Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

BERCY 3
10, RUE DU CENTRE
93464 NOISY-LE-GRAND CEDEX
Standard : (+33) 1 57 33 99 00

Politique de vérification de signature électronique du service proposé par l'AIFE

Version - Date	Emetteur	Statut/Suivi des modifications
V1.0 – 18/05/2020	AIFE	Version 1 de la politique

Objectif du document	Ce document constitue la politique du service de vérification de signature de l'AIFE, dont l'OID est précisé au chapitre 1. Il décrit les processus et les mécanismes de vérification appliqués sur les documents soumis au service.
Mots clefs	Signature électronique ; Vérification de signature ; eIDAS ; RGS ; Certificat ; Autorité de Certification
Résumé	Le service de vérification de signature est accessible librement, il produit un rapport technique d'intégrité de la signature et de validité des certificats utilisés selon les critères définis dans ce document.

Sommaire

1 INTRODUCTION

1.1 Présentation générale

Le présent document constitue la politique de vérification de signature électronique mise en œuvre par le service de vérification proposé par l'AIFE[1].

Le document de politique de vérification expose, à l'attention des utilisateurs, la stratégie et les différents paramètres de vérification appliqués. Il permet ainsi de comprendre parfaitement les résultats de vérification produits, quels que soient les documents fournis. Un rapport de vérification de signature est fourni par le service dès lors qu'il a pu vérifier au moins une signature dans le document.

Le plan et le contenu de cette politique sont conformes aux spécifications techniques de la norme ETSI [SIGN_POLICY_TOC]. Ainsi, les paramètres sont classés selon différentes catégories :

- Les paramètres liés aux cas d'usage opérationnels ;
- Les paramètres liés aux règles associées à ces cas d'usage ;
- Les paramètres liés aux acteurs impliqués ;
- Les autres paramètres.

1.2 Domaine d'application ou métier

1.2.1 Portée et limites de la politique de vérification de signature

Le service proposé par l'AIFE effectue une vérification technique de conformité de la signature : elle ne prend en compte aucune considération métier, par exemple sur le contenu du document, la qualité du signataire ou le respect de processus métier de signature. Les critères de vérification sont détaillés ci-après dans le document.

Le service est capable de vérifier plusieurs signatures présentes dans le document.

1.2.2 Domaines d'application

L'AIFE n'a pas restreint le service de vérification à un domaine d'application spécifique. Les utilisateurs sont seuls responsables de l'interprétation des rapports de vérification délivrés, en fonction de leur propre contexte d'utilisation.

Le respect de la réglementation et notamment l'Arrêté du 22 mars 2019 relatif à la signature électronique des contrats de la commande publique permettent d'indiquer le cadre légal sur lequel se fonde la politique de signature**.**

1.2.3 Contexte transactionnel

Le service de vérification peut être sollicité par un utilisateur pour vérifier un document de façon unitaire, et sans contrainte de délai par rapport à la signature présente dans le document.

1.3 Nom et identification du document, de la politique et des exigences de conformité

1.3.1 Nom de ce document et de la politique de vérification de signature

Ce document est nommé « Politique du service de vérification de signature de l'AIFE » et décrit la politique du même nom.

1.3.2 Identification de ce document et de la politique de vérification de signature

Ce document est identifié par sa référence [PolSignature1.2.250.1.219.6.4.1.1] et son numéro de version v1.

Cette politique de vérification de signature est identifiée par l'OID : 1.2.250.1.219.6.4.1.1

1.3.3 Exigences de conformité

Le service de vérification de signature est conforme aux standards du règlement européen eIDAS [eIDAS]. Le service de vérification de signature n'est toutefois pas qualifié au sens de ce règlement (en particulier les rapports de vérification ne sont pas signés par le service).

[1] URL : https://esignature.chorus-pro.gouv.fr/

Le plan et le contenu de ce document se conforment aux exigences de la norme ETSI TS 119 172-1 [SIGN_POLICY_TOC].

1.3.4 Points de distribution

Le présent document est publié à l'adresse suivante :

https://esignature.chorus-pro.gouv.fr/politiquedesignature

1.4 Gestion de la politique

1.4.1 Entité gérant la politique

La politique est gérée par l'AIFE, en lien avec ses partenaires qui utilisent aussi ce service.

