Contrôle électronique des documents certifiés

Les documents ont été certifiés (signés) par Dexia Banque au moyen d'un certificat émis par Certipost.

La signature garantit les éléments suivants :

- **L'intégrité** : vous êtes certains que le document n'a pas été modifié depuis sa signature.

- **L'authenticité** : Vous êtes certains que le document a été signé par le signataire mentionné dans le certificat, en l'occurrence Dexia Banque Belgique. En installant le certificat racine de Certipost et en l'utilisant pour le contrôle, vous êtes également certain de l'authenticité du signataire (donc que le certificat a bien été attribué à Dexia Banque).

- **La non-répudiation :** Vous êtes certain que le certificat utilisé pour signer les documents n'a pas été révoqué et est toujours valable au moment de son utilisation.

Afin de permettre ces 3 niveaux de contrôles, il est nécessaire d'installer le certificat racine (root-certificate) de CertiPost. Cette installation ne doit avoir lieu qu'une seule fois par PC.

Le contrôle électronique de la signature ne fonctionne qu'avec le logiciel ADOBE READER version 7 et supérieur. L'utilisation d'une version antérieure donne un message d'erreur. Cette non-compatibilité provient du fait que le certificat utilisé est un certificat de dernière génération (2048 bits) non compatibles avec les anciennes versions d'Adobe. Nous recommandons dès lors une mise à jour gratuite de la version d'ADOBE READER (à partir de www.adobe.be). Cette mise à jour est disponible pour tout PC équipé d'une version égale ou supérieure à Windows 2000 SP 3.
Si vous ne pouvez pas installer Adobe 7 et que vous utilisez Adobe 6, vous recevrez un message indiquant que la signature n'est pas valable. Il ne faut pas tenir compte de ce message.

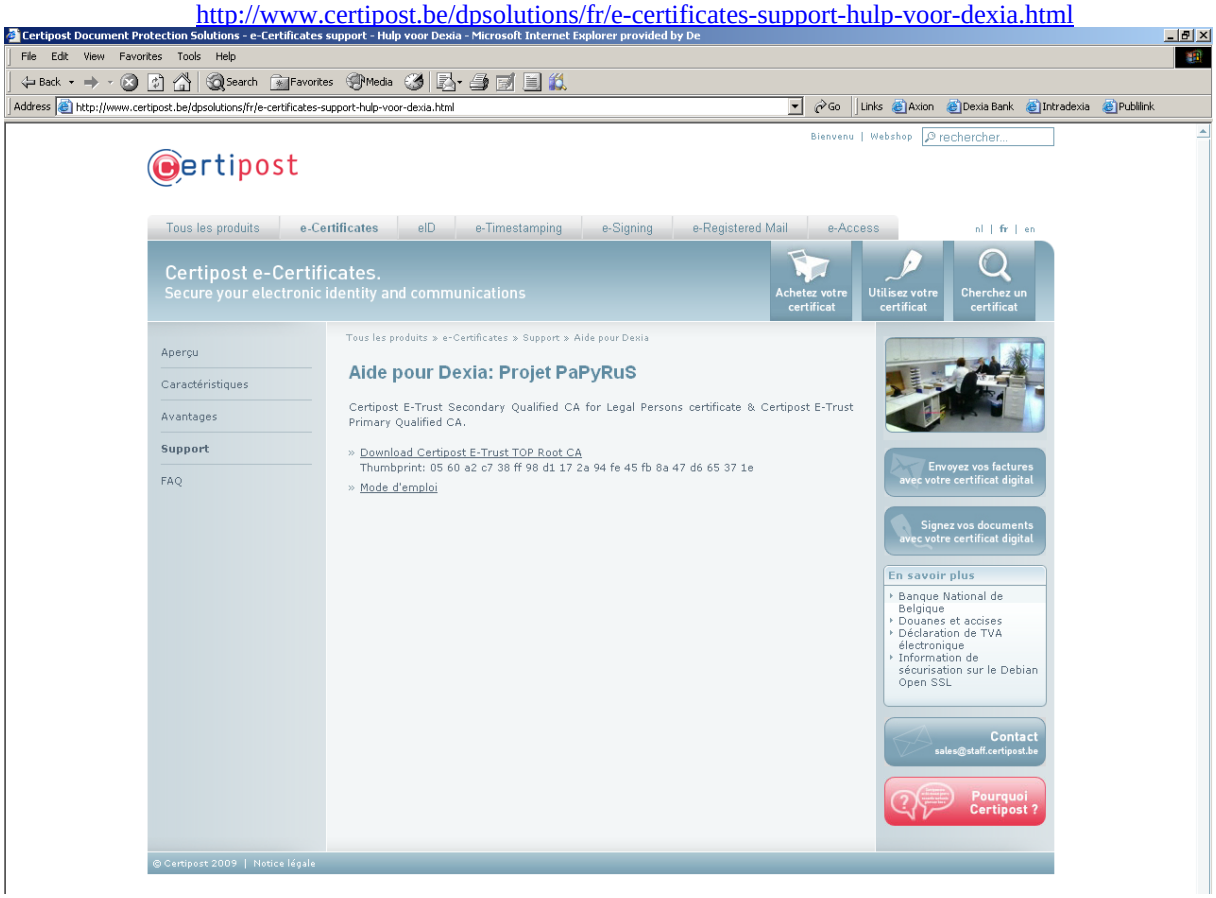
Pour installer le certificat, deux procédures peuvent être suivies (au choix) => Suivre les étapes du chapitre 1 **ou** du chapitre 2.

