

NBB-SF • de Berlaimontlaan 14 • BE-1000 BRUSSEL

uw schrijven van	uw kenmerk	ons kenmerk	uw correspondent	datum
		EX/2007-4805/F HS/MT	H. Schollaert Toegangsbeheer CSSR tel. + 32 2 221 54 86 fax + 32 2 221 32 99 e-mail : access.cssr@nbb.be	2007-09-26

Nieuwe certificaten - CSSR (Central Server for Statistical Reporting)

Geachte mevrouw, Geachte heer

Met dit schrijven informeren wij u dat de Nationale Bank van België (NBB) belangrijke wijzigingen heeft aangebracht aan haar infrastructuur voor het beheer van elektronische certificaten (PKI).

De vervanging van de PKI-infrastructuur laat ons toe maximaal gebruik te maken van standaardoplossingen en zo een betere service aan te bieden. Zo zal het mogelijk zijn om niet-geëncrypteerde bestanden op te laden in de CSSR. Hiertoe wordt een bijkomende optie voorzien in het menu. Het verzenden van geëncrypteerde en gesignde bestanden als bijlage van een e-mail blijft parallel beschikbaar, evenals het opladen ervan in de CSSR. De overschakeling is bovendien een noodzakelijke voorafgaandelijke stap om het gebruik van certificaten toe te laten die door een derde partij worden uitgegeven. Ook wensen we u te informeren dat het verzenden van zip-bestanden mogelijk is, zowel geëncrypteerd (waarbij de compressie gebeurt voor de encryptie) als niet-geëncrypteerd.

Deze aanpassingen hebben echter een impact op de kredietinstellingen en de Instellingen voor Collectieve Belegging met monetair karakter, aangezien de berichten die de rapporterende instellingen en de CSSR met elkaar uitwisselen, ondertekend worden met elektronische certificaten die gebruik maken van de PKI-infrastructuur.

Als gevolg hiervan dienen alle bestaande certificaten vervangen te worden door certificaten die gegenereerd worden door de nieuwe PKI-infrastructuur van de NBB. Bij deze operatie is uw medewerking vereist.

U kan uw bestaande certificaten nu reeds omzetten zonder dat u hiervoor naar de NBB dient te komen: het volstaat dat u de omzettingsprocedure uitvoert via een specifieke website die de NBB daartoe ter beschikking stelt. In bijlage vindt u de noodzakelijke documentatie om het huidige certificaat om te zetten en het nieuwe certificaat te gebruiken in uw communicatie met de CSSR. In geval van problemen kan u onze technische Helpdesk contacteren van maandag tot vrijdag van 7u45 tot 17u15 (02.221.40.60 of helpdesk@nbb.be).

Financiële statistieken
Nationale Bank van België n.v.
de Berlaimontlaan 14
BE-1000 BRUSSEL
tel. + 32 2 221 43 73 – fax + 32 2 221 31 97
www.nbb.be

De te respecteren planning is de volgende:

- Conversie van het huidige certificaat:
uit te voeren vóór 16 november 2007.
- Gebruik van het nieuwe certificaat in de testomgeving (nieuwe URL: <https://cssr-test.nbb.be/DQS>):
mogelijk vanaf 17 september 2007 - verplicht vanaf 16 november 2007.
- Gebruik van het nieuwe certificaat in de productieomgeving (nieuwe URL: <https://cssr.nbb.be/DQS>):
mogelijk vanaf 1 oktober 2007 - verplicht vanaf 16 november 2007.
- Gebruik van het huidige certificaat in de test- en productieomgeving:
parallel mogelijk tot uiterlijk 15 november 2007.

Tot slot benadrukken wij het belang ervan dat u deze operatie correct uitvoert. **Vanaf 16 november 2007 zal de communicatie met de CSSR immers enkel mogelijk zijn met het nieuwe certificaat of, indien gewenst, via een certificaat uitgegeven door een derde partij.** Indien u binnen uw onderneming beschikt over een IT-dienst, raden wij u dan ook aan hen dit schrijven over te maken zodat zij u eventueel de nodige bijstand kunnen verlenen.

Wij blijven steeds te uwer beschikking indien u bijkomende inlichtingen wenst en danken u bij voorbaat voor uw medewerking.

Hoogachtend

A. Peters
CSSR Project Leider

R. Acx
Chef van het Departement
Algemene statistiek

1. Algemene informatie

- Lees grondig de bijgevoegde documentatie en instructies.
- De toelating om in uw communicatie met de CSSR gebruik te maken van elektronische certificaten, is onderworpen aan de aanvaarding van de documenten "Certificate Policy" (CP) en "Certificate Practice Statement for external counterparties" (CPS).

