NOM DU CLIENT
PROJET

PROPOSITION TECHNICO-FONCTIONNELLE
CERTSIGN API USER SIMPLE

CertEurope, une société du groupe Oodrive
www.certeurope.fr
26, rue du Faubourg Poissonnière, 75010 Paris – France
Tel : +33 (0)1 45 26 72 00 / Fax : +33 (0)1 45 26 72 01

Table des matières

LE PROJET

Ici il faudra indiquer quel est le contexte :
Environnement métier ?
Qui sont les signataires ?
Quels sont les documents à signer ?
Quels sont les enjeux (probabilité de contestation d'une signature, sommes en jeux, etc.) ?
Ceci pour s'assurer que la signature simple est adaptée au contexte.

LA SOLUTION API SIGNATURE SIMPLE DE CERTEUROPE

Glossaire

API : Interface d'accès programmatique.

Archivage électronique : Un Système d'Archivage électronique fournit un environnement physique et informatique sécurisé garantissant l'intégrité et la pérennité des documents pendant toute la durée de leur conservation. Un tel système est composé à la fois de processus fonctionnels et organisationnels ainsi que de composants logiciels et matériels conformes à la norme NF Z42-013, et permet l'archivage légal (à valeur probante) des documents. Le fournisseur d'un tel service est appelé Tiers-Archiveur.

Authentification : un processus électronique qui vise à vérifier l'identité prétendue du Signataire. Dans un contexte de transaction « à distance », aucun procédé d'authentification n'est fiable à 100%. Cependant, il existe diverses techniques d'authentification permettant d'avoir un niveau de confiance adapté à la criticité des documents à signer.

Certificat électronique : Fichier électronique attestant qu'une bi-clé appartient au Signataire. Il est délivré par une Autorité de Certification. En signant le Certificat électronique, l'Autorité de Certification valide le lien entre l'identité du Signataire et la bi-clé. Le Certificat électronique a une durée de validité limitée au processus de signature et est à usage unique.

> **Autorité de certification (AC)** : Au sein d'un **Prestataire de Service de Confiance (PSC)** , une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSC, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du Certificat électronique), dans les Certificats électroniques émis au titre de cette politique de certification.
>
> **Prestataire de Service de Confiance (PSC)** : personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié.
>
> **Service de Confiance** : un service électronique normalement fourni contre rémunération qui consiste
> - en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'Horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services; ou
> - en la création, en la vérification et en la validation de certificats pour l'authentification de site internet; ou
> - en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services;

Client : Personne morale implémentant le service de Signature électronique dans une application ou un site Web afin de faire signer électroniquement des documents par ses utilisateurs (ci-après dénommés Signataires).

Horodatage électronique : L'horodatage électronique consiste à apposer à un fichier une date fiable sous la forme d'un jeton d'horodatage. Un jeton d'horodatage garantit l'existence du fichier à une date donnée et que le fichier n'a pas été modifié depuis cette date.

OTP (« One Time Password ») : mot de passe à usage unique.

Signataire : Personne physique souhaitant signer électroniquement un document soumis par le Client via son application ou son site Web.

Signature électronique : des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le Signataire utilise pour signer.

Description générale technico/fonctionnelle

CertSign User API Simple est un service (API REST) qui permet à un utilisateur d'un(e) site/application de signer électroniquement un ou plusieurs documents PDF, conformément au niveau SIMPLE de la réglementation eIDAS.

L'API CertSign User API Simple permet :

- la génération, à la volée, d'un Certificat électronique au nom du Signataire,
- la Signature électronique de un ou plusieurs documents PDF, grâce à ce Certificat électronique, éventuellement soumise à la validation d'un code OTP.
- l'Horodatage électronique du document,
- la suppression définitive de la clef privée de Signature électronique,
- le retour des documents signés électroniquement vers le site appelant,
- l'envoi éventuel des documents signés électroniquement pour Archivage électronique à valeur probante.

La documentation d'intégration présente, de manière exhaustive, le fonctionnement l'API de Signature électronique CertSign User API Simple.

La Signature électronique de niveau « simple » permet une grande souplesse au Client, pour l'authentification du Signataire, qui se fait sous son entière responsabilité. A ce titre, le risque d'annulation d'une Signature électronique peut être réduit si le Client s'assure que les informations personnelles (nom, prénom, adresse mail, …) nécessaires à la réalisation de la Signature électronique, appartiennent réellement au Signataire et se ménage toutes les preuves nécessaires.

