Certificat et Signature électronique

by LegalBox

Certificat et Signature électronique

Table des matières :

1. Qu’est-ce qu’une signature électronique

> « ***La signature électronique consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache.*** *La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat (Décret 2001-272 du 30 Mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique).* »

Source :
http://www.marche-public.fr/Marches-publics/Definitions/Entrees/Dematerialisation/Signature-electronique.htm

La signature électronique a donc la même valeur probatoire qu’une signature papier.

La signature électronique est un ensemble de données numériques permettant l’identification d’un auteur et l’intégrité du document signé.

Pour être équivalente à la signature manuscrite, la signature électronique doit être sécurisée, avoir été créée par un dispositif sécurisé de création de signature et vérifiée par l'utilisation d'un certificat électronique qualifié délivré par des prestataires de services de certification électroniques qualifiés.

(source : ANSSI)

2. Qu'est-ce qu'un certificat électronique ?

> « *Un certificat de signature électronique est un* ***document sous forme électronique*** *qui a pour but* ***d'authentifier l'identité de la personne*** *signataire (carte d'identité),* ***l'intégrité des documents échangés*** *(protection contre toute altération) et* ***l'assurance de non-répudiation*** *(impossibilité de renier sa signature).* »

(source : http://www.marche-public.fr/Certificat-signature-electronique.htm)

Le certificat électronique est l'élément qui vous permettra de réaliser une signature électronique et vous garantira la valeur légale du document signé.

Un certificat électronique est composé de 3 éléments indispensables :

- Informations factuelles:

› Identité du titulaire

› Organisation du titulaire

› Date de validité du certificat

› Identité de l'autorité de certification

› Fonctionnalités autorisées du certificat

› Lien vers la politique de certification

› Lien vers la liste des certificats révoqués

- La clé privée
- La clé publique

Un certificat électronique est délivré par une autorité de certification. Le certificat est signé par l'autorité de certification, avec sa propre clé privée.

Les certificats électroniques sont classés selon trois niveaux :

- Niveau 1 : aucun contrôle de l'identité du détenteur du certificat
- Niveau 2 : L'identification du détenteur est contrôlée sur pièces justificatives
- Niveau 3 : L'identification du détenteur est contrôlée par un rendez-vous physique

Le certificat électronique est disponible sur deux types de support : support logiciel ou support matériel (clé usb ou carte à puce).

Les certificats les plus répandues sont les certificats RGS* et RGS**

- RGS* : Le certificat RGS* est un certificat logiciel. Il est téléchargé et installé sur le disque dur de l'ordinateur.
- RGS** : Le certificat RGS** est un certificat sur support matériel. Le certificat est contenu dans une clé USB ou une carte à puce. Ce support est conseillé dans la plupart des cas au vu de son niveau d'identification et de confidentialité. Si le support est une clé USB, le certificat est stocké sur la clé et protégé par un code confidentiel (transmis par voie postale et personnalisable).

Les prestataires (autorité de certification reconnue) fournissant des certificats électroniques de type RGS* et RGS** (liste non-exhaustive) :

- Certinomis
- Chambersign
- Certeurope
- Almerys
- Click & Trust
- OpenTrust
- Caisse des dépôts et consignations
- Banque de France
- Certigreffe
- DHIMYOTIS
- etc.

3. Gestion de la signature électronique dans le Hub Electronique de Documents

Le Hub Electronique de Document est basé sur une PKI (ou ICP, Infrastructure à Clé Publique) interne, qui permet de faire circuler les documents et garantir la traçabilité, l'horodatage, l'intégrité et la non répudiation des actions.

LegalBox a déployé cette Infrastructure à Clés Publiques interne (ICP) organisé autour d'une Autorité de Certification racine. L'ICP fournit des certificats à des entités secondaires, notamment à une Autorité de Certification intermédiaire « utilisateurs », pour les besoins de certification interne, et émet les certificats des utilisateurs finaux.

A noter : LegalBox n'est pas autorité de certification reconnue mais peut intégrer tout type de certificat (Certinomis, Chambersign, Certeurop, etc.) peu importe le support (logiciel, token, carte à puce, etc.).