Ingevolge de aanpassing van de PKI-infrastructuur van de Nationale Bank van België werd een nieuwe versie van deze documenten opgesteld (versie 2.0). U kan deze nieuwe versie downloaden van de nieuwe registratiesite (enrollment-site), op het adres <https://ssl.nbb.be/nbbxenroll>.

U dient zich expliciet akkoord te verklaren met de nieuwe versie 2.0 van deze documenten. Daartoe verzoeken wij u ons bijgevoegd formulier ondertekend terug te sturen tegen uiterlijk 16 november 2007.

- Om de omzettingprocedure van uw elektronische certificaten succesvol uit te voeren, moet u beschikken over:
 - een pc met volgende minimale configuratie:
 - besturingssysteem Windows 2000 SP2 (of recenter)
 - Internet Explorer versie 6 (of hoger)
 - belangrijk: andere besturingssystemen en internetbrowsers worden momenteel niet ondersteund
 - local administrator-rechten op deze pc. Indien dit niet het geval is, zal u een foutbericht krijgen. Gelieve in dat geval de IT-dienst binnen uw eigen organisatie te contacteren voor bijstand.
- U heeft eveneens volgende handleidingen nodig, die u kan downloaden van de nieuwe registratiesite (enrollment-site), op het adres <https://ssl.nbb.be/nbbxenroll> :
 - "Aanmaken van een NBB-certificaat" (-> Downloads -> Enrollment procedure)
 - "Internet Explorer certificaat management" (-> Downloads -> Certificate management).
- Indien u over meerdere certificaten beschikt, dient u de hieronder beschreven procedure voor alle certificaten te doorlopen.
- U moet achtereenvolgens volgende stappen uitvoeren:
 - conversie van het huidige certificaat in een nieuw certificaat en installatie van het nieuwe certificaat in de internetbrowser (zie infra, punt 2)
 - export van het nieuwe certificaat (zie infra, punt 3)
 - aanloggen op de internettoepassing van de CSSR (zie infra, punt 4).

2. Conversie van het huidige certificaat in een nieuw certificaat en installatie van het nieuwe certificaat in de internetbrowser

- Ga naar de enrollment-site door volgend internetadres in uw internetbrowser in te voeren: <https://ssl.nbb.be/nbbxenroll>.
- Om te vermijden dat u dit adres in de toekomst telkens opnieuw moet voeren, raden wij u aan het aan uw "Favorieten" toe te voegen.
- Vul de Username (= NUIN-nummer of NBB Unique Identification Number) in die u oorspronkelijk van de NBB onder verzegelde omslag heeft gekregen om het huidige certificaat aan te maken. Vul vervolgens het door u gewijzigde Password in dat in diezelfde omslag bijgevoegd was. Indien u uw Username en/of het Password vergeten bent en niet meer over de oorspronkelijke documenten beschikt, gelieve dan contact op te nemen met het toegangsbeheer van de CSSR op het nummer 02.221.54.86 (van maandag tot vrijdag van 8u30 tot 16u45).
- Nadat u deze gegevens heeft ingevuld, zal een scherm verschijnen met o.a. het e-mailadres dat u destijds meegedeeld heeft bij de originele aanvraag van het certificaat. Dit e-mailadres wordt geregistreerd in het nieuwe certificaat. Indien het niet meer correct is, dient het door toegangsbeheer CSSR gewijzigd te worden. De werkwijze is de volgende:

- Breek de procedure tot omvorming van het certificaat af door op "Log out" te klikken.
 - Verwittig toegangsbeheer CSSR via een e-mail naar access.cssr@nbb.be en vermeld expliciet dat het bij de conversie van het certificaat op de enrollment-site afgebeelde e-mailadres niet meer correct is en dat u dit wenst te laten wijzigen. Het is daarbij absoluut noodzakelijk dat u ons het nieuwe e-mailadres, uw deelnemerscode en uw Username (NUIN) meedeelt.
 - Toegangsbeheer CSSR zal de nodige aanpassingen doorvoeren en u dit via e-mail bevestigen.
 - De volgende werkdag kan u het huidige certificaat omzetten in een nieuw certificaat.
- Het vervolg van de procedure om een certificaat te converteren is beschreven in het document "Aanmaken van een NBB-certificaat". Volg nauwgezet de instructies vanaf hoofdstuk 4 (Werkwijze om een NBB-certificaat te genereren en te installeren), punt 5 (Installeer het Root CA Certificate).

