|  |
| --- |
| Template de Politique de signature de DOCAPOSTE Trust & Sign  Service de signature générique |

|  |  |
| --- | --- |
| Fichier | DOCAPOSTE\_Template\_PS\_Master.docx |
| Date | 16/01/2023 |
| Référence/version | 0.2 |
| Date d’entrée en vigueur | 16/01/2023 |



**Historique**

|  |  |  |
| --- | --- | --- |
| Version | Auteur | Objet |
| V0.1 | SEALWEB | Version initiale du document. |
| V0.2 | DOCAPOSTE | Revue et validation. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Acronymes**

|  |  |
| --- | --- |
| Acronyme | Définition |
| API | Application Programming Interface |
| CA | Certificate Authority |
| CP | Certificate Policy |
| CRL | Certificate Revocation List |
| CSR | Certificate Signing Request |
| DER | Distinguished Encoding Rules |
| DN | Distinguished name |
| DTS | DOCAPOSTE Trust & Sign |
| IANA | Internet Assigned Numbers Authority |
| OCSP | Online Certificate Status Protocol |
| OID | Object IDentifier |
| PEN | Private Enterprise Number |
| PEM | Privacy-Enhanced Mail |
| QSCD | Qualified Signature and Seal Creation Device |
| RA | Registration authority |
| SIREN | Système d'identification du répertoire des entreprises |
| SN | Serial Number |
| TSU | Time-Stamping Unit |
| WS | Web Service |

Objet

Le présent document modèle, Politique de signature « ***NOM\_SIGNATURE*** » de la plate-forme DOCAPOSTE TRUST & SIGN, contient un modèle de politique de signature qui s’applique aux transactions électroniques entre les partenaires de la société DOCAPOSTE TRUST & SIGN et les clients de ces derniers, signataires des documents.

Ce modèle de politique de signature se veut d’être décliné par le Client de Docaposte pour l’adapter à son contexte et à ses propres processus de signature. Il contient les éléments par défaut qui seront disponibles sur la plateforme DOCAPOSTE TRUST & SIGN. Suivant le cas le document présente des variables que le Client doit définir ou des choix que doit faire le Client.

TABLE DES MATIERES

[1 Présentation 5](#_Toc131683651)

[1 Introduction 10](#_Toc131683652)

[1.1 Champ d’application 10](#_Toc131683653)

[1.2 Identification 10](#_Toc131683654)

[2 Gestion de la politique de signature 11](#_Toc131683655)

[2.1 Publication du document 11](#_Toc131683656)

[2.1.1 Processus de mise à jour 11](#_Toc131683657)

[2.1.2 Circonstance rendant une mise à jour nécessaire 11](#_Toc131683658)

[2.1.3 Prise en compte des mises à jour 11](#_Toc131683659)

[2.1.4 Contact 11](#_Toc131683660)

[2.1.5 Information des acteurs pour donner suite à une mise à jour 11](#_Toc131683661)

[2.1.6 Entrée en vigueur de la nouvelle version et période de validité 12](#_Toc131683662)

[3 Acteurs et rôles 13](#_Toc131683663)

[3.1 Listes des acteurs 13](#_Toc131683664)

[3.2 Rôles et obligations des différents acteurs 13](#_Toc131683665)

[3.2.1 Rôle et Obligation de NOM\_CLIENT 13](#_Toc131683666)

[3.2.2 Rôle et obligations du signataire 14](#_Toc131683667)

[3.2.3 Rôle et obligations de DOCAPOSTE Trust & Sign 15](#_Toc131683668)

[3.2.4 Rôle et obligations des destinataires 17](#_Toc131683669)

[3.3 Limitation de responsabilité de DOCAPOSTE Trust & Sign 17](#_Toc131683670)

[4 Description de l’environnement de signature 18](#_Toc131683671)

[4.1 Caractéristiques techniques de l’environnement de signature 18](#_Toc131683672)

[4.2 Données signées 18](#_Toc131683673)

[4.3 Processus de signature 18](#_Toc131683674)

[5 Caractéristiques des signatures 20](#_Toc131683675)

[5.1 Type de signature 20](#_Toc131683676)

[5.2 Norme de signature 20](#_Toc131683677)

[5.3 Certificat utilisé pour la signature « legacy » 21](#_Toc131683678)

[5.4 Certificat utilisé pour le scellement 21](#_Toc131683679)

[5.5 Date et heure de signature 21](#_Toc131683680)

[5.6 Algorithme de signature 21](#_Toc131683681)

[5.7 Autres caractéristiques 21](#_Toc131683682)

[6 Vérification de la signature 22](#_Toc131683683)

[6.1 Condition pour déclarer valide le fichier signé 22](#_Toc131683684)

[6.2 Procédure de vérification de signature 22](#_Toc131683685)

[6.2.1 Vérification de l’empreinte du document et de la signature 22](#_Toc131683686)

[6.2.2 Vérification de la chaîne de certificats 22](#_Toc131683687)

[6.2.3 Vérification des jetons d’horodatage 23](#_Toc131683688)

[7 Création du fichier de preuve 24](#_Toc131683689)

[7.1 Format et contenu du fichier de preuve 24](#_Toc131683690)

[7.2 Traces contenues dans le fichier de preuve 24](#_Toc131683691)

[7.3 Scellement du fichier de preuve 25](#_Toc131683692)

[7.4 Conservation du fichier de preuve 25](#_Toc131683693)

[8 Modalité d’archivage 26](#_Toc131683694)

[9 Autres aspects 27](#_Toc131683695)

[9.1 Politique de confidentialité 27](#_Toc131683696)

[9.1.1 Informations considérées comme confidentielles 27](#_Toc131683697)

[9.1.2 Communication à des tiers 27](#_Toc131683698)

[9.2 Dispositions juridiques 27](#_Toc131683699)

[9.2.1 Droit applicable 27](#_Toc131683700)

