Certificats et Signatures

Outil d'administration

Ce document est la propriété de SIATEL.
Il ne peut être reproduit ou communiqué sans l'autorisation écrite de SIATEL.

Table des matières

Pré-requis pour la signature 5

Licence spécifique 5

Pré-requis pour l'utilisation des clés USB eToken 5

Installer SafeNet Authentication Client 5

Utiliser SafeNet Authentication Client 6

Présentation des fonctionnalités de signature 7

Types de signatures 7

Signature électronique 7

Signature manuscrite 10

Types de certificats électroniques 10

Certificat stocké en local 11

Certificat stocké sur le serveur 11

Certificat sur clé USB eToken 11

Méthodes de signature 12

Manuelle - Outil « Apposer une signature électronique » 12

Manuelle - Outil « Apposer une signature visible » 13

Automatique - Tâche de processus « Signature électronique » 14

Gestion des certificats via l'Outil d'administration 17

Importer un certificat stocké en local 17

Créer une autorité de certification interne à Gargantua 18

Ajouter des certificats auto-signés 18

Affecter un certificat 19

Affecter un certificat au serveur 20

Affecter un certificat à un ou plusieurs utilisateurs 20

Voir les informations sur un certificat 20

Exporter un certificat 21

Supprimer un certificat stocké sur le serveur 22

Pré-requis pour la signature

Licence spécifique

Les fonctionnalités de signature décrites ci-après ne sont pas incluses automatiquement dans toutes les installations de Gargantua. Si vous souhaitez en bénéficier, votre organisation doit donc faire l'acquisition d'une licence spécifique : vous aurez ensuite accès à la branche **Certificats** de l'Outil d'administration, ainsi qu'à toutes les fonctionnalités associées.

Pré-requis pour l'utilisation des clés USB eToken

Installer SafeNet Authentication Client

Les fonctionnalités de signature avec clé USB sécurisée offertes par Gargantua 7 reposent sur les solutions d'authentification forte développées par SafeNet (www.safenet-inc.com).

Pour signer les documents avec une clé dans Gargantua, il faut donc :

- Au niveau logiciel, installer l'application SafeNet Authentication Client sur chacun des postes utilisateurs ;
- Au niveau matériel, utiliser les clés eToken correspondantes.

Pour installer l'application SafeNet Authentication Client, procédez comme suit :

1. Exécutez le fichier SafeNetAuthenticationClient_x32_x64_8.00-SP1.exe situé dans le kit d'installation fourni par SIATEL (**SafeNetAuthenticationClient8_0_SP1** > **32X64 Installer**).

   L'assistant d'installation s'affiche.

2. Cliquez sur **Next**.
3. Dans la liste déroulante, choisissez la langue appropriée, puis cliquez sur **Next**.
4. Sélectionnez le bouton radio **I accept the license agreement**, puis cliquez sur **Next**.
5. Sélectionnez le type d'installation **Standard**, puis cliquez sur **Next**.
6. Sélectionnez le dossier d'installation de l'application sur votre disque dur : vous pouvez ou bien conserver la valeur par défaut, ou bien choisir un autre emplacement à l'aide du bouton **Browse**.
7. Cliquez sur **Next** pour lancer l'installation, puis patientez jusqu'à ce qu'un message de succès s'affiche.
8. Cliquez sur **Finish**.

   Vous disposez désormais de SafeNet Authentication Client sur votre poste local : vous pouvez maintenant utiliser Gargantua pour signer des documents à l'aide d'une clé eToken.

Utiliser SafeNet Authentication Client

SafeNet Authentication Client dispose de son propre guide utilisateur, inclus dans le kit d'installation de l'application (**SafeNetAuthenticationClient8_0_SP1** > **Documentation** > **SAC_User_Guide_8.0_SP1_Windows_Rev_A.pdf**).

Dans le cadre de votre utilisation de SafeNet Authentication Client avec Gargantua, vous serez plus particulièrement amené à :

- Importer des certificats vers la clé USB eToken, afin de pouvoir l'utiliser pour signer : voir « Importing a Certificate Onto a Token », p. 46 du guide utilisateur SafeNet ;
- Exporter des certificats à partir de la clé : voir « Exporting a Certificate from a Token », p. 50 ;
- Supprimer des certificats présents sur la clé : « Deleting a Certificate », p. 54 ;
- Changer le mot de passe général de la clé : « Changing the Token Password », p. 36.

Présentation des fonctionnalités de signature

Types de signatures

Une signature Gargantua peut être de type électronique (visible ou invisible) et/ou manuscrite. Les combinaisons suivantes sont possibles :

- La **signature électronique** permet de signer un document à l'aide d'un certificat électronique.
- La **signature électronique visible** permet de signer un document à l'aide d'un certificat électronique visible directement dans le corps du document PDF.
- La **signature manuscrite** permet d'apposer une signature sous la forme d'un fichier image sans utiliser de certificat électronique.
- La **signature électronique et manuscrite** permet de combiner une signature sous la forme d'un fichier image avec un certificat électronique.
- La **signature électronique visible et manuscrite** permet de combiner une signature sous la forme d'un fichier image avec un certificat électronique visible directement dans le corps du document PDF.

Signature électronique

La signature électronique permet d'**appliquer un certificat électronique** sur un document.

Un certificat électronique est un fichier contenant :

- Un ensemble d'informations sur l'identité de son propriétaire ;
- Deux clés de chiffrement :
    - La clé privée permet au propriétaire du certificat de l'apposer sur des documents numériques en fournissant un mot de passe.
    - La clé publique permet aux destinataires des documents de vérifier l'authenticité du certificat et, donc, l'exactitude des informations sur sa provenance.

