PaPyRuS : sécurité et contrôle des documents PDF

Les documents sont certifiés par Belfius Banque au moyen d'un certificat émis par Certipost.

La signature garantit :

- **Intégrité:** est-ce bien un document original qui n'a pas été modifié ?
- **Authenticité**: est-ce bien un document original fournit par Belfius ? Le contrôle est fait sur base d'un certificat root. Cela nous assure l'authenticité de la signature.
- **Non révocation:** le certificat utilisé pour la signature est-il non révoqué (pas annulé) et toujours valable au moment de l'utilisation ?

Pour pouvoir vérifier ces 3 points, il faut installer un certificat-racine (root-certificate) sur votre PC.

Le contrôle électronique de la signature ne fonctionne qu'avec le logiciel ADOBE READER version 7 ou supérieure. L'utilisation d'une version antérieure donne un message d'erreur. Cette non-compatibilité est un problème lié au logiciel lui-même. Nous recommandons dès lors une mise à jour gratuite de la version d'ADOBE READER (à partir de www.adobe.be).

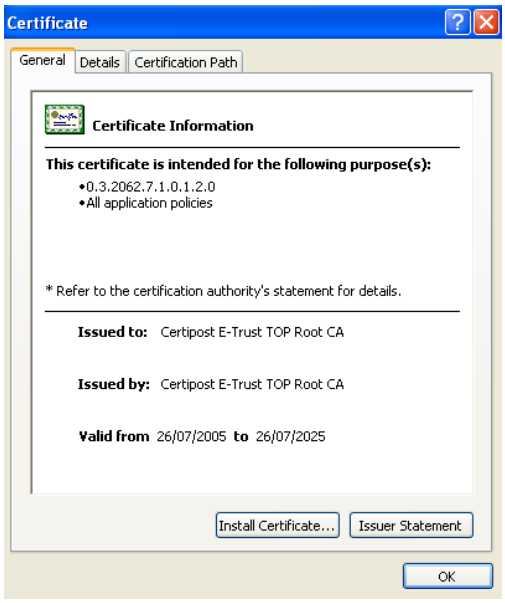
Pour installer le certificat, deux procédures peuvent être suivies (au choix) => Suivre les étapes de la procédure 1 **ou** de la procédure 2.

Procédure 1 : installation via Windows & configuration de l'Adobe Reader

Etape 1 : Installation du certificat à partir de WINDOWS

Le 'root-certificate' est disponible directement sur le site de Certipost (source indépendante)

- Cliquez sur le lien : http://www.certipost.be/download/trust/certs/cacer.crt
- Une fenêtre apparaît vous proposant d'ouvrir (open) ou sauvegarder (save) le fichier « cacer.cer ». Choisissez « ouvrir » puis encore une fois « ouvrir »
- Une nouvelle fenêtre qui affiche les caractéristiques du certificat s'ouvre.

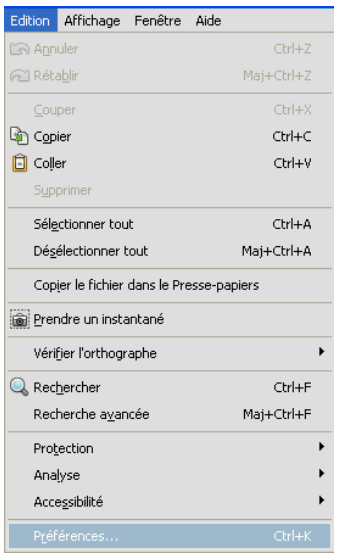


- Cliquez sur le bouton « INSTALL CERTIFICATE ». Il suffit ensuite de confirmer les options par défaut proposées (choisir 'Next' deux fois de suite et ensuite 'Finish'). La fenêtre indique alors que le certificat a été correctement installé.