Remarque : Les copies d'écran et les termes des logiciels Windows et Adobe mentionnés dans ce document proviennent de la version anglaise. Si vous possédez une version en français ou en néerlandais, les termes utilisés seront différents mais la procédure à suivre est identique.

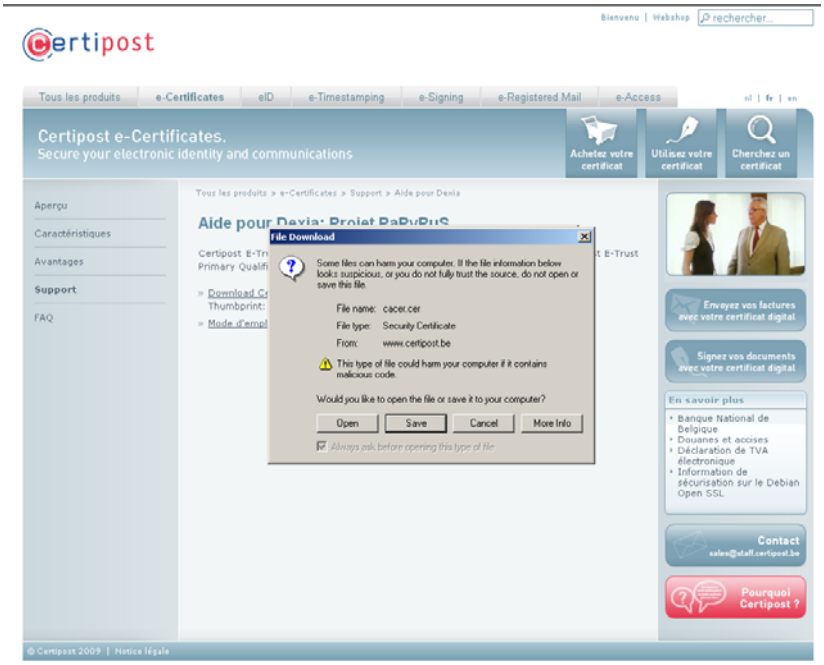
1. INSTALLATION via WINDOWS & CONFIGURATION DE L'ADOBE READER

1.1. Installation à partir de WINDOWS

- Le 'root-certificate' est disponible :
  - soit à partir du site internet dédié au projet PAPYRUS
  - soit directement à partir du site de Certipost (source indépendante) : http://www.certipost.be/dpsolutions/fr/e-certificates-support-hulp-voor-dexia.html

