

## **DLex® – Signer électroniquement vos emails avec LEXel Win® et DLex®**

Copyright Pyramiq – BE –Août 2009 (V 2.09.08.01)

---

### **Environnement et installation**

---

**Le matériel:** selon la forme du certificat utilisé et le support sur lequel il est distribué, certains périphériques devront préalablement être installés sur le PC.  
Reportez-vous pour cela aux instructions du fournisseur de votre lecteur de carte à puce ou clé USB.

**DLex®:** Version 2.09.08.01 ou supérieure.

**LEXel Win®** Version 3.07.04

### **Principe de base**

---

A partir du 1<sup>er</sup> septembre 2009 tous les courriers électroniques à caractère professionnel devront être signés avec un certificat de signature valide.

Les courriers électroniques générés au départ de LEXel Win® et de DLex® peuvent ainsi être signés électroniquement.

**La signature électronique porte sur le corps du mail et non sur les éventuelles pièces jointes, lesquelles doivent le cas échéant être signées séparément dans MS Word ou Acrobat Writer.**

Ce document vous explique les différentes étapes à suivre pour utiliser cette fonctionnalité dans le respect de vos habitudes de travail en termes de productivité et de traitement par lot (parapheur électronique **pour DLex® uniquement**).

Indépendamment de la procédure expliquée ici, DLex®, tout comme LEXel Win®, vous permet déjà de signer électroniquement vos envois électroniques à l'aide de la carte d'identité électronique belge.

**L'utilisation du certificat de signature contenu sur votre carte d'identité électronique fait l'objet d'une explication détaillée dans un mémo (Nov. 2008) disponible sur la page d'accueil de l'Extranet de l'O.B.F.G. (<http://obfg.be>)** – Nous vous invitons à consulter cette documentation si vous souhaitez utiliser ce certificat de signature.

Néanmoins, cette signature est peu souple et présente certains inconvénients.

Chaque email doit être signé et envoyé, mail par mail, par le détenteur du certificat utilisé → pas de délégation ni de traitement "par lot" aisé et/ou sûr. De plus, le code PIN doit être introduit à l'envoi de chaque courrier électronique.

En revanche, si vous utilisez un certificat du type de celui que nous vous proposons ici, DLex® et LEXel Win® vous permettent de conserver une meilleure productivité dans votre travail.

DLex® va encore plus loin en intégrant un traitement par lot des emails sortants vous garantissant ainsi un haut niveau de productivité.

Dans notre illustration, un certificat *GlobalSign* de Class 2 a été choisi. La procédure décrite est cependant applicable à tout certificat de ce type, quelle que soit l'autorité de certification que vous

aurez choisie. Cette approche a été menée en étroite concertation avec l'O.B.F.G. qui devrait la valider "officiellement" dans un proche avenir. Elle répond dès lors entièrement aux prescrits du règlement eTIC du 19 mai 2009.

La mise en œuvre de cette fonctionnalité s'effectue selon 5 étapes:

1. L'acquisition du certificat auprès de l'autorité de certification choisie
2. Le déploiement de votre certificat
3. La configuration de MS Outlook: installation du certificat
4. La configuration de *DLex*®: automatisation du processus et traitement par lot
5. Sauvegarde de votre certificat

► Un document signé électroniquement a la même valeur qu'un écrit signé, il incombe donc à son auteur de le signer lui-même, tout comme il signe les documents manuscrits engageant sa responsabilité professionnelle.

## Etape 1: acheter un certificat de signature

Cette rubrique vous explique la procédure d'acquisition d'un certificat *Global Sign* de Class 2 ou de Class 2 PRO.

Contrairement aux certificats de Class 1 qui ne certifie que votre adresse email, un certificat de Class 2 certifie **vosre identité**.

L'achat d'un certificat se fait exclusivement par Internet et le paiement DOIT être effectué en ligne par le biais d'une carte de crédit.

Prévoyez donc de disposer des éléments suivants en cours de procédure d'acquisition:

- Votre carte d'identité,
- Une carte de crédit,
- Les coordonnées exactes de facturation,
- Les coordonnées exactes du cabinet,
- Deux mots de passe alphanumériques différents d'au moins 8 caractères vous seront également demandés

### 1. Choisir son certificat

**PersonalSign Class 2** ou **PersonalSign Class 2 PRO**: découvrez les différences entre les certificats proposés par GlobalSign à l'adresse suivante:

<http://www.globalsign.eu/digital-certificates/>

Les prix sont les suivants (information communiquée sans engagement):

Type de certificat	1 an TTC	2 ans TTC	3 ans TTC
PersonalSign Class 2	63,25 €	67,85 €	74,75 €
PersonalSign Class 2 PRO	79,35 €	113,85 €	136,85 €

Pour les grandes entités, Global Sign propose une formule avec administration centralisée. Ce produit s'appelle **ePKI ou Enterprise PKI**. Nous vous recommandons de vous adresser directement à Global Sign pour obtenir une offre personnalisée.

[bert.mellaerts@globalsign.com](mailto:bert.mellaerts@globalsign.com) ou 016 / 89 19 00

PersonalSign Class 2: idéal pour les avocats en personne physique et/ou les collaborateurs qui doivent gérer des dossiers personnels au sein d'une structure plus vaste.