Lors de l'action de signature dans le Hub, vous pouvez utiliser l'applet de signature permettant de choisir un certificat externe (ex : certificat sur token usb). Si vous souhaitez utiliser le certificat LegalBox, l'utilisation de l'applet n'est pas nécessaire. Il vous suffit de sélectionner la signature numérique dans le menu d'action :

Pour donner une garantie toujours plus élevée de l'intégrité d'un document, vous pouvez y ajouter des jetons d'horodatage. L'horodatage permet de garantir la non-altération du document et de fournir une preuve d'antériorité. Il certifie donc l'heure de signature.

4. Signature manuscrite scannée et signature numérique dans le Hub

Depuis le 13 mars 2000 l'écrit électronique a la même valeur que l'écrit manuscrit « l'auteur est responsable de ses actes donc de ses écrits ».

- Signature scannée

Le Hub Électronique de document permet d'apposer sur un document en fin de traitement une signature

manuscrite scannée. Néanmoins les éléments de preuve et la traçabilité associée au circuit restent stockés dans le Hub.

La signature scannée est gérée par le Hub en tant que duplicata de signature conforme à l'original électronique. Elle a, à ce jour, une valeur légale par son procédé informatique qui requiert un acte volontaire du signataire pour la créer (jurisprudence du 11 nov. 2006).

La signature scannée est particulièrement utile si le document original électronique issu du Hub doit être « re-matérialisé » en vue de générer des documents papiers destinés à être imprimés ou affichés.

La signature scannée a une valeur probante si elle est apposée par la personne titulaire de la signature et que le procédé utilisé garantit l'intégrité de la manipulation et l'authenticité de l'auteur qui doit avoir recours à un certificat électronique.

- Signature numérique

Le Hub propose une bibliothèque de signatures numériques. Une signature numérique est un couplage de signature électronique et de signature scannée visible sur le document.

Il est possible de personnaliser chaque signature avec des formules de politesse ou des tampons. Le nombre de signatures numériques dans la bibliothèque est illimité.

- Les tags de signature scannée et de date

Le Hub gère les emplacements des dates et signatures scannées à l'aide des tags #signature# et #date# qui sont placés dans le document. L'utilisateur décide directement de l'emplacement des éléments de date et signature.

Si votre document est un PDF non modifiable, vous pouvez cocher la case « ajouter les tags #signature# et #date » lors de la configuration du courrier sortant. L'emplacement de ces tags est paramétré par l'interface d'administration du hub (veuillez contacter l'équipe LegalBox pour définir ce paramétrage).

5. Types de certificats pris en charge par le Hub

- Certificat LegalBox (non référencé par le MINEFE) :

LegalBox crée des certificats pour tous les utilisateurs du Hub. Ces certificats sont émis conformément à la Politique de Certification (PC) de LegalBox, elle-même conforme au Référentiel Général de Sécurité (RGS) édicté par l'ANSSI.

Ces certificats LegalBox permettent d'effectuer des signatures et d'apposer des visas à valeur probatoire

car l'identité du porteur du certificat est démontrable dans la mesure où il est le seul à disposer de son couple identifiant/mot de passe.

Le certificat LegalBox permet aussi d'assurer l'intégrité du document entre chaque étape du circuit.

- Cas des documents sortants :

Lorsqu'il s'agit d'un document sortant, le certificat LegalBox ne pourra pas être utilisé. En effet, dans le cas d'un document sortant le certificat doit émaner d'une autorité de certification (AC) référencée par le MINEFE. Il faudra alors utiliser un certificat de niveau 1 ou niveau 2.

- Certificat de niveau 1 :

Le certificat de niveau 1 émane d'une autorité de certification (AC) reconnue par le MINEFE et est présenté sur support logiciel. Il peut être utilisé de deux manières :

- Installé en local dans le magasin de certificat du navigateur web. La signature se fait alors sur le poste de l'utilisateur en utilisant un applet Java.
- Stocké sur le serveur et rattaché au compte utilisateur. L'empreinte de signature est alors calculée directement sur le serveur.