[9.2.2 Propriété intellectuelle 27](#_Toc131683701)

[9.2.3 Données personnelles 27](#_Toc131683702)

[10 Annexes 0](#_Toc131683703)

[10.1 Information sur la PKI Dictao Trust Service 0](#_Toc131683704)

[10.2 Informations sur les services d’horodatage tiers 0](#_Toc131683705)

# Présentation

Le document intégré dans le reste de ce document à partir de la page suivante est la politique de signature à adapter aux exigences et au contexte de *NOM\_CLIENT*.

|  |
| --- |
| Politique de signature de NOM\_CLIENT  Service de signature « *NOM\_SIGNATURE* » |

|  |  |
| --- | --- |
| Fichier | *NOM\_CLIENT* \_PS.docx |
| Date | xx/xx/xxxx |
| Référence/version | 1 |
| Date d’entrée en vigueur | xx/xx/xxxx |



**Historique**

|  |  |  |
| --- | --- | --- |
| Version | Auteur | Objet |
| V1 | *NOM\_CLIENT* | Version initiale du document. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Acronymes**

|  |  |
| --- | --- |
| Acronyme | Définition |
| API | Application Programming Interface |
| CA | Certificate Authority |
| CP | Certificate Policy |
| CRL | Certificate Revocation List |
| CSR | Certificate Signing Request |
| DER | Distinguished Encoding Rules |
| DN | Distinguished name |
| DTS | DOCAPOSTE Trust & Sign |
| IANA | Internet Assigned Numbers Authority |
| OCSP | Online Certificate Status Protocol |
| OID | Object IDentifier |
| PEN | Private Enterprise Number |
| PEM | Privacy-Enhanced Mail |
| QSCD | Qualified Signature and Seal Creation Device |
| RA | Registration authority |
| SIREN | Système d'identification du répertoire des entreprises |
| SN | Serial Number |
| TSU | Time-Stamping Unit |
| WS | Web Service |

Objet

Le présent document modèle, Politique de signature « ***NOM\_SIGNATURE*** » de la plate-forme de signature de *NOM\_CLIENT*, est destiné à s’appliquer aux transactions électroniques entre *NOM\_CLIENT* et les clients de *NOM\_CLIENT*, signataires des documents.

Le présent document décrit le contexte et les propres processus de signature de NOM\_CLIENT basés sur la plate-forme DOCAPOSTE TRUST & SIGN . Il contient les éléments disponibles sur la plateforme de signature.

TABLE DES MATIERES

[1 Présentation 5](#_Toc131683706)

[1 Introduction 10](#_Toc131683707)

[1.1 Champ d’application 10](#_Toc131683708)

[1.2 Identification 10](#_Toc131683709)

[2 Gestion de la politique de signature 11](#_Toc131683710)

[2.1 Publication du document 11](#_Toc131683711)

[2.1.1 Processus de mise à jour 11](#_Toc131683712)

[2.1.2 Circonstance rendant une mise à jour nécessaire 11](#_Toc131683713)

[2.1.3 Prise en compte des mises à jour 11](#_Toc131683714)

[2.1.4 Contact 11](#_Toc131683715)

[2.1.5 Information des acteurs pour donner suite à une mise à jour 11](#_Toc131683716)

[2.1.6 Entrée en vigueur de la nouvelle version et période de validité 12](#_Toc131683717)

[3 Acteurs et rôles 13](#_Toc131683718)

[3.1 Listes des acteurs 13](#_Toc131683719)

[3.2 Rôles et obligations des différents acteurs 13](#_Toc131683720)

[3.2.1 Rôle et Obligation de NOM\_CLIENT 13](#_Toc131683721)

[3.2.2 Rôle et obligations du signataire 14](#_Toc131683722)

[3.2.3 Rôle et obligations de DOCAPOSTE Trust & Sign 15](#_Toc131683723)

[3.2.4 Rôle et obligations des destinataires 17](#_Toc131683724)

[3.3 Limitation de responsabilité de DOCAPOSTE Trust & Sign 17](#_Toc131683725)

[4 Description de l’environnement de signature 18](#_Toc131683726)

[4.1 Caractéristiques techniques de l’environnement de signature 18](#_Toc131683727)

[4.2 Données signées 18](#_Toc131683728)

[4.3 Processus de signature 18](#_Toc131683729)

[5 Caractéristiques des signatures 20](#_Toc131683730)

[5.1 Type de signature 20](#_Toc131683731)

[5.2 Norme de signature 20](#_Toc131683732)

[5.3 Certificat utilisé pour la signature « legacy » 21](#_Toc131683733)

[5.4 Certificat utilisé pour le scellement 21](#_Toc131683734)

[5.5 Date et heure de signature 21](#_Toc131683735)

[5.6 Algorithme de signature 21](#_Toc131683736)

[5.7 Autres caractéristiques 21](#_Toc131683737)

[6 Vérification de la signature 22](#_Toc131683738)

[6.1 Condition pour déclarer valide le fichier signé 22](#_Toc131683739)

[6.2 Procédure de vérification de signature 22](#_Toc131683740)

[6.2.1 Vérification de l’empreinte du document et de la signature 22](#_Toc131683741)

[6.2.2 Vérification de la chaîne de certificats 22](#_Toc131683742)

[6.2.3 Vérification des jetons d’horodatage 23](#_Toc131683743)

[7 Création du fichier de preuve 24](#_Toc131683744)

[7.1 Format et contenu du fichier de preuve 24](#_Toc131683745)

[7.2 Traces contenues dans le fichier de preuve 24](#_Toc131683746)

[7.3 Scellement du fichier de preuve 25](#_Toc131683747)

[7.4 Conservation du fichier de preuve 25](#_Toc131683748)

[8 Modalité d’archivage 26](#_Toc131683749)

[9 Autres aspects 27](#_Toc131683750)