En cas de départ d'un collaborateur, celui-ci peut "récupérer" son certificat et l'accès à la gestion de celui-ci (renouvellement, révocation...) indépendamment du cabinet qu'il quitte.

Il s'agit donc du certificat le plus souple à l'utilisation.

PersonalSign Class 2 **PRO**: en tous points comparable au précédent, ce certificat vous permet en outre de poser des actes au nom du cabinet (Société)

### 2. Acheter le certificat choisi

La procédure d'acquisition chez GlobalSign est pratiquement identique pour les deux types de certificats concernés.

Un certificat PersonalSign Class 2 peut être commandé en ligne en suivant le lien ci-dessous:

<http://www.globalsign.eu/authentication-secure-email/digital-id/buy-personalsign-2.html>

Un certificat PersonalSign Class 2 **PRO** peut être commandé en ligne en suivant le lien ci-dessous:

<http://www.globalsign.eu/authentication-secure-email/digital-id/buy-personalsign-2-pro.html>

- Choisissez la région "Europe" et poursuivez
  - a. Account Setup:
    - ✓ Complétez le formulaire en ligne (**pas de caractère spéciaux ni d'accent ni de "et" commercial - &)**)
    - ✓ Choisissez un nom d'utilisateur et un mot de passe (pas de caractère spéciaux ni d'accent). Ceux-ci vous permettront d'accéder ultérieurement au portail d'administration de votre (vos) certificat(s), le GCC: GlobalSign Certificate Center.
    - ✓ Acceptez les conditions Globalsign pour poursuivre (NEXT).
  - b. Product détail
    - ✓ Sous menu "Product detail": selon le certificat choisi, vous pourrez y souscrire pour 1, 2 ou 3 ans. Cet écran vous montre le prix des options retenues – Ne rien cocher d'autre ici.

### PersonalSign Class 2

GlobalSign Certificate Center - Windows Internet Explorer

https://system.globalsign.com[oc]public/certificate/neworder.do

File Edit View Favorites Tools Help

GlobalSign Certificate Center.

1. Account Setup 2. Product Details 3. Completed

Product Details Certificate Identity Details Payment Confirm Details

**Product Details - PersonalSign 2**

**Certificate Validity** Required

Multi-year offers, significant per annum savings

<input type="radio"/> 1 year	€63.25
<input type="radio"/> 2 year	€67.85
<input checked="" type="radio"/> 3 year	€74.75

**Campaign Code**

If you have a Campaign Code such as a Referral Code please enter and click Apply. This page will be reloaded with your appropriate discount.

**Coupon Code**

If you have a one-off Coupon Code for a particular promotion please enter and click Apply. This page will be reloaded with your appropriate discount.

**I have an externally generated CSR**

Check only if you are an Advanced User and have an externally generated Certificate Signing Request (CSR)

Yes, I have an externally generated CSR (advanced users only)