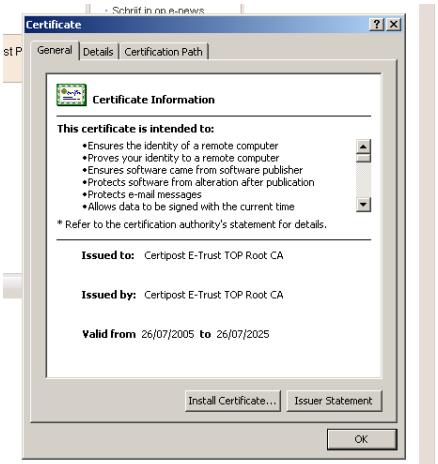


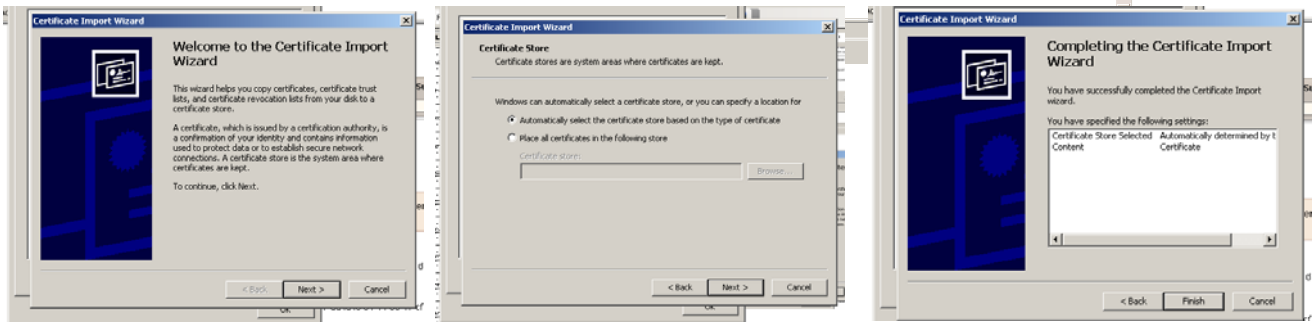
- Surfez sur le site mentionné et cliquez sur le certificat **« Download Certipost E-Trust TOP Root CA Thumbprint: 05 60 a2 c7 38 ff 98 d1 17 2a 94 fe 45 fb 8a 47 d6 65 37 1e »**.



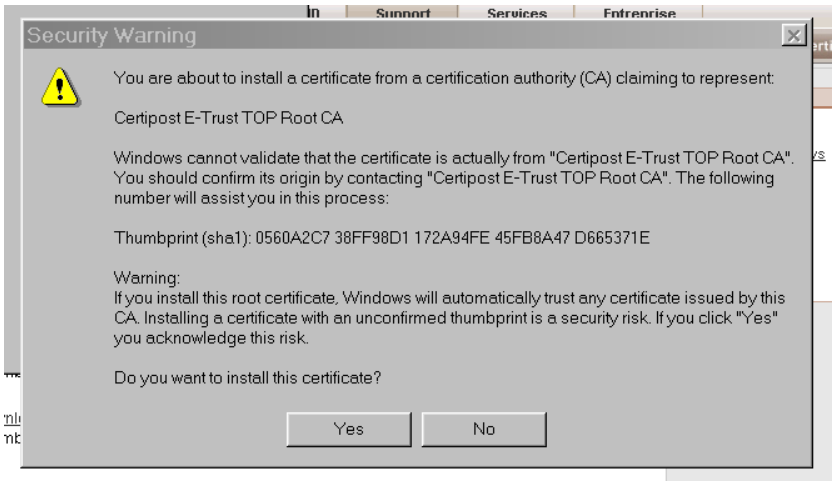
- Une fenêtre apparaît et demande si le fichier doit être ouvert (« Open ») ou enregistré (« Save »). Choisissez « Open ».

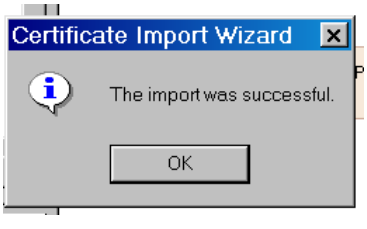
- Une fenêtre apparaît et affiche les caractéristiques du certificat. Cliquez sur le bouton « INSTALL CERTIFICATE ».





Il suffit ensuite de confirmer les options par défaut proposées (choisir ‘Next’ deux fois de suite et ensuite ‘Finish’).