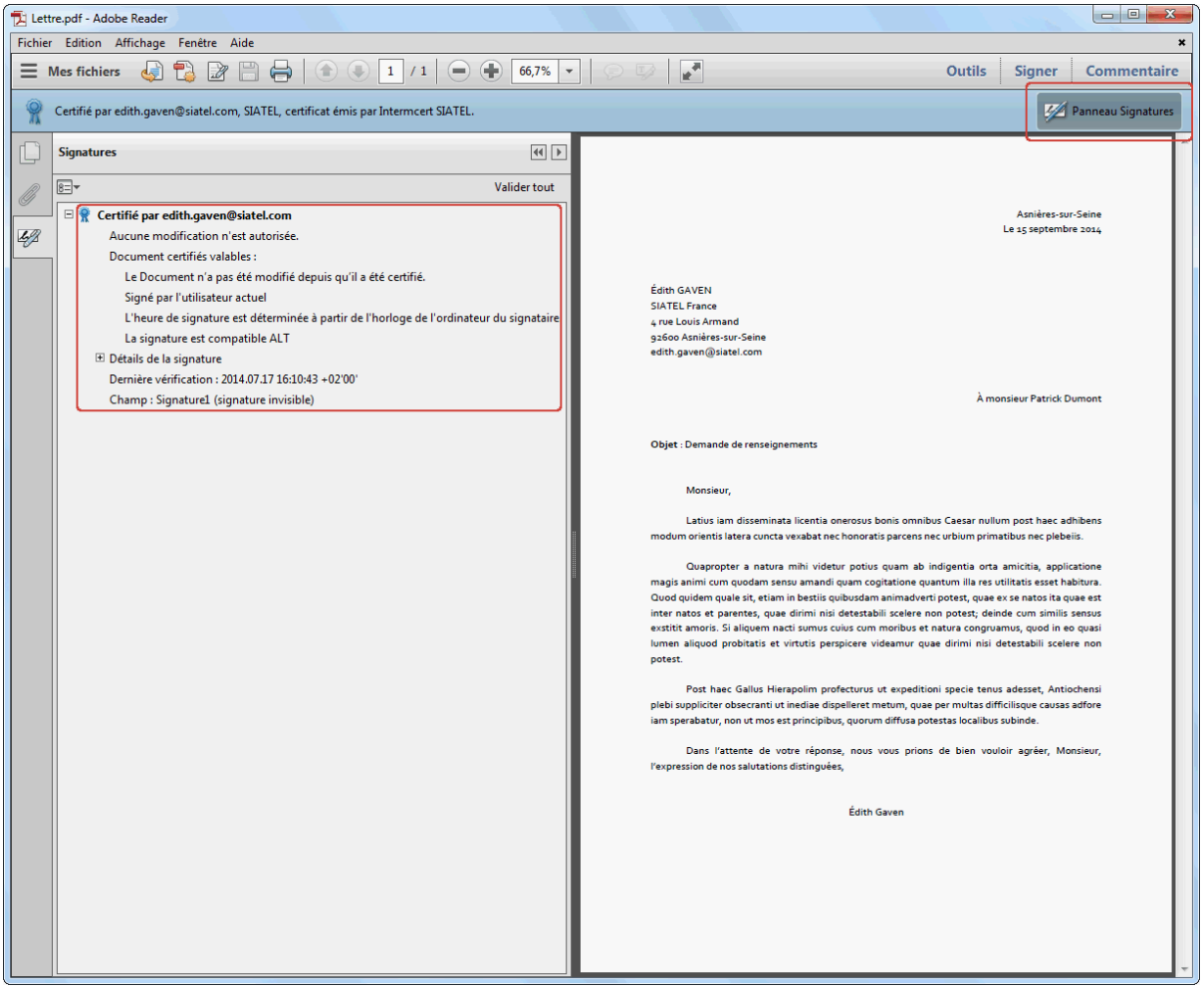
La validation des signatures électroniques repose sur l'existence d'**autorités de certification** capables de générer les certificats et de garantir leur authenticité. Des entités telles que VeriSign se sont donc spécialisées dans le rôle de tiers de confiance commercialisant et authentifiant les certificats. Toutefois, une organisation peut également **mettre en place à usage interne sa propre autorité de certification** et générer ainsi des certificats dits « auto-signés ».

Les fonctionnalités de signature électronique offertes par Gargantua permettent d'employer ces deux méthodes de validation. Vous pouvez :

- Signer les documents à l'aide de certificats au format .p12 ou .pfx achetés auprès d'autorités de certification indépendantes ;
- Créer sur le serveur Gargantua une autorité de certification permettant de générer et d'utiliser des

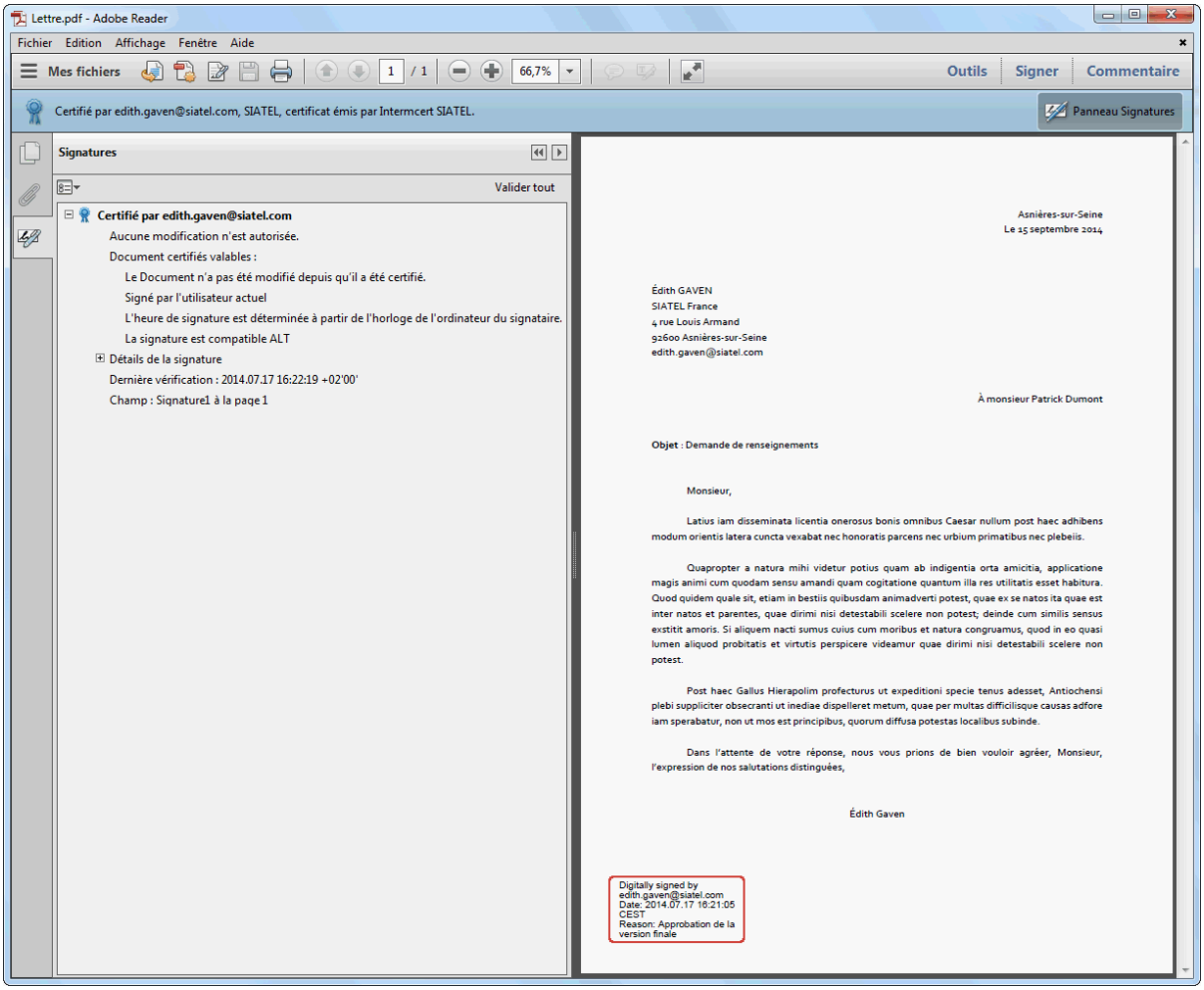
certificats auto-signés.

