Forum Standaardisatie

Consultatiedocument Vervanging MD5 door SHA-2

Datum 6 augustus 2010

Colofon

Projectnaam	Consultatiedocument Vervaning MD5 door SHA-2
Versienummer	1.5 (definitief)
Locatie	
Organisatie	Forum Standaardisatie Postbus 84011 2508 AA Den Haag forumstandaardisatie@logius.nl
Auteurs	ir. Dennis Krukkert

Inhoud

1 Inleiding

1.1 Achtergrond en voorgeschiedenis

Medio 2007 is door de ministeries van Economische Zaken (EZ) en Binnenlandse Zaken en Koninkrijksrelaties (BZK) het actieplan Nederland Open in Verbinding (hierna: actieplan) aan de Tweede Kamer voorgelegd. De Tweede Kamer heeft het actieplan met instemming aangenomen. Eén van de actielijnen in het actieplan betreft open standaarden. Kort gezegd is het doel het stimuleren van het gebruik van open standaarden, in eerste instantie binnen de overheid, met als doel het vergroten van de interoperabiliteit en het reduceren van de leveranciersafhankelijkheid.

De betreffende standaarden vallen onder een 'pas toe of leg uit' beleid: uitgangspunt is het gebruik van een open standaard; wanneer een organisatie geen open standaard wil of kan gebruiken, moet dat beargumenteerd uitgelegd worden.

Binnen de actielijn van de open standaarden is het doel te komen tot een lijst met standaarden die valt onder het 'pas toe of leg uit' principe.

Naast de lijst met open standaarden voor ‘pas toe of leg uit’ wordt ook een lijst met gangbare standaarden bijgehouden. Deze lijst bevat een overzicht met open standaarden die binnen de (semi-) publieke sector ‘de facto’ zijn. Voor standaarden op de lijst met gangbare standaarden geldt niet het ‘pas toe of leg uit’ beleid.

1.2 Plaats van de consultatie in het proces

Secure Hash Algorithm 2 (hierna SHA-2) is aangemeld ter vervanging van Message Digest Algorithm 5 (hierna MD5) op de lijst met gangbare standaarden. Aanleiding voor de melding is dat het gebruik van MD5 door diverse organisaties wordt afgeraden in verband met geconstateerde beveiligingsproblemen. Het toetsingsproces van de standaard kent drie stappen:

- het opstellen van een advies door een inhoudelijk expert
- de openbare consultatie van het expertadvies
- de daarop volgende besluitvorming van het Forum en College.

De huidige fase - die van de openbare consultatie - heeft als doel de brede toetsing van het door de expert opgestelde advies. Dit expertadvies is opgesteld door dr. ir. Eddy Olk van TNO met ondersteuning van ir. Denns Krukkert.

Alle reacties uit de consultatie worden verzameld en worden, samen met het expertadvies, aan het Forum en College Standaardisatie aangeboden. Na het doorlopen van de openbare consultatie, wordt een duidelijk advies aan het Forum en College Standaardisatie opgeleverd over het wel of niet vervangen van MD5 door SHA-2 met het voorgestelde toepassingsgebied, voorzien van overwegingen en verdere verduidelijking. Indien het College uiteindelijk instemt met het advies, zal MD5 worden vervangen door SHA-2.

2 Consultatieprocedure

2.1 Het expertadvies

Onderwerp van deze consultatie is het "Expertadvies vervanging MD5 door SHA-2", datum 5 augustus 2010, versie 1.4. Het expertadvies is te vinden op www.open-standaarden.nl.

2.2 Vragen aan u

In hoofdstuk 3 van dit consultatiedocument wordt een aantal vragen aan u gesteld over wat in het expertadvies 'Vervanging MD5 door SHA-2' is opgenomen.

2.3 Uw reactie

Uw gewaardeerde reactie bestaat uit een duidelijke, onderbouwde schriftelijke beantwoording van de vragen zoals gesteld in hoofdstuk 3. De onderbouwing is van belang omdat enkel onderbouwde antwoorden inzicht kunnen geven aan het Forum en College Standaardisatie waarom eventueel wel of niet van het expertadvies zou moeten worden afgeweken.

Na afloop van de termijn (zie hierna) waarbinnen reactie kunnen worden gegeven maakt het Bureau Standaardisatie deze in beginsel openbaar op de website www.open-standaarden.nl. Als u van mening bent dat (delen van) uw reactie van (bedrijfs-)vertrouwelijke aard is en als zodanig dient te worden behandeld, dient u dit gemotiveerd aan te geven. In dit geval dient u twee versies van uw reactie aan het Bureau toe te zenden: een vertrouwelijke en een openbare versie.

Het Bureau Standaardisatie zal de naar zijn oordeel relevante inzichten uit de consultatieronde gebruiken om, naast het expertadvies, aan het Forum en College Standaardisatie voor te leggen. Op deze manier kunnen het Forum en College een afgewogen besluit nemen over het al dan niet vervangen van MD5 door SHA-2 op de lijst met gangbare standaarden.

2.4 Termijn en adres

Uw reactie op de vragen in het voorliggende consultatiedocument kunt u schriftelijk of per e-mail, indienen op het volgende adres:

Per e-mail:
forumstandaardisatie@gbo.overheid.nl,
onder vermelding van 'Consultatieprocedure SHA-2'.

Per post:
GBO Overheid
Bureau Forum Standaardisatie
o.v.v. Consultatieprocedure SHA-2
Postbus 84011
2508 AA Den Haag

Uw reactie dient **voor maandag 13 september 2010** in het bezit te zijn van het Bureau Forum Standaardisatie.

3 Consultatie

3.1 Inleiding

Onderstaand wordt een aantal vragen aan u gesteld omtrent het expertadvies 'Vervanging MD5 door SHA-2'. Gelieve in uw beantwoording dezelfde nummering aan te houden. Graag, zoals al eerder opgemerkt, waar mogelijk ook de onderbouwing van uw antwoord bijvoegen zodat inzichtelijk wordt op basis waarvan u tot een (eventueel afwijkend) oordeel komt.

3.2 Vragen over het expertadvies

Hoofdstuk 2 beschrijft het advies van aan het Forum en College standaardisatie

Vraag:

1. Bent u het eens met het advies om MD5 te vervangen door SHA-2 op de lijst met gangbare standaarden. [pagina 5 van het expertadvies].
2. Bent u het eens met het geadviseerde functionele toepassingsgebied van SHA-2? [paragraaf 3.1 van het expertadvies]
3. Bent u het eens met de conclusie van de experts ten aanzien van de uitsluitingscriteria? [paragraaf 3.2 van het expertadvies]
4. Bent u het eens met de conclusie van de experts inzake de openheid van de standaard SHA-2? [paragraaf 3.3 van het expertadvies]
5. Bent u het eens met de conclusie van de experts dat er in voldoende mate consensus is over het gebruik van SHA-2 in plaats van MD5? [paragraaf 3.4 van het expertadvies]