- **Création de la commande**

Le Client transmet à CertEurope toutes les informations relatives au Signataire : prénom, nom, adresse de messagerie, téléphone portable, afin de créer un dossier de commande de Certificat électronique.

- **Authentification du Signataire**

L'Authentification du Signataire est réalisée par le Client sous son entière responsabilité. La validité de la Signature électronique dépend en grande partie de la faculté du Client à démontrer que le Signataire est bien la personne dont les informations personnelles (nom, prénom, adresse e-mail, numéro de mobile) ont été transmises à CertSign User API Simple pour la réalisation de la Signature électronique.
Pour renforcer la sécurité, il est fortement recommandé d'imposer la saisie d'un code à usage unique (OTP, One Time Password) envoyé par SMS/e-mail au Signataire afin d'autoriser la Signature électronique. Les paramètres de saisie du code sont définis pour chaque Client.
Dans le cadre de la contractualisation en ligne, par exemple, le paiement CB (3D-Secure, non inclus dans l'API), qui assure une Authentification forte, peut être utilisé en lieu et place ou en complément de l'OTP inclus dans l'API de Signature électronique.

Le service OTP inclus dans l'API permet de :

- **Envoyer** un OTP (One Time Password) par SMS ou par mail,
- **Vérifier** un code OTP en regard du numéro de téléphone ou du mail d'un internaute,
- **Authentifier** un code OTP en regard du numéro de téléphone ou du mail d'un internaute

Les codes OTP envoyés peuvent être personnalisés selon une **politique définie**. Ils peuvent :

- Ne servir qu'une fois ou être utilisés plusieurs fois
- Etre supprimés après n tentatives infructueuses
- Etre composés de caractères numériques, alphanumériques, majuscule obligatoire, etc.

Pour chaque Client, il est possible de dédier un ou plusieurs « codes applications » afin de personnaliser :

- L'expéditeur du SMS
- Le texte du SMS

- **Signature électronique**

La Signature électronique est réalisée par CertSign User API Simple exclusivement :

- sur les documents PDF et PDF/A
- au format PADES (PDF Advanced Electronic Signature – Signature électronique enveloppée).

Les documents ne doivent pas contenir des images ayant des zones de transparence.

Une image représentant une signature peut éventuellement être ajoutée sur le PDF en complément de la Signature électronique. L'image de la signature a pour seule fonction de conserver l'impact psychologique de la signature manuscrite. Une signature scannée incluse dans un PDF n'a pas valeur de Signature électronique. L'emplacement de la signature dans le document et le logo qui l'accompagne sont au choix du site Client. La signature ainsi produite peut être affichée directement sur le PDF avec un rendu personnalisé.

- **Horodatage électronique**

Composante non obligatoire de la Signature électronique, CertEurope intègre nativement à chaque Signature électronique, un jeton d'Horodatage électronique.

- **Pour assurer l'intégrité du document** en comparant l'empreinte du document contenu dans le jeton d'Horodatage électronique et l'empreinte du document recalculée. Si les deux sont identiques le document est bien celui qui a été horodaté, il n'a subi aucune modification.
- **Pour assurer l'antériorité**. Le jeton d'Horodatage électronique contient une date et une heure exactes et certifiées pour prouver l'existence du document à partir de ce moment précis.
- **Pour consolider l'opposabilité**. La signature de chaque jeton d'Horodatage électronique par le Tiers de Confiance CertEurope protège de toute contestation liée au temps (l'opposabilité est une propriété qui dépend de l'intégrité des documents dans le temps et de la force de l'Authentification).

- **Visualisation/vérification de la Signature électronique**

Les Signatures électronique PADES sont visualisables et vérifiables directement dans l'outil Acrobat Reader installé de manière standard sur la plupart des postes de travail ou téléchargeable gratuitement. Le panneau « signature » comporte une vue de synthèse et les détails garantissant l'intégrité du document, la validité de la Signature électronique, l'Horodatage électronique ainsi que les mentions légales.

Les Signatures électroniques sont reconnues par Adobe. Par conséquent, elles sont présentées comme étant valides lors de l'affichage dans un navigateur avec ses paramètres « par défaut » (c'est-à-dire dans le cas d'une installation récente de Windows 7, IE 8+ ou Firefox 10+ ou Chrome 1+, Adobe Acrobat Reader, etc …). L'affichage des détails (panneau signatures) inclut la date et l'heure de la Signature électronique.