Les documents signés à l'aide de Gargantua sont convertis au format PDF. Les informations concernant le propriétaire et l'authenticité du certificat utilisé sont alors accessibles dans le **Panneau Signatures** d'Adobe Acrobat Reader :



Signature électronique visible

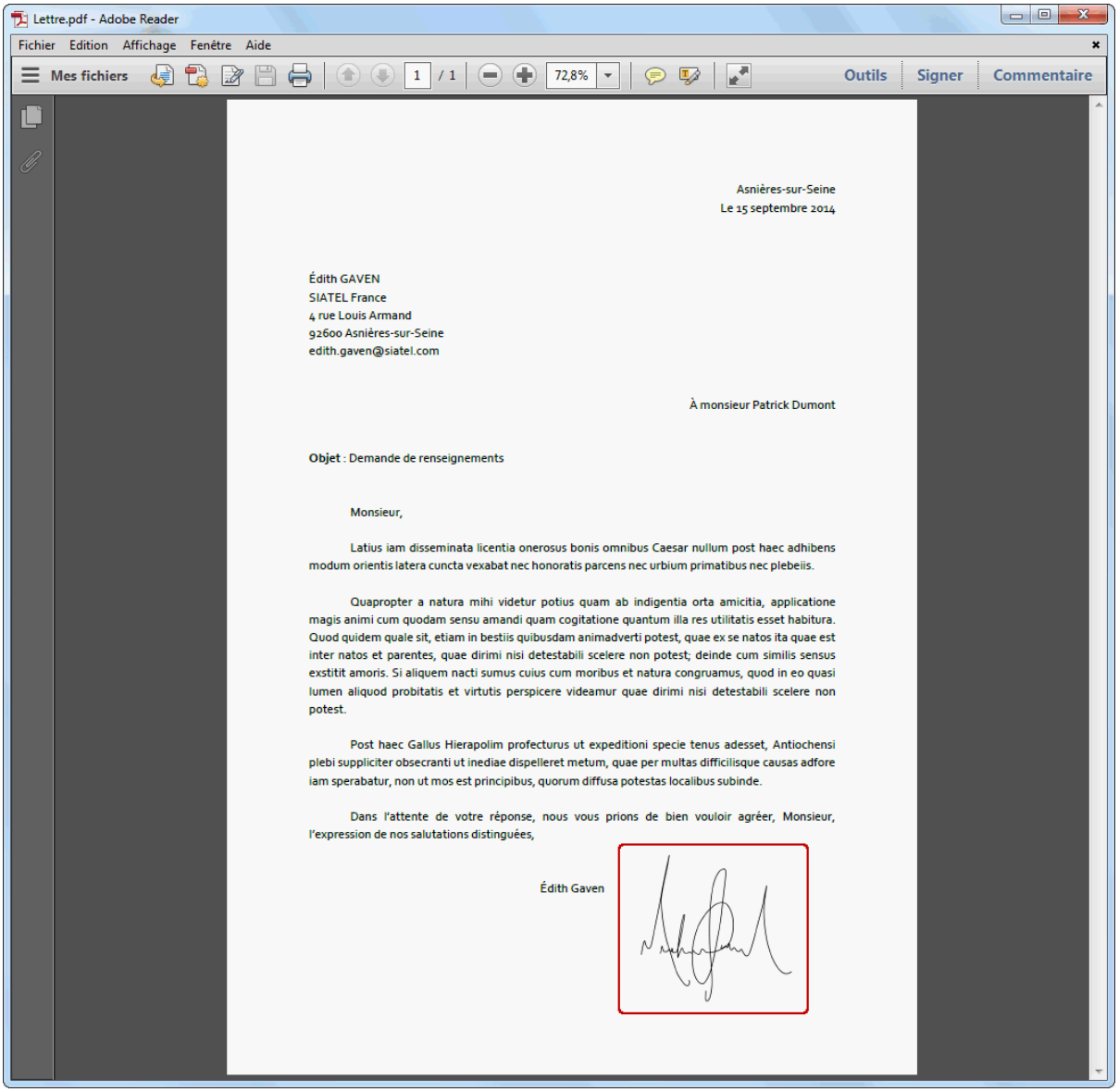
Une signature électronique est toujours disponible depuis le **Panneau Signatures** d'Adobe Acrobat Reader. Cependant, si vous souhaitez qu'elle soit **visible directement dans le corps du document PDF**, vous pouvez utiliser la fonctionnalité de signature électronique visible :



Lors de l'apposition de la signature, l'utilisateur du Client web Gargantua peut sélectionner la page du document et l'emplacement sur la page où la signature sera visible.

Signature manuscrite

La signature manuscrite permet d'apposer une signature **sous la forme d'un fichier image**. Elle peut être utilisée seule ou combinée à une signature électronique :



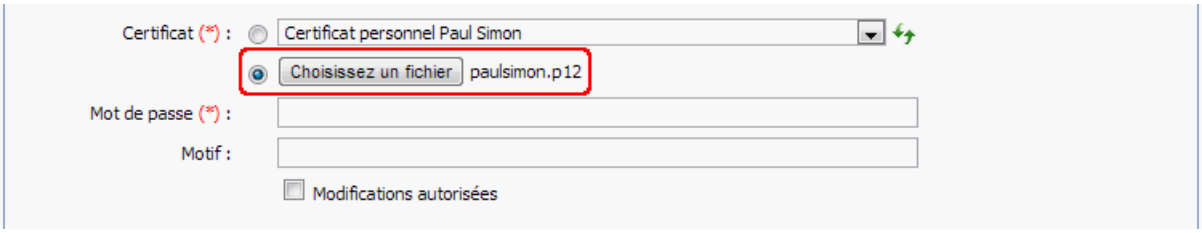
Types de certificats électroniques

Lors de l'apposition d'une signature électronique (visible ou non), les utilisateurs peuvent sélectionner trois types de certificats électroniques.