- Certificat de niveaux 2, 3 et 3+ :

Le certificat de niveau 2 émane d'une autorité de certification (AC) reconnue par le MINEFE et peut être présenté sur support physique de type Token USB. Les certificats de niveaux 3 et 3+ nécessitent que le porteur ait vérifié son identité en face à face auprès de l'AC.

Ces certificats ne sont pas installés en local dans le magasin de certificat du navigateur web. La signature se fait donc sur le poste de l'utilisateur en utilisant un applet Java. La signature est ensuite déposée sur le serveur.

Dans tous les cas listés ci-dessus, un contrôle est opéré automatiquement sur la validité de l'AC ayant généré le certificat (qu'elle soit reconnue ou non par le MINEFE) et sur les listes de révocation associées.

6. Vérification du certificat de signature électronique

Le Hub permet d'associer une signature électronique à un utilisateur dans un contexte précis. Cette association est obligatoire pour qu'un utilisateur puisse signer un document avec un certificat.

Cette association présente plusieurs avantages, dont :

› La vérification de l’identité du signataire ;

› La vérification de l’habilitation de signature ;

› La vérification de l’utilisation du bon certificat.

Ainsi, une personne non habilitée ne pourra pas signer de document. Et une personne habilitée ne pourra signer qu’avec le certificat associé à son habilitation.

Dans le cas des flux Hélios qui doivent être signés au moyen de certificats RGS**, le Hub contrôle que le certificat électronique présenté par l’utilisateur correspond bien au flux à signer. En effet, un élu peut avoir plusieurs mandats et être amené à signer des flux pour des organismes différents (ex : Mairie, Foyer, CCAS, etc.). Or, si aucun contrôle n’est opéré sur le certificat présenté par l’élu, le flux peut être signé par erreur avec un mauvais certificat et être rejeté par la DGFIP dans un second temps.

Afin d’éviter ces désagréments, le Hub permet d’associer la clé publique d’un certificat RGS** à un utilisateur, à un numéro de SIRET et à une fonction (adjoint de l’élu, président du CCAS, etc.). De fait, lors de l’import du flux PES V2 en sortie du logiciel de gestion financière, le Hub reconnait le numéro de SIRET (obligatoirement présent dans le flux PES V2) et associe le flux à un circuit de validation spécifique, à un signataire en bout de chaine et à la clé publique du certificat attendu pour la signature. Ainsi, si le signataire présente par mégarde un mauvais certificat, il ne sera pas autorisé à signer

7. Paramétrage technique

- **Paramétrer le certificat et les jetons d’horodatage**

A paramétrer dans le compte utilisateur

paraph.folder.configuration.TYPE_MAIL_OUT

{
"signature": {
"enabled": true,
"type": "pades",
"certificate": {
"enabled": true,
"id": *ID à récupérer dans l'onglet certificat du compte utilisateur*
},
"timestamp": {
"enabled": false,
"url": "",