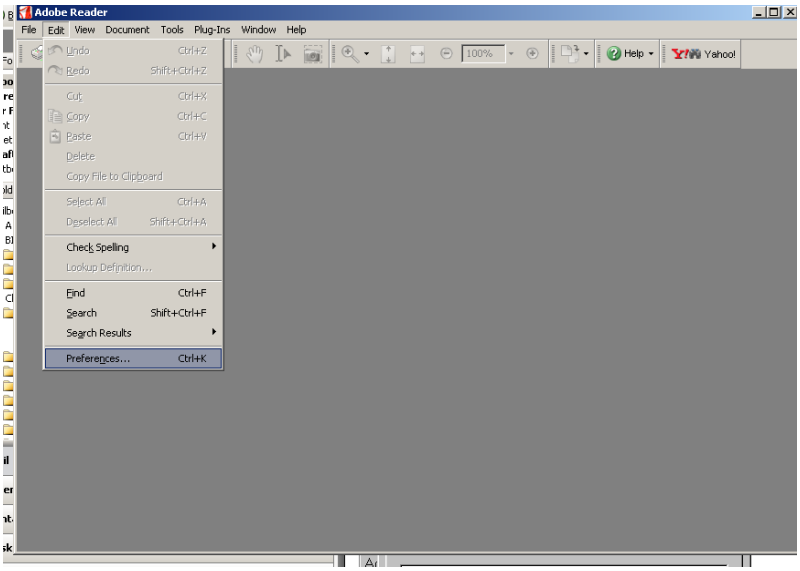


La fenêtre affiche encore un écran de confirmation : choisir « Yes », puis « OK »

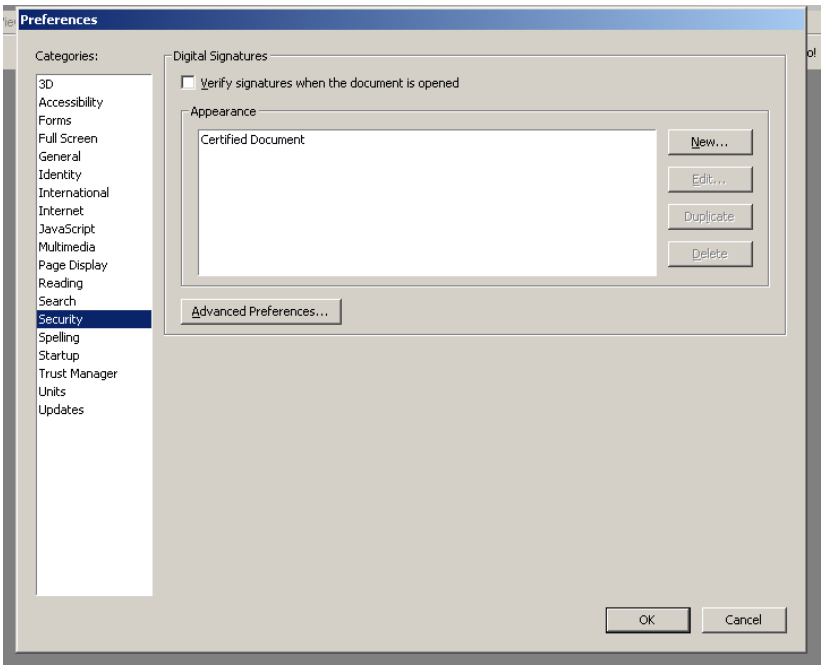
- Via cette procédure le certificat a été installé dans le ‘root-store’ de Windows. L’étape 2 permettra d’indiquer que l’application ADOBE peut utiliser ce certificat.

1.2. Configuration de l'application ADOBE (adobe reader 7.0).

Choisissez le menu EDIT / PREFERENCES => une fenêtre va s'ouvrir.



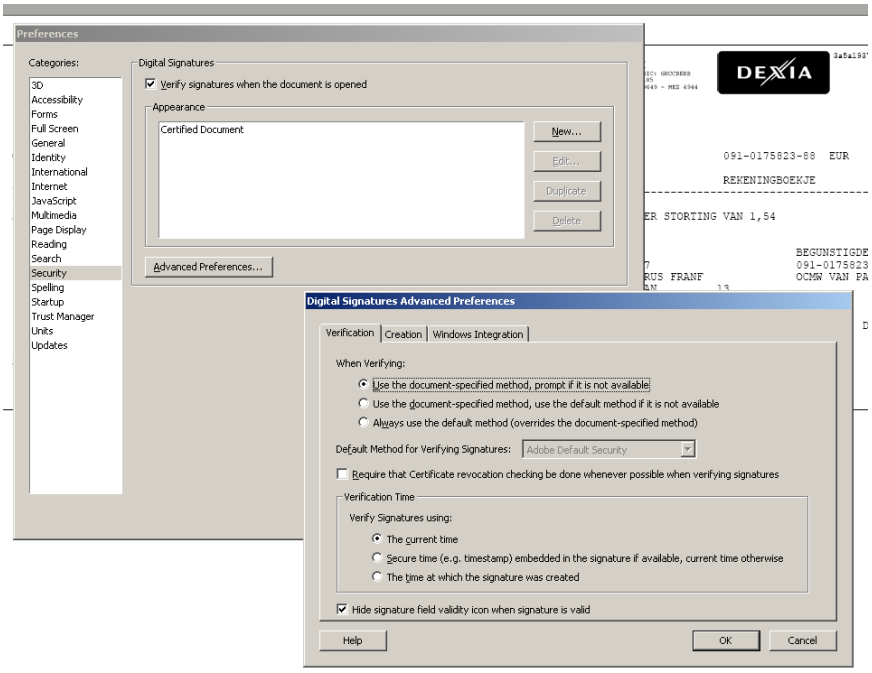
Choisissez le chapitre SECURITY/ADVANCED PREFERENCE