*Pour accéder à la signature électronique, les utilisateurs doivent sélectionner les documents appropriés et cliquer sur l' outil « Apposer une signature électronique » ou sur l' outil « Apposer une signature visible » (hors option « **Signature manuscrite** » seule).*

Certificat stocké en local

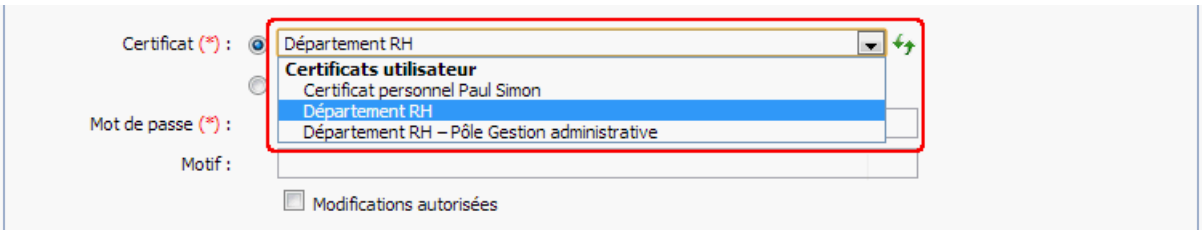
Les utilisateurs du Client web Gargantua peuvent signer électroniquement un ou plusieurs documents à l'aide d'un fichier de certificat au format .p12 ou .pfx présent sur leur disque dur :



Certificat stocké sur le serveur

Les utilisateurs du Client web Gargantua peuvent signer électroniquement un ou plusieurs documents à l'aide de certificats téléchargés et stockés pour eux sur le serveur Gargantua.

Les certificats affectés à l'utilisateur courant apparaissent dans la liste déroulante **Certificat** :



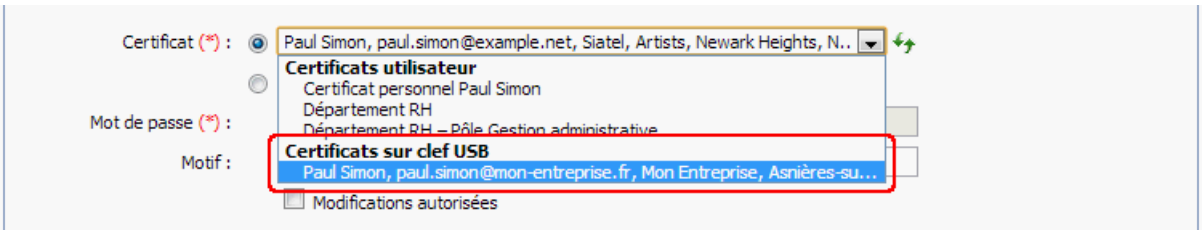
Cette méthode présente l'avantage de rendre les certificats disponibles depuis n'importe quel poste de travail, tout en offrant une protection contre le vol.

Certificat sur clé USB eToken

Enfin, les utilisateurs du Client web Gargantua peuvent signer les documents électroniquement à l'aide de certificats stockés sur une clé USB sécurisée de type eToken (voir Pré-requis pour l'utilisation des clés USB eToken).

Ils doivent connecter la clé à leur poste de travail, puis entrer le mot de passe de celle-ci. La liste déroulante des certificats disponibles pour l'utilisateur est alors actualisée de manière à inclure les certificats présents sur

la clé :



Méthodes de signature

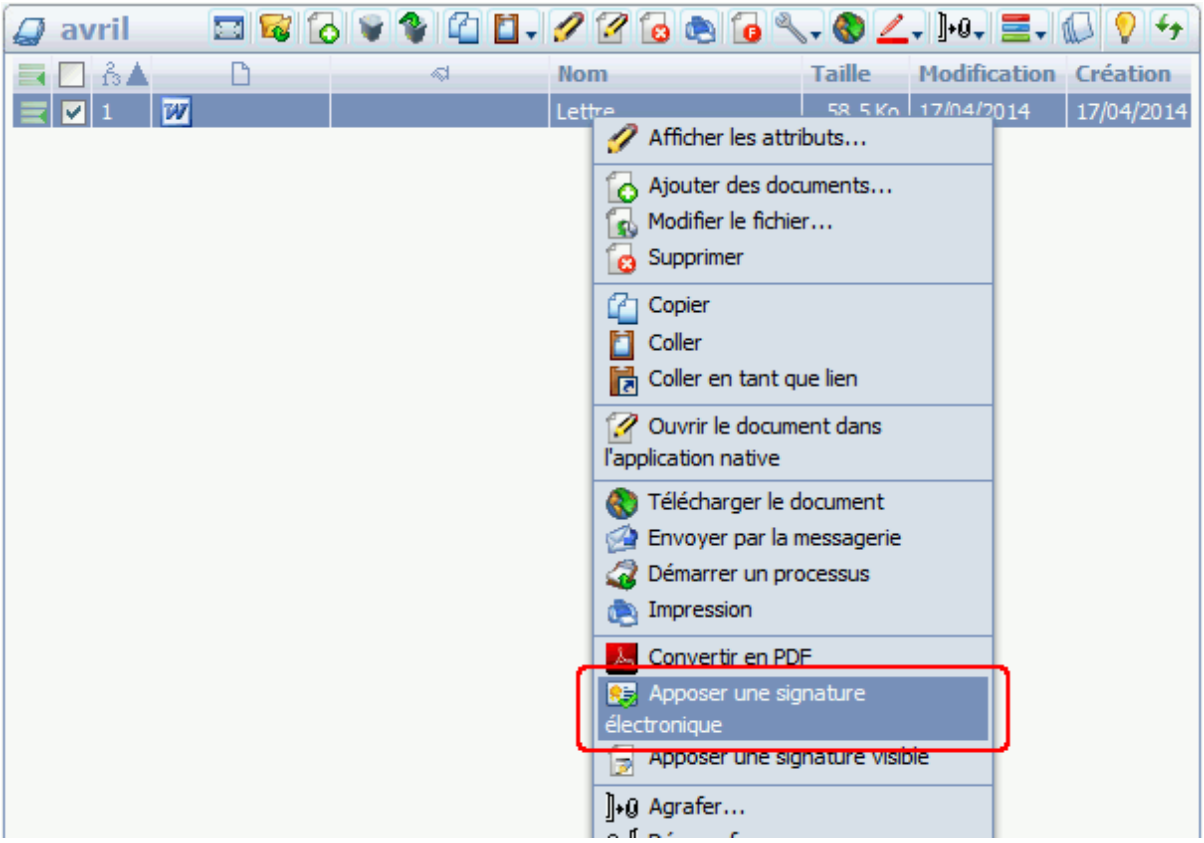
Gargantua permet de signer des documents de manière manuelle depuis l'explorateur à l'aide des outils Apposer une signature électronique ou Apposer une signature visible, ou de manière automatique à l'aide d'une tâche de workflow de type signature.