"username": "",
"password": ""
}
}
}

- **Paramétrer l’usage de l’applet par défaut**

A paramétrer dans le compte de l’organisation

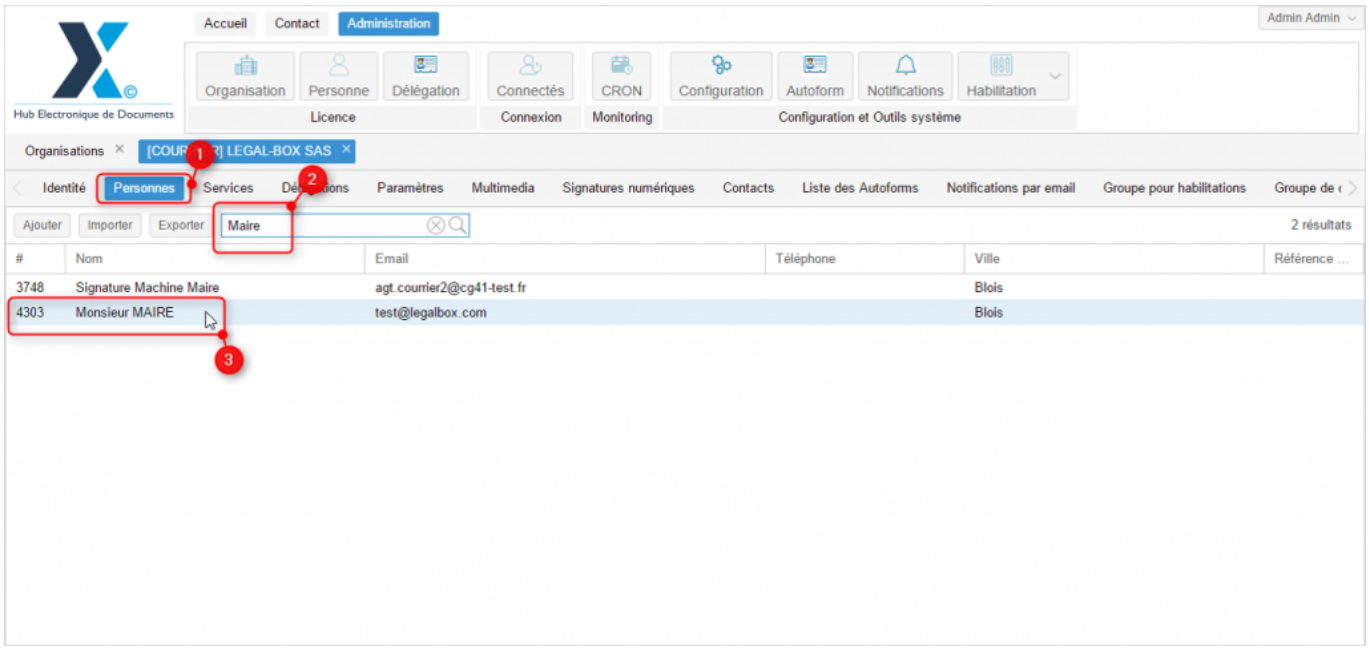
paraphFolderTypeSkeleton

{
"optionsByParaphFolderType": {
"TYPE_MAIL_OUT": {
"useSignatureApplet": true,
"signatureAppletCheckedByDefault": false
}
}
}

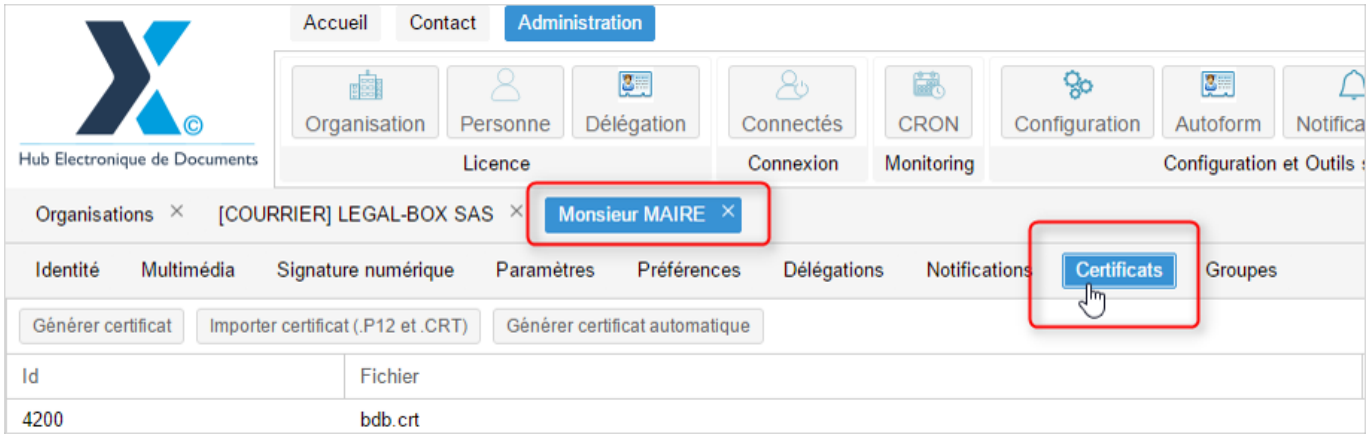
- **Intégrer un certificat RGS* dans le magasin d’un certificat utilisateur**