La vérification des Signatures électroniques réalisées peut être effectuée avec ou sans connexion aux services CertEurope. En effet, la Signature électronique au format PDF étant complètement intégrée au fichier PDF, les outils d'Adobe, Reader ou Acrobat, sont capables d'effectuer cette vérification. Les listes de révocation des Certificats électroniques étant ajoutées à la Signature électronique, la vérification peut même être réalisée si l'outil Adobe utilisé n'arrive pas à joindre les points de distribution des listes de révocation des Certificats électroniques.

- **Archivage électronique à valeur probante**

En option, CertSign User API Simple permet de déposer les documents signés et les dossiers de preuve dans un service d'Archivage électronique à valeur probante et de conservation légale. Il s'agit du coffre-fort électronique de CDC Arkhinéo (filiale de la Caisse des Dépôts et Consignations). Dans le cadre de la signature simple, le contenu des dossiers de preuve est entièrement à la charge du Client (voir préconisations plus loin).
Il est possible d'y retrouver facilement, via l'interface web de CDC ARKHINEO, les dossiers archivés grâce à un identifiant fourni lors des requêtes de signature. L'infrastructure de gestion de preuve permet une traçabilité totale, et notamment de faire le lien entre le dossier de preuve stocké dans le coffre-fort électronique et les documents électroniques signés.
Si l'Archivage électronique est activé, il est possible de récupérer en toute autonomie, via l'interface CDC ARKHINEO, les documents signés. Pour récupérer les dossiers de preuve, il est nécessaire d'en faire la demande auprès des services CertEurope.

En cas de non-reconduction du service de mise en archive des documents, le Client pourra disposer d'une prestation de maintien en archive et de consultation/récupération des données (à définir lors de la rupture des dépôts).
En cas de rupture définitive du contrat d'Archivage électronique des documents, les données pourront être restituées directement au Client. Enfin, en cas de défaillance de CertEurope, les données seront également récupérables auprès du Tiers-Archiveur, la société CDC Arkhineo.

Valeur probatoire de la Signature électronique de niveau « simple » (eIDAS)

- **Contexte réglementaire**

EIDAS, article 3, définition de la signature électronique :
Signature électronique : *« des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le Signataire utilise pour signer. »*

EIDAS article 25, valeur probatoire de la signature de niveau simple :
« L'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée. »

Le procédé de Signature électronique mis en œuvre permet de réaliser une signature dite « simple » au sens du règlement européen (eIDAS) et n'est pas présumé fiable. Mais l'écrit signé ainsi sous forme électronique ne pourra être refusé en justice au titre de preuve dès lors que le procédé permet d'identifier le Signataire et de garantir le lien avec l'acte signé. En cas de contestation, il est nécessaire de prouver la fiabilité du procédé de Signature électronique utilisé.

- **Contexte d'utilisation**

Les conditions permettant de donner une valeur probatoire à la signature simple (eIDAS) :

- La bonne Authentification du Signataire,
- Une Signature électronique opérée via la génération d'un Certificat électronique par un Tiers de Confiance.
- La constitution et l'Archivage électronique d'un dossier de preuve capable de démontrer l'authenticité des documents et des Signataires, le consentement du Signataire et de tracer les évènements.

Il est impératif d'encadrer l'utilisation du service de Signature électronique. Ainsi, le contexte d'utilisation doit être clairement explicité :

- L'identification du Signataire incombe au Client.
- L'identification du Signataire s'appuie exclusivement sur les informations fournies par le Client.
- CertEurope peut compléter l'Authentification du Signataire par le Client, en envoyant un code OTP au Signataire.
- CertEurope s'engage à la délivrance et à l'opération de signature sur la base des éléments communiqués par le Client.
- CertEurope met à disposition du Client, le document ainsi signé,
- CertEurope s'engage à la conservation des preuves techniques liées à ces opérations
- En option, la conservation des documents et dossiers de preuve peut s'effectuer dans un coffre-fort à valeur probante de la société Arkhinéo.

- **Gestion de la preuve**

Le risque d'annulation d'une Signature électronique simple peut être réduit si le Client :

- s'assure que les informations personnelles (nom, prénom, adresse mail, numéro de téléphone) nécessaires à la réalisation de la signature sont exactes et appartiennent réellement au Signataire,
- et se ménage toutes les preuves nécessaires.

