

BNB-SF • boulevard de Berlaimont 14 • BE-1000 BRUXELLES

| | | | | |
|----------------|----------------|-------------------------|--|------------|
| vos références | vos références | vos références | vos références | date |
| | | EX/2007-4805/F HS/MT | H. Schollaert Gestion des accès CSSR tél. + 32 2 221 49 39 fax + 32 2 221 32 99 e-mail: access.cssr@nbb.be | 2007-09-26 |

Nouveaux certificats - CSSR (Central Server for Statistical Reporting)

Madame, Monsieur,

Par cette lettre, nous vous informons que la Banque nationale de Belgique (BNB) a apporté des modifications importantes à son infrastructure de gestion des certificats électroniques (PKI).

Le remplacement de l'infrastructure PKI nous permet d'utiliser au maximum des solutions standard offrant un meilleur service. Ainsi, il sera possible de charger des fichiers non-encryptés dans le CSSR. A cet effet, une option supplémentaire sera prévue dans le menu. L'envoi des fichiers encryptés et signés comme annexe d'un e-mail reste parallèlement disponible, ainsi que le chargement de ces fichiers dans le CSSR. De plus, le changement est une étape nécessaire en vue de permettre l'utilisation de certificats émis par une tierce partie. Nous souhaitons également vous informer que l'envoi des fichiers zip est possible, aussi bien les fichiers encryptés (où la compression se produit avant l'encryptage) que les non-encryptés.

Ces modifications ont toutefois un impact pour les établissements de crédit et les organismes de placement collectif à caractère monétaire qui consultent et alimentent le CSSR, étant donné que les messages échangés entre les déclarants et le CSSR sont signés par des certificats électroniques qui utilisent l'infrastructure PKI.

En conséquence, tous les certificats existants devront être remplacés par des certificats générés par la nouvelle infrastructure PKI de la BNB. Cette opération nécessite votre collaboration.

Vous pouvez dès maintenant convertir vos certificats existants. Pour ce faire, vous ne devez pas vous rendre à la BNB, il suffit d'exécuter la procédure de conversion mise à votre disposition sur un site Internet spécifique. En annexe, vous trouverez la documentation nécessaire pour convertir le certificat actuel et pour utiliser le nouveau certificat dans les communications avec le CSSR. En cas de problème, notre Helpdesk technique se tient à votre disposition du lundi au vendredi de 7h45 à 17h15 (02 221 40 60 ou helpdesk@nbb.be).

Statistiques financières
Banque nationale de Belgique s.a.
boulevard de Berlaimont 14
BE-1000 BRUXELLES
tél. + 32 2 221 43 73 – fax + 32 2 221 31 97
www.nbb.be

TVA BE 0203.201.340
RPM Bruxelles

Le planning à respecter est le suivant:

- Conversion du certificat actuel:
 - à effectuer jusqu'au 15 novembre 2007 au plus tard.
- Utilisation du nouveau certificat dans l'environnement de test (nouvel URL: <https://cssr-test.nbb.be/DQS>): possible à partir du 17 septembre 2007 - obligatoire à partir du 16 novembre 2007.
- Utilisation du nouveau certificat dans l'environnement de production (nouvel URL: <https://cssr.nbb.be/DQS>): possible à partir du 1 octobre 2007 - obligatoire à partir du 16 novembre 2007.
- Utilisation du certificat actuel dans les environnements de test et de production: possible en parallèle jusqu'au 15 novembre 2007 au plus tard.

Enfin, nous insistons sur l'importance pour vous d'une réalisation correcte de votre part de cette opération. **En effet, à partir du 16 novembre 2007, la communication avec le CSSR ne sera plus possible qu'avec le nouveau certificat ou, si souhaité, via un certificat fourni par une tierce partie.** Si au sein de votre entreprise, vous disposez d'un service IT, nous vous conseillons de lui transmettre ce courrier afin qu'il puisse vous assister si nécessaire.

Nous restons à votre disposition pour tout renseignement complémentaire et vous remercions d'avance pour votre collaboration.

Veuillez agréer, Madame, Monsieur, l'assurance de notre considération distinguée.

A. Peters
Responsable du projet CSSR

R. Acx
Chef du Département
Statistique générale

1. Information générale

- Lisez attentivement la documentation et les instructions jointes.
- L'autorisation d'utiliser des certificats électroniques pour vos communications avec le CSSR est subordonnée à l'acceptation des documents "Certificate Policy" (CP) et "Certificate Practice Statement for external counterparties" (CPS).

