Datum
21 september 2010

notitie

Verzamelde reacties publieke consultatie SHA-2

Lijnparaaf	Medeparaaf	Afschrift aan

De staatssecretaris van Economische Zaken heeft op maandag 17 september 2007 het actieplan open standaarden en open source software aan de Tweede Kamer gestuurd. Het doel van het actieplan is om de informatievoorziening toegankelijker te maken, onafhankelijkheid van ICT leveranciers te creëren en de weg vrij te maken voor innovatie.

Een onderdeel van het actieplan is het opstellen van een lijst met standaarden, die vallen onder het principe "pas toe of leg uit" (comply-or-explain). Tevens wordt er een lijst opgesteld met gangbare standaarden, maar voor standaarden op deze lijst geldt niet het “pas toe of leg uit” principe. Het College Standaardisatie spreekt zich uit over de standaarden die op beide lijst zullen worden opgenomen, o.a. op basis van een expertbeoordeling van de standaard.

SHA-2 is voorgedragen voor opname op de lijst met gangbare standaarden als vervanger voor de MD5 standaard. Door TNO is een expertadvies opgesteld waarin geadviseerd wordt om MD5 inderdaad te vervangen. Conform procedure is het expertadvies vijf weken publiek geconsulteerd. Dit document bevat alle ontvangen reacties op de consultatieronde van SHA-2.

In dit document vindt u achtereenvolgens de reacties van:

- RBS
- Ministerie van VWS
- Gemeente Enschede
- Inspectie Verkeer en Waterstaat
- Ministerie van Financiën
- Belastingdienst
- Ministerie van BZK
- Ministerie van LNV
- Ministerie van Justitie
- Ministerie van OCW
- IDSW

Reactie RBS

Datum
21 september 2010

Van: Potgieser, Peter
Aan: Bart Knubben

Onderwerp: Je vraag naar feedback

Hi Bart,

In antwoord op je vraag naar feedback:

Ik heb via de NormCommissie Financiële Diensten in de achterban (alleen) naar het Expertadvies MD5 en SHA-2 kunnen laten kijken. (vanuit beveiligingsoogpunt het meest relevant). Het expertadvies is in lijn met de NIST lijst "Approved algorithms for secure hashing" en met ISO standaard 10118 (Hash Functions). Ook op het aangegeven toepassingsgebied kwam daarbij geen commentaar.

Vriendelijke groet,
Peter

Reactie Ministerie van VWS

Datum
21 september 2010

Van: Haveman, dhr. drs. H.B.

Aan: Bart Knubben

Onderwerp: RE: REMINDER: Openbare consultatie IPv6, PKIoverheid en SHA-2 standaarden

Bart

Ter info; onze VWS-informatie is voldoende ingebracht en verwerkt via de expertmeetings
Akkoord dus.

Hans

Reactie Gemeente Enschede

Datum
21 september 2010

Aan: Bart Knubben
Van: Hans Koenders

Ik heb eerder de vraag uitgezet bij het IMG 100.000+ overleg, bij de VNG en de het Overleg Open Gemeenten (waaraan ook BZK en NOiV deelnemen) en intern in de gemeente Enschede.
In z'n algemeenheid stel ik vast dat de materie niet erg "leeft". Het beeld dat ik aantref is dat óf betrokkenen in de gemeenten toch wel heel erg leken zijn, óf zij de open standaard logisch vinden.

In het Overleg Open Gemeenten is gesproken over de voorgenomen open standaarden. Ik ervaar daar vertrouwen in de adviezen van de experts. Die zijn óók in deze drie gevallen heel goed leesbaar en plausibel. Een korte rondvraag bij deskundigen bij mij in de buurt leert me dat IPv6 volstrekt logisch is en dat SHA-2 inderdaad risico's vermindert.
Het advies omtrent PKI-Overheid getuigt ervan dat de experts zich goed bewust zijn van de grenzen van de open standaarden. Voor mij is PKI zó standaard dat ik me niet meer realiseer dat het een andere typologie van standaard is.

Mijn toets in mijn -natuurlijk beperkte- omgeving leert, dat ik Marcel Meijs, als lid van het College van Standaardisatie graag meegeef in te stemmen met de adviezen.

Met vriendelijke groet
Hans Koenders

Reactie Inspectie Verkeer en Waterstaat

Datum
21 september 2010

Van: Duijne, J. van (Jennifer) **Namens** Inspecteur Generaal - IVW

Aan: Bart Knubben
Onderwerp: RE: REMINDER: Openbare consultatie IPv6, PKIoverheid en SHA-2 standaarden

Beste Bart,

Jenny Thunnissen heeft geen opmerkingen, het is prima zo.

Groet, Jennifer van Duijne

Reactie Ministerie van Financiën

Datum
21 september 2010

Van: Linden, FMJ (Frank) van (BEDR/ICT)

Aan: Bart Knubben
Onderwerp: Reactie MinFin op consultatie IPV6, PKI-overheid en SHA-2

Beste Bart,

Het Ministerie van Financien heeft verder geen aanvullende opmerkingen of vragen over het gedegen onderzoek van de expertgroepen over de respectieve onderwerpen PKIoverheid. IPV6 en SHA-2.
Minfin kan instemmen met de adviezen. (PKIoverheid nog geen Open standaard, het belang van IPV6, ook de Overheid zal deze standaard moeten gaan invoeren om connectiviteit te behouden, SHA-2 ipv MD-5 t.b.v. authenticatie en integriteitscontrole)

MinFin ziet het belang van de introductie IPV6 en zal de activiteiten ook in haar roadmap gaan opnemen om als departement haar connectiviteit te behouden.