Pour organiser la preuve, il convient de :

- Définir un chemin de preuve
- Constituer et archiver un dossier de preuve

Chemin de preuve

Il conviendra de fiabiliser l'identification de chaque personne s'apprêtant à signer un document, en constituant un faisceau de preuves. Pour collecter ces éléments de preuves, une technique consiste à mettre en œuvre ce que nous appelons « un chemin de preuve ».

Le chemin de preuve est un processus formaté et systématique ayant pour objectifs de :

- collecter un maximum d'éléments de preuve permettant d'Authentifier le Document et son/ses Signataire(s)
- durcir le mécanisme de contractualisation en ligne afin de dissuader la souscription de visiteurs malveillants ou irresponsables

Moyens :

- journalisation, Horodatage électronique et conservation des actions de la plateforme et de chaque Signataire identifié,
- mise en œuvre du protocole sécurisé de réalisation de la signature : confirmation d'identité via sms ou courriel, système de cases à cocher engageant chaque Signataire à déclarer avoir pris connaissance du document à signer, système obligeant le Signataire à visualiser chaque page du document à signer.
- conservation et Archivage électronique du document et du chemin de preuve associé au sein du Coffre-fort électronique.

En pratique

Voici les bonnes pratiques dans le cadre du chemin de preuve afin de consolider au maximum les faisceaux de preuve d'Authentification du Signataire :

Action	**Accès à l'interface de signature** Le Signataire se connecte à un compte (HTTPS) OU le Signataire reçoit un mail qui l'invite à cliquer sur un lien qui l'amène sur l'interface de signature (HTTPS).
Gain (sécurité)	Si les données d'identification associées au compte utilisateur (ou à l'URL du lien dans le mail) ont été vérifiées, cela augmente la force de l'authenticité de la Signature électronique. Tracer le cheminement permet de montrer que le Signataire est venu signer volontairement.
Sinon	N'importe qui peut signer, ce procédé n'apporte aucune valeur juridique.

Action	**Lecture intégrale des documents (pour signature et/ou information)** L'interface de Signature électronique présente tous les documents finalisés que le Signataire doit lire, soit pour signature, soit pour information (conditions générales). Pas de Signature électronique sur la base d'un formulaire.
Gain (sécurité)	L'impossibilité de signer tant que le Signataire n'a pas scrollé toutes les pages de tous les documents jusqu'en bas permet d'apporter la preuve que le Signataire a pris connaissance de tous les documents avant de signer, et donc qu'il a signé en toute connaissance de cause.
Sinon	Il ne sera pas possible de prouver que le Signataire a signé en toute connaissance de cause.

Action	**Expression du consentement** L'interface de Signature électronique présente, en dessous des documents à signer et/ou à côté du bouton [SIGNER], des cases à cocher pour exprimer explicitement le consentement : -« Je certifie avoir pris connaissance des conditions générales d'utilisation du service de signature.» -« Je déclare avoir lu l'intégralité du contrat. » -« En cliquant sur le bouton SIGNER ci-dessous, je reconnais avoir compris la portée de mon engagement contractuel vis-à-vis de... » Un bouton [REFUS] se présente à côté du bouton [SIGNER] pour donner au Signataire la possibilité de quitter le processus de signature en cas de non-consentement.
Gain (sécurité)	L'impossibilité de signer tant que le Signataire n'a pas coché toutes les cases permet d'apporter la preuve que le Signataire a signé en toute connaissance de cause. Supprime le risque de click par erreur.
Sinon	Il ne sera pas possible de prouver que le Signataire à signer en toute connaissance de cause.

Action	**Authentification à double facteur (OTP)** Après avoir cliqué sur le bouton [SIGNER], le Signataire reçoit un code OTP par SMS ou e-mail (que le Client connait et a vérifié), qu'il doit renseigner sur l'interface de Signature électronique. Cette action est nécessaire pour que la Signature électronique s'opère.
Gain (sécurité)	Conforte l'Authentification forte du Signataire
Sinon	Il ne sera pas possible de prouver l'Authentification du Signataire.

Action	**Mise à disposition des documents signés** Le Signataire est informé du bon déroulement de la Signature électronique ET les documents signés lui sont restitués.
Gain (sécurité)	Permet aux Signataires de porter réclamation dans un délai à définir en cas de désaccord sur le contenu des documents signés et/ou la Signature électronique elle-même, pour une gestion à l'amiable.
Sinon	Le Signataire peut répudier la signature en cas de contentieux

Action	**Archivage électronique des documents** Les documents sont archivés sur un système d'Archivage électronique à valeur probante
Gain (sécurité)	Supprime le risque de perte des documents et permet d'apporter une preuve complète d'intégrité en cas de contentieux.
Sinon	Risque de perte du document. Limite la preuve d'intégrité du document.

