeste désignant chaque version linguistique du numéro complet est généré. En outre, chacune des versions linguistiques correspond à une seule langue de l'UE et a la forme d'un document PDF/A qui est traité comme un flux d'octets binaires lors du calcul des condensés de messages.

   Il convient de noter que les numéros complets sont gérés de manière exclusive et verrouillés par la SCA pendant la génération du manifeste, afin de garantir un calcul cohérent des condensés, ce qui est crucial pour le processus.
3. Après avoir été authentifié avec succès par la SCA, un signataire autorisé peut sélectionner un numéro complet pour signature, à condition que le manifeste correspondant ait été généré au cours de l'étape précédente.
4. Après avoir réussi à sélectionner un numéro à signer, le signataire autorisé s'engage dans le processus de signature pour ce numéro particulier:
   a. afin de respecter dûment le principe Wipiwis, le signataire autorisé est obligé d'examiner au moins trois versions linguistiques différentes, en utilisant un visualisateur conforme PDF/A avant de pouvoir signer le numéro. Si l'édition du JO ou du JO-Act comporte moins de trois versions linguistiques, le signataire autorisé a l'obligation d'examiner toutes les versions linguistiques disponibles;

      Il convient de noter que la SCA permet au signataire d'examiner n'importe quelle version linguistique du numéro à signer. Le signataire PEUT donc, s'il le souhaite, examiner la totalité du contenu à signer.
   b. le signataire autorisé peut délibérément choisir de rejeter le numéro, ce qui interrompt le processus de signature, ou de poursuivre la signature en pressant le bouton «Signer»;
   c. après pression du bouton «Signer»:
      i. la SCA crée une demande de signature sur le portail central de signature électronique de la Commission européenne, en transmettant le manifeste à signer et en redirigeant le signataire autorisé vers le portail;
      ii. le signataire autorisé s'authentifie sur le portail de signature électronique, et reçoit le manifeste à signer, conformément aux principes du Wipiwis;
      iii. le portail de signature électronique est connecté à l'intergiciel installé sur le poste de travail du signataire autorisé et le certificat de signature qualifié du signataire, délivré par un QTSP européen accrédité, est récupéré (cf. [règlement eIDAS]). Ce certificat est présenté au signataire autorisé, qui, à son tour, est invité à entrer le code PIN correspondant protégeant le QSCD afin d'autoriser le QSCD à créer la signature par une clé privée correspondant au certificat de signature sélectionné, finalisant ainsi le processus de signature;
   d. l'intergiciel envoie la valeur de la signature créée sur le portail de signature électronique, qui crée à son tour une signature XAdES correspondante (cf. [ETSI 2022-XAdES]).

5. Cette signature XAdES est ensuite renvoyée à la SCA, qui vérifie, notamment, par le portail de signature électronique, la validité des algorithmes utilisés et s'assure que le certificat de signature de la signature en question est autorisé et appartient à la même personne qui a été authentifiée en tant que signataire autorisé.
6. Si la vérification est positive, la signature électronique est complétée, en passant par le portail de signature électronique, par un horodatage de signature fourni par un QTSP accrédité (cf. [règlement eIDAS]).
7. La signature étendue au cours de la précédente étape de traitement est transférée pour publication sur le site web EUR-Lex. En même temps, une copie identique de la signature est conservée par la SCA.
8. Lorsque le délai de latence de 24 heures requis pour une signature résultant de la précédente étape de traitement est écoulé, la signature est de nouveau complétée à un format autodurable, afin de prolonger la validité de la signature pour une période plus longue, à l'aide du service d'horodatage de confiance d'un QTSP européen accrédité (cf. [règlement eIDAS]).
9. La signature étendue au cours de la précédente étape de traitement est transférée pour publication sur le site web EUR-Lex et remplace la signature de l'étape 7, qui n'avait pas encore été complétée à un format autodurable.
10. Outre la publication sur le site web EUR-Lex, des copies identiques des documents composant un numéro du JO ou du JO-Act, avec la signature correspondante sous un format autodurable, sont transférées au système de conservation numérique à long terme, qui est géré par l'OP et préserve à long terme les documents officiels des institutions de l'UE. Les aspects concernant la mise en œuvre de la conservation à long terme ne font PAS l'objet de la présente politique de signature.

