

Datum laatste wijziging: 27/08/2009

## **Algemeen**

- Waarom vindt een overstap naar een nieuwe CA plaats?
- Wat doet een CA?
- Wat is een Certificate Revocation List (CRL)?
- Verandert er iets aan het niveau van beveiliging?
- Zijn er kosten verbonden aan de overstap naar een nieuwe CA?
- Kan ik mijn certificaat gewoon verlengen?
- Kan ik zien of ik met de nieuwe of oude ABC-tool werk?
- Kan ik zien of mijn certificaat is uitgegeven door de nieuwe of de oude CA?
- Is deze CA wijziging van invloed op ABZ Digitale Paspoorten (DP's)?
- Is deze CA wijziging hetzelfde als die voor ABZ Digitale paspoorten (DP's)?

## **Voor Bedrijfscertificaat beheerder**

- Wat merk ik ervan?
- Wat moet ik doen?
- Wat moet ik doen wanneer ik geen toegang krijg tot ABZ of een andere omgeving?
- Wanneer krijg ik met de wijzigingen van de CA te maken?
- Vanaf wanneer kan ik de nieuwe ABC-tool gebruiken?
- Moet ik op het moment dat de nieuwe CA er is mijn certificaat vernieuwen?
- Is het certificaat veranderd?
- Wat moet ik doen als ik het ABZ certificaat gebruik binnen de omgeving van [ANVA](#)?

## **Voor Relying Parties**

- Wat merkt ik er van?
- Wat moet ik doen?
- Met welke situaties kan ik te maken krijgen?
- Hoe kan ik testen of mijn certificaat controle nog werkt?
- Welke mogelijkheden zijn er om de intrekingsstatus te controleren?

**Algemeen – Waarom vindt een overstap naar een nieuwe CA plaats?**

Volgens de richtlijnen en veiligheidsprotocollen van VeriSign, vastgelegd in haar “Certification Practice Statement (CPS)”, wijzigen zij eens in de 10 jaar de bron van waaruit certificaten worden uitgegeven, de zogenaamde “Certification Authority (CA)”.

Dit moment staat nu voor de deur. Vanaf oktober 2009 betreft ABZ haar digitale certificaten ten behoeve van het Bedrijfscertificaat van deze nieuwe CA en is de omschakeling naar de nieuwe CA voor Bedrijfscertificaten een feit.

**Algemeen – Wat doet een CA?**

Een Digitaal Certificaat wordt uitgegeven door een “Certification Authority (CA)” en ondertekent met de geheime privé sleutel van de CA. Een CA is verantwoordelijk voor het uitgeven en beheer van digitale certificaten (zie ook het CPS op de ABZ website <http://www.abz.nl/over-abz/cps/bc-cps.html> ).

**Algemeen - Wat is een Certificate Revocation List (CRL)?**

De CRL is een lijst waarin alle **ingetrokken** certificaten worden gepubliceerd die gedurende de looptijd nog geldig zijn. Deze lijst wordt ook wel de “black list” genoemd en is op een publiek toegankelijk internet adres beschikbaar. De locatie hiervan staat beschreven in het CPS van ABZ evenals in de uitgegeven Bedrijfscertificaten zelf.

**Algemeen – Verandert er iets aan het niveau van beveiliging?**

Het beveiligingsniveau blijft op het niveau zoals u gewend bent van ABZ, als Trusted Third Party

**Algemeen – Zijn er kosten verbonden aan de overstap naar een nieuwe CA?**

ABZ belast geen kosten door voor de overstap naar een nieuwe CA. Echter, het opnemen van de publieke sleutel van de nieuwe CA in klantspecifieke software of “keystores” komt voor rekening van de klant.

**Algemeen – Kan ik mijn certificaat gewoon verlengen?**

Na het ophalen en installeren van een nieuwe versie van de ABC-tool gaat het verlengen van een certificaat op de gebruikelijke manier. Achter de schermen wordt een “oud” certificaat omgezet in een “nieuw” certificaat. De gebruiker merkt geen verschil.

**Algemeen - Kan ik zien of ik met de nieuwe of de oude ABC-tool werk?**

Bij gebruik van de nieuwe ABC-tool wordt een ABZ logo getoond, dit is niet het geval bij de oude versie

**Algemeen - Kan ik zien of mijn certificaat is uitgegeven door de nieuwe of de oude CA?**

Herkenning is mogelijk door binnen de ABC-tool de functie “Tonen” te gebruiken, aan de hand van de naam van het “Uitgever” veld in het certificaat. Als in dit veld Solera staat is het een certificaat dat is uitgegeven door de nieuwe CA.