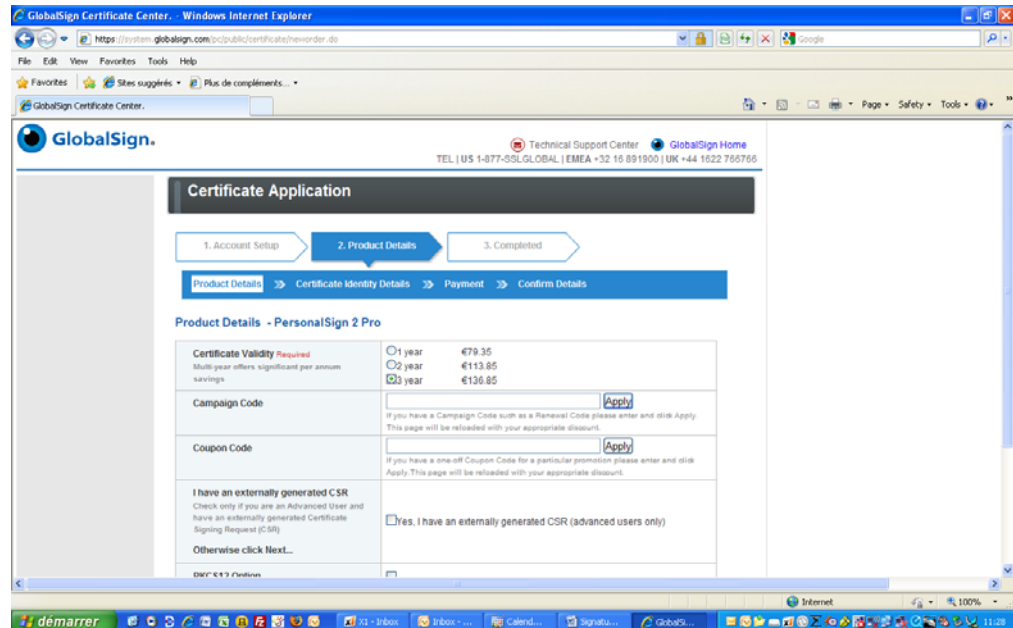
**Otherwise click Next...**

**PKCS12 Option**

**TOTAL COST (inc. Tax)** €74.75

demarrer

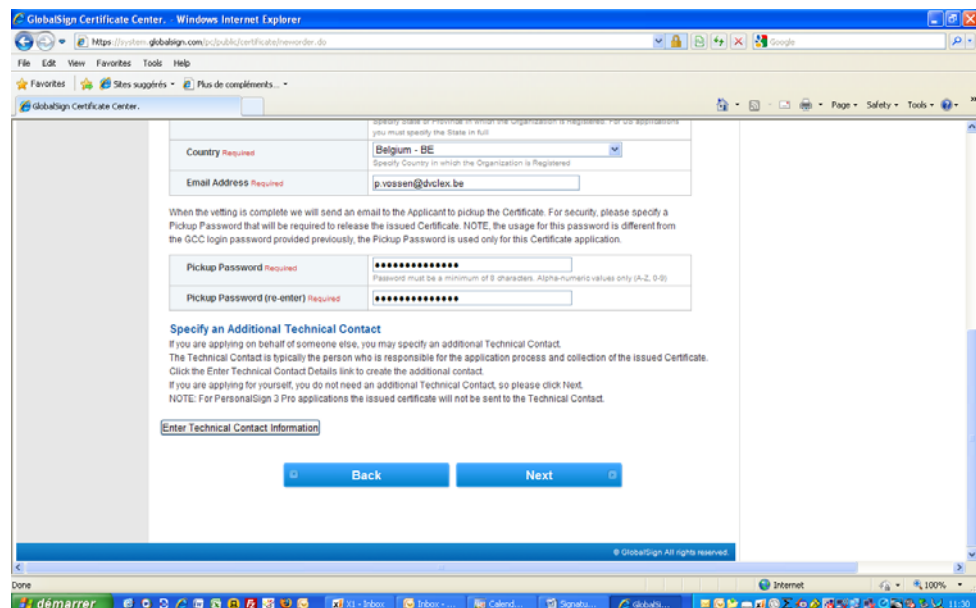
## PersonalSign Class 2 PRO



- ✓ Sous menu "Certificate Identity Details"

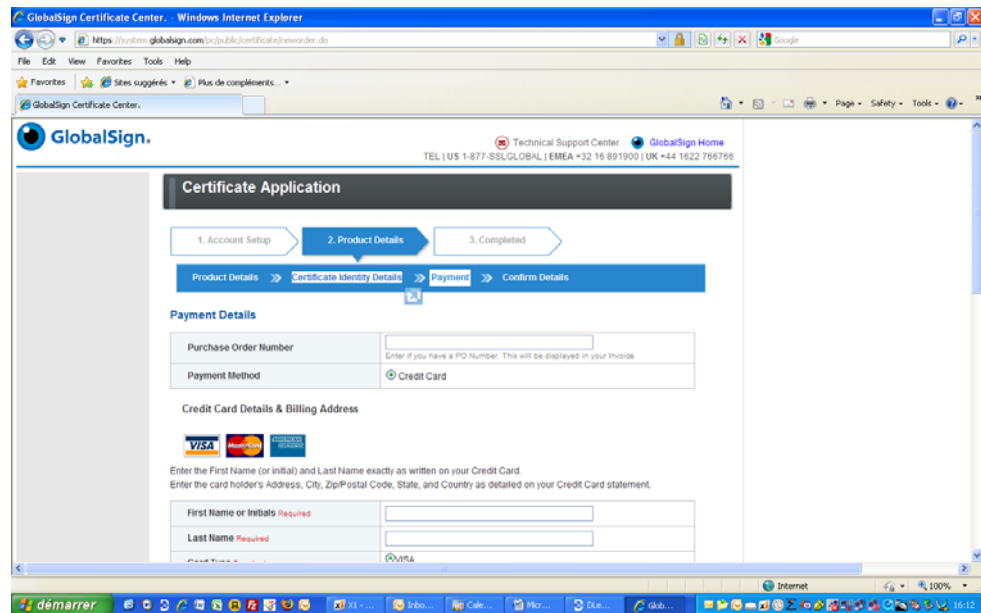
Choisissez ici un "Pickup password": ce mot de passe (qui peut être identique au précédent pour votre commodité) vous sera demandé au stade de la récolte du certificat, soit juste avant de l'installer réellement sur votre pc.

► **Conservez précieusement les codes personnels que vous encodez tout au long de cette procédure !**