Suite à la modification de l'infrastructure PKI de la Banque nationale de Belgique, une nouvelle version de ces documents a été rédigée (version 2.0). Cette nouvelle version peut être téléchargée sur le nouveau site d'enregistrement (enrollment site) à l'adresse <https://ssl.nbb.be/nbbxenroll>.

Vous devez marquer explicitement votre accord avec la version 2.0 de ces documents. A cet effet, nous vous demandons de nous renvoyer, avant le 16 novembre 2007, le formulaire en annexe dûment signé.

- Pour réaliser avec succès la procédure de conversion de vos certificats électroniques, vous devez disposer :
 - d'un pc avec la configuration minimale suivante :
 - système d'exploitation Windows 2000 SP2 (ou plus récent) ;
 - Internet Explorer version 6 (ou supérieure) ;
 - attention : les autres systèmes d'exploitation et d'Internet browsers ne sont pas supportés actuellement.
 - des droits d'administrateur sur ce pc. Si ce n'est pas le cas, vous recevrez un message d'erreur. Veuillez alors contacter le service IT de votre société pour assistance.
- Vous aurez également besoin des manuels suivants, téléchargeables depuis le site d'enregistrement (enrollment site) à l'adresse <https://ssl.nbb.be/nbbxenroll> :
 - "Gestion d'un certificat BNB" (-> Downloads ->Enrollment procedure)
 - "Gestion des certificats en Internet Explorer" (-> Downloads -> Certificate management)
- Si vous disposez de plusieurs certificats, vous devrez exécuter la procédure décrite ci-dessous pour chaque certificat.
- Vous devez successivement exécuter les étapes suivantes:
 - conversion du certificat actuel en nouveau certificat et installation du nouveau certificat dans l'internet browser (cf. point 2 ci-après)
 - exportation du nouveau certificat (cf. point 3 ci-après)
 - connexion à l'application Internet de le CSSR (cf. point 4 ci-après)

2. Conversion du certificat actuel en nouveau certificat et installation du nouveau certificat dans l'Internet browser

- Aller sur l'enrollment site en introduisant l'adresse suivante dans votre Internet browser: <https://ssl.nbb.be/nbbxenroll>.
- Pour éviter de devoir réintroduire cette adresse à l'avenir, nous vous conseillons de l'ajouter à vos "Favoris".
- Introduire votre Username (= numéro NUIN ou NBB Unique Identification Number) que vous avez reçu, à l'origine, de la BNB dans une enveloppe fermée afin de créer le certificat actuel. Ensuite, introduire le mot de passe qui était dans la même enveloppe et que vous avez modifié. Si vous avez oublié votre Username et/ou le Password et que vous ne disposez plus des documents originaux, veuillez contacter le gestionnaire des accès du CSSR du lundi au vendredi de 8h30 à 16h45 au numéro 02 221 49 39.
- Lorsque vous aurez introduit ces données, un écran reprenant notamment la dernière adresse e-mail que vous avez communiquée lors de votre demande originale du certificat, apparaîtra. Cette adresse e-mail sera enregistrée dans le nouveau certificat. Si elle n'est plus correcte, elle doit être modifiée par le gestionnaire des accès CSSR. A cette fin, la procédure est la suivante:

- Interrompre la procédure de transformation du certificat en cliquant sur "Log out".
 - Avertir le gestionnaire des accès CSSR au moyen d'un e-mail adressé à access.cssr@nbb.be. Dans cet e-mail, mentionner explicitement que lors de la conversion d'un certificat sur l'enrollment site, l'adresse e-mail mentionnée n'est plus correcte et que vous souhaitez la modifier. Il est absolument indispensable de nous communiquer la nouvelle adresse e-mail, votre code participant et votre Username (NUIN).
 - Le gestionnaire des accès CSSR apportera les modifications nécessaires et vous le confirmera via e-mail.
 - Le jour ouvrable suivant, vous pourrez convertir le certificat actuel en nouveau certificat.
- La suite de la procédure de conversion du certificat est décrite dans le document "Gestion d'un certificat BNB". Suivez attentivement les instructions à partir du chapitre 4 (Procédure de génération et installation d'un certificat BNB), point 5 (installer le Root CA Certificate).