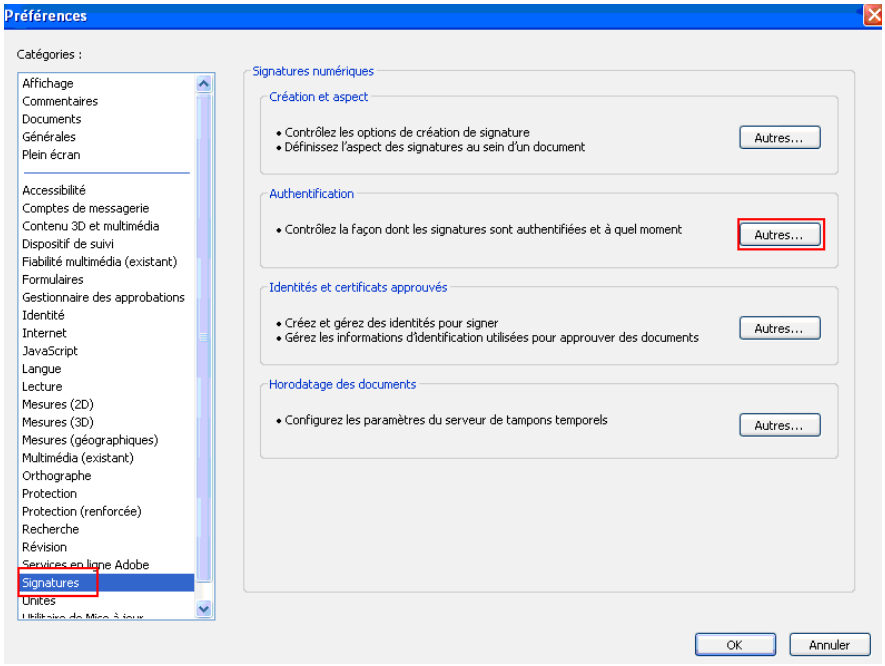
Via cette procédure le certificat a été installé dans le 'root-store' de Windows.
L'étape suivante permettra d'indiquer que l'application ADOBE peut utiliser ce certificat.

Etape 2 : Configuration de l'application ADOBE

- **Ouvrez Adobe Reader** puis allez dans le menu **« Edition »-« Préférences… »**



- A gauche, au niveau des catégories, cliquez sur le menu « Signatures » puis sur le bouton « autres » au niveau du menu « Authentification ».



- Sur l'écran obtenu (préférences d'authentification des signatures) :

  - **Sous le menu « Comportement d'authentification** », DESACTIVEZ « exiger la vérification de révocation des certificats lors de l'authentification des signatures »

    Cette option indique si le contrôle de non-révocation doit être réalisé. Il faut savoir que ce contrôle est opéré via l'internet (le pc doit être connecté à l'internet) et demande donc une connexion internet. Vu la valeur ajoutée limitée de ce contrôle et le fait qu'il dépende de votre connexion internet, <u>vous êtes libre de choisir si cette option doit être activée ou pas.</u>

