

Datum laatste wijziging: 22/12/2008

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 mijn certificaat is uitgegeven door de nieuwe of de oude CA?
- Is deze CA wijziging ook van invloed op ABZ bedrijfscertificaten (ABC's)?

Voor DP houders

- Wat merkt u ervan?
- Wat moet u doen?
- Wat moet u doen wanneer ik geen toegang krijg tot ABZ of een andere omgeving?
- Wat moet u doen wanneer ik een lege pop-up zie na aanmelding op een site?

Voor Relying Parties

- Wat merkt u er van?
- Wat moet u 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?

FAQ – Wijziging Certification Authority (CA)

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 15 december aanstaande betreft ABZ haar digitale certificaten ten behoeve van het Digitaal Paspoort van deze nieuwe CA en is de omschakeling naar de nieuwe CA voor digitale paspoorten een feit.

Algemeen – Wat doet een CA?

Een Digitaal Certificaat wordt uitgegeven door een “Certification Authority (CA)” en ondertekend met de geheime privé sleutel van de CA. Een CA is verantwoordelijk voor het uitgeven en beheer van digitale certificaten (zie ook het CPS statement op de ABZ website).

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 certificaten zelf.

Algemeen – Veranderd er iets aan het niveau van beveiliging?

Het beveiligingsniveau blijft op het niveau zoals u gewend bent van ABZ.

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?

Het verlengen van een certificaat gaat op de gebruikelijke manier. Achter de schermen wordt een “oud” certificaat omgezet in een “nieuw” certificaat. De gebruiker merkt geen verschil. Mogelijk dat gevraagd wordt om acceptatie van de nieuwe CA, wanneer de reguliere updates van uw operating systeem (bijvoorbeeld Microsoft) nog niet zijn toegepast.

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

Herkenning is mogelijk aan de hand van de naam van het “issuer” veld in het certificaat, alleen dit vraagt om specifieke kennis en inzichten en is voor het gebruik van uw Digitaal Paspoort niet noodzakelijk. Voor het gebruik van het certificaat maakt het niet uit door welke CA het is uitgegeven, dit blijft op dezelfde manier werken.

Algemeen - Is deze CA wijziging ook van invloed op ABZ bedrijfscertificaten (ABC's)?

Nee, ABZ Bedrijfscertificaten worden uitgegeven onder een andere CA. Deze CA wordt pas in juni 2009 vervangen. Indien u beheerder bent van een ABZ Bedrijfscertificaat informeren wij u hierover in het tweede kwartaal van 2009.

DP houder - Wat merk ik ervan?

U merkt in principe niets van de overgang (u gaat automatisch gebruik maken van een andere uitgevende instantie). Mogelijk dat gevraagd wordt om acceptatie van de nieuwe CA, wanneer de reguliere updates van uw operating systeem (bijvoorbeeld Microsoft) nog niet zijn toegepast.

DP houder - Wat moet ik doen?

U hoeft in principe niets te doen. De leverancier van uw operating systeem (Bijvoorbeeld Microsoft) verzorgt reguliere updates, waarin de nieuwe uitgevende instantie (CA) is opgenomen. Mogelijk dat gevraagd wordt om acceptatie van de nieuwe CA, wanneer u de reguliere updates nog niet heeft toegepast. Indien u een andere browser of besturingssysteem gebruikt, komt de nieuwe CA over het algemeen mee met de updates van de betreffende browser.

DP houder - Wat moet ik doen wanneer ik geen toegang krijg tot ABZ of een andere omgeving?

Waarschijnlijk zijn op uw computer bepaalde updates van uw operating systeem (Bijvoorbeeld Microsoft) niet geïnstalleerd, waardoor de herkenning ontbreekt van de nieuwe uitgevende instantie (CA). Overleg met uw systeembeheerder om alle updates voor uw operating systeem te installeren.

DP houder - Wat moet ik doen wanneer ik een lege pop-up zie na aanmelding op een site?

In dit geval herkent de organisatie bij wie u zich wilt aanmelden, uw certificaat niet. Overleg met uw systeembeheerder en neem contact op met de organisatie die u toegang geeft tot haar diensten op basis van uw certificaat. Deze organisatie dient de nieuwe CA als "vertrouwd" op te nemen in haar omgeving. Een melding aan ABZ stellen wij op prijs, zodat wij uw verzoek kunnen ondersteunen.

Relying Parties - Wat merkt u ervan?

Gebruikers van ABZ certificaten gaan gebruik maken van een andere uitgevende instantie. Deze uitgevende instantie, en alle tussenliggende instanties dienen in uw proxy of webserver bekend te zijn. Het onderwerp (subject) van de ABZ certificaten gaat niet veranderen. Als u dit onderwerp gebruikt om een relatie te leggen met de bij u intern bekende identiteit, hoeven er dus geen aanpassingen plaats te vinden.

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 (3 stuks in totaal: 1 root en 2 intermediates) zijn apart beschikbaar op de abz.nl en de dp.abz.nl sites. 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, maar nog geldig certificaat krijgt een lege pop-up te zien 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.

b. De gebruiker met een oud certificaat, maar nog geldig certificaat krijgt een lege pop-up te zien 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.

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 door gebruik te maken van een ingetrokken certificaat dat na 15 december 2008 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 beschikbaar bij de CA op basis van een handmatige controle.

URL: <http://pki.getronicspinkroccade.nl/crl/KPNTelecomBVCA/LatestCRL.crl>

b. Machinematige controle op basis van machine interpretatie van de CRL.

De CRL is beschikbaar in verschillende formaten. Voorbeelden zijn:

<http://pki.getronicspinkroccade.nl/crl/KPNTelecomBVCA/LatestCRL> (PKCS7 formaat)

<http://pki.getronicspinkroccade.nl/crl/KPNTelecomBVCA/LatestCRL.crl> (DER formaat)

<http://pki.getronicspinkroccade.nl/crl/KPNTelecomBVCA/LatestCRL.Idif> (Idif formaat)

.