[9.1 Politique de confidentialité 27](#_Toc131683751)

[9.1.1 Informations considérées comme confidentielles 27](#_Toc131683752)

[9.1.2 Communication à des tiers 27](#_Toc131683753)

[9.2 Dispositions juridiques 27](#_Toc131683754)

[9.2.1 Droit applicable 27](#_Toc131683755)

[9.2.2 Propriété intellectuelle 27](#_Toc131683756)

[9.2.3 Données personnelles 27](#_Toc131683757)

[10 Annexes 0](#_Toc131683758)

[10.1 Information sur la PKI Dictao Trust Service 0](#_Toc131683759)

[10.2 Informations sur les services d’horodatage tiers 0](#_Toc131683760)

# Introduction

## Champ d’application

Conformément à l’article 1367 du Code Civil, une signature, qu’elle soit manuscrite ou électronique, « manifeste le consentement des parties aux obligations qui découlent de cet acte. (…) Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. (…) ».

La signature électronique permet donc :

* De garantir l’intégrité des données signées,
* D’identifier celui qui l’appose
* De manifester son consentement aux obligations qui découlent de cet acte de signature et donc assurer la non-répudiation par le signataire des données signées

Le présent document, Politique de signature « *NOM\_SIGNATURE* » s’applique aux transactions électroniques entre les partenaires de la société DOCAPOSTE Trust & Sign et les clients de ces derniers, signataires des documents. Les transactions concernées sont les suivantes :

Présenter ici la liste des types de transactions couvertes chez le Client. Par exemple :

* Signature de contrats bancaires
* Signature de contrats d'assurance
* Validation de formulaires métiers
* etc

Le service de signature « *NOM\_SIGNATURE* » de DOCAPOSTE Trust & Sign correspond à un niveau de signature simple au sens du Règlement eIDAS.

Le présent document, Politique de signature « *NOM\_SIGNATURE* », décrit les conditions du *NOM\_CLIENT* dans lesquelles les documents signés à destination de leurs clients signataires sont produits et signés.

## Identification

La présente politique de signature est identifiée de manière non ambiguë par un OID qui identifie de façon unique le présent document ainsi que le processus qui lui est associé. La présente politique de signature est identifiée par l’OID : OID\_CLIENT

# Gestion de la politique de signature

## Publication du document

La présente politique de signature est publiée à l’adresse suivante :

|  |  |
| --- | --- |
| URL de publication : | URL\_CLIENT (Lien http/https de publication de la Politique de Signature chez le Client) |

### Processus de mise à jour

La Présente Politique de Signature est la propriété de *NOM\_CLIENT*. La mise à jour de ce document est soumise à la relecture de DOCAPOSTE Trust & Sign pour assurer l’adéquation du contenu de ce document avec les spécifications de la plateforme de signature DOCAPOSTE TRUST & SIGN.

### Circonstance rendant une mise à jour nécessaire

La mise à jour d’une politique de signature est un processus impliquant tous les acteurs et faisant l’objet d’une démarche rigoureuse. Il est enclenché essentiellement pour procéder à des modifications importantes, pour prendre en compte de nouveaux besoins, de nouveaux acteurs, améliorer le cadre juridique ou combler des lacunes. La présente politique est réexaminée lors de toute modification majeure des processus de signature chez *NOM\_CLIENT*.

### Prise en compte des mises à jour

Avant toute publication officielle, la politique de signature est validée formellement par *NOM\_CLIENT*. Cette validation est un pré-requis avant la publication du document à jour sur le site indiqué au paragraphe 2.1.

### Contact

Toutes demandes spécifiques sur le service de signature de *NOM\_CLIENT* peuvent être adressées au contact suivant :

|  |  |
| --- | --- |
| *NOM\_CLIENT* - NOM\_SIGNATURE | |
| Personne à contacter | xxx |
| Adresse postale | xxx |
| Numéro de téléphone | xxx |
| Adresse électronique | xxx |

### Information des acteurs pour donner suite à une mise à jour

Lorsqu’une mise à jour a été planifiée, les informations relatives à cette évolution sont mises en ligne sur les lieux de publication. Indépendamment de ce mode de communication, les acteurs peuvent à tout moment se renseigner auprès du point de contact susmentionné pour obtenir plus d’informations.

La publication d’une nouvelle version de la politique de signature consiste à archiver la version précédente et mettre en ligne dans le répertoire prévu à cet effet (voir 2.1), les éléments suivants :

* Document au format PDF (éventuellement scellé électroniquement par un cachet Client, cf 5.4)
* OID du document
* Date d’entrée en vigueur

### Entrée en vigueur de la nouvelle version et période de validité

La nouvelle version de la politique de signature entre en vigueur 15 jours ouvrés après sa mise en ligne et reste valide jusqu'à la publication d'une nouvelle version.

La date d’entrée en vigueur est indiquée explicitement dans la première page du présent document.

# Acteurs et rôles

## Listes des acteurs

Les différents acteurs impliqués dans le processus de signature sont :

* NOM\_CLIENT, client de DOCAPOSTE Trust & Sign, qui prépare le document à signer et réalise les opérations d’enregistrement du signataire ; il peut être l’émetteur du document à signer, mais également un intermédiaire entre l’émetteur du contrat et le signataire (dans le cas d’un courtier par exemple) ;
* DOCAPOSTE Trust & Sign, qui opère la plateforme de signature, ainsi que les différents services de confiance (A.C., A.H.) nécessaires au service de signature ;
* Le signataire ;
* Le destinataire éventuel du document signé.

## Rôles et obligations des différents acteurs

### Rôle et Obligation de NOM\_CLIENT

* Préparation du document à signer

NOM\_CLIENT est en charge de la préparation du document à signer et de sa fourniture, via une interface informatique sécurisée, au service de signature DOCAPOSTE TRUST & SIGN. NOM\_CLIENT est responsable de la constitution, du format et du contenu du document.