Les certificats électroniques se paramètrent à partir du compte utilisateur. Pour ajouter des certificats RGS* dans le magasin d'un certificat utilisateur, veuillez suivre le mode opératoire suivant :

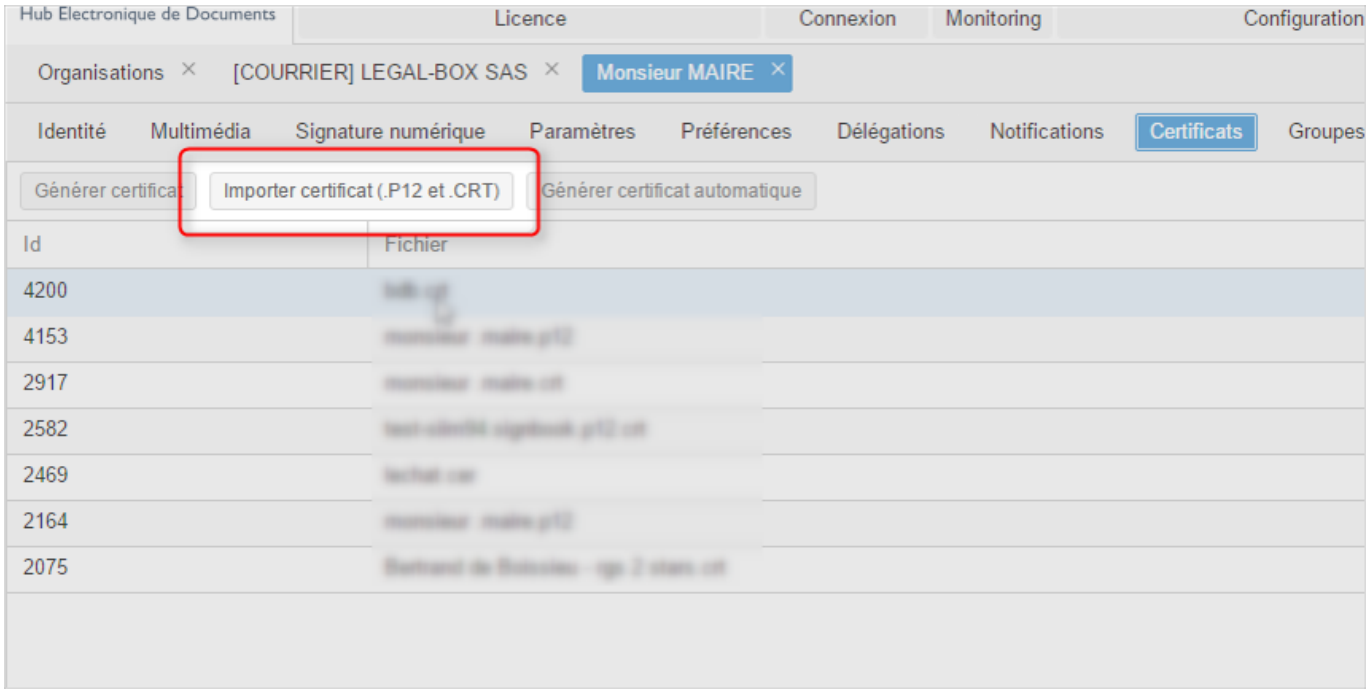
› Cliquez sur l'onglet "Personne" (1), insérez le nom de l'utilisateur (2) puis double-cliquez sur l'utilisateur dans la liste (3) :



› Sur la page du profil utilisateur, **cliquez sur l'onglet "certificat" au niveau de l'utilisateur:**



› Cliquez sur le bouton **"Importer certificat (.p12 et .crt)" :**



› **Remplissez les champs demandés** pour l'insertion d'un nouveau certificat **:**

? Sélectionnez le type de certificat

? Passez le champ "state" en "actived"

? Insérez le mot de passe de la clé privée (si besoin)

? Chargez le fichier de certificat en cliquant sur "choisissez le fichier"

? Cliquez sur "valid" pour valider l'importation du certificat