3.1.1.4 Situation d'urgence

Lorsqu'il est impossible de créer le cachet ou la signature du JO ou du JO-Act comme indiqué aux points 3.1.1.2ou 3.1.1.3en raison d'une indisponibilité imprévue et exceptionnelle de la SCA du JO, l'Office des publications applique un QESeal ou un QESig sur chaque document PDF/A correspondant à chaque version linguistique du numéro du JO ou du JO-Act. Tous les documents PDF/A cachetés/signés sont transférés pour publication sur le site web EUR-Lex.

3.1.2 BSP b): données à signer

- Les signatures et les cachets du JO ou du JO-Act s'appuient sur un manifeste XML (cf. [Bartel 2008] et [ETSI 2022-XAdES]) qui regroupe toutes les versions linguistiques, disponibles au format PDF/A, se rapportant à un numéro du JO ou du JO-Act dans une signature unique devant satisfaire aux exigences suivantes: chaque version linguistique logiquement associée à un numéro du JO ou du JO-Act *DOIT* avoir sa propre valeur de condensé;
- afin que soit respecté le principe Wipiwis, toute version linguistique logiquement associée à un numéro du JO ou du JO-Act *DOIT* être présentée, pour examen, au signataire lors de la création de signature, pour que celui-ci puisse vérifier, à son entière discrétion, le contenu de la signature comme décrit au point 3.1.1.3;
- une visualisation adéquate *DOIT* être garantie au moyen d'un lecteur conforme PDF/A;
- seules les versions linguistiques se rapportant au numéro particulier en cours de signature DOIVENT être présentées au signataire lors du processus de signature;
- les caractéristiques techniques de toutes les versions linguistiques logiquement associées à un numéro du JO ou du JO-Act *DOIVENT* être vérifiées lors de la création du cachet et de la signature, afin de garantir la cohérence.

En cas de situation d'urgence décrite au point 3.1.1.4ci-dessus, les exigences suivantes s'appliquent:

- chaque version linguistique d'un numéro du JO ou du JO-Act *DOIT* avoir son propre QESeal ou QESig;
- afin que soit respecté le principe Wipiwis, toute version linguistique logiquement associée à un numéro du JO ou du JO-Act *DOIT* être examinée par le signataire lors de la création de signature, pour que celui-ci puisse vérifier, à son entière discrétion, le contenu de la signature;
- une visualisation adéquate *DOIT* être garantie au moyen d'un lecteur conforme PDF/A.

3.1.3 BSP c): lien entre les données signées, d'une part, et la ou les signatures et le ou les cachets, d'autre part

Une signature ou un cachet du JO ou du JO-Act s'applique à toutes les versions linguistiques – dont chacune est formatée comme un document PDF/A – d'un numéro du JO ou du JO-Act.

Lors de la création d'une signature ou d'un cachet du JO ou du JO-Act, le contenu numérique d'un document à signer/cacheter est condensé en une chaîne d'octets binaires à l'aide du plus solide algorithme de condensation pris en charge qui satisfait aux exigences du point 7.3 de [ETSI 2022-Crypto].

Les valeurs de condensé des différents documents sont regroupées avec les URI des noms des fichiers originaux dans un manifeste XML, sans application de transformations supplémentaires (cf. [Bartel 2008]).

Le manifeste, incluant les attributs signés, est signé ou cacheté en employant le format XAdES (cf. [ETSI 2022-XAdES]) pour le profil spécifié dans la décision 2011/130/UE de la Commission du 25 février 2013.

En cas de situation d'urgence décrite au point 3.1.1.4ci-dessus, chaque document PDF/A représentant chacune des versions linguistiques du numéro du JO ou du JO-Act est signé ou cacheté en employant le format PAdES (cf. [ETSI 2016-PAdES] [eIDAS]).

3.1.4 BSP d): communautés visées

La communauté visée désigne toute partie qui utilise le JO et qui doit vérifier son authenticité, ainsi que toutes les parties chargées de la mise en œuvre de la SCA et de la SAA utilisées afin de créer des signatures ou des cachets électroniques et de les compléter pour les numéros du JO ou du JO-Act.

3.1.5 BSP e): attribution des responsabilités quant à la validation et à l'extension des signatures

3.1.5.1 Vérification de la signature et du cachet du JO ou du JO-Act

Toute partie utilisatrice, en particulier tout citoyen européen, peut télécharger un numéro du JO ou du JO-Act publié sur le site web EUR-Lex, ainsi que la signature ou le cachet XAdES détaché correspondant (cf. [ETSI 2022-XAdES]), pour vérification.