1.4.2 Point de contact

Toute question relative au présent document ou au service de vérification peut être transmise à :

- Adresse mail : commandepubliquenumerique.aife@finances.gouv.fr
- Adresse postale : AIFE, Bercy 3 – 10, rue du centre – 93160 Noisy le Grand

1.4.3 Procédure d'approbation de la politique

La politique est approuvée après examen et relecture par l'AIFE, et avant déploiement de sa mise en œuvre. Cette relecture a pour objectifs d'assurer :

- La conformité de la politique avec les exigences réglementaires applicables au service ;
- La concordance entre les engagements exprimés dans la politique et les moyens techniques et organisationnels mis en œuvre par l'AIFE et ses partenaires.

1.4.4 Amendements à la politique

Les amendements à la politique sont élaborés par l'AIFE, par exemple pour se conformer à des évolutions réglementaires ou normatives ou améliorer les fonctionnalités du service. Une proposition d'amendement doit être approuvée avant sa mise en œuvre effective pour les utilisateurs.

Toute évolution de la présente politique ayant un impact majeur sur le service de vérification entraine une évolution de son OID, afin que les utilisateurs puissent clairement distinguer quelle politique de vérification a été utilisée pour un rapport de vérification produit.

Les modifications de la politique du service sont publiées au plus tard à la mise en production du service qui les implémente.

1.5 Définitions et acronymes

AIFE	Agence pour l'informatique financière de l'État
API	Application Programming Interface : Interface programmatique permettant à une application de solliciter le service de vérification.
BSP	Business Scoping Parameters : Paramètres du service de vérification
CRL	Certificate Revocation List : Liste des certificats révoqués par une Autorité de Certification
ETSI	European Telecommunications Standards Institute
OCSP	Online Certificate Status Protocole : Protocole d'interrogation en ligne d'une Autorité de Certification pour obtenir le statut de révocation d'un certificat
OID	Object Identifier : Identifiant universel représenté par une suite d'entiers séparés par un point, et utilisé pour identifier de façon univoque une politique de vérification
PAdES	PDF Advanced Electronic Signature : Signature électronique de document PDF conforme aux standards ETSI [PAdES_SIGN]
PISTE	PISTE est la plateforme d'intermédiation des services pour la transformation de l'Etat, une plateforme mutualisée des services API de l'État et de la sphère publique, mise en œuvre par l'Agence pour l'Informatique Financière de l'État (AIFE). https://developer.aife.economie.gouv.fr/
RGS	Référentiel Général de Sécurité
UE	Union Européenne
XAdES	XML Advanced Electronic Signature : Signature électronique de document XML conforme aux standards ETSI [XAdES_SIGN]

1.6 Documents associés

[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 https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32014R0910
[HOMOLOGATION]	L'homologation de sécurité du RGS https://www.ssi.gouv.fr/uploads/2014/06/guide_homologation_de_securite_en_9_etapes.pdf
[PAdES_SIGN]	ETSI EN 319 142-1 : Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures - V1.1.1 (2016-04) https://www.etsi.org/deliver/etsi_en/319100_319199/31914201/01.01.01_60/en_31914201v010101p.pdf
[RGPD]	Règlement (UE) n°2016/679 du Parlement européen et du Conseil du 27 avril 2016 https://www.cnil.fr/fr/reglement-europeen-protection-donnees
[RGS_V2]	Référentiel général de sécurité, Version 2.0 du 13 juin 2014 https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0/
[SIGN_POLICY_TOC]	ETSI TS 119 172-1 Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents - Version V1.1.1 (2015-07) https://www.etsi.org/deliver/etsi_ts/119100_119199/11917201/01.01.01_60/ts_11917201v010101p.pdf
[XAdES_SIGN]	ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures" https://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.01.01_60/en_31913201v010101p.pdf

2 EXIGENCES CONCERNANT L'APPLICATION DE VERIFICATION

L'application de vérification de signature est sous la responsabilité de l'AIFE.

La sécurité de l'application et du système d'information mis en œuvre pour le service de vérification est auditée dans le cadre de l'homologation de sécurité du service.

3 PARAMETRES METIER (BSP)

Remarque : le terme « BSP » correspond au terme « Business Scoping Parameters » de [SIGN_POLICY_TOC].

