



## Verwijdering DigiNotar uit Adobe Reader

Adobe heeft aangekondigd<sup>1</sup> dat op dinsdag 13 september 2011 DigiNotar Qualified CA<sup>2</sup> verwijderd zal worden van de Adobe Approved Trust List (AATL) vanwege een security incident bij DigiNotar. Adobe Reader is een applicatie waarmee PDF bestanden kunnen worden gelezen. PDF bestanden kunnen digitaal ondertekend worden door middel van een elektronische handtekening.

Een direct gevolg van de verwijdering is dat alle documenten die digitaal ondertekend zijn door een door DigiNotar Qualified CA gecertificeerde partij (er zijn er totaal 3945) een waarschuwing zullen geven in Adobe Acrobat en Reader<sup>3</sup> (die gebruikt maakt van de AATL). De waarschuwing betreft de betrouwbaarheid van het document (zie figuur 1). Daarnaast bestaat door het security incident bij DigiNotar de mogelijkheid dat documenten zijn voorzien van valse handtekeningen.

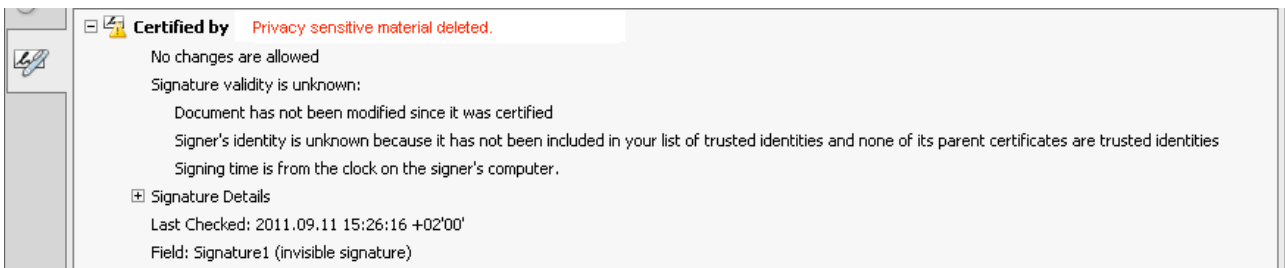


Figuur 1: Voorbeeld van verwachte waarschuwing

## Wat betekent de waarschuwing

Met de knop aan de rechterkant van de waarschuwing ("Signature Panel") kan meer informatie worden opgevraagd over de handtekening. In documentatie op de website van Adobe<sup>4</sup> is terug te vinden dat vier aspecten worden gecontroleerd bij digitaal ondertekende documenten:

- 1) Is het document aangepast sinds het is ondertekend?
- 2) Is het certificaat van de ondertekenaar te herleiden naar een vertrouwde partij?
- 3) Is het certificaat van de ondertekenaar zelf betrouwbaar (niet ingetrokken)?
- 4) Wat is de bron van het tijdstip van ondertekenen?



Figuur 2: Details van een digitale handtekening

In de details (zie figuur 2) is terug te vinden dat volgens Adobe Reader het document niet is aangepast sinds het moment van ondertekenen (punt 1). Het validatieproces geeft een negatieve melding bij punten 2 en 3 (zelfde regel) omdat het certificaat van de ondertekenaar niet kan worden herleid naar een vertrouwde partij (Trust Anchor). Daarmee is de ondertekende partij zelf onvertrouwd geworden. Voor punt 4 wordt gemeld dat het tijdstip van ondertekenen afkomstig is van de lokale computer van degene die de handtekening heeft gezet.

Samengevat betekent het dat Adobe Reader twijfelt aan de betrouwbaarheid van het document vanwege het ontbreken van garanties over de identiteit van degene die de handtekening heeft gezet. Het gevolg is niet dat alle documenten met deze waarschuwing waardeloos zijn geworden

<sup>1</sup> Zie <http://blogs.adobe.com/security/2011/09/diginotarremovalaatl.html>

<sup>2</sup> "Diginotar Qualified CA", serial number "5b d5 60 9c 64 17 68 cf 21 0e 35 fd fb 05 ad 41"

<sup>3</sup> Versie X per direct, versie 9 na een update. Zie voetnoot 1 voor meer informatie.