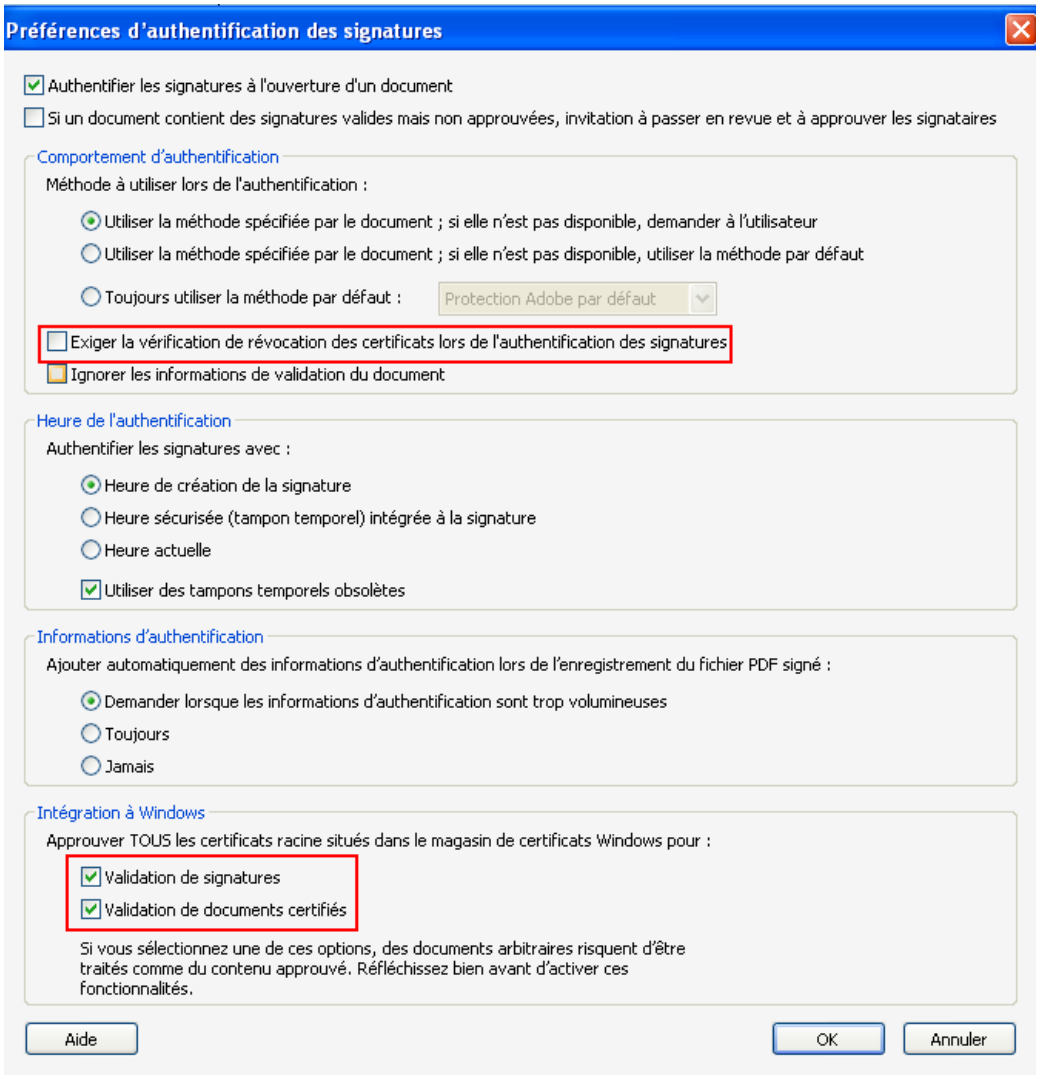
    Le contrôle de non révocation est nécessaire pour vérifier que le certificat que Belfius Banque utilise pour mettre la signature électronique n'est pas révoqué. Une révocation de certificat est –dans le cas de Papyrus »- purement théorique. Ces certificats sont en effet installés sur du matériel sécurisé et n'ont pas de valeur commerciale (ils sont seulement utilisés pour signer nos documents de reporting). Le risque que ce certificat soit un jour « volé » est nul et ce certificat ne pourrait jamais se trouver sur une liste CRL (liste des certificats révoqués)

    <u>Remarque</u> (si vous activez l'option): si votre accès internet utilise un proxy, n'oubliez pas de paramétrer votre proxy pour qu'il autorise le contrôle de liste CRL. Il doit notamment veiller à ce que

    a) il n'y ait pas de « caching » des crl's
    b) Il n'y ait pas d'authentification ou une authentification http/1.0 pour le site de certipost.

- **Sous le menu « Intégration à Windows »,** COCHEZ les 2 options

- **Cliquez sur OK**



Remarque : les paramètres ne doivent être définis qu'une seule fois par PC, car ceux-ci sont sauvegardés. Les règles choisies seront dès lors appliquées lors de l'ouverture du prochain document.
Si un document est déjà ouvert, celui-ci peut être recontrôlé. Il faut, pour ce faire, cliquez avec le bouton droit sur l'image de la signature et choisir l'option '**Signature**'

Procédure 2 : installation directement à partir d'adobe.