Manuelle - Outil « Apposer une signature électronique »

L'outil **Apposer une signature électronique** permet uniquement de signer avec un certificat électronique **non visible** dans le corps du document PDF.

Pour utiliser cet outil, les utilisateurs doivent avoir le droit d'accès « Apposer une signature électronique » (profils de sécurité) sur les documents concernés.

Cet outil peut être appliqué sur plusieurs documents à la fois.



Manuelle - Outil « Apposer une signature visible »

L'outil **Apposer une signature visible** regroupe l'ensemble des types de signatures qui sont visibles directement dans le corps du document PDF :

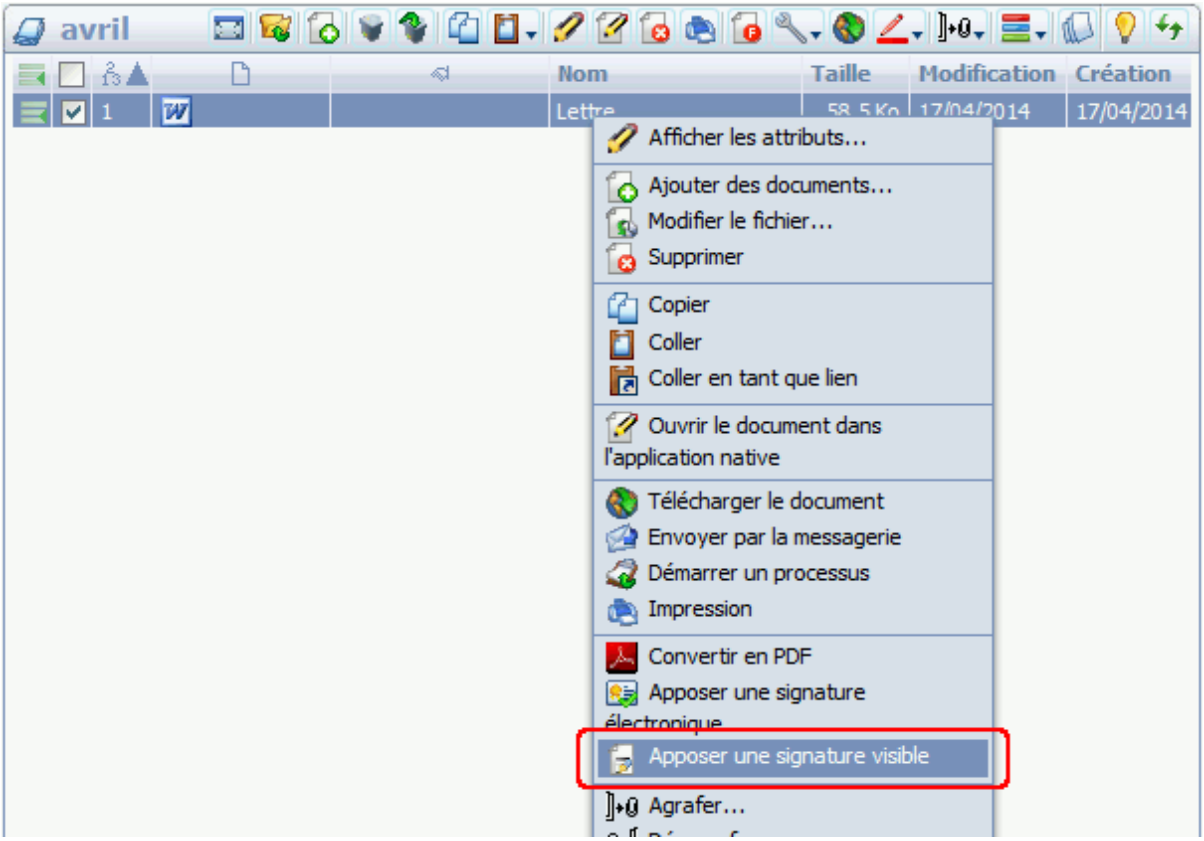
- La **signature électronique visible** permet de signer un document à l'aide d'un certificat électronique visible directement dans le corps du document PDF.
- La **signature manuscrite** permet d'apposer une signature sous la forme d'un fichier image sans utiliser de certificat électronique.
- La **signature électronique et manuscrite** permet de combiner une signature sous la forme d'un fichier image avec un certificat électronique.
- La **signature électronique visible et manuscrite** permet de combiner une signature sous la forme d'un fichier image avec un certificat électronique visible directement dans le corps du document PDF.

*Pour avoir cet outil dans leur barre d'outils, les utilisateurs doivent avoir le privilège **« Signature visible »** (écran de gestion de l'utilisateur, du groupe ou du rôle).*

*Pour utiliser cet outil, les utilisateurs doivent avoir le droit d'accès **« Apposer une signature électronique »** (profils de sécurité) sur les documents concernés.*

*Pour utiliser cet outil, une image de signature doit avoir été préalablement téléchargée sur le serveur (**« Paramétrage »** > **« Paramètres de la signature et des certificats »** > **« Signature manuscrite »**).*

Cet outil peut être appliqué sur un seul document à la fois.



Automatique - Tâche de processus « Signature électronique »

Les documents peuvent être signés automatiquement dans le cadre de processus de workflow, avec des tâches signature électronique mises en place par les administrateurs Gargantua.