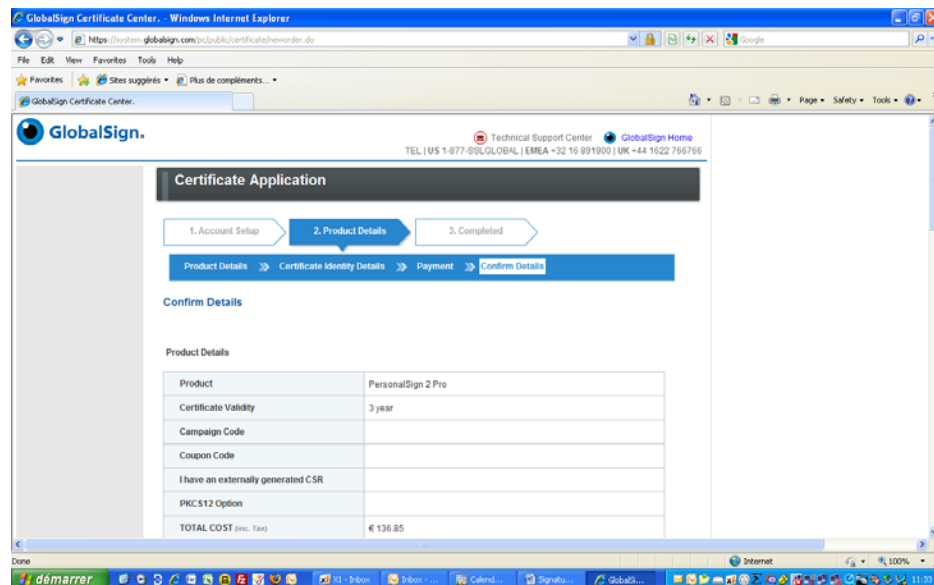
✓ Sous menu "Payment"

Procédez ici à la transaction via votre carte de crédit



✓ Sous menu "Confirm details"

Procédez ici à l'ultime confirmation de vos données et validez en acceptant les conditions de Globalsign.

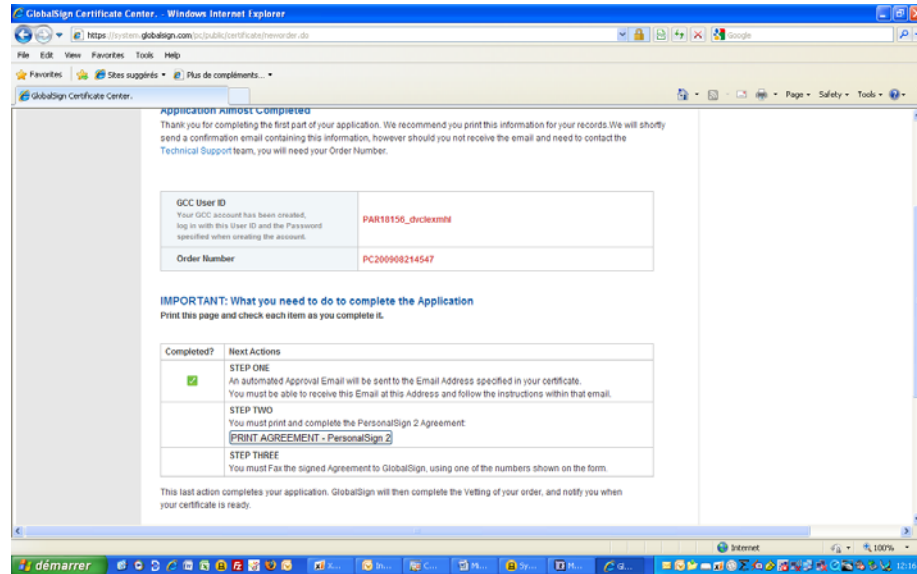


c. Completed

Cet écran vous délivre les paramètres complet d'accès au Globalsign Certificate Center (GCC) ainsi que la référence de la commande que vous venez d'effectuer. Consignez précieusement ces informations, elles vous seront utiles par la suite.

► Selon le certificat choisi (2 ou 2 PRO) l'opération suivante sera différente

PersonalSign Class 2



**Avec ce certificat, vous devez imprimer l'agrément, le dater, le signer et le faxer à l'autorité de certification GlobalSign accompagné d'une impression de votre carte d'identité.**

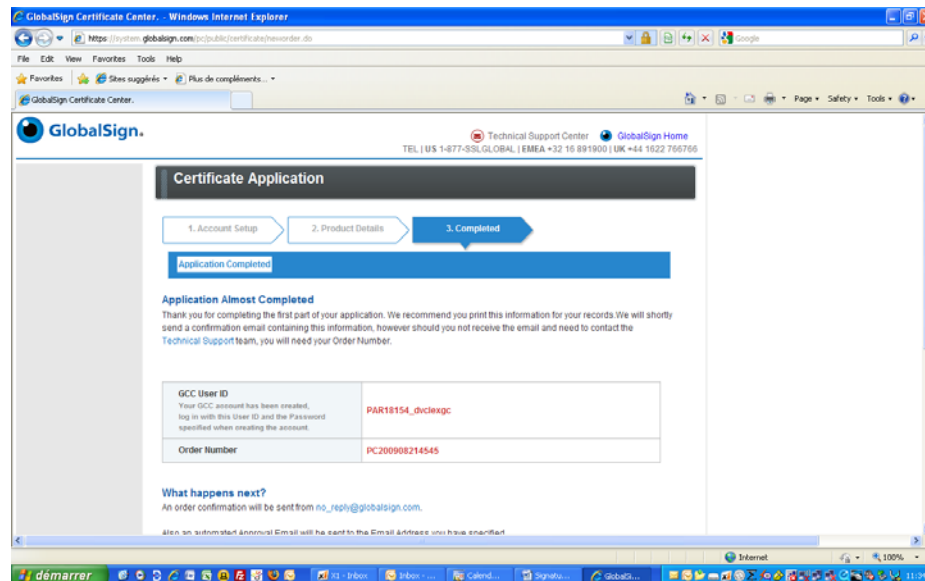
**When completed, FAX to:**

Europe:	+32 16 79 52 30
United Kingdom:	+44 1622 235589
United States:	617 830 0779