Si vous avez suivi la procédure1, cette procédure-ci n'est pas nécessaire.

Etape 1 : sauvegarde du root-certificat

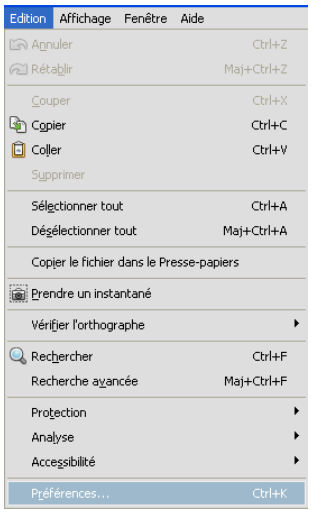
Le 'root-certificate' est disponible directement sur le site de Certipost (source indépendante)

- Cliquez sur le lien : http://www.certipost.be/download/trust/certs/cacer.crt

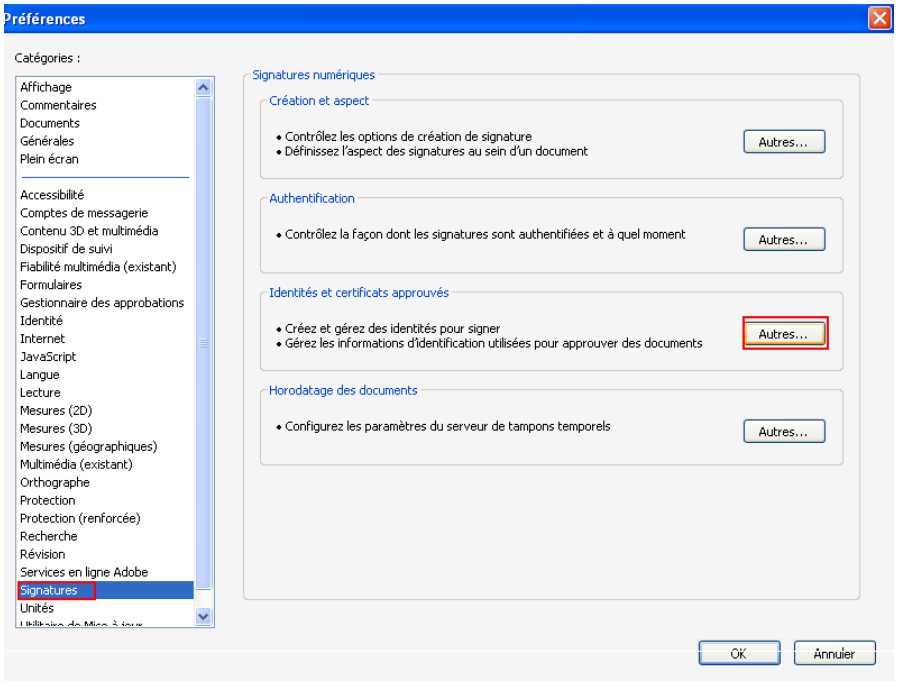
- Une fenêtre apparaît vous proposant d'ouvrir (open) ou sauvegarder (save) le fichier « cacer.cer ». Choisissez « sauvegarder » et désigner l'endroit où il doit être sauvegardé.

