

**Van:** Servicecentrum Logius

**Verzonden:** dinsdag 26 juli 2011

**Onderwerp:** Reminder: DigiD eenmalig inloggen en SHA256



Logius  
Ministerie van Binnenlandse Zaken en  
Koninkrijksrelaties

## PKIoverheid – SHA256

Geachte heer/mevrouw,

Op 30 mei 2011 heeft u van ons een bericht ontvangen over het vervangen van het PKIoverheid-certificaat voor DigiD eenmalig inloggen naar een nieuw SHA1 certificaat in juni en de voorbereiding die u moet treffen voor de nieuwe SHA256-certificaten in augustus. Inmiddels is het nieuwe SHA1-certificaat in juni geïnstalleerd. Om verstoringen in uw dienstverlening te voorkomen, willen we u nogmaals attenderen op de wijziging die u moet aanbrengen in uw systeem voor het nieuwe SHA256-certificaat in augustus. Hieronder kunt u lezen wat u wanneer moet doen en wat Logius precies doet.

### **Wat doet Logius in augustus 2011**

De datum waarop DigiD eenmalig inloggen overgaat op het beter beveiligde SHA256-certificaat is 16 augustus 2011. De planning voor de vervanging van het huidige SHA1-certificaat voor een nieuw SHA256-certificaat staat hieronder.

*Maandag 1 augustus 2011 07:00*

Logius installeert het SHA256-certificaat in de preproductie-omgeving.

*Van maandag 1 augustus tot en met 15 augustus 2011*

Logius stelt een 'freeze periode' in waar geen nieuwe klanten worden aangesloten op productie-omgeving.

*Maandag 15 augustus 2011 07:00*

Logius installeert het SHA256-certificaat in de productie-omgeving.

### **Wat moet u doen vóór en in augustus**

Neem contact op met uw ICT-afdeling en/of leverancier om ervoor te zorgen dat uw applicaties en systemen voor DigiD eenmalig inloggen, die met PKIoverheid-certificaten werken, de SHA256-technologie ondersteunen.

Als het nieuwe SHA256-certificaat door Logius is geïnstalleerd, wordt ook de metadata aangepast. Zodra de metadata is aangepast, moeten aangesloten webdiensten deze metadata inlezen. Hiervoor is een herstart van uw webdienst nodig.

*Maandag 1 augustus 2011 na 07:00*

Herstart uw webdienst in de preproductie-omgeving om de nieuwe metadata in te lezen.

*Maandag 15 augustus 2011 na 07:00*

Herstart uw webdienst in de productie-omgeving om de nieuwe metadata in te lezen.

**Let op:** DigiD eenmalig inloggen werkt pas weer zodra uw webdienst de metadata heeft ingelezen. Voer daarvoor op 1 en 15 augustus direct vanaf 07:00 uur de herstart uit.

Logius heeft de meest recente informatie rondom SHA256 op haar website geplaatst. Daarnaast gaan wij er van uit dat u zonder tegenbericht klaar bent voor de overgang naar SHA256. Mocht dat niet het geval zijn neem dan contact op met Servicecentrum Logius.

#### **Veilige dienstverlening via internet**

Uit recent internationaal onderzoek blijkt dat het algoritme onderliggend aan het SHA1-certificaat niet langer de garantie biedt onkraakbaar te zijn. Reden om het zogenoemde SHA256 algoritme te gebruiken dat vele malen veiliger is. Zo kunnen uw gebruikers ook in de toekomst veilig blijven inloggen met DigiD.

#### **Meer informatie**

Als u na het lezen van deze brief vragen heeft, dan kunt u op werkdagen van 8.00 tot 17.00 uur contact opnemen met Servicecentrum Logius op het telefoonnummer 0900 555 4555 (10 ct p/m) of per e-mail via [servicecentrum@logius.nl](mailto:servicecentrum@logius.nl).

Met vriendelijke groet,

Gertie Dullens  
Hoofd afdeling Markt