3. Exportation du nouveau certificat

- Le nouveau certificat que vous avez créé est installé dans l'Internet browser de votre pc. Le but de l'opération d'exportation est de créer un fichier qui contient ce certificat et qui peut être conservé sur un support au choix.
- Si vous utilisez l'Offline Signing Tool (OST) il est indispensable d'exporter le nouveau certificat que vous avez installé dans votre Internet browser.
- Même si vous n'utilisez pas l'OST, nous vous conseillons de réaliser une exportation du nouveau certificat afin de disposer d'une copie de sécurité (back-up)
- Si vous souhaitez installer le nouveau certificat sur un autre pc, il est également indispensable que vous exportiez le certificat afin de pouvoir l'importer dans l'Internet browser de l'autre pc (cf. point 4 ci-après).
- La procédure pour exporter un certificat est décrite dans le document "Gestion des certificats en Internet Explorer". Suivez attentivement les instructions de ce manuel (chapitres 1 et 2).
- Si le bouton « Certificat » (voir chapitre 2, 5ème bullet de ce manuel) n'est pas activé, vous devez prendre contact avec le service IT de votre société pour assistance.
- Cochez toutes les mentions comme indiqué sur les print screens dans le manuel. Attention: ce n'est pas la configuration standard.
- Conservez soigneusement et dans un endroit sécurisé le mot de passe que l'on vous demande d'introduire lors de l'opération d'exportation. Vous avez besoin de ce mot de passe pour importer le certificat dans l'Internet browser d'un autre pc, pour utiliser l'Offline Signing Tool et éventuellement pour importer le back-up du certificat dans votre Internet browser. Si par la suite, vous ne retrouvez plus ce mot de passe, vous devrez exécuter à nouveau la procédure d'exportation dans laquelle on vous demandera d'introduire un nouveau mot de passe.

4. Importation du nouveau certificat

- Vous devez effectuer cette procédure uniquement si vous devez à nouveau installer le back-up d'un certificat dans votre Internet browser ou si vous souhaitez installer le certificat dans l'Internet browser d'un autre pc (cf. point 3 ci-avant).
- La procédure pour importer un certificat est décrite dans le document "Gestion des certificats en Internet Explorer". Suivez attentivement ce manuel (chapitre 3).
- Attention, le mot de passe demandé est celui que vous avez défini lors de l'exportation du certificat (cf. point 3 ci-avant). Si vous ne retrouvez plus ce mot de passe, vous devrez effectuer une nouvelle exportation dans laquelle on vous demandera d'introduire un (nouveau) mot de passe suivie d'une nouvelle importation.

- Remarque: à la page 11 du manuel, la possibilité vous est offerte de cocher "Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option". Ceci n'est pas obligatoire. Si vous le faites, vous devrez, à chaque connexion à l'application informatique du CSSR, introduire un deuxième mot de passe supplémentaire.

5. Se connecter à l'application CSSR

- Tant l'environnement de test que l'environnement de production reçoivent une nouvelle adresse internet.
 - La nouvelle adresse Internet pour l'environnement de test est:
<https://cssr-test.nbb.be/DQS>.
 - La nouvelle adresse Internet pour l'environnement de production est:
<https://cssr.nbb.be/DQS>.
- Pour éviter de devoir réintroduire ces adresses à l'avenir, nous vous conseillons de les ajouter à vos "Favoris".
- Vous pouvez évidemment aussi accéder à l'environnement de test ou de production en naviguant via le site Internet général de la Banque nationale. Dans ce cas, vous ne pouvez vous connecter qu'avec le certificat actuel.
- L'envoi (ou le chargement) des fichiers, soit avec l'ancien soit avec le nouveau certificat, reste parallèlement possible jusqu'au 16 novembre 2007. Attention : dès la conversion de l'ancien certificat via les procédures décrites ci-dessus, les fichiers renvoyés par le CSSR, où l'option d'encryptage a été activée, seront encryptés à l'aide du nouveau certificat.
- Si vous utilisez les nouvelles adresses internet, une fenêtre s'ouvre avec les certificats installés dans votre Internet browser. Effectuez ensuite les étapes suivantes:
 - Choisir le certificat adéquat et cliquez sur "OK".
 - *Uniquement d'application si vous avez choisi l'option "Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option" lors de l'importation du certificat (manuel "Gestion des certificats en Internet Explorer" - page 11 - remarque): une fenêtre s'ouvre dans laquelle il vous est demandé d'introduire la CryptoAPI Private Key-password que vous avez définie lors de l'importation du certificat (voir ci-dessus, point 4).*
 - Une fenêtre s'ouvre. Introduire le mot de passe lié à votre certificat. Attention, ce n'est pas le mot de passe que vous avez défini lors de l'exportation du certificat, mais le mot de passe avec lequel vous vous êtes connecté sur l'enrollment-site (cf. point 2 ci-avant).
 - Cliquez sur "Log in". L'application CSSR s'ouvre.
- Lorsque vous vous connectez pour la première fois il est possible que:
 - une fenêtre apparaisse dans laquelle il vous est demandé si vous souhaitez installer un Truepass-applet. Vous devez répondre positivement en cliquant sur "Install".
 - un message d'avertissement apparaisse dans lequel il vous est demandé si vous acceptez le certificat BNB. Vous devez répondre positivement en cliquant sur "Yes".
- Si vous recevez un message d'erreur, il est possible que cela provienne du fait que vous ne disposez pas des droits d'administration sur votre pc. Dans ce cas, veuillez contacter le service IT de votre société pour assistance.