3.1 Paramètres relatifs au cas d'usage

3.1.1 BSP (a) : Processus de vérification de signature

Le service de vérification de signature est disponible via les interfaces suivantes :

- Une page Web, accessible librement, où l'utilisateur soumet une signature à vérifier (et, en cas de signature détachée, le document original signé) et obtient en retour un rapport affiché sur le site et téléchargeable sous forme PDF ;
- Une API, accessible sur le portail PISTE aux applications enregistrées et authentifiées, où une application soumet une signature à vérifier (et, en cas de signature détachée, le document original signé) et obtient en retour un rapport au format XML et/ou au format PDF selon sa demande.

Le service de vérification de signature traite la vérification d'un seul document à la fois. Lorsque l'utilisateur souhaite vérifier plusieurs documents, il doit invoquer le service plusieurs fois consécutivement : chaque document est traité unitairement et indépendamment des documents précédemment vérifiés.

Dans un document, le service peut détecter plusieurs signatures. Dans ce cas, le service vérifie chacune de ces signatures indépendamment, et sans garantir aucun ordre de traitement de celles-ci. Le rapport produit indiquera le rapport de validation de chaque signature identifiée.

Lorsque la vérification du document soumis par l'utilisateur a déjà été réalisée dans la même journée ou que le service n'est pas en mesure de déterminer si le certificat est toujours valable, le service renvoie le rapport précédemment généré sans effectuer de nouvelle vérification.

Si une signature du document soumis n'est pas considérée valide par le service et que la même signature de ce même document a déjà été vérifiée auparavant par le service et était valide à ce moment-là, alors le service renvoie, en sus du rapport généré pour la nouvelle vérification, le rapport précédent indiquant le statut valide.

3.1.2 BSP (b) : Données signées

Le service accepte exclusivement en entrée les signatures au format XAdES (voir [XAdES_SIGN]) ou PAdES (voir [PAdES_SIGN]). Parmi les signatures de type XAdES, le service ne traite que les signatures XAdES enveloppées ou détachées (dans ce dernier cas, il n'y a pas de restriction sur le type du document original signé).

Lorsque le document soumis au service n'est pas conforme à l'un de ces formats, le service renvoie une erreur et aucune vérification de signature n'est effectuée.

Dans tous les cas, la taille du document signé est limitée à une volumétrie maximale de 10 Mo.

3.1.3 BSP (c) : Lien entre les données signées et les signatures

Le lien entre les données signées et les signatures dépend du format du document soumis au service :

- La signature est au format PAdES
  Dans ce cas, la ou les signatures sont incluses dans le document PDF soumis, conformément au standard PAdES. Le service est conçu pour la vérification de signature portant sur la totalité du document PDF (y compris les signatures potentiellement déjà présentes).
- La signature est une signature détachée au format XAdES
  La signature détachée contient une ou plusieurs signatures portant sur un unique document (au format quelconque) fourni au service concomitamment à cette signature.
- La signature est une signature enveloppée au format XAdES
  La signature est présente dans le document XML soumis au service et s'applique à des données incluses dans ce document.

Pour les signatures citées ci-dessus, le service traite les signatures conformes aux standards eIDAS, pour les niveaux XAdES ([XAdES_SIGN]) ou PAdES ([PAdES_SIGN]) suivants :

- Baseline-B
- Baseline-T
- Baseline-LT
- Baseline-LTA

3.1.4 BSP (d) : Population cible

Le service de vérification de l'AIFE est proposé sur un site internet libre d'accès, ainsi que sur le portail PISTE sur lequel les applications utilisatrices doivent avoir été enregistrées selon les modalités standards propres à ce portail.

3.1.5 BSP (e) : Responsabilités quant à la validation et l'extension de signature

L'utilisateur du service de vérification s'engage à :

- Fournir un document ne contenant aucune bombe logique (virus, malware, etc.) ;
- Dans le cas d'une signature détachée, fournir le document original associé à la signature détachée.

Le service de vérification :

- Effectue une vérification technique de la signature, en s'assurant de son intégrité et de la validité des certificats de signature dans le contexte du service. Le service n'effectue aucune vérification sur le contenu des données signées ni sur la valeur métier ou juridique des signatures trouvées ;
- S'appuie sur les listes de confiance mises à disposition par les organes de contrôle européens (conformément au règlement eIDAS) et sur les informations de révocation publiées par les autorités de certification impliquées. Si l'une des ressources nécessaires n'est pas disponible, le service est dans l'incapacité de conclure sur le statut d'une signature.