La nouvelle fenêtre contient trois onglets.

Onglet 1 : VERIFICATION

L'option **'require that certificate revocation checking be done…"** 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 connection internet. Vu la valeur ajoutée limitée* de ce contrôle et le fait qu'il dépende de votre connexion internet, vous êtes libre de choisir si cette option doit être activée ou pas.



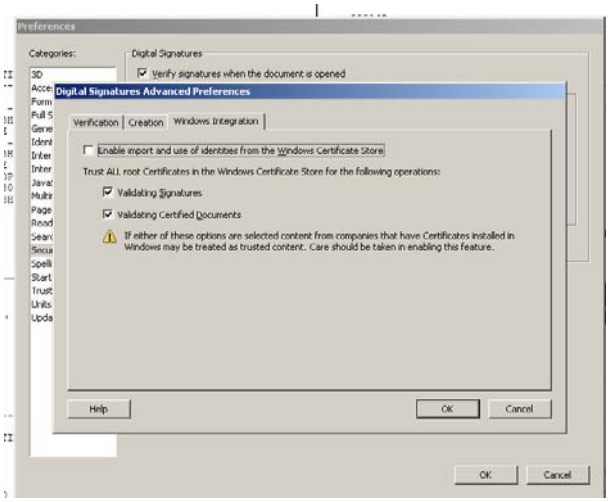
Remarque complémentaire
(uniquement si l'option mentionnée est activée).

Le contrôle CRL transite via Internet : il faut également veiller –si vous accéder à internet via un proxy- à ce que celui-ci soit paramétré pour permettre ce contrôle CRL. Contactez votre gestionnaire de réseau à ce sujet. 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.

**Le contrôle de non révocation est utile pour vérifier que le certificat utilisé par Dexia Banque pour apposer la signature du document n'est pas révoqué au moment de la signature. Une révocation d'un certificat est –dans ce cadre- un événement purement théorique. En effet ces certificats sont d'une part installés sur des appareils sécurisés et protégés de Dexia Banque et d'autre part n'ont pas de valeur marchande (ils ne sont utilisés que dans le cadre de PaPyRuS). Le risque de « corruption » ou de « vol » du certificat est donc inexistant et celui ci ne devrait jamais apparaître sur la liste CRL (liste des certificats révoqués).*

Onglet 3 : Windows Integration : cochez l'option '**Validating certified document'**.



En effet, vous avez –dans la première étape- installé le certificat via Windows. Le contrôle du document s'opérant via ADOBE, cette option indique que ADOBE peut utiliser les certificats intégrés en Windows.

Vous pouvez dès lors fermer les fenêtres ouvertes en cliquant deux fois sur OK.

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, cliquer avec le bouton droit sur l'image de la signature et choisir l'option '**Validate Signature**'

2. INSTALLATION directement à partir d'ADOBE.

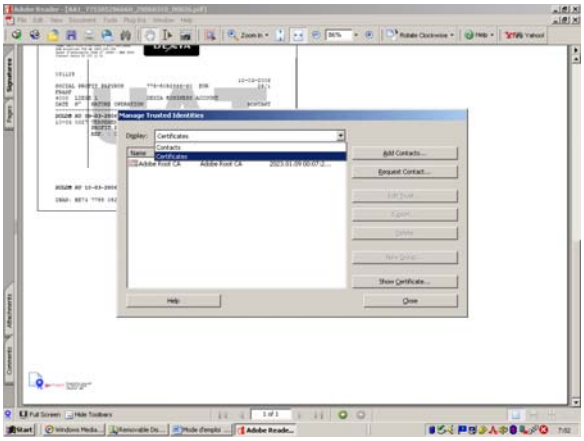
Si vous avez suivi la procédure reprise sous le point 1, cette procédure-ci n'est pas nécessaire.