Etape 2 : installation du certificat à partir d'Adobe Reader

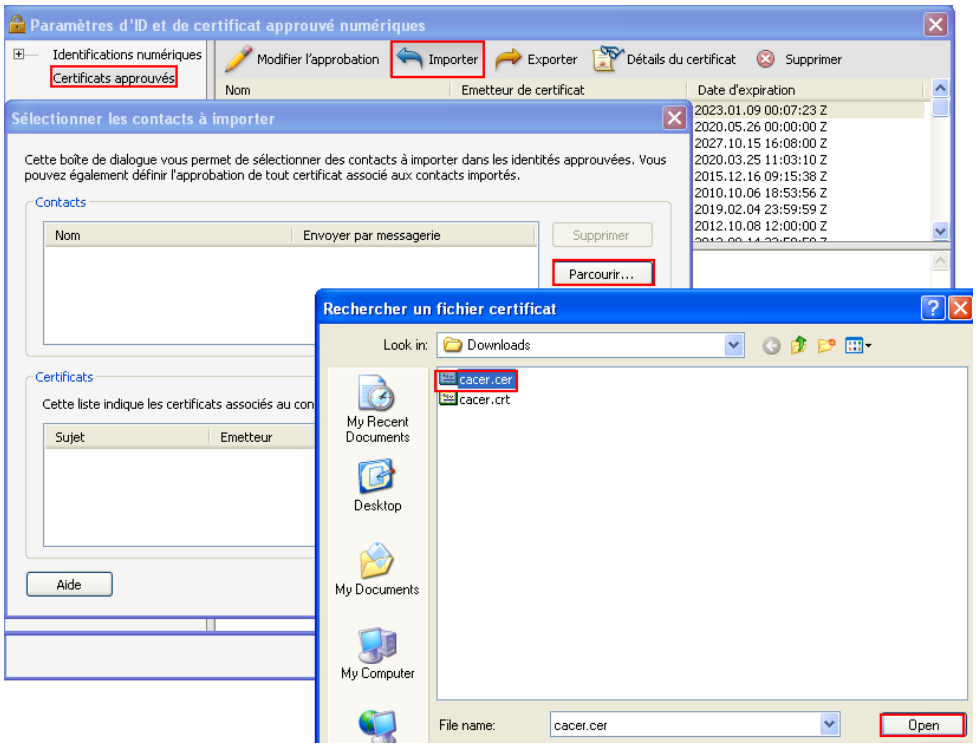
- **Ouvrez Adobe Reader** puis allez dans le menu **« Edition »-« Préférences…** »



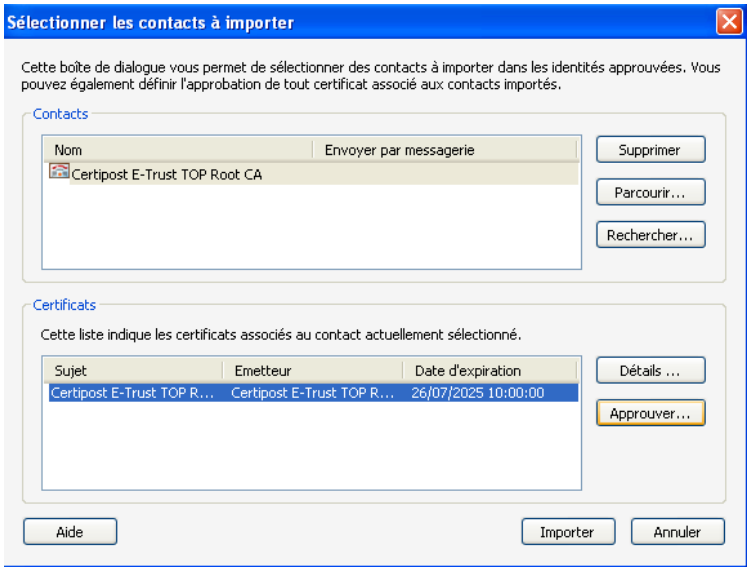
- Sur la gauche, au niveau des catégories, cliquez sur le menu « Signatures » puis sur le bouton « Autres …» au niveau de « identités et certificats approuvés » .