**Remember to include:**

- This Form
- A copy of your Photo ID such as Passport, Photo ID or Driving License

PersonalSign Class 2 PRO



**Ce certificat entraîne une vérification de l'autorité de certification qui s'effectue par téléphone au numéro mentionné dans le formulaire. Il vous sera demandé (en français) si vous disposez bien d'un mandat vous permettant d'engager la société en plus de votre propre personne physique.**

**Cette vérification est habituellement effectuée endéans les 24 heures qui suivent la demande.**

**Nous vous recommandons de créer un compte Globalsign Certificate Center (GCC) distinct pour chaque collaborateur afin de lui permettre d'en conserver la maîtrise en cas de départ du cabinet. L'opération ci-dessus est dès lors à répéter autant de fois qu'il y a de collaborateurs eu sein du cabinet.**

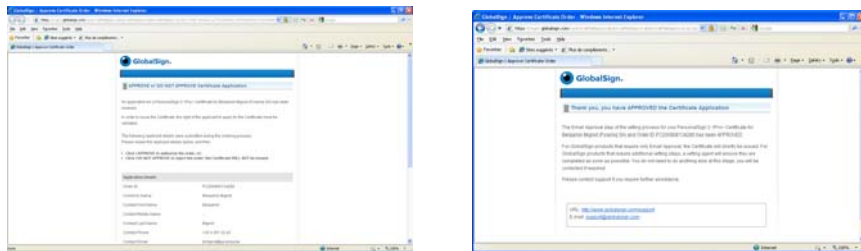
**Concernant les associés (Certificats PRO), vous pouvez en revanche utiliser le premier compte GCC créé et "ajouter" des nouveaux certificats sur ce même compte pour les autres associés.**

**En cas de difficulté dans la procédure ci-dessus, GlobalSign vous fournira le support nécessaire. Vous devez pour cela former le +32 16 89 19 00**

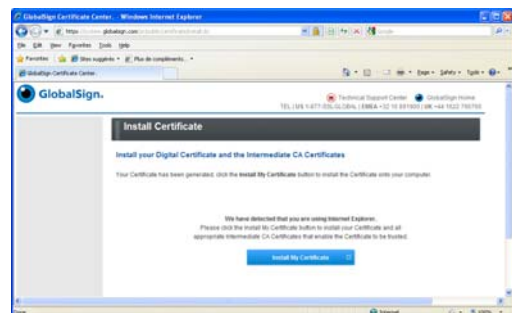
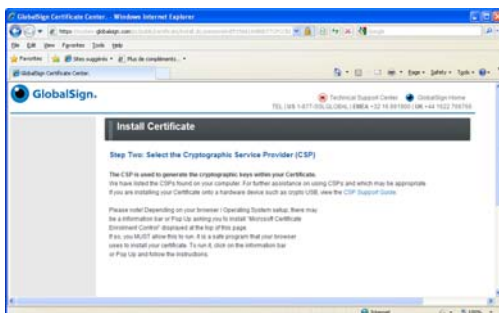
**Etape 2: gérer votre certificat de signature – Installation**

Tout au long du processus d'acquisition / installation de votre certificat, vous allez recevoir 5 emails de la part de GlobalSign:

- ✓ (1) *PC200908044058: PersonalSign 2 Order Received for <VOTRE NOM>*: confirmation de la réception de votre commande d'un certificat.
- ✓ (2) *Welcome to GlobalSign*: message de bienvenue.
- ✓ (3) *Order ID PC200908044058 GlobalSign PersonalSign 2 - Approve Application*: ce mail contient un lien sur lequel **vous devez cliquer** pour approuver le certificat afin de permettre au processus de se terminer.



- ✓ (4) *PC200908044058: PersonalSign 2 Certificate for <VOTRE NOM> is ready to be issued*: ce message contient un lien sur lequel **vous devez cliquer** pour télécharger votre certificat et l'installer sur votre PC – Vous aurez besoin ici du "pickup password" choisi plus haut. **L'installation du certificat sur votre PC sera interrompue par deux messages d'erreur Windows auxquels vous devez répondre "OUI"**.



- ✓ (5) *PC200908044058: PersonalSign 2 Certificate for <VOTRE NOM> has been issued*: ce dernier message vous confirme que vous avez bien téléchargé le certificat

### Etape 3: configuration de MS Outlook

---

L'installation d'un certificat de signature dans MS Outlook est détaillée ci-dessous pour les versions 2003 & 2007:

**Toute la procédure pour MS Outlook 2003 (anglais) sur:**

[http://www.globalsign.com/support/personal-certificate/per\\_outlook03.php](http://www.globalsign.com/support/personal-certificate/per_outlook03.php)

