Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Forum Standaardisatie

Logius
Servicemanagement

Contactpersoon
Dhr M.A. Janssen

T 070-8887967

Datum
19 mei 2011

memo

Signaal m.b.t. SHA-2 op lijst gangbare standaarden

Inleiding

November 2010 is door het College Standaardisatie besloten dat op de lijst met gangbare standaarden MD5 wordt vervangen door SHA-2. Dit naar aanleiding van een notitie c.q. korte analyse van het Forum Standaardisatie[1]. Door het plaatsen van SHA-2 op de lijst met gangbare standaarden wordt, in de ogen van de lezer, het beeld opgeroepen dat het hier om een standaard gaat die algemeen in de praktijk gebruikt wordt. Dit is echter (nog) niet het geval.

Analyse

PKIoverheid geeft vanaf 1-1-2011 in principe alleen nog maar certificaten uit o.b.v. het SHA-256 algoritme. De komende 2 á 3 jaar gaat Logius deze certificaten plaatsen op haar voorzieningen. Eerder dit jaar is op een enkele Logius voorziening al een PKIoverheid SHA-256 certificaat geplaatst of er is aangekondigd dat deze geplaatst gaat worden. Dit heeft geleid tot enige commotie bij afnemers (o.a. manifestpartijen). Wat was het geval? De software die deze afnemers gebruikten was dermate verouderd dat deze het SHA-256 niet kon ondersteunen. Zie hier voor een lijst met de minimale systeemeisen.

Conclusie / advies

Ik geef in overweging om bij een volgende analyse van een gangbare standaard mee te nemen of deze standaard praktische restricties kent bij de implementatie van de standaard.

[1] https://www.forumstandaardisatie.nl/sites/default/files/FS/2010/0406/concept-CS-20100518.04I-notitie-vervanging-MD5-door-SHA-2.pdf