Le service de vérification ne propose aucune fonctionnalité d'extension de signature.

3.2 Paramètres d'origine juridique/légale/réglementaire

3.2.1 BSP (f) : Nature juridique des signatures

Les signatures traitées par le service sont des signatures ou des cachets qualifiés ainsi que des signatures ou des cachets avancés réalisés avec des certificats x509. Le support de la clé privée de signature ou de cachet

n'est pas contraint, ce peut être un dispositif qualifié de création de signature ou de cachet, ou un dispositif non qualifié, matériel ou logiciel.

3.2.2 BSP (g) : Engagement des signataires

Le service n'impose aucune exigence quant aux engagements pris par les signataires pour les documents soumis à la vérification.
Lorsque les propriétés de la signature comprennent un attribut relatif à l'engagement (« commitmentType » ou « Reason ») du signataire, le service de vérification restitue cette information dans le rapport de validation.

3.2.3 BSP (h) : Garanties sur la date des signatures

Le service de vérification traite aussi bien les signatures horodatées que non horodatées, et n'apporte aucune garantie sur la fiabilité de ces dates.

Afin de vérifier la validité du certificat de signature (expiration, révocation) et de s'assurer de la qualification du certificat (périodes de qualification du service de certification), le service de vérification détermine une date présumée de signature, qui est :

- Lorsque la signature est horodatée, la date présumée de signature est la date du jeton d'horodatage apposée sur la signature. Ceci est vrai quel que soit le service d'horodatage, qu'il soit qualifié eIDAS, RGS ou non.
- Lorsque la signature n'est pas horodatée, la date présumée de signature est celle indiquée par le signataire dans la signature, si elle est bien présente.
- A défaut de jeton d'horodatage et de date renseignée dans la signature, la date présumée de signature est la date de la requête au service de vérification.

Le rapport de vérification précise dans tous les cas, les informations trouvées dans la signature (date indiquée par le signataire et date du jeton d'horodatage). Le service de vérification ne fait aucune présomption sur la fiabilité de cette date. Il revient à l'utilisateur du service de juger de la vraisemblance de la date utilisée, à partir de la date utilisée et du niveau de qualification de l'éventuel service d'horodatage utilisé.

Lorsque le service renvoie à l'utilisateur un rapport généré récemment par le service pour le même document (cf. §3.1.1), alors le statut indiqué dans le rapport a été évalué selon la date présumée de signature du précédent appel et non celui de l'appel courant.

3.2.4 BSP (i) : Formalités de signature et de vérification

Le service de vérification n'effectue aucune vérification et n'a aucune exigence sur le processus de signature utilisé par le signataire des documents soumis au service.

Les utilisateurs du service de vérification doivent être informés de façon claire, et avant l'utilisation du service, des fonctionnalités, contraintes et limites de celui-ci. En particulier :

- Le présent document de politique est accessible librement (cf. §1.3.4) ;
- Le site Web donnant accès la fonction de vérification de signature présente les objectifs et limites du service ;
- Les responsables des applications connectées à l'API du service de vérification sont informés de cette politique, s'engagent à la respecter et à informer les utilisateurs finaux qui auraient accès au service de vérification via leur application.

Le processus de vérification d'un document comprend les étapes suivantes :

- Identification des signatures présentes dans le document soumis ;
- Pour chaque signature :
  - Vérification de l'intégrité des données signées ;
  - Vérification de la validité du certificat du signataire :
    - Vérification de la chaine de certification du certificat;
    - Vérification de l'utilisation du certificat dans sa période de validité ;
    - Vérification de la non révocation du certificat (via les CRL ou les jetons OCSP)
  - Vérification du jeton d'horodatage s'il est présent
    - Vérification de l'intégrité des données horodatées

- Vérification de la chaîne de certification du certificat du service d'horodatage ;
- Vérification de l'utilisation du certificat du service d'horodatage dans sa période de validité ;
- Vérification de la non révocation du certificat du service d'horodatage (via les CRL ou les jetons OCSP).

La validité d'une chaine de certification est réalisée en prenant en compte des Autorités de Certification sélectionnées par l'AIFE, comme indiqué au §3.3.2. Lorsque le statut de révocation d'un certificat ne peut pas être déterminé (indisponibilité des CRL et du service OCSP publiés par l'Autorité de Certification), le service de vérification l'indique dans le rapport produit.