Comme une norme de signature européenne interopérable et les services d'un QTSP européen accrédité (cf. [règlement eIDAS]) sont utilisés lors de la création de signature et de cachet, la vérification peut être effectuée à l'aide de tout utilitaire de vérification tiers qui est conforme aux normes employées, pour autant que la validation du manifeste puisse être réalisée sur la base de la politique de signature du JO.

En cas de situation d'urgence décrite au point 3.1.1.4ci-dessus, chaque document PDF/A représentant chacune des versions linguistiques du numéro du JO ou du JO-Act est signé ou cacheté en employant le format PAdES (cf. [ETSI 2016-PAdES]). Leur vérification peut être effectuée à l'aide de n'importe quel service de vérification tiers conforme à la norme employée.

3.1.5.1.1 Vérification côté serveur

Afin de faciliter la vérification de signature et de cachet, l'OP PEUT, à titre gratuit, proposer une SVA du JO fonctionnant côté serveur selon le flux de travail de vérification spécifié ci-après:

1. le vérificateur télécharge le fichier PDF/A à vérifier, ainsi que le fichier de la signature ou du cachet qui lui est associé, à l'aide de la fonctionnalité de téléchargement de fichiers fournie par la SVA;
2. la SVA calcule le condensé du fichier PDF/A téléchargé et vérifie si le condensé calculé est contenu dans la partie du manifeste de la signature téléchargée;
3. après vérification positive du condensé, la vérification selon la norme XAdES de la signature ou du cachet candidat téléchargé est effectuée, pour autant que le certificat de signature ou de cachet identifie un signataire autorisé du JO pour la période déterminée par l'horodatage de la signature. La SVA vérifie également, sur la base de l'horodatage de la signature, que le signataire était autorisé à signer au moment de la création de la signature;
4. la vérification est positive si toutes les étapes précédentes s'achèvent avec succès. Dans le cas contraire, la vérification est négative. En tout état de cause, un rapport compréhensible sur le processus de vérification est présenté au vérificateur.

3.1.5.1.2 Vérification côté client

Afin de faciliter la vérification de signature et de cachet, l'OP PEUT, à titre gratuit, proposer une SVA du JO fonctionnant côté client selon le flux de travail de vérification spécifié ci-après:

1. le vérificateur démarre la SVA téléchargée, sa signature de code est automatiquement vérifiée par l'environnement d'exécution et l'exécution est autorisée par le vérificateur après vérification positive de la signature de code;
2. le vérificateur sélectionne un fichier PDF/A dans une version linguistique donnée à vérifier, ainsi que le fichier de la signature ou du cachet candidat qui lui est associé, dans le système de fichiers du PC local à l'aide du dialogue de sélection de fichiers fourni par la SVA;
3. la SVA calcule le condensé du document sélectionné et vérifie si le condensé calculé est contenu dans le manifeste de la signature ou du cachet candidat sélectionné;
4. après vérification positive du condensé, la vérification selon la norme XAdES de la signature ou du cachet candidat sélectionné est effectuée;
5. la vérification est positive si toutes les étapes précédentes s'achèvent avec succès et si le certificat de signature ou de cachet identifie un signataire autorisé du JO pour la période déterminée par l'horodatage de la signature.

   Il convient de noter que les informations sur les signataires autorisés PEUVENT être connues de la SVA sur la base d'une configuration préétablie (par défaut). Toutefois, le condensé du certificat de signature ou de cachet est, en outre, indiqué dans le résultat de la SVA, de manière que le vérificateur puisse le comparer manuellement avec les informations publiées sur les signataires légaux pour la période de création de signature ou de cachet, qui est également indiquée dans le résultat de la SVA.

3.2 BSP principalement influencés par les dispositions juridiques/réglementaires liées à l'application /au processus métier en question

3.2.1 BSP f): caractère juridique des signatures

Les signatures et les cachets électroniques apposés sur les JO ou JO-Act DOIVENT être des QESig et des QESeal au sens du [règlement eIDAS].

L'exigence précitée est prévue notamment par le règlement du Conseil relatif à la publication électronique du *Journal officiel de l'Union européenne* (cf. point 2.2).

L'obtention d'un QC par chaque signataire est une condition préalable à l'utilisation du système de signature.