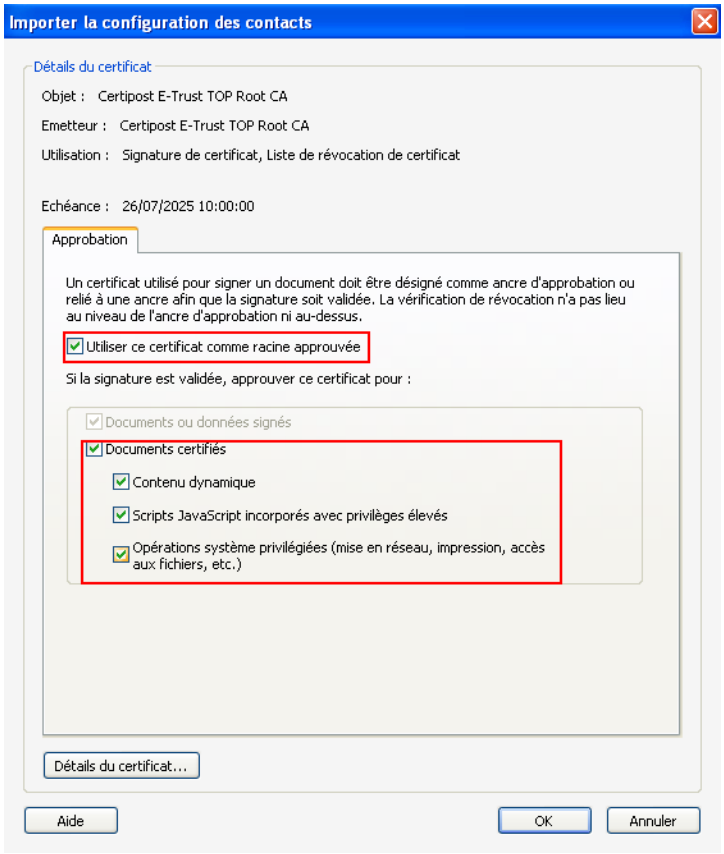
- Sur l'écran obtenu (paramètres d'ID et de certificat approuvé numériques) :
  - Cliquez sur « certificats approuvés » (menu à gauche)
  - Cliquez sur « importer » (en haut)
  - Via le bouton « parcourir … » retrouvez le certificat que vous avez au préalable sauvegardé (étape 1).
  - Sélectionnez le certificat puis cliquez sur « ouvrir »



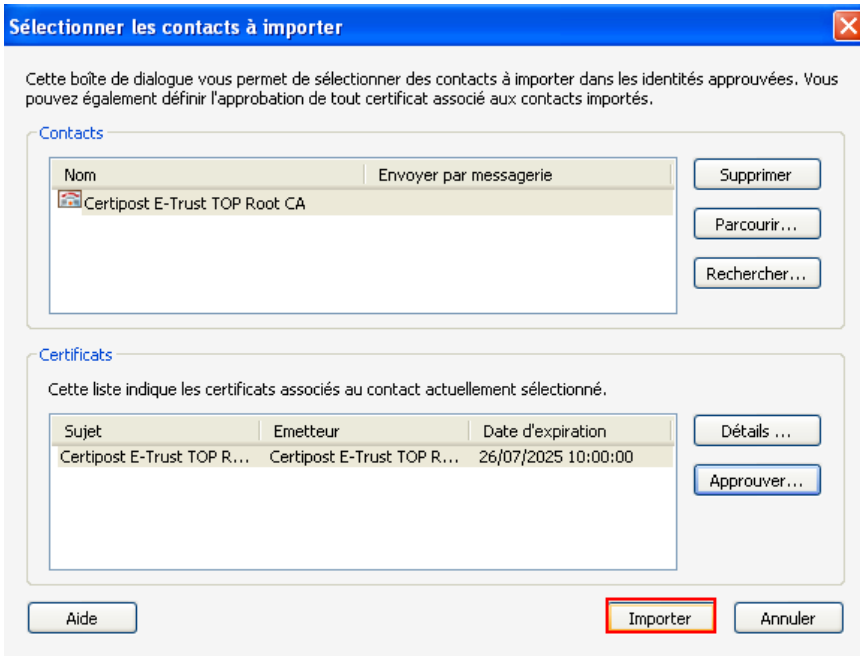
- Sélectionnez-le dans la seconde partie de la fenêtre et cliquez ensuite sur « approuver… »