* Validation de l’identité du signataire

NOM\_CLIENT est responsable de l’identification du signataire avant de déclencher le processus de signature.

Cette identification repose sur :

A définir en fonction du contexte du Client :

* Informations issues de la base KyC
* Informations auto-déclarées par le signataire (formulaire en ligne)
* Informations vérifiées en face-à-face en agence
* Etc

Les informations transmises par NOM\_CLIENT à la plateforme de signature et qui apparaissent dans le certificat doivent être validées lors de cette phase d’identification par NOM\_CLIENT.

Options ci-dessous à retenir dans le cas où les pages de signature sont présentées par NOM\_CLIENT. Sinon voir le §3.2.3 quand DOCAPOSTE TRUST & SIGN présente les pages de signature.

* Conformité entre le document signé et le document présenté au signataire

Dans le cadre du processus de signature, NOM\_CLIENT s’engage à ne réaliser aucune altération du document en dehors des strictes opérations nécessaires à la création de la signature électronique. En particulier, NOM\_CLIENT s’engage à ce que le document présenté au signataire soit strictement identique au document sur lequel sera réalisée l’opération d’apposition de signature.

* En fonction du contexte client s’il est déterminé que la présentation de l’OID dans les pages de signature est nécessaire:Présentation de l’OID de la politique de signature

Dans le cadre du processus de signature, NOM\_CLIENT s’engage à intégrer aux pages de signature la référence à la présente politique de signature et à son OID.

* Remise du document signé au signataire

En fin de processus de signature, DOCAPOSTE TRUST & SIGN remet à NOM\_CLIENT le document signé qui se charge de le mettre à disposition du signataire.

A définir par NOM\_CLIENT pour les modalités de la remise du document signé au signataire :

* Mis à disposition dans les pages de signatures fournies par Docaposte
* Mis à disposition dans l'espace Client de NOM\_CLIENT
* Envoyé par email
* etc ...

### Rôle et obligations du signataire

* Environnement de signature

L’environnement de signature est mis à disposition par NOM\_CLIENT au travers :

Des pages de signature de Docaposte

De ses propres interfaces visibles du signataire.

De manière transparente pour le signataire, les fonctions de signature sont appelées par ces interfaces.

Il est recommandé au signataire de prendre toutes les précautions nécessaires à la sécurisation de son poste de travail. Cet environnement de signature peut être son matériel personnel, mais il peut être également être mis à disposition du signataire par NOM\_CLIENT ou un intermédiaire sous la responsabilité de NOM\_CLIENT.

* Contrôle des documents signés

Le signataire doit contrôler, avant d’apposer sa signature, les données qui lui sont présentées.

* Moyen d’authentification

Le signataire s’authentifie avant signature, à l’aide d’un moyen d’authentification. Ce moyen d’authentification est opéré par :

DOCAPOSTE TRUST & SIGN,

NOM\_CLIENT avec des moyens d’authentification qui lui sont propres

Lister les moyens d’authentification mis en œuvre :

* OTP SMS
* OTP mail
* Application mobile NOM\_CLIENT
* etc
* Type de certificat utilisé

Option 1 :

Aucun certificat de signature de personne physique n’est généré au nom du signataire. Dans ce cas un certificat de scellement est mis en œuvre (voir 5.4).

Option 2 :

Le certificat de signature de personne physique est un certificat à durée de vie limitée et usage unique fourni par l’autorité de certification Dictao Trust Services (voir 10.1). Le signataire ne peut utiliser que le type de certificat identifié par la présente politique de signature dans le cadre de ce processus de signature.

### Rôle et obligations de DOCAPOSTE Trust & Sign

Option à retenir dans le cas où les pages de signature sont présentées par Docaposte. Sinon voir le §3.2.1 quand NOM\_CLIENT présente les pages de signature.

* Conformité entre le document signé et le document présenté au signataire

Dans le cadre du processus de signature, DOCAPOSTE TRUST & SIGN s’engage à ne réaliser aucune altération du document en dehors des strictes opérations nécessaires à la création de la signature électronique. En particulier, DOCAPOSTE TRUST & SIGN s’engage à ce que le document reçu de NOM\_CLIENT soit strictement identique au document présenté au signataire.

En fonction du contexte client s’il est déterminé que la présentation de l’OID dans les pages de signature est nécessaire:

* Présentation de l’OID de la politique de signature

Dans le cadre du processus de signature, DOCAPOSTE TRUST & SIGN s’engage à intégrer aux pages de signature la référence à la présente politique de signature et à son OID.

* Conformité entre le document reçu de NOM\_CLIENT et le document signé

Dans le cadre du processus de signature, DOCAPOSTE TRUST & SIGN s’engage à ne réaliser aucune altération du document en dehors des strictes opérations nécessaires à la création de la signature électronique. En particulier, DOCAPOSTE TRUST & SIGN s’engage à ce que le document reçu de NOM\_CLIENT soit strictement identique au document sur lequel sera réalisée l’opération d’apposition de signature.

* Protection des clés privées de scellement et de signature personnelle

DOCAPOSTE TRUST & SIGN s’engage à assurer la protection des clés privées du service de scellement et ainsi de la clé de signature personne physique à usage unique, suivant le processus retenu par NOM\_CLIENT, et à les maintenir sous le contrôle du service de signature de DOCAPOSTE Trust & Sign. Pour cela :

* Lorsque la clé privée de signature personnelle est utilisée, elle est créée à l’initialisation de la transaction de signature et est détruite immédiatement après
* Aussi bien la clé privée de signature personnelle que la clé privée de scellement, le cas échéant, ne peuvent être utilisée pour la création de signature ou le scellement du document qu’après la présentation du document à signer et le cas échéant, l’authentification du signataire si NOM\_CLIENT a choisi cette option.
* Horodatage

Option 1 :

Aucun horodatage n’est mis en œuvre.