Les éléments spécifiques des QESig et QESeal requis DOIVENT satisfaire aux exigences de qualité suivantes:

- dispositif de signature et de cachet: QSCD conformes à l'annexe II du [règlement eIDAS];
- fourniture de certificats: QC conforme à l'annexe I du [règlement eIDAS];
- garantie indépendante concernant la fourniture de certificats: QC émis par un service de certification d'un QTSP contrôlé ou accrédité dans tout pays auquel le [règlement eIDAS] s'applique;
- suite cryptographique de signature: seules les suites de signature énumérées au point 7.3 de [ETSI 2022-Crypto] doivent être utilisées;
- solutions LTV: les formats de signature et de cachet XAdES (cf. [ETSI 2022-XAdES]) du JO ou du JO-Act DOIVENT être complétés au format -LTA, incluant le renouvellement des horodatages d'archivage ou une autre solution (des mécanismes d'archivage sécurisés externes PEUVENT être considérés comme une alternative au renouvellement des horodatages d'archivage, à condition qu'ils soient de qualité équivalente ou supérieure);
- application de création de signature: la SCA du JO DOIT satisfaire aux exigences de qualité imposées par les politiques de la CE et être conforme aux dispositions du règlement du Conseil relatif à la publication électronique du *Journal officiel de l'Union européenne*.

3.2.2 BSP g): engagement pris par le signataire

Les signatures et les cachets électroniques apposés sur les numéros du JO ou du JO-Act DOIVENT être créés au nom de l'OP conformément au règlement du Conseil relatif à la publication électronique du *Journal officiel de l'Union européenne*.

L'engagement pris par un signataire autorisé du JO exprime le fait que les données signées représentent un numéro authentique du JO ou du JO-Act qui a été dûment validé par rapport aux règles relatives au champ d'application métier (cf. point 3.1.1) et publié par l'OP conformément au règlement du Conseil relatif à la publication électronique du *Journal officiel de l'Union européenne*, dans le but de servir de source authentique du droit de l'UE.

Aucune indication explicite du type d'engagement NE DOIT être contenue dans une signature du JO (cf. point 5.2.3 de [ETSI 2022-XAdES]).

3.2.3 BSP h): niveau de garantie concernant les éléments temporels

Un horodatage de signature DOIT être ajouté à la signature ou au cachet du JO ou du JO-Act qui sont créés de la manière décrite aux points 3.1.1.2ou 3.1.1.3, le même jour (heure locale à Luxembourg) que la date de la signature ou du cachet du numéro du JO ou du JO-Act, afin de certifier que la signature ou le cachet n'a pas été créé après la date de publication. Il est ainsi garanti que l'ensemble de signataires autorisés à la date de publication est applicable pour la signature ou le cachet.

La SCA du JO DOIT garantir que toutes les signatures XAdES-B-T créées satisfont à cette exigence.

L'horodatage utilisé pour créer des horodatages de signature dans les signatures XAdES-B-T DOIT être un horodatage qualifié.

Les signatures au format PAdES créées en cas de situation d'urgence décrite au point 3.1.1.4PEUVENT être créées sans horodatage de signature.

Si les signatures au format PAdES créées en cas de situation d'urgence décrite au point 3.1.1.4sont créées à l'aide d'un horodatage de signature, celui-ci DOIT être un horodatage qualifié et appliqué le même jour (heure locale à Luxembourg) que la date de la signature ou du cachet du numéro du JO ou du JO-Act, afin de certifier que la signature ou le cachet n'a pas été créé après la date de publication.

AVERTISSEMENT: cela signifie qu'en cas de situation d'urgence, si un horodatage de signature est inclus dans la signature, il peut s'agir d'un horodatage non qualifié.

Tous les autres horodatages, y compris les horodatages d'archivage et de contenu, le cas échéant, DOIVENT être des horodatages qualifiés.

3.2.4 BSP i): formalités de signature

Il est de la responsabilité de la SCA du JO de mettre à la disposition du signataire une interface garantissant, autant que possible, un environnement de signature et de cachet juridiquement valide. L'interface doit:

- prévoir la fourniture d'une assistance-conseil et d'informations appropriées sur le processus de signature et de cachet de l'application;
- assurer la cohérence entre l'utilisation des données appropriées de création et de vérification de signature et de cachet, les dispositifs de création de signature et de cachet, les données à signer, ainsi que la portée et la finalité prévues de la signature et du cachet (ou de l'acte de signature ou d'apposition du cachet);
- permettre et faire apparaître une expression claire de la volonté de signer et de l'intention de l'utilisateur d'être lié par la signature ou le cachet;
- permettre et faire apparaître un consentement éclairé.

La SVA du JO DOIT mettre à la disposition des parties utilisatrices (y compris le signataire) des procédures adéquates pour la vérification et l'archivage de la signature ou du cachet électronique et des données de vérification.