#### En résumé:

- ✓ Dans le menu **Outils**, cliquez sur **Options**, puis sur l'onglet **Sécurité**.
- ✓ Cliquez sur **Paramètres**.
  - ▶ Remarque Si vous possédez une identification numérique, ses paramètres d'utilisation sont automatiquement configurés à votre place. Pour utiliser une autre identification numérique, spécifiez celle-ci en suivant les étapes restantes dans cette procédure. **Ceci pourrait être le cas si vous avez préalablement installé le certificat de signature de votre carte d'identité.**
- ✓ Dans la partie inférieure de la section **Préférences des paramètres de sécurité**, cliquez sur **Nouveau**.
- ✓ Dans la zone **Nom des Paramètres de sécurité**, entrez un nom.
- ✓ Dans la liste **Format crypté**, cliquez sur **S/MIME**.
- ✓ En regard de la zone **Certificat de signature**, cliquez sur **Choisir**, puis sélectionnez votre nouveau certificat **GlobaSign Class 2** pour la signature numérique.
  - ▶ Remarque Pour savoir si le certificat est destiné à une signature numérique et au cryptage, dans la boîte de dialogue **Sélectionner un certificat**, cliquez sur **Afficher le certificat**.
- ✓ Activez la case à cocher **Envoyer ces certificats avec les messages signés** pour que tous vos messages soient signés par défaut

**Toute la procédure pour MS Outlook 2007 (anglais) sur:**

[http://www.globalsign.com/support/personal-certificate/per\\_outlook07.html](http://www.globalsign.com/support/personal-certificate/per_outlook07.html)

#### En résumé:

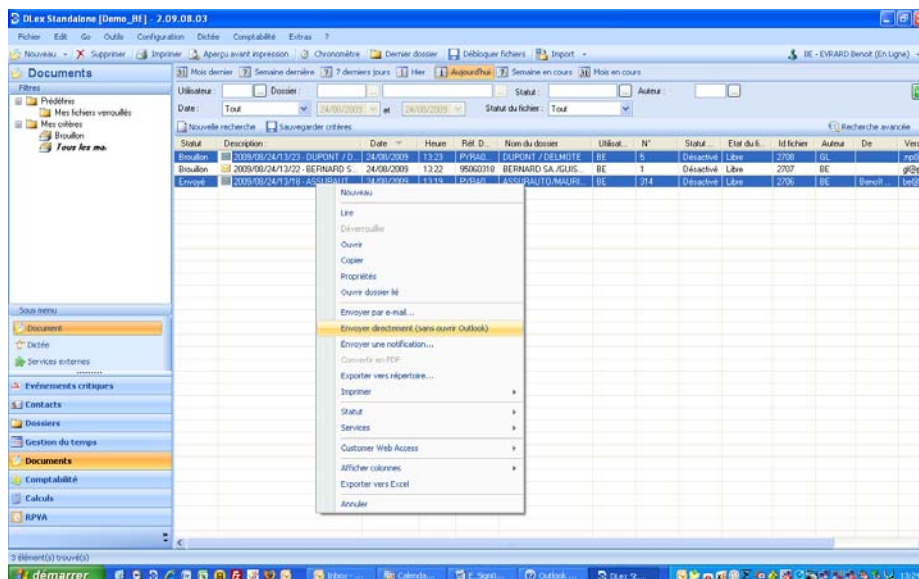
- ✓ Dans le menu **Outils**, cliquez sur **Centre de gestion de la confidentialité**, puis sur **Sécurité de messagerie électronique**.
- ✓ Sous **Courrier électronique chiffré**, cliquez sur **Paramètres**.
  - ▶ Si vous possédez une identification numérique, ses paramètres d'utilisation sont automatiquement configurés à votre place. Pour spécifier une autre identification numérique, suivez les étapes restantes de cette procédure. **Ceci pourrait être le cas si vous avez préalablement installé le certificat de signature de votre carte d'identité.**
- ✓ Dans la partie inférieure de la section **Préférences des paramètres de sécurité**, cliquez sur **Nouveau**.
- ✓ Dans la zone **Nom des Paramètres de sécurité**, entrez un nom.
- ✓ Dans la liste **Format de chiffrement**, cliquez sur **S/MIME**.
- ✓ En regard de la zone **Certificat de signature**, cliquez sur **Choisir**, puis sélectionnez votre nouveau certificat **GlobaSign Class 2** pour la signature numérique.
- ✓ Activez la case à cocher **Envoyer ces certificats avec les messages signés** pour que tous vos messages soient signés par défaut

## Etape 4: configuration de DLex®

Pour les utilisateurs de **LEXel Win®**, il convient de procéder à l'envoi des mails en utilisant la procédure qui transite par la fenêtre de création d'un nouveau message de MS Outlook. Tout ce qui vient de vous être expliqué est alors d'application.

La véritable valeur ajoutée de **DLex®** se situe dans le traitement par lot des projets d'emails à envoyer après relecture et éventuelles corrections de leurs auteurs.

1. Un projet de mail peut être abordé en mode collaboratif (brouillon, correction, relecture...)
2. Après l'ultime correction, l'avocat peut signer et envoyer directement son email signé au départ de DLex® tel qu'il le fait déjà aujourd'hui (**NE SIGNEZ LE MAIL QUE JUSTE AVANT DE L'ENVOYER**)
3. Traitement par lot: Dans **Documents**, sélectionnez les emails préalablement signés (voir ci-dessus) qui doivent être envoyés, clic-droit sur la liste et **Envoyer directement (sans ouvrir Outlook)**



4. DLex® se charge de sélectionner le certificat de signature de l'auteur et d'envoyer les mails correctement signés de la celui-ci.