Option 2 :

DOCAPOSTE TRUST & SIGN appose un horodatage Legacy sur les signatures créées (voir 10.1).

Option 3 :

DOCAPOSTE TRUST & SIGN appose un horodatage (voir 10.2) sur les signatures créées via le service suivant :

Horodatage DOCAPOSTE avec certificat certifié

Horodatage Certinomis qualifié

En cas d’indisponibilité sur ce service d’horodatage, un repli peut être réalisé sur le service d’horodatage Legacy DOCAPOSTE TRUST & SIGN (voir 10.1).

* Vérification de la signature

Option 1 :

Il n’est pas procédé par la plateforme de signature DOCAPOSTE TRUST & SIGN de vérification de signature avant remise du document signé.

Option 2 :

Une vérification de signature est réalisée par la plateforme de signature DOCAPOSTE TRUST & SIGN avant de remettre le document signé.

Option 3 :

Une vérification de signature est réalisée par la plateforme de signature DOCAPOSTE TRUST & SIGN et est utilisée pour créer une signature au format étendu (voir 5.2) avant de remettre le document signé.

* Journalisation et création du fichier de preuve

DOCAPOSTE TRUST & SIGN s’engage à consigner les traces des différentes opérations et appels techniques du processus de signature dans un fichier de preuve de la transaction. Ce fichier de preuve est scellé par DOCAPOSTE TRUST & SIGN pour en assurer l’intégrité.

DOCAPOSTE TRUST & SIGN s’engage à n’opérer aucune altération des traces inscrites dans le fichier de preuve.

Le fichier de preuve est décrit plus en détail dans la section 7.

* Archivage

Les modalité de l’archivage sont sous la responsabilité de NOM\_CLIENT, voir la section 8.

### Rôle et obligations des destinataires

Les destinataires doivent mettre en œuvre les moyens leur permettant de s’assurer de l’origine du document signé, de son intégrité et de l’identité de du signataire.

Pour se faire, les destinataires peuvent mettre en œuvre par eux-mêmes des moyens de vérification des signatures électroniques des informations reçues, en s’appuyant sur les informations fournies dans le présent document.

Les éléments nécessaires mis à disposition sont les suivants :

* OID de la Politique de Signature
* Chaîne d'AC DOCAPOSTE Trust & Sign
* Certificat en cours de validité au moment de la transaction
* Certificat non révoqué au moment de la transaction

## Limitation de responsabilité de DOCAPOSTE Trust & Sign

DOCAPOSTE TRUST & SIGN n’est pas responsable :

* Du contenu des informations signées
* D’une mauvaise utilisation des certificats, ou d’une inadéquation entre le certificat mis-en-œuvre et l’usage auquel il est destiné
* D’une mauvaise utilisation de la plate-forme de signature par le signataire.

Certaines données, notamment les statuts de révocation, sont mis à jour au moins quotidiennement. Par conséquent, il se peut qu’une signature soit déclarée valide si elle est réalisée entre le moment où la demande de révocation a été décidée par DOCAPOSTE TRUST & SIGN et le moment où sa révocation a été publiée par l’autorité de certification et prise en compte par la plate-forme de validation. DOCAPOSTE TRUST & SIGN ne peut être alors tenue responsable de cet état de fait.

# Description de l’environnement de signature

## Caractéristiques techniques de l’environnement de signature

Les serveurs hébergeant la plate-forme de DOCAPOSTE TRUST & SIGN sont protégés selon les normes de sécurité en vigueur en conformité avec les recommandations de la norme ISO 27001. L’accès physique et technique à ces équipements et aux informations confidentielles qui s’y trouvent est contrôlé, par exemple : protection par pare-feu, installation des seuls logiciels utilisés pour effectuer les tâches du service, antivirus, mots de passe non partagés, mise à jour systématique des logiciels, ...

## Données signées

Les données signées par le signataire sont des documents contractuels au format PDF soumis à sa signature par NOM\_CLIENT.

Ces données sont présentées et acceptées par le signataire durant le processus de signature

Les documents PDF peuvent, antérieurement ou postérieurement à la signature, être scellés électroniquement, typiquement par NOM\_CLIENT ou par un tiers autorisé de NOM\_CLIENT, afin de garantir l’origine du document. Les documents pourront également être signés par un cocontractant.

En plus de l’empreinte du document, la signature technique peut contenir différents attributs de signature peuvent être ajoutés à la signature et feront partie des données signées :

| Attribut de signature | Optionnel ou obligatoire | Signification et commentaires |
| --- | --- | --- |
| SignedData.certificates | Obligatoire | Certificat utilisé pour la signature |
| Signature-Policy-Identifier | Optionnel | Identifiant unique de la présente politique de signature, dans le cas où le format EN 319 142 est utilisé |
| Service: provide claimed time of signing | Obligatoire | Date présumée de signature. Il s’agit de la date de signature lue sur le serveur au moment où celle-ci est réalisée. Elle est indépendante de la date fournie éventuellement par un horodatage ultérieur. |
| Location | Optionnel | Champ optionnel indiquant le lieu présumé de signature tel que déclaré par le signataire (par exemple : à Paris) |
| Reason | Optionnel | Champ optionnel permettant d’indiquer des éléments d’engagements complémentaires à la signature (par exemple « lu et approuvé ») |
| ContactInfo | Optionnel | Champ optionnel permettant d’indiquer des éléments de contact complémentaires à la signature (par exemple l’adresse email ou le téléphone du signataire) |

Les champs optionnels ne peuvent être ajoutés que s’ils ont été présentés au signataire.