3. Export van het nieuwe certificaat

- Het nieuwe certificaat dat u gecreëerd heeft, wordt geïnstalleerd in de internetbrowser van uw pc. Het doel van de export-operatie is de creatie van een bestand dat dit certificaat bevat en dat op een drager naar keuze kan bewaard worden.
- Indien u gebruik maakt van de Offline Signing Tool (OST), is het noodzakelijk dat u het nieuwe certificaat dat u in uw internetbrowser geïnstalleerd heeft, exporteert.
- Ook indien u de OST niet gebruikt, raden wij ten zeerste aan toch een export te doen van het nieuwe certificaat en zo een veiligheidskopie (back-up) te nemen.
- Indien u het nieuwe certificaat ook op een andere pc wenst te plaatsen, is het eveneens noodzakelijk dat u het certificaat exporteert, om het daarna te importeren in de internetbrowser van de andere pc (zie infra, punt 4).
- De werkwijze om een certificaat te exporteren is beschreven in het document "Internet Explorer certificaat management". Volg nauwgezet de instructies van deze handleiding (hoofdstuk 1 en 2).
- Indien de Certificates-knop (zie hoofdstuk 2, 5e bullet van de handleiding) niet geactiveerd is, dient u de IT-dienst binnen uw eigen organisatie te contacteren voor bijstand.
- Vink alle vermeldingen exact aan zoals getoond wordt op de print-screens in de handleiding. Opgelet, dit is niet de standaardconfiguratie.
- Bewaar op een veilige plaats het paswoord dat u gevraagd wordt in te voeren bij de export-operatie. U heeft dit paswoord nodig om het certificaat te importeren in de internetbrowser van een andere pc, om de Offline Signing Tool te gebruiken en om eventueel de back-up van het certificaat te importeren in uw internetbrowser. Indien u later dit paswoord niet meer zou terugvinden, zal u de export-operatie opnieuw moeten doen waarbij u zal gevraagd worden een nieuw paswoord in te brengen.

4. Import van het nieuwe certificaat

- U moet deze procedure enkel uitvoeren indien u om bepaalde redenen de back-up van een certificaat opnieuw in uw internetbrowser moet plaatsen of indien u het certificaat in de internetbrowser van een andere pc wenst te plaatsen (zie supra, punt 3).
- De werkwijze om een certificaat te importeren is beschreven in het document "Internet Explorer certificaat management". Volg nauwgezet deze handleiding (hoofdstuk 3).
- Opgelet, het gevraagde paswoord is datgene dat u gedefinieerd heeft bij de export van het certificaat (zie supra, punt 3). Indien u dit paswoord niet meer zou terugvinden, zal u de export-operatie opnieuw moeten doen waarbij u zal gevraagd worden een nieuw paswoord in te brengen, gevolgd door een nieuwe import.
- Opmerking: op p.11 van de handleiding wordt u de mogelijkheid gegeven "Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option" aan te vinken. Dit is niet verplicht. Indien u dit doet, zal u elke keer als u zich aanlogt op informaticatoepassing van de CSSR, een tweede extra paswoord moeten ingeven.

5. Aanloggen op de CSSR

- Zowel de testomgeving als de productieomgeving krijgen een nieuw internetadres.
 - Het nieuwe internetadres voor de testomgeving is <https://cssr-test.nbb.be/DQS>.
 - Het nieuwe internetadres voor de productieomgeving is <https://cssr.nbb.be/DQS>.
- Om te vermijden dat u deze internetadressen in de toekomst telkens opnieuw moet invoeren, raden wij u aan ze aan uw "Favorieten" toe te voegen.
- U kan natuurlijk ook steeds via de algemene website van de Nationale Bank navigeren naar de test- of productieomgeving. In dat geval kan u zich enkel met het huidige certificaat aanloggen.
- Het inzenden (of opladen) van bestanden blijft met de oude en de nieuwe certificaten in parallel mogelijk tot 16 november 2007. Opgelet: vanaf de omzetting van het oude certificaat via de hierboven beschreven procedures zullen door de CSSR teruggestuurde bestanden, waarbij de optie tot encryptie geactiveerd werd, geëncrypteerd worden aan de hand van het nieuwe certificaat.
- Indien u de nieuwe internetadressen hanteert, opent zich een venster met de certificaten die in uw internetbrowser geïnstalleerd zijn. Voer vervolgens volgende stappen uit:
 - Selecteer het juiste certificaat en klik op "OK".
 - *Enkel van toepassing indien u de optie "Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option" gekozen heeft bij de import van het certificaat (handleiding "Internet Explorer certificaat management" - p.11, opmerking): er verschijnt een venster waarin u gevraagd wordt het CryptoAPI Private Key-paswoord te geven dat u gedefinieerd heeft bij de import van het certificaat (zie supra, punt 4).*
 - Een venster opent zich. Voer het paswoord in dat aan het certificaat verbonden is. Opgelet, dit is niet het paswoord dat u gedefinieerd heeft bij de export van het certificaat, maar het paswoord waarmee u zich hebt aangemeld op de enrollment-site (zie supra, punt 2).
 - Klik op "Log in". De toepassing van de CSSR wordt geopend.
- Wanneer u voor de eerste keer aanlogt is het mogelijk dat:
 - een venster verschijnt waarin u gevraagd wordt of u een Truepass-applet wil installeren. U moet hierop bevestigend antwoorden door op "Install" te klikken.
 - een waarschuwingsbericht verschijnt waarin u gevraagd wordt of u het NBB-certificaat aanvaardt. U moet hierop bevestigend antwoorden door op "Yes" te klikken.
- Indien u een foutbericht krijgt, is dit mogelijk te wijten aan het feit dat u geen local administrator-rechten heeft over uw pc. Gelieve in dat geval de IT-dienst binnen uw eigen organisatie te contacteren voor bijstand.