- Le 'root-certificate' est disponible :
  - soit à partir du site internet dédié au projet PAPYRUS :
  - soit directement à partir du site de Certipost (source indépendante) : http://www.certipost.be/dpsolutions/fr/e-certificates-support-hulp-voor-dexia.html

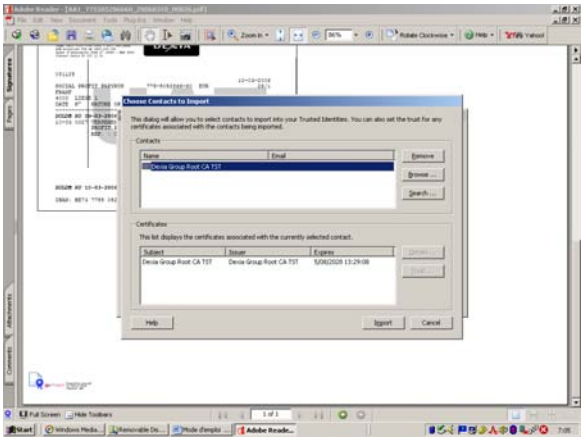
- Surfez sur le site mentionné et cliquez sur le certificat**« Download Certipost E-Trust TOP Root CA Thumbprint: 05 60 a2 c7 38 ff 98 d1 17 2a 94 fe 45 fb 8a 47 d6 65 37 1e ».** Une fenêtre apparaît et demande si le fichier doit être ouvert (« Open ») ou enregistré (« Save »). Choisissez « SAVE ». Vous devez ensuite choisir l'endroit ou le certificat doit être enregistré (en local).

Dans l'application ADOBE, choisissez Menu DOCUMENT / TRUSTED IDENTITIES => une fenêtre s'ouvre.

Dans le 'display', choisissez le sujet « CERTIFICATES » et ensuite cliquez sur le bouton 'Add Contacts..'.

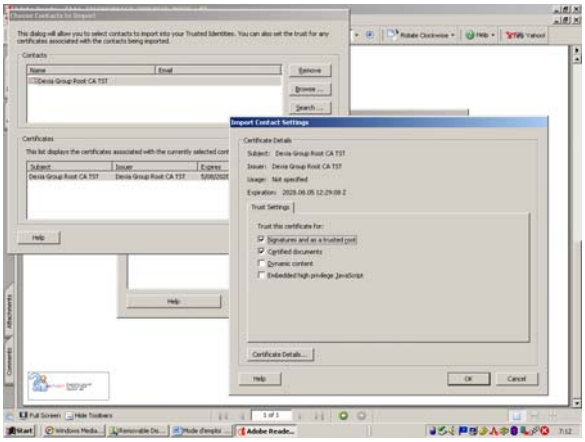


Une seconde fenêtre s'ouvre. Choisissez l'option 'BROWSE' et retrouvez le certificat que vous avez au préalable sauvegardé. Sélectionnez-le dans la seconde partie de la fenêtre et cliquez ensuite sur TRUST.



La fenêtre suivante permet de choisir les caractérisques d'utilisation du certificat. Choisissez les options « signature and as a trusted root » & « Certified Document ». Cliquez sur OK.

Le certificat est dès lors directement installé parmi les 'trusted identities' d'Adobe.



3. COMMENT CONTRÔLER LE DOCUMENT OUVERT

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

Si vous obtenez un résultat comme le montre l'image n°1, vous pouvez considérer votre document comme entièrement valide et intègre.

Si vous obtenez un résultat comme le montre l'image n°2, 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 –dans certains cas- 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 PUBLIWEB.

Si vous obtenez un résultat comme le montre l'image 3, cela signifie que le contrôle n'a pas montré d'irrégularité mais que l'identité de Dexia 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

c) il n'y ait pas de « caching » des crl's
d) 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 généralement de procéder de nouveau aux options décrites sous le point 1 (INSTALLATION & CONFIGURATION) et notamment de désactiver l'option « require that certificate revocation checking be done… ».

Plus de détails sur la signature peuvent être obtenus via l'onglet 'signatures' à gauche du document.