## Gestion des emails entrants – AVIS IMPORTANT

► Contrairement à la plupart des logiciels, DLex® n'ajoute aucune information aux messages entrants. Ceci est capital dans le cadre des échanges électroniques entre avocats dans la mesure où l'ajout d'une information, même masquée, par votre logiciel en altère le contenu et **en fait dès lors irrémédiablement disparaître la signature électronique de l'émetteur**, et donc la preuve au sens juridique du terme.

### Etape 5: sauvegarder votre certificat

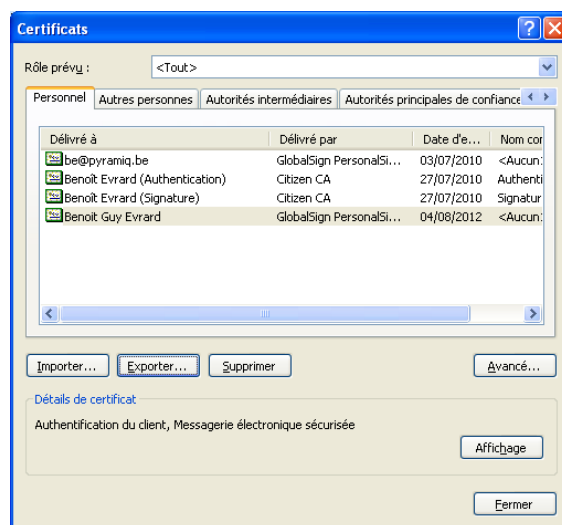
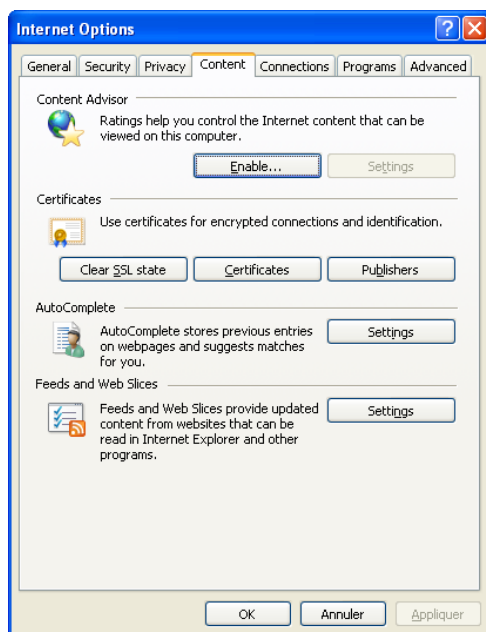
En cas d'incident majeur ou de mises à jour du système d'exploitation, votre certificat sera effacé de votre poste de travail. Pour des raisons de sécurité, aucune copie de votre certificat n'est conservée par GlobalSign, il vous incombe donc intégralement d'en assurer la sauvegarde.