6. Offline Signing Tool (OST)

- Ce paragraphe est uniquement important pour les déclarants qui utilisent l'OST pour signer les fichiers envoyés vers le CSSR.
- Une nouvelle version de l'OST (version 2.2) est disponible ainsi qu'une documentation adaptée. Elle se trouve sur l'enrollment site (-> Downloads). Les certificats publics pour l'utilisation de l'OST se trouvent à

l'endroit habituel sur le site de la BNB, <http://www.nbb.be/cssr>, "Demande d'un nom d'utilisateur et questions fréquemment posées (FAQ)", "Accès à l'aide d'un certificat électronique de la BNB".

- Si vous utilisez actuellement l'OST, nous vous conseillons vivement de passer à la nouvelle version.
 - Attention, à la page 13 du dossier d'instructions l'OST, on vous demande d'introduire une passphrase. C'est le mot de passe que vous avez défini lors de l'exportation de certificat (cf. point 3 ci-avant). Si vous ne retrouvez plus ce mot de passe, vous devez effectuer une nouvelle exportation où il vous sera demandé d'introduire à nouveau un (nouveau) mot de passe.
 - Avec les nouveaux certificats, il sera possible de charger des fichiers non-encryptés dans le CSSR (les fonctionnalités restent inchangées, mais le message acknowledgement disparaît). A cet effet, une option supplémentaire sera prévue dans le menu. La sécurisation est, ici, garantie par le fait que la session entre le client (browser) et le serveur est encryptée via SSL et qu'une applet, qui est chargée dans le browser, fait en sorte qu'une signature digitale soit incluse dans le fichier. L'envoi des fichiers encryptés et signés comme annexe d'un e-mail reste parallèlement disponible, ainsi que le chargement de ces fichiers dans le CSSR.
-

Formulaire à renvoyer à :

BANQUE NATIONALE DE BELGIQUE - Service SX
Gestionnaire des accès CSSR
boulevard de Berlaimont 14
1000 BRUXELLES

ACCEPTATION DES DOCUMENTS

"CERTIFICATE POLICY" (version 2.0) ET "CERTIFICATE POLICY STATEMENT" (version 2.0) DE LA BANQUE NATIONALE DE BELGIQUE

Je soussigné

Nom:

Prénom:

Fonction:.....

Valablement qualifié pour engager et représenter la société:

BIC-code:

Nom :

Adresse du siège social:.....

atteste par la présente que ladite société:

- a) a reçu les documents "Certificate Policy" (version 2.0) et "Certificate Policy Statement" (version 2.0) relatifs à l'utilisation des certificats électroniques délivrés par la Banque Nationale de Belgique;
- b) en accepte toutes les dispositions sans la moindre réserve;
- c) s'engage à en respecter scrupuleusement toutes les procédures, obligations et responsabilité;
- d) reconnaît et accepte en conséquence que l'utilisation des clés liées au certificat électronique qui lui a été communiqué par la Banque Nationale de Belgique, pour signer toute transmission d'information par voie électronique, équivaut à l'apposition d'une signature digitale de force et de valeur équivalente à celle d'une signature manuscrite, entraînant l'irréversibilité de ce message et l'impossibilité de répudier son contenu.

Fait à, le

Signature autorisée :

Nom du signataire :
(qualité)