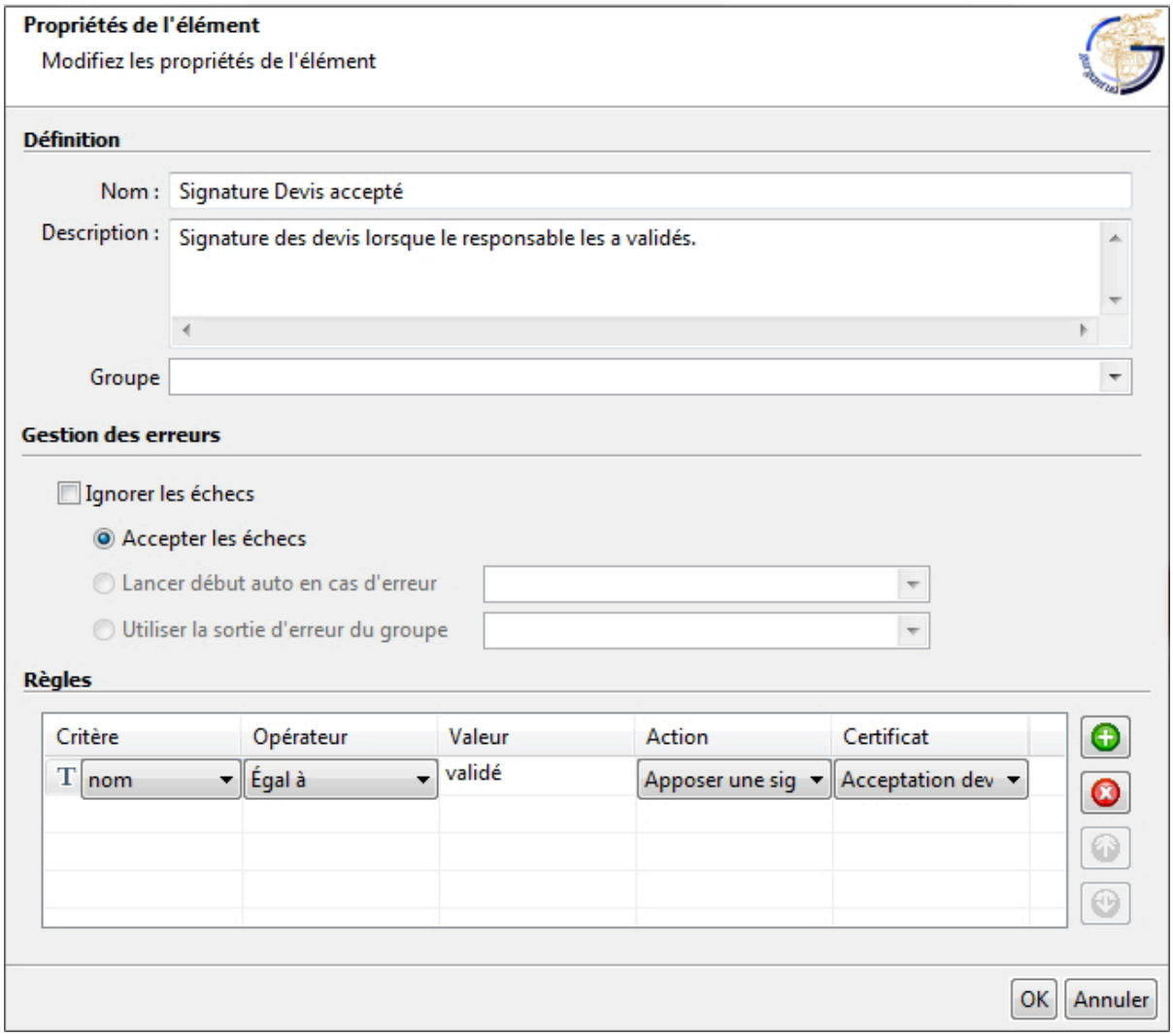
Pour créer et paramétrer une tâche signature électronique, procédez comme suit :

1. Dans le volet gauche de l'Outil d'administration, déployez les branches appropriées, puis cliquez sur le nom du processus dans lequel vous souhaitez insérer une tâche signature.

L'écran **Gestion des processus** s'affiche dans le volet droit.

2. Si l'onglet **Schéma** n'est pas sélectionné par défaut, sélectionnez-le.
3. Dans la barre de sélection des éléments de processus, cliquez sur l'icône et faites-la glisser dans la zone de création du processus pour ajouter une nouvelle **Tâche signature électronique**.
4. Après avoir ajouté les connecteurs nécessaires, double-cliquez sur la nouvelle tâche .

   La boîte de dialogue **Propriétés de l'élément** s'affiche :



5. Saisissez le nom et, éventuellement, une description de la tâche.
6. Ajoutez éventuellement la tâche à un groupe.
7. À l'aide du bouton , ajoutez au moins une règle définissant les conditions et les modalités de signature des documents joints au processus :
   - **Critère** : Sélectionnez un critère permettant de trier les documents pour savoir s'ils doivent être signés ou non et, si oui, à l'aide de quel certificat. Le critère peut porter sur le formulaire du document, sur le type du fichier correspondant (.doc, .tif, .txt...), ou encore sur le contenu

du champ **nom** du formulaire.

- **Opérateur** : Choisissez l'opérateur de comparaison approprié.
- **Valeur** : Saisissez ou sélectionnez la valeur à comparer avec les propriétés de chaque document pour savoir si le critère de signature est rempli.
- **Action** : Sélectionnez **Apposer une signature électronique** (l'option **Crypter** permet quant à elle de transformer les documents en PDF chiffrés, accessibles en lecture seule mais protégés contre toute modification ou copier-coller).
- **Certificat** : Sélectionnez le certificat à utiliser pour signer les documents correspondant à cette règle. Seuls les certificats affectés au serveur sont disponibles ici (voir Affecter un certificat à un ou plusieurs utilisateurs).

Chaque document ne pouvant être signé électroniquement qu'une seule fois, les règles définies pour la tâche signature électronique sont mutuellement exclusives. Si un document remplit plusieurs conditions, seule la première règle sera appliquée.

8. Si nécessaire, vous pouvez supprimer ou déplacer des règles à l'aide des boutons , et .
9. Lorsque vous avez terminé, cliquez sur **OK** pour fermer la boîte de dialogue.

Les documents remplissant les règles énoncées seront désormais signés automatiquement dans le cadre du processus.

Gestion des certificats via l'Outil d'administration

Importer un certificat stocké en local

La branche **Certificats** de l'Outil d'administration vous permet de stocker et de gérer de manière centralisée, sur le serveur, les différents certificats utilisés par les utilisateurs Gargantua pour valider et authentifier les documents.

Pour télécharger sur le serveur un certificat stocké sur votre disque dur, procédez comme suit :

1. Dans le volet gauche de l'Outil d'administration, cliquez sur la branche **Certificats**.

   L'écran **Gestion des certificats** s'affiche dans le volet droit.

2. En bas à droite du volet droit, cliquez sur le bouton **Importation**.

   L'explorateur de fichiers s'affiche.

3. Naviguez jusqu'à l'emplacement où vous avez sauvegardé le fichier de certificat à importer, sélectionnez-le, puis cliquez sur **Ouvrir**.

   Les certificats importés doivent obligatoirement être au format .p12 ou .pfx.

   Une boîte de dialogue s'affiche.

4. Saisissez le mot de passe du certificat, puis cliquez sur **OK**.

   Une boite de dialogue s'affiche.