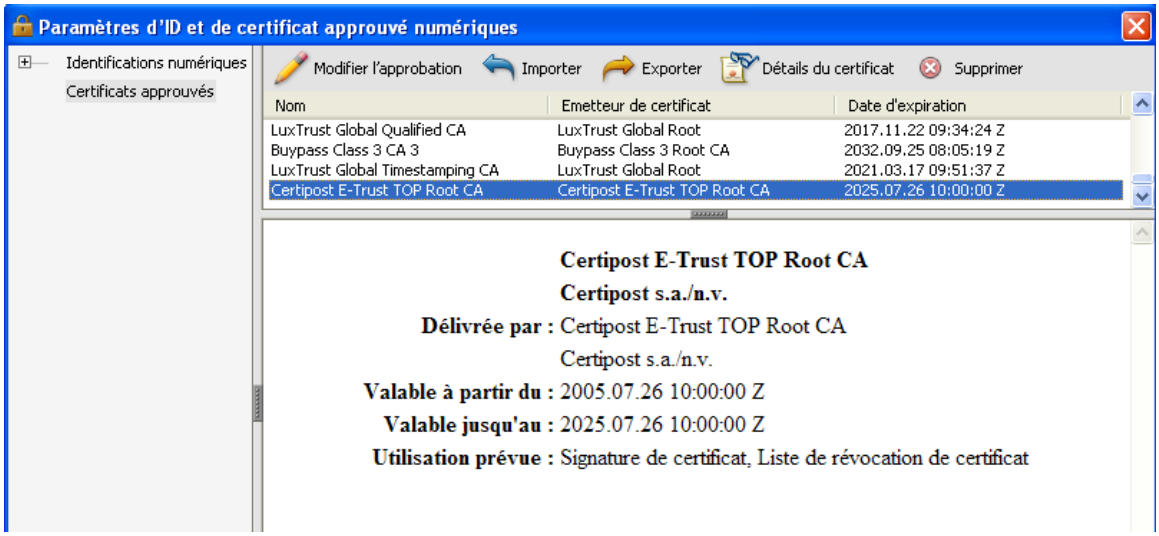
- Activez « utiliser ce certificat comme racine approuvée » et les autres options puis cliquez sur OK.



- Cliquez sur « importer »



Le certificat se trouve maintenant dans la liste des certificats approuvés :



Comment contrôler un document ouvert ?

Une fois les options précédentes réalisées, le contrôle est automatique et chaque document ouvert sera contrôlé.

- Si vous obtenez comme résultat :  , vous pouvez considérer votre document comme entièrement valide et intègre.

- Si vous obtenez comme résultat  , cela signifie que le système a détecté une erreur :

    - soit vous utilisez une version d'Adobe non compatible (version 6 ou moins) ;
    - soit le document a bel et bien été modifié depuis sa signature. Dans certains cas, la version initiale du document peut être retrouvée via un clic droit sur le dessin de la signature et en choisissant l'option 'View signed version'. Nous vous rappelons que les versions originales du document peuvent toujours être obtenues via BelfiusWeb.

- Si vous obtenez comme résultat :  , cela signifie que le contrôle n'a pas montré d'irrégularité mais que l'identité de Belfius Banque n'a pas pu être confirmée :

    - soit parce que le 'root-certificate' n'a pas été correctement installé ;
    - soit parce que le système a voulu contrôler la 'non-révocation' mais que le serveur de contrôle sur internet n'est pas accessible.

    Ce problème de contrôle de la 'non-révocation' est soit lié à un problème d'accès à internet, soit lié au fait que votre accès internet n'autorise pas le contrôle de liste CRL (lié au proxy). Vous pouvez consulter votre responsable IT et demandez qu'il vérifie les paramètres d'accès via le proxy. Celui ci doit notamment veiller à ce que

    a) il n'y ait pas de « caching » des crl's

    b) Il n'y ait pas d'authentification ou une authentification http/1.0 pour le site de certipost.

    Une autre alternative à ces problèmes d'accès est de désactiver le contrôle du crl (contrôle dont la valeur ajoutée est limitée) : il suffit de suivre l'étape 2 de la procédure 1 et désactiver l'option « exiger la vérification de révocation des certificats lors de l'authentification des signatures ».
    Plus de détails sur la signature peuvent être obtenus via l'onglet 'signatures' à gauche du document.