**Algemeen - Is deze CA wijziging ook van invloed op ABZ Digitale Paspoorten?**

Nee, ABZ Digitale Paspoorten worden uitgegeven onder een andere CA. Deze CA is recentelijk in december 2008 vervangen.

**Algemeen – Is deze CA wijziging hetzelfde als voor ABZ Digitale Paspoorten?**

Nee, ABZ omdat ABZ Digitale Paspoorten worden uitgegeven onder een andere CA is er ook een andere hiërarchie van certificaten.

**Bedrijfscertificaat beheerder - Wat merk ik ervan?**

U ontvangt in komende maanden een informatie set waarin staat beschreven hoe u een nieuwe versie van de ABC-tool kunt downloaden en installeren. Nadat u dit heeft gedaan blijft de huidige werkwijze voor het intrekken, verlengen en ophalen gelijk.

**Bedrijfscertificaat beheerder - Wat moet ik doen?**

Zodra u de melding krijgt dat de nieuwe ABC-tool beschikbaar is, kunt u de nieuwe versie van de ABC-tool downloaden van de ABZ-site. Vanaf dat moment kunt u met deze tool net zo werken als met de vorige versie.

**Bedrijfscertificaat beheerder - Wat moet ik doen wanneer ik geen toegang krijg tot ABZ of een andere omgeving?**

Waarschijnlijk zijn op uw computersystemen bepaalde updates van uw operating systeem niet geïnstalleerd en heeft in bepaalde applicaties geen update plaatsgevonden van de keystore's, waardoor de herkenning van de nieuwe uitgevende instantie (CA) uitblijft.

In dit geval worden de uitgevende en intermediate-instantie van uw certificaat niet herkend.

Overleg met uw systeembeheerder of neem contact op met de organisatie die u toegang geeft tot haar diensten op basis van uw certificaat. Organisaties dienen de nieuwe CA als "vertrouwd" op te nemen in hun omgevingen. Een melding aan ABZ stellen wij op prijs, zodat wij uw verzoek kunnen ondersteunen.

**Bedrijfscertificaat beheerder – Wanneer krijg ik met de wijziging van de CA te maken?**

Op het moment dat er een Bedrijfscertificaat opgehaald of verlengd wordt en nadat de CA-wijziging heeft plaatsgevonden.

**Bedrijfscertificaat beheerder – Vanaf wanneer kan ik de nieuwe ABC-tool gebruiken?**

De nieuwe ABC-tool is te gebruiken vanaf het moment dat ABZ deze ter beschikking stelt. De tool kan zelf bepalen of er een certificaat moet worden opgehaald bij de oude of bij de nieuwe CA.

**Bedrijfscertificaat beheerder – Moet ik op het moment dat er een nieuwe CA is mijn certificaten vernieuwen?**

De huidige certificaten blijven geldig tot hun oorspronkelijke verloopdatum

**Is het certificaat veranderd?**

Ja er zijn wijzigingen in het certificaat. Deze wijzigingen veranderen de werking van het certificaat niet. Zie hiervoor het aparte document op

<http://www.abz.nl/nieuws/nieuwsberichten/2008/ca-migratie/index.html>

**Bedrijfscertificaat beheerder – Wat moet ik doen als ik het ABZ certificaat gebruik binnen de omgeving van ANVA?**

Momenteel test [ANVA](#) de nieuwe ABC-tool van ABZ en deze wordt uiterlijk per 1 oktober 2009 als aparte patch uitgeleverd door ANVA. ANVA4/5 maakt gebruik van een softwaretool van ABZ (menu BYKDG: Beheer/ Systeem/ Kantoor/ Datacommunicatie/ Gebruikers-gegevens) voor het installeren en importeren van bedrijfscertificaten. Deze tool haalt het certificaat op van een beveiligde website (de 'Certification Authority') en plaatst dit automatisch in de ANVA X-net directory.