Dossier de preuve

Le dossier de preuve est l'ensemble des éléments de preuve collectés pour :

- assurer l'intégrité des documents
- assurer l'identité du/des Signataire(s)
- tracer les actions du/des Signataires et de la plateforme, de la connexion au site à la récupération des documents signés en passant par le dispositif de consentement.

En pratique

L'intégrité des documents est assurée par les processus :

- de Signature électronique et Horodatage électronique qui prouvent l'état d'un document à une date et une heure donnée
- d'Archivage électronique à valeur probante qui garantit la conservation du document dans le temps

L'ajout, dans le dossier de preuve, du/des document(s) présentés pour signature par la plateforme permet de consolider la preuve d'intégrité.

L'Authentification se faisant à distance, elle ne peut pas être assurée à 100%. Il est donc recommandé de collecter des faisceaux d'éléments d'identification convergents :

- IP du poste utilisé pour signer
- Login de connexion à l'espace client HTTPS
- Données d'identification utilisées pour la Signature électronique (nom, prénom, e-mail, mobile)
- Confirmation de transaction CB, le cas échéant
- Données utilisées pour l'envoi du code OTP (e-mail ou mobile)

Les traces techniques permettent de d'établir les faits (connexion, parcours, consentement, signature, récupération des documents signés). Elles peuvent contenir les traces générées par le serveur et/ou l'application :

- de connexion et de navigation vers l'interface de Signature électronique.
- du recueil du consentement :
  - tous les documents (à signer et pour information) ont été scrollés jusqu'en bas
  - tous les critères d'acceptation ont été cliqués
  - le bouton [SIGNER] a été activé suite aux actions précédentes puis cliqué
- d'envoi et de saisie du code OTP sur l'interface de Signature électronique
- des requêtes de Signature électronique
- références de la transaction (celles de la plateforme et de CertEurope)
- de confirmation de Signature électronique et de mise à disposition des documents signés
  - traces des mails et/ou de des fonctions d'affichage sur l'interface.

Ces traces peuvent être agrégées dans un fichier PDF et/ou XML par exemple. Le PDF permet un accès facile à des éléments de preuve facilement interprétables. Le XML permet de mettre à disposition des données plus précises et complètes. En cas de litige, CertEurope fournit une attestation de délivrance de Certificat électronique et de réalisation de Signature électronique. Cette attestation viendra compléter le Dossier de preuves.

Cinématique de l'API CertSign User API Simple

La documentation d'intégration présente, de manière exhaustive, le fonctionnement l'API de Signature électronique CertSign User API Simple. Pour mieux appréhender la documentation technique, la cinématique d'appel de l'API est présentée ci-dessous. L'implémentation de l'API doit être effectuée en toute connaissance des bonnes pratiques présentées plus loin dans le chapitre *Gestion de la preuve*.

URL du service (bac à sable) : https://sign-sandbox.certeurope.fr

- **Créer une commande aves les informations liées au Signataire**

Fonction *createEphemeralOrder* **POST** /ephemeral/orders

Cette fonction consiste à créer un dossier de commande pour le Signataire. Pour créer la commande, le Client doit renseigner les informations personnelles du Signataire (nom, prénom, e-mail, mobile). Le service de signature rend l'identifiant de la commande ainsi que son statut.

En entrée :	**En retour :**
Données d'identification du Signataire Dossier de preuve (facultatif) Activation OTP ou non (fortement recommandé) Identifiant Client de la commande	Identifiants de la commande Statut de la commande

- **Récupérer le statut de la commande**

Fonction *getOrderStatus* **GET** /ephemeral/orders/?id=1555544&externalId=EZAA11

Cette fonction permet au Client de vérifier à tout moment le statut de ces dossiers de commandes. Il suffit d'indiquer le numéro de commande retourné par le service ou bien celui qu'il a renseigné lors de la création de commande.

En entrée :	**En retour :**
Identifiants de la commande	Statut de la commande

- **Annuler une commande**

Fonction *deleteOrder* **DELETE** /ephemeral/orders/?id=1555544&externalId=EZAA11

Avant la phase de génération su certificat à usage unique, le Client peut demander l'annulation d'un dossier de commande.