3.2.5 BSP (j) : Pérennité des signatures

Le service de vérification n'impose aucune exigence concernant la pérennité des signatures. La signature est vérifiée en utilisant une daté présumée de signature détaillée au §3.2.3.

3.2.6 BSP (k) : Archivage

Le service de vérification ne conserve aucun document soumis pour vérification.

Les rapports de validation produits par le service de vérification sont conservés pour une durée minimale de 7 ans afin de pouvoir restituer ce rapport pour une nouvelle vérification du même document (voir §3.1.1).

3.3 Paramètres relatifs aux moyens et intervenants impliqués dans le cycle de vie des cachets

3.3.1 BSP (l) : Identité des signataires

Le service de vérification n'impose aucune exigence sur l'identité des signataires ni sur leurs rôles.

L'identité des signataires est indiquée dans le rapport de validation, sa valeur étant le sujet du certificat de signature.

3.3.2 BSP (m) : Niveau de garantie pour l'authentification des signataires

Le service de vérification n'impose pas directement un niveau de garantie pour l'authentification des signataires. Le service vérifie en revanche la politique de certification qui a été suivie pour l'émission du certificat du signataire. Les politiques de certification considérées de confiance sont :

- Les politiques de certification présentes dans une liste de confiance eIDAS (émise par l'un des Etats membres de l'UE) ;
- Des politiques de certification sélectionnées par l'AIFE, par exemple sur leur niveau de sécurité. La liste précise des ces politiques de certification est disponible sur demande.

Le niveau de qualification (eIDAS ou RGS) ou de certification du certificat est indiqué dans le rapport lorsqu'il est connu du service.

Lorsque le certificat du signataire n'est pas émis selon une politique de certification reconnue, le certificat n'est pas considéré comme fiable, et la signature a donc un statut invalide dans le rapport de vérification.

3.3.3 BSP (n) : Dispositif de création de signature

Comme pour le niveau de garantie de l'authentification des signataires, le service de vérification n'impose pas un dispositif spécifique de création de signature mais vérifie la politique de certification qui détermine le ou les dispositifs de signature utilisables. Le dispositif de signature peut donc potentiellement être qualifié ou non, logiciel ou matériel.

Lorsqu'il le peut, le service de vérification indique si le dispositif de création de signature est qualifié ou non, et s'il est matériel ou logiciel.

3.4 Autres paramètres

3.4.1 BSP (o) : Informations supplémentaires associées aux signatures

Le service de vérification n'impose aucune information supplémentaire associée aux signatures.

Le service de signature indique dans le rapport les informations ci-dessous, lorsque celles-ci sont présentes dans la signature et insérées conformément aux standard PAdES et XAdES :

- Localisation de la signature ;
- Politique de signature.

Ces informations sont insérées par la signature à la création de la signature, leur authenticité ne peut pas être vérifiée.

3.4.2 BSP (p) : Mécanismes cryptographiques

Le service de vérification n'impose pas de mécanisme cryptographique spécifique.

Le rapport de vérification indique l'algorithme de la clé privée du signataire ainsi que sa taille.

3.4.3 BSP (q) : Environnement technique

La page Web proposée par le service de vérification est accessible par les principaux navigateurs disponibles sur des configurations standard.
Les contraintes techniques d'accès à l'API sont communiquées aux responsables des applications clientes autorisées à accéder au service.

4 EXIGENCES SUR LES MOYENS TECHNIQUES ET L'IMPLEMENTATION DES STANDARDS

Lorsque cela est nécessaire, les exigences portant sur les moyens techniques et l'implémentation des standards sont directement précisées dans les paragraphes pertinents du §3.

5 AUTRES PROBLEMATIQUES METIERS ET LEGALES

Ces considérations sont régies par les Conditions Générales d'Utilisation du service.

6 AUDITS ET CONFORMITE

Dans le cadre de l'homologation RGS de sécurité du service, l'AIFE a mené une analyse de risques relative au service proposé et mis en place les mesures de sécurité appropriées en relation avec celle-ci.

Des audits de sécurité confirment régulièrement la sécurité du système d'information sous-jacent. Ils permettent à l'Autorité d'Homologation de l'AIFE de prononcer son homologation conformément aux dispositions du RGS [HOMOLOGATION].