**Relying Parties - Wat merkt u ervan?**

Gebruikers van ABZ Bedrijfscertificaten gaan gebruik maken van een andere uitgevende instantie. Deze uitgevende instantie, en alle tussenliggende instanties dienen in uw proxy of webserver bekend te zijn. Bij de uitgever (issuer) van de certificaten is de uitgevende partij TTP Services ABZ Nederland CA toegevoegd. In het onderwerp (subject) van de ABZ Bedrijfscertificaten is de naam ABZ Nederland BV vervangen door Solera BV. Het e-mail veld blijft onderdeel van het onderwerpveld u kunt dit gegeven dus blijven gebruiken om een relatie te leggen met de bij u intern bekende identiteit.

**Relying Parties - Wat moet u doen?**

U moet zorgen dat de nieuwe uitgevende instantie bekend is in uw proxy of webserver. Nadere informatie en een stappenplan voor installatie van het root- en intermediate certificaat is te vinden op:  
<https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=SO8201>  
Let op: de root en intermediate certificaten zijn apart beschikbaar op de <http://www.abz.nl/services/identity-en-access-management/abc-tool/index.html>  
Deze certificaten zijn beschikbaar in een zipfile en kunnen geïnstalleerd worden op de gebruikelijke wijze van uw operating systeem.

**Relying Parties – Met welke situaties kan ik te maken krijgen?**

- a. De gebruiker met een oud certificaat, maar nog geldig certificaat krijgt een foutmelding als hij op uw omgeving probeert binnen te komen.  
Waarschijnlijke oorzaak: de oude uitgevende instantie en tussenliggende instantie is niet meer bekend binnen uw proxy of webserver.
- b. De gebruiker met een nieuw en nog geldig certificaat krijgt een foutmelding als hij op uw omgeving probeert binnen te komen.  
Waarschijnlijke oorzaak: de nieuwe uitgevende instantie is niet bekend binnen uw proxy of webserver. Deze dient toegevoegd te worden zoals beschreven in voorgaande vraag en antwoord.  
Op <https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=SO8201> staat stapsgewijs beschreven hoe de intermediate en root certificaat bekend te maken is.
- c. De gebruiker krijgt toegang met een gedurende de looptijd ingetrokken certificaat.  
Waarschijnlijke oorzaak: er vindt alleen een controle plaats tegen de oude of alleen tegen de nieuwe CRL in plaats van controle tegen zowel de oude als de nieuwe CRL. Als uw proxy of webserver de CRL gegevens uit het certificaat leest, kan deze situatie zich niet voordoen.

**Relying Parties - Hoe kan ik testen of mijn certificaat controle nog werkt?**

Testen tegen de ABZ LDAP werkt op de voor u bekende manier. De status van het certificaat is op te vragen uit de ABZ Repository (de zogenaamde 'white list'). Dit verdient zelfs de voorkeur, want de gegevens in de Repository worden vrijwel direct bijgewerkt in geval van intrekking. Alle geldige certificaten zijn bekend in deze Repository. Indien niet bekend in deze Repository dan dient het certificaat als ingetrokken of niet bestaand te worden beschouwd.

Het testen tegen de nieuwe CRL kan plaatsvinden na ontvangst van de melding van ABZ dat de nieuwe CA in productie is, door gebruik te maken van een ingetrokken certificaat dat na de productiedatum is aangevraagd.

Test Root en Intermediate certificaten zijn beschikbaar op:

<https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR657>

Op <https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=S:SO10543&actp=search&searchid=1227710657758> staat beschreven hoe een test root certificaat in de browser is te installeren.

Veel voorkomende vragen en oplossingen zijn beschikbaar op <https://www.verisign.com/index.html>

**Relying Parties – Welke mogelijkheden zijn er om de intrekingsstatus te controleren?**

- a. De intrekingsstatus (de zogenaamde 'black list') is online nog niet beschikbaar
- b. Controle op basis de CRL is nog niet beschikbaar

De CRL komt beschikbaar in verschillende formaten, voorbeelden zijn:

<http://pki.pinkroccade.com/crl/SoleraNederlandBVABZBedrijfsApplicatieCertificaten/LatestCRL>  
(PKCS7 formaat)

<http://pki.pinkroccade.com/crl/SoleraNederlandBVABZBedrijfsApplicatieCertificaten/LatestCRL.crl>  
(DER formaat)

<http://pki.pinkroccade.com/crl/SoleraNederlandBVABZBedrijfsApplicatieCertificaten/LatestCRL.Idif> (Idif  
formaat)