## Processus de signature

Ce paragraphe peut être complété en intégrant les captures d'écran du processus de signature vu par le signataire

Le processus de signature peut présenter, certaines variations, par exemple, sur le nombre de documents à signer ou la présentation préalable de documents précontractuels. Cependant, l’ensemble des processus obéissent au schéma global suivant :

1. L’application métier de NOM\_CLIENT prépare une enveloppe de signature contenant :
   1. L’ensemble des documents à signer ou présenté pour approbation au signataire ;
   2. Les caractéristiques de l’enveloppe de signature (ordre de présentation des documents, contenu des messages d’approbation) ;
   3. Les caractéristiques du signataire.
2. La plate-forme de signature prépare le processus de signature en s’appuyant sur les éléments de l’enveloppe de signature (préparation des écrans de signature).
3. Lors de la connexion du signataire sur la plate-forme, les écrans lui sont présentés. En particulier, pour chaque document à signer, le document PDF est présenté tel qu’il a été soumis par NOM\_CLIENT (à l’exception d’éventuelles modifications techniques n’altérant pas le fond du document tel que l’ajout du champ de signature, la réalisation d’opérations techniques de mise en forme), et la plate-forme offre la possibilité au signataire de le consulter dans son intégralité.
4. L’application recueille alors explicitement le consentement du signataire par une action explicite et non-ambiguë (typiquement case à cocher d’approbation et clic sur un bouton « Signer »). Le document est alors envoyé au service de signature.
5. En fonction de la modalité définie en 3.2.2, une authentification du signataire est réalisée
6. Si l’authentification a réussi, le service de signature appose les informations du signataire dans le document et génère une signature ou un scellement électronique suivant la modalité définie en 3.2.2, liant ainsi logiquement des données que le signataire utilise pour signer au document lui-même. Si l’authentification du signataire n’est pas établie, le processus ne peut aboutir.
7. En fonction de la modalité définie en 3.2.2, le document signé est ensuite envoyé au service d’horodatage.
8. S’il existe plusieurs signataires, le processus est répété à partir de l’étape 1 pour chacun des signataires
9. Une fois la transaction terminée, le ou les documents signés par l’ensemble des signataires impliqués, ou leurs hachés sont inclus, avec l’ensemble des traces de transaction, dans l’enveloppe de preuve. L’enveloppe de preuve est alors scellée par DOCAPOSTE TRUST & SIGN pour assurer son intégrité.

# Caractéristiques des signatures

## Type de signature

La signature électronique est intégrée au document signé (signature PDF). Si des processus font intervenir de la co-signature ou de la sur-signature, il sera inclus des révisions du document PDF, chaque révision contenant un niveau de signature électronique.

## Norme de signature

L’ensemble des signatures simple créées sont conformes au format PAdES (Signature PDF) suivant la norme EN 319142-1, avec un niveau B-B au minimum.

Conformément à la norme, les propriétés signées contiennent a minima les éléments suivants :

* Le certificat de signature utilisateur ou de scellement
* La date et l’heure de signature (celle-ci s’appuie sur l’heure du service de signature, synchronisé avec l’observatoire de Paris à intervalle régulier et au moins une fois toutes les 24h)

Option 1 :

Le format ISO-31000-1 est utilisé. Ce format ne comporte pas d’option pour inclure la référence au présent document et à l’OID de la présente politique directement dans le format de signature.  
  
En fonction du contexte client s’il est déterminé que la présentation de l’OID dans les pages de signature est nécessaire:

L’OID de la présente politique de signature et une URL permettant d’y accéder sont présentées au signataire dans les pages de signature.

Option 2

Le format PAdES B est utilisé suivant la norme EN 319 142-1. La référence au présent document avec l’OID de la présente politique est intégrée à travers l’attribut de signature correspondant.

En fonction du contexte client s’il est déterminé que la présentation de l’OID dans les pages de signature est nécessaire:

L’OID de la présente politique de signature et une URL permettant d’y accéder sont présentées au signataire dans les pages de signature.

Ces informations peuvent être complétées par d’autres données signées. Voir section 4.2 pour le détail des attributs de signature.

Option 1 :

Le fichier signé est immédiatement horodaté , intégrant la signature électronique et un jeton d’horodatage, permettant de déterminer la date et l’heure exacte de la signature.

* Lorsque le format PAdES B a été retenu :

Le fichier généré est conforme au profile PAdES B-T.

Option 2 :

Le fichier signé est immédiatement horodaté, intégrant la signature électronique et un jeton d’horodatage, permettant de déterminer la date et l’heure exacte de la signature.

Un format étendant le scellement constitutif de la signature est ensuite généré, incluant les informations de révocation du certificat et la chaîne complète de celui-ci.

* Lorsque le format PAdES B a été retenu :

Le fichier généré est conforme au profile PAdES B-LT.

## Certificat utilisé pour la signature « legacy »

Les certificats sont émis pour le certificat utilisateur, par l’AC Dictao Trust Services selon l’une des politiques de certification suivante :

* 1.3.6.1.4.1.54916.1.10.1.1
* 1.3.6.1.4.1.54916.1.10.2.1
* 1.3.6.1.4.1.54916.1.10.4.1
* 1.3.6.1.4.1.54916.1.15.4.1

## Certificat utilisé pour le scellement

NOM\_CLIENT a plusieurs possibilités au sujet du scellement :

Aucun scellement

Scellement DOCAPOSTE Trust & Sign Legacy (OID 1.3.6.1.4.1.54916.1.10.3.1 et 1.3.6.1.4.1.54916.1.10.5.1)

Scellement DOCAPOSTE Certinomis certifié (OID 1.2.250.1.86.2.6.3.22.1)

## Date et heure de signature

La date et l’heure de signature sont antérieures à l’heure donnée par le jeton d’horodatage.