<sup>4</sup> Zie <http://www.adobe.com/it/security/pdfs/DigitalSignaturesInPDF.pdf>

omdat de inhoud niet meer zou kloppen. Documenten die in het verleden zijn ondertekend kunnen nog steeds betrouwbaar genoeg zijn. Bijvoorbeeld als de ondertekenende- en validerende partij langs andere wegen een zekere mate van vertrouwen in elkaars identiteit hebben gekregen. Het is niet verstandig om documenten die na het security incident (juli 2011) zijn ondertekend door een door DigiNotar Qualified CA gecertificeerde partij als betrouwbaar te accepteren. Voor het bepalen van het tijdstip van ondertekenen kunt u bovendien niet uitsluitend op een tijd van de lokale computer van de ondertekenaar vertrouwen<sup>5</sup>.

### **Risicoafweging en maatregelen**

Er zijn een aantal mogelijkheden om met de waarschuwing om te gaan en elke mogelijkheid heeft zijn eigen risicoprofiel. Hieronder worden enkele maatregelen en bijbehorende risico's beschreven. De maatregel met het minste risico wordt eerst beschreven, die met het meeste risico als laatste.

#### *1) Opnieuw ondertekenen.*

Laat alle documenten die een waarschuwing geven op inhoud controleren en opnieuw ondertekenen door een gecertificeerde partij. De maatregel geeft het laagste risico, maar het vervangingsproces is arbeidsintensief en kan veel tijd kosten.

#### *2) Handmatig toevoegen van een certificaat aan de trust list.*

Adobe Reader heeft mogelijkheden<sup>6</sup> om handmatig het trust niveau van een certificaat aan te passen. Hierdoor zal de waarschuwing verdwijnen. Om te voorkomen dat een frauduleuze partij (in de context van PDF documenten zijn hiervan tot nu toe geen gevallen bekend) vertrouwd wordt, kan meer zekerheid over de identiteit van de ondertekenende partij worden verkregen via een ander kanaal. Dit kan bijvoorbeeld door de betreffende partij te bellen en het 'fingerprint' kenmerk van het certificaat te controleren. Deze optie is eenvoudig uitvoerbaar voor een klein aantal ondertekenaars. Het risico is beperkt doordat het document en certificaat buiten de CA structuur om gecontroleerd wordt.

#### *3) Niets doen.*

Als de waarschuwing alleen vermeldt dat de ondertekenaar niet geverifieerd kan worden en het document is voor juli 2011 in een veilige omgeving gemaakt en opgeslagen, dan is de kans relatief klein dat het een om een frauduleus document gaat. Het risico van deze optie is wel dat frauduleuze documenten niet meer opvallen omdat geen onderscheid wordt gemaakt tussen documenten met en zonder waarschuwing. De waarschuwing verliest hier zijn functie.

#### *4) Voeg handmatig Diginotar Qualified CA weer toe aan de trust list.*

Deze maatregel wordt sterk afgeraden. De maatregel heeft als enige voordeel dat voor DigiNotar Qualified CA gecertificeerde documenten de waarschuwing zal verdwijnen. De kans dat frauduleuze documenten niet gedetecteerd worden is groot. Deze optie is uitsluitend het overwegen waard als het risico van een verstoring van een kritisch bedrijfsproces hoger is dan het risico dat ontstaat door het gebruik van frauduleuze documenten.

#### *5) Zet de updates uit.*

Deze maatregel wordt sterk afgeraden. Zonder update zal de verwijdering van DigiNotar uit Adobe Reader niet plaatsvinden. Zie maatregel 4 voor verdere uitleg.

Alle frauduleuze DigiNotar certificaten worden door DigiNotar revoked. Als gevolg zal Adobe Reader een foutmelding zal geven bij controle (via OCSP en CRL) van documenten die zijn ondertekend door een sleutel met een (bekend) frauduleus DigiNotar certificaat, ook als voor maatregel 4 of 5 is gekozen. Er zijn geen (bekende) aan Diginotar Qualified CA of PKIOverheid gerelateerde frauduleuze certificaten bekend. Alle (3200) Diginotar PKIOverheid certificaten worden vervangen, waarna ook de DigiNotar PKIOverheid CAs ook revoked wordt.

### **Conclusie**

Gebruikers van Adobe Reader wordt geadviseerd een afweging te maken tussen de gevolgen van een maatregel voor het bedrijfsproces en het restrisico dat zij bereid zijn daarbij te accepteren.

---

<sup>5</sup> Hiervoor is een tijd van een trusted time stamp server nodig

<sup>6</sup> Zie [http://blogs.adobe.com/security/2008/08/setting\\_signature\\_trust\\_in\\_ado\\_2.html](http://blogs.adobe.com/security/2008/08/setting_signature_trust_in_ado_2.html) onder "User Trust Setting #1"