6. Offline Signing Tool (OST)

- Dit deel is enkel van belang voor de rapporterende instellingen die de OST gebruiken om bestanden te ondertekenen die naar de CSSR verstuurd worden.
- Er is een nieuwe versie van de OST beschikbaar (versie 2.2), evenals een bijgewerkte documentatie. Beide bevinden zich op de enrollment-site (-> "Downloads"). De publieke certificaten voor het gebruik van de OST bevinden zich op de vertrouwde plaats op de website van de NBB, <http://www.nbb.be/cssr>, "Aanvraag gebruikersnaam en veel gestelde vragen (FAQ)", "Toegang met een elektronisch certificaat van NBB".
- Indien u momenteel de OST gebruikt, raden wij u ten sterkste aan over te stappen op deze nieuwe versie.
- Opgelet, op pagina 13 van de OST-handleiding wordt u gevraagd een passphrase in te voeren. Dit is het paswoord dat u gedefinieerd heeft bij de export van het certificaat (zie supra, punt 3). Indien u dit paswoord niet meer zou terugvinden, zal u de export-operatie opnieuw moeten doen waarbij u zal gevraagd worden een nieuw paswoord in te brengen.

- Met de nieuwe certificaten zal het mogelijk zijn om niet-geëncrypteerde bestanden op te laden in de CSSR (functionaliteiten blijven hetzelfde, maar het acknowledgement bericht verdwijnt). Hiertoe wordt een bijkomende optie voorzien in het menu. De beveiliging wordt hier gegarandeerd door het feit dat de sessie tussen de client (browser) en de server geëncrypteerd wordt via SSL en dat een applet die in de browser geladen wordt, zorgt voor een digitale handtekening bij het bestand. Het verzenden van geëncrypteerde en gesignde bestanden als bijlage van een e-mail blijft parallel beschikbaar, evenals het opladen ervan in de CSSR.
-

Formulier terug te sturen naar : NATIONALE BANK VAN BELGIË - Dienst SX
Toegangsbeheer CSSR
de Berlaimontlaan 14
1000 BRUSSEL

AANVAARDING VAN DE DOCUMENTEN

"CERTIFICATE POLICY" (versie 2.0) EN "CERTIFICATE POLICY STATEMENT" (versie 2.0) VAN DE NATIONALE BANK VAN BELGIË

Ik, ondergetekende

Naam:

Voornaam:

Functie:.....

Geldig bevoegd om de vennootschap:

BIC-code:

Naam :

Adres van de maatschappelijke zetel:.....

te verbinden en te vertegenwoordigen, bevestigt bij deze dat voornoemde vennootschap:

- a) de documenten "Certificate Policy" (versie 2.0) en "Certificate Policy Statement" (versie 2.0) betreffende het gebruik van de elektronische certificaten afgeleverd door de Nationale Bank van België heeft ontvangen;
- b) al de bepalingen zonder enig bezwaar aanvaardt;
- c) alle procedures, verplichtingen en aansprakelijkheden strikt zal navolgen;
- d) bijgevolg aanvaardt dat het gebruiken van de sleutels verbonden aan het elektronisch certificaat dat haar door de Nationale Bank van België medegedeeld werd om alle door elektronische verbinding informatie verzending te tekenen, gelijk is aan het aanbrengen van een digitale handtekening met gelijke kracht en waarde als deze van een handgeschreven handtekening dat als gevolg heeft de onomkeerbaarheid van dit bericht en de onmogelijkheid van zijn inhoud te verlooehenen.

Gedaan te, op

Bevoegde handtekening :

Naam van de ondertekenaar:.....
(hoedanigheid)