L’horodatage électronique est réalisé par :

DOCAPOSTE Trust & Sign Legacy

DOCAPOSTE Certinomis certifié

DOCAPOSTE Certinomis qualifié

## Algorithme de signature

L’empreinte des données signées est effectuée avec l’algorithme SHA-256 ou un algorithme de robustesse équivalente ou supérieure. Le document est ensuite scellé avec la clé RSA 2048 bits (ou une clé d’une robustesse équivalente ou supérieure) du service de signature simple

## Autres caractéristiques

Afin d’améliorer l’expérience utilisateur, un « visuel » de signature, matérialisant la signature du ou des signataires, est systématiquement ajouté au document PDF et permet l’identification du signataire.

Le contenu de ce visuel :

Le contenu exact du visuel est au choix de NOM\_CLIENT, cocher ou modifier les options appropriées ci-dessous

contient l’identité du signataire

reprend des éléments les plus pertinents de la signature tels que la date et le fournisseur de la solution de signature (DOCAPOSTE TRUST & SIGN)

inclut des éléments visuels tels qu’une image

# Vérification de la signature

Cette section est le pendant de la partie précédente décrivant le processus et le format d’une signature électronique.

## Condition pour déclarer valide le fichier signé

La vérification consiste implicitement à vérifier qu’un document signé est conforme au format décrit, mais certains détails doivent être précisés ici, comme, par exemple, l’utilisation d’un service OCSP ou la liste des autorités de certification reconnues.

## Procédure de vérification de signature

La vérification de la signature porte sur:

* La vérification du respect de la norme de signature, en particulier que la signature créée correspond bien au document signé.
* La vérification du certificat du signataire et de tous les certificats de la chaîne de certification (validité temporelle, statut, signature cryptographique).
* Optionnellement, la vérification du jeton d’horodatage.

### Vérification de l’empreinte du document et de la signature

Cette vérification permet de s’assurer que ni le document, ni la signature, ni le certificat du signataire n’ont été altérés durant le processus de signature. Cette étape consiste à :

* Recalculer le haché des données signées du document PDF et le comparer avec le haché contenu dans la signature. Deux hachés identiques signifient que le document n’a pas été altéré depuis l’apposition de la signature.
* Recalculer le haché des données signées et le vérifier avec la signature cryptographique elle-même à l’aide de la clé publique contenue dans le certificat du signataire. Cette opération permet de s’assurer que les données signées sont bien liées à la clé publique du signataire, et donc à son certificat.

Ces vérifications permettent de s’assurer que :

* Le document est intègre
* Que le document a bien été signé à l’aide de la clé privée du signataire.

La seconde étape de vérification consiste à s’assurer que le certificat du signataire n’était pas révoqué au moment de la création de la signature.

### Vérification de la chaîne de certificats

La vérification du statut des certificats est réalisée en s’appuyant sur les statuts émis par les autorités de certification concernées. La signature est valide vis-à-vis de cette politique de signature si, en plus des éléments de vérification de la section précédente, les éléments suivants sont établis :

* Le certificat est intègre et a bien été émis :
  + pour le certificat cachet QCP de DOCAPOSTE Trust & Sign, par l’AC Certinomis standard G2
  + pour les certificats de cachet Legacy,
    - par l’AC Dictao Trust Services propriété de DOCAPOSTE Trust & Sign selon les OID 1.3.6.1.4.1.54916.1.10.3.1, 1.3.6.1.4.1.54916.1.10.5.1 de certificats de cachet,
  + pour les autres certificats de cachets,
    - par une AC certifié eIDAS suivant un profil de niveau NCP+, QCP ou QCP-QSCD
  + pour les certificats de signature personnelle
    - par l’AC Dictao Trust Services propriété de DOCAPOSTE Trust & Sign selon un des profils
      * 1.3.6.1.4.1.54916.1.10.1.1,
      * 1.3.6.1.4.1.54916.1.10.2.1,
      * 1.3.6.1.4.1.54916.1.10.4.1,
      * 1.3.6.1.4.1.54916.1.15.4.1.
* Le statut du certificat n’est pas révoqué à la date de signature donnée par l’horodatage.
* L’ensemble des certificats de la chaîne de certificats sont valides et non révoqués jusqu’à l’AC Racine Dictao Trust Services

### Vérification des jetons d’horodatage

Si l’option d’horodatage a été retenue au paragraphe 3.2.3, le processus de validation est étendu aux points suivants :

* Vérification que le jeton d’horodatage provient bien du service d’horodatage sélectionné par NOM\_CLIENT
* L’ensemble des horodatages et des certificats de la chaîne d’horodatage sont valides et n’ont pas fait l’objet de révocation au moment de la date d’émission de l’horodatage.

# Création du fichier de preuve

DOCAPOSTE TRUST & SIGN garde des traces de chacune des étapes de la transaction de signature afin de constituer un fichier de preuve.

## Format et contenu du fichier de preuve

Le fichier de preuve est un dossier au format zip contenant :

* L’ensemble des éléments signés ou présentés et validés par les différents signataires (ou leur haché)
* L’ensemble des traces techniques de la transaction
* Un scellement horodaté de l’ensemble des fichiers de son contenu par DOCAPOSTE TRUST & SIGN permettant de garantir son origine et son intégrité

Le fichier de preuve s’appuie uniquement sur des formats ouverts et n’utilise aucune technologie propriétaire.

## Traces contenues dans le fichier de preuve

L’ensemble des traces de la transaction sont conservées dans le fichier de preuve sous forme de fichier XML. Les événements suivants sont tracés :

* Création de la transaction
* Ajout d’un document à l’enveloppe de preuve
* Génération de clé de signature et demande de certificat.
* Signature d’un document ou scellement d’un document
* Ajout d’un horodatage
* Validation d’une signature ou d’un scellement
* Calcul d’un affichage du document
* Accès d’un signataire à la plate-forme de signature
* Authentification d’un signataire (lorsque cette option a été retenue par le partenaire)
  + si l’authentification est prise en charge par DOCAPOSTE TRUST & SIGN, les traces sont automatiquement intégrées
  + si le partenaire de DOCAPOSTE TRUST & SIGN réalise lui-même l’authentification, l’ajout des traces est réalisé par lui au moyen de l’interface DOCAPOSTE TRUST & SIGN mise à sa disposition et sous sa responsabilité. DOCAPOSTE TRUST & SIGN est alors en charge de l’ajout des traces transmises dans le fichier de preuve.
* Acceptation d’un document par le signataire
* Abandon ou fin de la transaction
* Erreur durant la transaction

Le partenaire peut, via l’interface mise à sa disposition par DOCAPOSTE TRUST & SIGN, ajouter tout type de document de son choix dans le fichier de preuve. Cet ajout de fichier se fait sous la responsabilité du partenaire, en particulier dans le respect du Règlement sur les données à caractère personnel.