En entrée :
Identifiants de la commande

- **Ajouter des documents**

Fonction

- *createEphemeralSignatureRequest* (sans OTP)
  POST /ephemeral/signatures?orderRequestId=1555544&externalOrderRequestId=EZAA11
- ou *createTriggeredEphemeralSignatureRequest* (avec OTP)
  POST /ephemeral/trigger/signatures?orderRequestId=1555544&externalOrderRequestId=EZA1

Ajout de 1 ou plusieurs documents à signer.

En entrée :	En retour :
Identifiants de la commande Liste : - Identifiant Client du fichier (requête de signature - facultatif) - Document à signer (présenté en base 64) - Données signature visible (facultatif) : position, texte, image - Données archivage à valeur probante (option)	Liste (pour chaque fichier en entrée) : - Identifiants de la commande - Identifiants des fichiers (requête sign.) - Statut du fichier (requête sign.)

- **Déclencher l'envoi de l'OTP (si l'OTP est demandé)**

Fonction *validateTriggeredEphemeralOrderRequest*
POST */ephemeral/trigger/signatures/validate/?*orderRequestId=1555544&externalOrderRequestId=123

Le Client doit afficher les documents à signer et recueillir le consentement du Signataire avant de déclencher l'envoi du code OTP en appelant cette fonction.

En entrée :
Identifiants de la commande

- **Déclencher le processus de signature**

Fonction
- *signEphemeralOrderRequest* (sans OTP)
  POST */ephemeral/*signatures/sign?orderRequestId=1555544&externalOrderRequestId=123&mode=SYNC
- ou *signTriggeredEphemeralOrderRequest* (avec OTP)
  POST */ephemeral/trigger/*signatures/sign?orderRequestId=1555544&externalOrderRequestId=123&mode=SYNC

Le Client doit permettre au Signataire de renseigner le code OTP qu'il vient de recevoir sur son téléphone ou sa boite aux lettre électronique. L'opération de Signature électronique se fait sous réserve que le code OTP soit correct. S'il s'agit du mauvais code, le Client reçoit une erreur. Le nombre de saisie possible et la durée de validité sont configurables.

En entrée :	En retour :
Identifiants de la commande Code OTP reçu (si l'OPT est demandé)	Liste (pour chaque fichier de la commande) : - Identifiants de la commande - Identifiants des fichiers (requête sign.) - Statut des fichiers (requête sign.)

- **Récupération d'un document signé**

Fonction *getSignatureRequestStatus* GET */ephemeral/*signatures/?id=1555544&externalId=EZAA11

Cette fonction permet de récupérer un document signé, ou à défaut, le statut du processus de signature.

En entrée :	En retour :
Identifiants du fichier (requête de signature)	Identifiants du fichier (requête de signature) Identifiants de la commande Statut du fichier (requête de signature) Document signé (base 64)

Process

- **Demande d'ouverture d'un compte de test**

A réception de la fiche d'ouverture de compte de test préalablement remplie par le client, les services de CertEurope :

- mettent à disposition du Client un environnement de test, ainsi que toute la documentation nécessaire,
- transmettent un code identifiant pour le Client,
- transmettent un certificat d'authentification serveur afin de permettre l'authentification du Client sur le serveur de recette.

- **Demande d'ouverture d'un compte de production**

L'accès à l'environnement de production nécessite la signature d'un contrat accompagné :

- des CGU CertSign et CGV CertEurope (et CGU de l'Option d'Archivage électronique le cas échéant),
- du présent document

A réception des éléments précités, les services de CertEurope :

- transmettent un code identifiant pour le Client,
- transmettent un certificat d'authentification serveur afin de permettre l'authentification du Client sur le serveur de production,
- Autorisent les IP fournies par le Client.

Tableau des fonctionnalités

LISTE DES FONCTIONNALITES	INCLUS	OPTION
Réunion de cadrage	**X**	
Livraison d'un environnement de qualification et de la documentation technique	**X**	
Accompagnement à la configuration	**X**	
Personnalisation du contenu et de la position de la signature visible	**X**	
Délivrance d'un Certificat électronique au nom du Signataire	**X**	
Opération de Signature électronique	**X**	
Intégration d'un jeton d'Horodatage électronique	**X**	
Vérification d'identité et déclenchement de la Signature électronique par envoi d'un OTP (SMS ou e-mail)		**Gratuit**
Suppression de la clé privée du Certificat électronique	**X**	
Logs applicatifs	**X**	
Archivage des logs applicatifs dans section CertEurope	**X**	
Archivage électronique à valeur probante dans section dédiée (CDC Arkhinéo)		**Payant**