5. Renseignez le champ **Nom** à l'aide d'une valeur qui vous permettra d'identifier facilement le certificat à l'avenir dans la **Liste des certificats**.
6. Décidez ensuite si vous souhaitez affecter le certificat à un ou plusieurs utilisateurs-personnes physiques (champ **Affecté à**), ou bien si vous souhaitez affecter le certificat au serveur afin qu'il puisse être utilisé pour les tâches signature électronique des processus de Workflow (option **Il s'agit d'un certificat de type serveur**).
7. Lorsque vous avez terminé, cliquez sur **OK**.

   Le certificat a bien été importé : il s'ajoute à la **Liste des certificats** hébergés sur le serveur.

*Les utilisateurs détenteurs de privilèges donnant accès au lien « **Paramétrage** » peuvent également télécharger des certificats sur le serveur par le biais du Client web (« **Paramétrage** »> « **Paramètres de la signature et des certificats** » > « **Paramètres des certificats utilisateur** »). Les certificats ainsi importés apparaissent ensuite dans la « **Liste des certificats** » de l'Outil d'administration, où ils peuvent être gérés, réaffectés, ou encore supprimés par les administrateurs.*

Créer une autorité de certification interne à Gargantua

Si vous ne souhaitez pas acquérir pour chacun de vos utilisateurs un certificat généré par un tiers de confiance, par exemple pour des raisons de coût, Gargantua vous permet de créer sur le serveur votre propre autorité de certification, puis de l'utiliser pour générer des certificats auto-signés à usage interne.

Pour créer votre autorité de certification à l'aide de l'Outil d'administration, procédez comme suit:

1. Dans le volet gauche de l'Outil d'administration, cliquez sur la branche **Certificats**.

   L'écran **Gestion des certificats** s'affiche.

2. En bas au centre du volet droit, cliquez sur le bouton **Créer mon certificat-racine maintenant**.

   Une boîte de dialogue s'affiche.

3. Renseignez les informations demandées, puis cliquez sur **OK**.

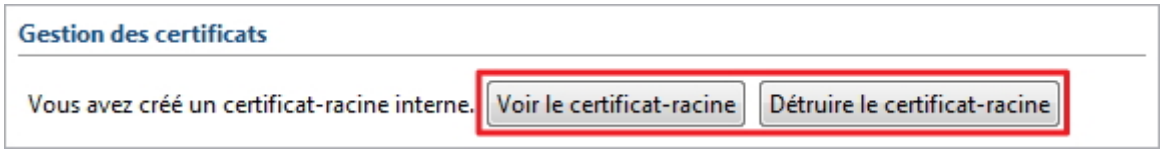
   Une boîte de dialogue s'affiche.

4. Saisissez le mot de passe que vous souhaitez attribuer au certificat-racine, puis cliquez sur **OK**.

   Votre autorité de certification a bien été créée.

   Le bouton **Créer mon certificat-racine** maintenant est remplacé par deux autres boutons:

   - **Voir le certificat-racine** : permet de voir les informations contenues dans le certificat-racine
   - **Détruire le certificat-racine** : permet de supprimer l'autorité de certification **et tous les certificats auto-signés qui en dépendent**.



Ajouter des certificats auto-signés

Après avoir créé votre autorité de certification sur le serveur Gargantua, vous pouvez commencer à ajouter des

certificats auto-signés :

1. Dans le volet gauche de l'Outil d'administration, cliquez sur la branche **Certificats**.

   L'écran **Gestion des certificats** s'affiche.

2. En bas à gauche du volet droit, cliquez sur le bouton **Ajouter**.

   La boîte de dialogue **Nouveau certificat utilisateur** s'affiche.

3. Renseignez les informations demandées. Vous devez notamment :
   - Choisir pour le certificat un **Nom** évocateur, qui vous permettra de l'identifier facilement à l'avenir dans la **Liste des certificats** ;
   - Décider si vous souhaitez affecter le certificat à un ou plusieurs utilisateurs-personnes physiques (champ **Affecté à**), ou bien si vous souhaitez l'utiliser pour les tâches signature électronique des processus de Workflow (option **Il s'agit d'un certificat de type serveur**).
4. Cliquez sur **OK**.

   La boîte de dialogue **Mot de passe du certificat** s'affiche.

5. Saisissez le mot de passe que vous souhaitez attribuer au certificat, puis cliquez sur **OK**.

   En fonction des caractéristiques de votre système, il est possible que la longueur des mots de passe pour les certificats auto-signés soit limitée à 7 caractères (voir le manuel d'installation, « Installation de Java » > « Extension Java de cryptographie sans limitation de puissance »).

   Le nouveau certificat auto-signé apparaît dans la **Liste des certificats** : il est désormais disponible pour signer des documents à usage interne.

Dans la « Liste des certificats », les certificats auto-signés sont reconnaissables à l'icône , tandis que les certificats importés sont précédés de l'icône .

Affecter un certificat

Au regard de leur affectation, il existe deux grandes catégories de certificats :

- Les certificats de type **Serveur**, utilisés pour signer les documents automatiquement dans le cadre des processus de Workflow ;
- Les certificats affectés à un utilisateur, groupe ou rôle, utilisés pour signer les documents au coup par coup par le biais du Client web.

Affecter un certificat au serveur

Pour affecter un certificat au serveur, procédez comme suit :

1. Cochez la case ☐ Serveur correspondante dans la **Liste des certificats**.

   Un message de confirmation s'affiche.

2. Cliquez sur **Oui**.

   Une boîte de dialogue s'affiche.

3. Entrez le mot de passe du certificat, puis cliquez sur **OK**.

   L'affectation a été réalisée : le certificat sera désormais disponible pour paramétrer des tâches signature électronique de Workflow ou autres opérations automatiques réalisées par le serveur.

Affecter un certificat à un ou plusieurs utilisateurs

Pour affecter un certificat à un utilisateur, groupe ou rôle, procédez comme suit :

1. Dans la **Liste des certificats**, cliquez sur l'icône 🔍 correspondante.

   Une boîte de dialogue s'affiche.

2. Dans le champ **Nom**, saisissez les premières lettres du nom de l'utilisateur, groupe ou rôle auquel vous souhaitez affecter le certificat.
3. Dans la liste qui s'affiche, double-cliquez sur le nom de l'utilisateur, groupe ou rôle approprié.

   L'affectation a bien été réalisée. Le ou les utilisateurs correspondants verront désormais le certificat dans la liste **Certificats utilisateur** du Client web.

Voir les informations sur un certificat

Pour visualiser les informations de signature contenues dans un certificat, procédez comme suit :

1. Sélectionnez le certificat dans la **Liste des certificats**.
2. Cliquez sur le bouton **Afficher les détails** en bas à gauche du volet droit.

   Les informations contenues dans le certificat apparaissent en grisé : vous pouvez les consulter mais pas les modifier.

   En outre, certaines informations protégées sont remplacées par la mention **Inconnu**.