## Scellement du fichier de preuve

Le scellement du fichier de preuve est réalisé à l’aide d’un certificat de cachet DOCAPOSTE TRUST & SIGN. La signature est au format XAdES détaché.

## Conservation du fichier de preuve

La durée et les conditions de conservation du fichier de preuve sont sous la responsabilité de NOM\_CLIENT .

Décrire les conditions requises par NOM\_CLIENT pour archiver dans un système de son choix ces éléments ou référencer le chapitre 8.

Compléter avec la durée garantie de conservation du document qui doit être cohérente avec la durée de conservation légale nécessaire.

# Modalité d’archivage

Option 1 :

NOM\_CLIENT récupère le fichier de preuve décrit dans la section 7 à la fin de chaque transaction.

* Décrire les conditions mises en œuvre par NOM\_CLIENT pour archiver dans un système de son choix ces éléments

Option 2 :

DOCAPOSTE Trust & Sign conserve pour le compte de NOM\_CLIENT les éléments de preuve décrit dans la section 7 dans un système d’archivage long terme sécurisé pour la durée indiquée en 7.4.

# Autres aspects

## Politique de confidentialité

### Informations considérées comme confidentielles

Les informations suivantes sont considérées comme confidentielles :

* Les données secrètes associées au certificat du signataire (clé privée, mot de passe, code d’authentification),
* Les journaux de l’application
* Les fichiers de preuves générés
* Les documents signés
* Les rapports d’audit sur cette application et sur les différents composants de l’infrastructure.

### Communication à des tiers

Les informations ne sont pas communiquées à des tiers.

## Dispositions juridiques

### Droit applicable

Le présent document est régi par la loi française (remplacer par le pays adapté si NOM\_CLIENT n’est pas une société française).

Toutes contestations et litiges survenant dans l’interprétation et la mise en œuvre du présent document seront soumis à la juridiction des tribunaux de Courbevoie (remplacer cette ville par celle du siège social de NOM\_CLIENT, ou bien d’une autre ville souhaitée).

### Propriété intellectuelle

Tous les logiciels participants à la constitution et à la validation des informations métiers signées sont mis à disposition des signataires par NOM\_CLIENT et pour les API de signature par DOCAPOSTE TRUST & SIGN. Les signataires ne disposent d’aucun droit de propriété intellectuelle sur ces différents éléments.

### Données personnelles

Les processus de signature de NOM\_CLIENT et DOCAPOSTE Trust & Sign sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la Loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et du 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).

# Annexes

## Information sur la PKI Dictao Trust Service

La PKI Dictao Trust Service est un actif de la société Dictao qui était immatriculé au RCS de Paris sous les numéros 429 383 979 et 397 491 184.

Le 2 Janvier 2015 a été réalisée la dissolution avec transmission universelle de patrimoine de la société Dictao à la société Idemia Identity & Security France, société par actions simplifiées, dont le siège social est domicilié au 2 Place Samuel de Champlain, 92400 Courbevoie et immatriculé au RCS de Nanterre, sous le numéro 440 305 282 . Entre 2015 et 2017, la société Idemia Identity & Security France appartenait au groupe Safran et était active sous la dénomination sociale de Safran Identity & Security.

**Le 31 décembre 2021, les activités de signature électronique de IDEMIA ont été cédées à la société DOCAPOSTE Trust & Sign** (société appartenant au groupe DOCAPOSTE), immatriculée au RCS de Créteil sous le numéro 898 993 191, sous le régime juridique des scissions.

Les actifs de Dictao dont la présente PKI, ainsi que les droits et des obligations de Dictao dans le strict respect des conditions contractuelles, ont donc été transférés à Docaposte Trust & Sign.

Les informations concernant cette PKI sont disponibles sur le site http://igc.dictao.com/

## Informations sur les services d’horodatage tiers

Les services d’horodatages suivants peuvent être utilisés par la plate-forme de signature Docaposte Trust & Sign :

* Horodatage Dictao Legacy

Ce service d’horodatage est décrit par la politique d’horodatage publiée ici :  
<http://igc.dictao.com/>

L’OID des certificat d’unité d’horodatage est 1.3.6.1.4.1.54916.1.10.6.1 et l’OID de la politique d’horodatage est 1.3.6.1.4.1.54916.1.20.1.1.

* Horodatage Docaposte Trust & Sign avec certificat d’unité d’horodatage Docaposte Certinomis

Ce service d’horodatage est décrit par la politique d’horodatage publiée ici : <https://pki.trustnsign.docaposte.com/certinomis/index.html>

L’OID des certificats d’unité d’horodatage est 1.2.250.1.86.2.6.5.24.1 et l’OID de la politique d’horodatage est 1.3.6.1.4.1.58052.2.1.3.1.

* Horodatage qualifié Docaposte Certinomis

Ce service d’horodatage est décrit par la politique d’horodatage publiée ici : <https://www.certinomis.fr/nos-certificats-racines/nos-politiques-de-certification>  
  
L’OID des certificats d’unité d’horodatage est 1.2.250.1.86.2.3.3.24.1 et l’OID de la politique d’horodatage est 1.2.250.1.86.5.1.1.1.1