3.2.5 BSP j): pérennité et résilience face au changement

Les numéros signés du JO ou du JO-Act et leurs signatures DOIVENT être conservés pendant une période illimitée. Le maintien de la validité des signatures du JO ou du JO-Act DOIT être garanti pour une telle période (cf. article 2 du règlement du Conseil relatif à la publication électronique du *Journal officiel de l'Union européenne*).

3.2.6 BSP k): archivage

Sans objet.

3.3 BSP liés principalement aux acteurs intervenant dans la création, l'extension ou la validation des signatures

3.3.1 BSP l): identité (et rôles/attributs) des signataires

3.3.1.1 Règles proposées concernant le signataire et son identification

Les signatures du JO ou du JO-Act DOIVENT être appliquées par des signataires autorisés, qui DOIVENT expressément être des fonctionnaires de l'OP possédant l'expertise requise pour valider les numéros du JO ou du JO-Act conformément aux règles relatives au champ d'application métier (cf. point 3.1.1.3). En ce qui concerne les cachets du JO ou du JO-Act, le signataire autorisé DOIT être l'OP lui-même en tant qu'entité de la Commission européenne.

Les signataires autorisés DOIVENT également être conscients de leur responsabilité et agir en toute bonne foi lors de l'authentification de textes juridiques représentant le droit de l'UE.

Le lien entre ces personnes physiques signataires et leurs données de vérification de signature DOIT être attesté dans un QC, au sens du [règlement eIDAS], qui confirme l'identité de ces personnes et leur appartenance à l'OP.

L'autorisation des signataires du JO DOIT être réalisée par le directeur général de l'OP (par délégation, le cas échéant).

3.3.1.2 Rôles et attributs des signataires

À l'exception de l'appartenance du signataire à l'OP, aucun autre attribut de rôle, de fonction ou de qualification NE DOIT nécessiter de certification dans le QC du signataire.

Il DOIT être de la responsabilité de la SCA du JO de garantir un contrôle d'accès et une autorisation en bonne et due forme des signataires avant de leur accorder l'accès aux dispositifs de signature du JO authentique.

Le contrôle d'accès et l'autorisation des signataires DOIVENT être réalisés sur la base d'un puissant mécanisme d'authentification mis en œuvre dans la SCA et des autorisations enregistrées au moyen des certificats de clés publiques correspondant aux signataires autorisés dans la base de données de gestion des utilisateurs de la SCA.

Les parties utilisatrices *PEUVENT* faire usage des certificats publiés des signataires du JO pour vérifier leur habilitation juridique.

3.3.1.3 Preuves d'habilitation connexes

Pas de spécifications autres que celles du point 3.3.1.2.

3.3.2 BSP m): niveau de garantie requis pour l'authentification du signataire

Le niveau de garantie requis pour l'authentification du signataire est assuré par son certificat qualifié et les moyens de création de sa signature, qui DOIVENT être un dispositif de création de signature/cachet qualifié défini dans le [règlement eIDAS].

3.4 Autres BSP

3.4.1 BSP o): autres informations à associer à la signature ou au cachet

3.4.1.1 Signataires autorisés du JO et autorités d'horodatage

La vérification de l'autorisation des signataires est un élément essentiel de la confiance à l'égard du JO authentique.

L'autorisation DOIT être rendue explicite par la publication des certificats électroniques de tous les signataires autorisés au moyen d'un support de confiance externe à la SCA/SVA.

Lors de la publication des signataires autorisés du JO, il DOIT être indiqué que le statut de contrôle des certificats de signataire est garanti pour la période de signature du JO ou du JO-Act en cours.

Les signataires autorisés du JO et les autorités d'horodatage NE DOIVENT PAS être publiés au JO, car cette façon de procéder créerait des problèmes de raisonnement circulaire, en particulier en ce qui concerne la validation à long terme.

Lorsque les signataires autorisés du JO ou les autorités d'horodatage changent au fil du temps, le précédent ensemble de signataires DOIT être publié à titre d'informations de confiance historiques. Ces informations sont nécessaires pour vérifier les numéros du JO ou du JO-Act signés par ces signataires.

Lors de la publication des signataires autorisés, la période pour laquelle les signataires énumérés sont ou étaient autorisés à signer DOIT être spécifiée, en tenant compte des contraintes temporelles de la présente version de la politique de signature.