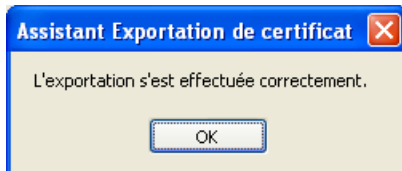
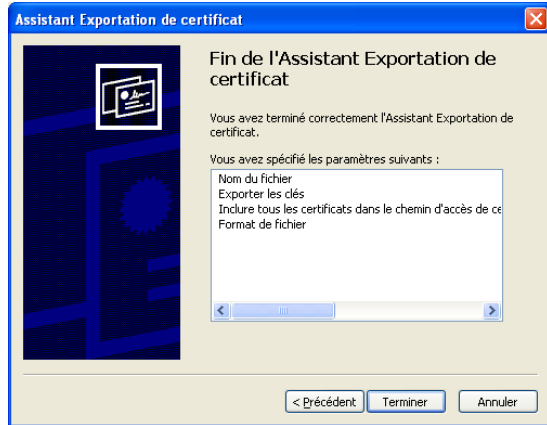
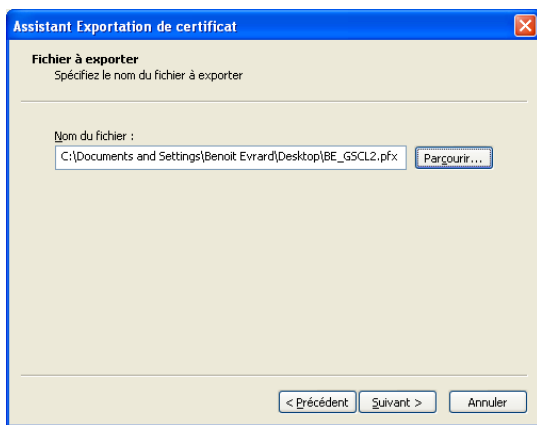
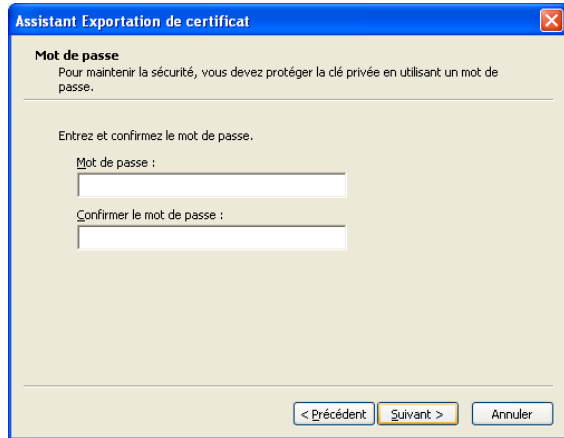
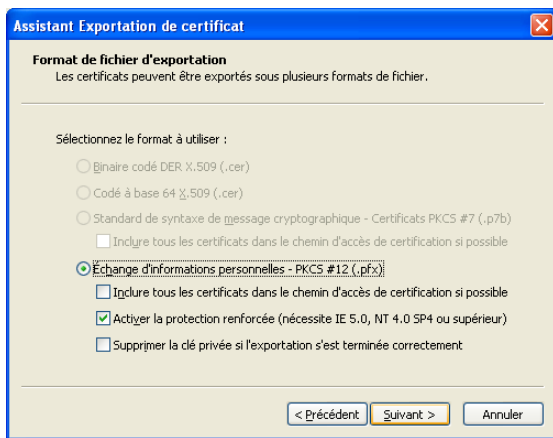
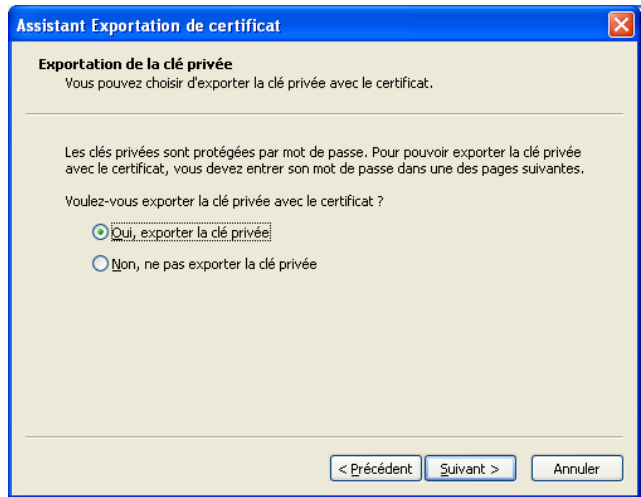
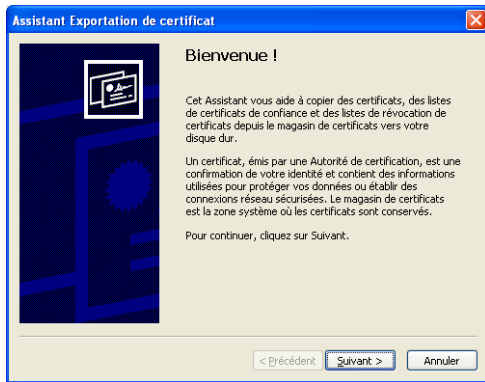
Votre certificat peut être exporté physiquement à tout endroit de votre poste de travail, de votre réseau ou sur une clé USB. Une fois votre certificat ainsi exporté copié ou déplacé sur un support externe (CD-ROM, clé USB, disque dur externe), effacez bien la copie provisoire réalisée sur votre poste de travail.

Pour ce faire suivez la procédure ci-dessous:

- ✓ Dans Internet Explorer : outils / options / onglet contenu / bouton certificat / choisir le certificat GlobalSign class 2 ou 2 PRO / exporter
- ✓ Suivant
- ✓ Choisir l'option "exporter la clé privée" sans quoi votre sauvegarde ne vous sera d'aucune utilité
- ✓ Suivant
- ✓ Suivant : encoder un mot de passe que vous devrez utiliser si vous devez réinstaller, votre certificat. **Ne pas mettre de mot de passe peut avoir des conséquences extrêmement dangereuses.**
- ✓ Suivant : choisir le répertoire de destination temporaire
- ✓ Terminer
- ✓ Déplacer ensuite le fichier .pfx créé sur un support externe
- ✓ Effacer-le du répertoire temporairement utilisé.

### Voir séquence illustrée ci-dessous





**Remarque importante**

Toutes les informations communiquées dans le cadre de ce nouveau règlement le sont de bonne foi. De même, l'intégration de cette nouvelle fonctionnalité dans DLex® vous est proposée d'initiative et sans coût à votre charge.

Néanmoins, s'agissant ici de la mise en œuvre d'une nouvelle fonctionnalité et non d'une évolution "naturelle" de votre logiciel, **toute assistance complémentaire fera l'objet d'une facturation en régie à notre tarif en vigueur.**

## SYNTHESE DE LA PROCEDURE

- |  |         |
|--|---------|
| 1. Achat du (des) certificat(s)                  | Etape 1 |
| 2. Installation du certificat sur votre PC       | Etape 2 |
| 3. Installation du certificat dans votre Outlook | Etape 3 |
| 4. Configuration de DLex®                        | Etape 4 |
| 5. Sauvegarder votre certificat                  | Etape 5 |