3. Pour accéder aux informations protégées, cliquez sur le bouton **S'identifier** puis entrez le mot de passe du certificat.

   Les informations protégées apparaissent désormais en clair.

4. Lorsque vous avez terminé, cliquez sur **OK**.

Exporter un certificat

L'Outil d'administration vous offre la possibilité d'exporter les certificats hébergés sur le serveur vers votre disque local ou vers une clé USB eToken, et ce qu'il s'agisse de certificats externes ou de certificats auto-signés.

Pour exporter un certificat vers votre disque dur, procédez comme suit :

1. En bas à droite de l'écran **Gestion des certificats**, cliquez sur le bouton **Exporter vers le disque dur**.

   L'explorateur de fichiers s'affiche.

2. Sélectionnez l'emplacement vers lequel exporter le certificat, puis cliquez sur **Enregistrer**.

   Un message de confirmation s'affiche.

3. Cliquez sur **OK**.

   Le certificat est désormais disponible sur votre disque dur à l'emplacement sélectionné.

Pour exporter un certificat vers une clé eToken, procédez comme suit :

1. Vérifiez que la clé cible est bien connectée à votre ordinateur.
2. En bas à droite de l'écran **Gestion des certificats**, cliquez sur la flèche ▼ sur la droite du bouton **Exporter vers le disque dur**.
3. Dans la liste qui s'affiche, sélectionnez **Exporter vers la clef USB**.

   Une boîte de dialogue s'affiche.

4. Entrez le mot de passe général de la clé, puis cliquez sur **OK**.

   Une boîte de dialogue s'affiche.

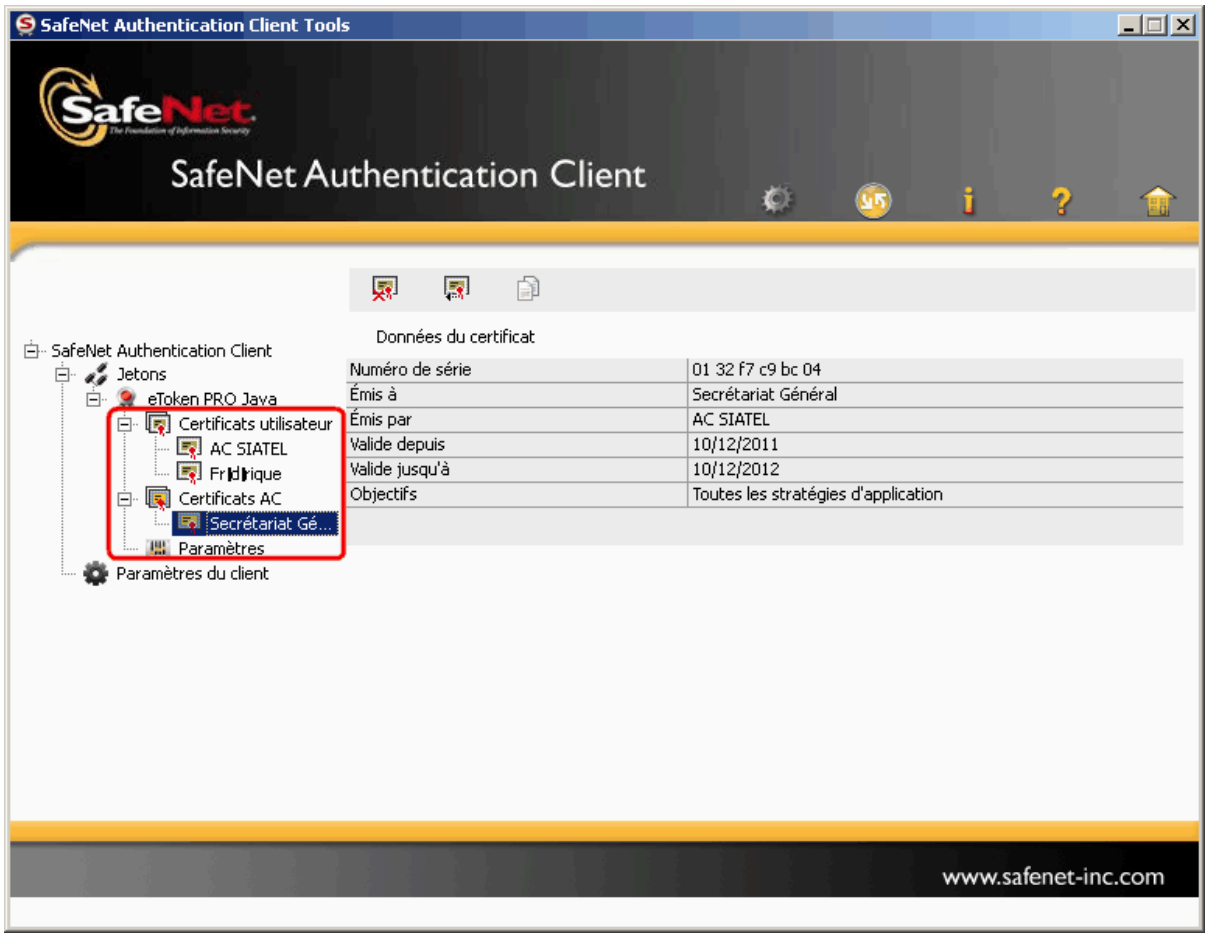
5. Entrez le mot de passe du certificat à exporter, puis cliquez sur **OK**.

   Un message de confirmation s'affiche.

6. Cliquez sur **OK**.

   Le certificat a bien été exporté vers la clé.

En explorant le contenu de cette dernière à l'aide de SafeNet Authentication Client, vous devez voir apparaître votre certificat, sous la rubrique **Certificats utilisateur** s'il s'agit d'un certificat externe, ou sous la rubrique **Certificats AC** s'il s'agit d'un certificat auto-signé :



Supprimer un certificat stocké sur le serveur

Pour supprimer un certificat stocké sur le serveur, procédez comme suit :

1. Sélectionnez le certificat dans la **Liste des certificats**.
2. En bas à gauche du volet droit de l'Outil d'administration, cliquez sur le bouton **Supprimer**.

   Un message d'avertissement apparaît.

3. Cliquez sur **Oui**.

   Le certificat a bien été supprimé : il n'apparaît plus dans la **Liste des certificats**.

Les utilisateurs détenteurs de privilèges donnant accès au lien « Paramétrage » peuvent également supprimer des certificats par le biais du Client web, à condition qu'il s'agisse de certificats qu'ils ont eux-mêmes téléchargés et que ces derniers n'aient pas été réaffectés à un ou plusieurs autres utilisateurs par un administrateur (voir Importer un certificat stocké en local).