3.4.1.2 Règles sur les attributs, la portée et la finalité de la signature et du cachet électroniques

Le processus de création de signature et de cachet DOIT faire un usage adéquat des attributs de signature, en particulier des attributs signés, qui sont des éléments d'information accompagnant la signature ou le cachet électronique et qui, conjointement avec les DTBS, sont couverts par la signature ou le cachet, en respectant les spécifications suivantes:

- l'identifiant du certificat de signature DOIT être utilisé. Il s'agit de l'identifiant du (ou d'une référence au) certificat contenant les données de vérification de signature correspondant aux données de création de signature ou de cachet utilisées par le signataire pour créer la signature ou le cachet électronique;
- une indication de politique de signature PEUT être utilisée (cf. point 1.2.2);
- le moment déclaré de signature DOIT être utilisé. Il correspond au moment auquel le signataire déclare avoir créé la signature ou le cachet.

  Il convient de noter que cette indication de temps est déterminée à partir du temps système courant du poste de travail du signataire. Il ne s'agit PAS d'un temps de confiance.

  Le propriétaire de la SCA du JO DOIT (par délégation du directeur général de l'OP) prendre les mesures nécessaires pour que le temps système courant des postes de travail de tous les signataires soit exact;

À cet effet, il est possible d'utiliser le protocole NTP avec une source de temps adéquate (cf. [Mills 2010]).

- AUCUNE indication de type d'engagement NE DOIT être utilisée;
- d'autres attributs signés PEUVENT être utilisés.

L'utilisation d'attributs de signature DOIT être conforme à [ETSI 2010] et à la décision 2011/130/UE de la Commission du 25 février 2013.

3.4.2 BSP p): suites cryptographiques

Voir point 3.2.1.

4 Exigences/mentions relatives à la mise en œuvre des mécanismes et normes techniques

4.1 Règles concernant l'horodatage de confiance

Le format de signature XAdES-B-LTA (cf. [ETSI 2022-XAdES]) requiert plusieurs horodatages qui DOIVENT être obtenus auprès d'un service d'horodatage qualifié accrédité dans un État membre de l'UE ou un pays de l'EEE.

Le propriétaire de la SCA du JO DOIT (par délégation du directeur général de l'OP) veiller à ce que la SCA soit configurée pour l'utilisation d'algorithmes cryptographiques appropriés.

4.2 Règles de validité à long terme

Le maintien de la validité des signatures du JO ou du JO-Act pendant la période de conservation prévue est assuré par la mise en œuvre du format de signature XAdES-B-LTA (cf. [ETSI 2022-XAdES]) et, ultérieurement, par l'ajout à la signature d'un horodatage d'archive qualifié supplémentaire pour prolonger sa validité, s'il y a lieu, ou d'une solution d'archivage adéquate offrant des garanties de maintien de la validité des signatures.

4.3 Autres problématiques métier et juridiques

Le JO étant publié du lundi au vendredi, et éventuellement le week-end, le propriétaire de la SCA du JO DOIT (par délégation du directeur général de l'OP) prendre les mesures nécessaires pour garantir l'opérabilité continue de la SCA.

À cet effet, des accords de niveau de service appropriés DEVRAIENT être établis.

Bien que les signatures et les cachets du JO ou du JO-Act puissent être vérifiés par toute SVA respectant les normes et règles définies par la politique de signature du JO, qui exige également la validation des manifestes, l'OP PEUT mettre à disposition, sur le site web EUR-Lex, une SVA librement accessible, afin de permettre aux parties utilisatrices, et notamment aux citoyens européens, de vérifier les signatures du JO ou du JO-Act sans devoir faire l'acquisition d'un utilitaire tiers.

À titre d'alternative, l'OP PEUT proposer une SVA sous la forme d'un utilitaire librement téléchargeable qui peut fonctionner indépendamment sur l'ordinateur de bureau de l'utilisateur et requiert uniquement que le vérificateur fasse confiance au logiciel lorsqu'il utilise les résultats produits par ce dernier.

5 Annexe

[Bartel 2008]	Bartel M., Boyer J., Fox B., LaMacchia B., Simon E. *XML Signature Syntax and Processing (Second Edition)* Recommandation W3C, 2008
[Bradner 1997]	Bradner S. *Key words for use in RFCs to indicate requirement levels* RFC 2119, Network Working Groupe, 1997
[Mealling 2010]	Mealling M. *A URN Namespace of Object Identifiers* RFC 3061, Network Working Groupe, 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
[Règlement eIDAS]	*Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE* JO 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)