Met vriendelijke groeten,

Frank van Linden

Reactie Belastingdienst

Datum
21 september 2010

Antwoorden

Vraag 1: Ja
Vraag 2: Ja
Vraag 3: Ja
Vraag 4: Ja
Vraag 5: Ja

Vraag : In hoeverre is het Patriot Act, (US Law 107 – 56) op deze standaard van toepassing? Zijn er in het kader daarvan verplicht ingebouwde back-doors aangebracht?

Voor toelichting op bovenstaande contact opnemen met:

J.E. (Jaap) van der Veen
Strategisch architect Informatiebeveiliging
.....
Ministerie van Financiën
Directoraat-Generaal Belastingdienst
IV-Beleid, Team Risicomanagement

Reactie Ministerie van BZK

Datum
21 september 2010

Van: Wierda, Hylke
Aan: Logius Forumstandaardisatie; Bart Knubben
Onderwerp: RE: Openbare consultatie IPv6, PKIoverheid en SHA-2 standaarden

Geachte heer Knubben,

Hierbij ontvangt u vanuit BZK de reactie op de openbare consultatieronde voor IPv6, PKIOverheid en SHA-2. Hierbij zijn de 3 adviezen in 1 document opgenomen.
Mocht u vragen hebben, dan verneem ik dat graag.

Met vriendelijke groet, mede namens Nicole Stolk,

Hylke Wierda
plv. CIO

SHA-2

Binnen geautomatiseerde processen is van belang dat de integriteit van bestanden/berichten op betrouwbare wijze geverifieerd kan worden.
Hiervoor wordt vaak gebruik gemaakt van zogenaamde hashing algoritmes, hiermee worden "vingerafdrukken" van de data gegenereerd die op reproduceerbare wijze op vastgestelde stappen in de processen gecontroleerd kunnen worden.

De mogelijkheid tot het betrouwbaar uitvoeren van dergelijke controles zijn onder andere van vitaal belang bij de validatie van PKI certificaten.

Tot op heden wordt vaak gebruik gemaakt van een techniek genaamd MD5, deze techniek stamt echter uit begin '90 jaren en heeft inmiddels door de toegenomen rekenkracht van de hedendaagse PC's een te lage zekerheidswaarde.
Door de Amerikaanse overheid is de SHA-2 "familie" ontwikkeld, de term familie duidt er in deze op dat er verschillende zwaartes (sleutellengtes) van mogelijk zijn.

De SHA-2 technieken zijn inmiddels door de industrie omarmd, en zijn door diverse overheden wereldwijd tot verplichting voor gerubriceerde materialen verheven, en hebben reeds een zeer brede implementatiebasis, impact van de invoering van deze standaard zal dan ook zeer beperkt zijn aangezien op alle hiervoor relevante toepassingsgebieden de software reeds breed uitgerold is.

Zie bijlage 3 voor de beantwoording van de door het Forum Standaardisatie gestelde vragen.

Bijlage 3: Beantwoording vragen SHA-2

Links:
Consultatiedocument
Expertadvies

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].
    a. Ja

2. Bent u het eens met het geadviseerde functionele toepassingsgebied van SHA-2? [paragraaf 3.1 van het expertadvies]
    a. Ja
3. Bent u het eens met de conclusie van de experts ten aanzien van de uitsluitingscriteria? [paragraaf 3.2 van het expertadvies]
    a. Ja
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]
    a. Ja
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]
    a. Ja

Datum
21 september 2010

Reactie Ministerie van LNV

Van: Rood, drs. P.H. (Pieter)
Aan: Bart Knubben; Logius Forumstandaardisatie

Onderwerp: RE: REMINDER: Openbare consultatie IPv6, PKIoverheid en SHA-2 standaarden

Beste Bart,
Bij deze de reactie op de openbare consultatie van LNV.
Met vriendelijke groet.
Pieter Rood

SHA-2

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].

Ja eens.
Verrassend dat MD5 nog als standaard stond terwijl industry best practices / NIST al jaren MD5 vervangen hadden door SHA_1.

2. Bent u het eens met het geadviseerde functionele toepassingsgebied van SHA_2? [paragraaf 3.1 van het expertadvies]

Ja eens.

3. Bent u het eens met de conclusie van de experts ten aanzien van de uitsluitingscriteria? [paragraaf 3.2 van het expertadvies]

Nee, niet volledig. 3.2 derde punt stelt:

- *Geen beperkt werkingsgebied.*
  Aan deze eis wordt voldaan, SHA_2 is niet organisatie_ of implementatiespecifiek.

Echter, het is mogelijk dat bestaande software die geen SHA-2 ondersteunt in gebruik is bij LNV of bij LNV-relaties. Wat dan ?

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]

Ja eens.

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]

Ja eens.

Reactie Ministerie van Justitie

Datum
21 september 2010

Van: Groustra F.R. - BD/DI
Aan: Logius Forumstandaardisatie
Onderwerp: SHA-2

Beste Bart,

Justitie is het eens met de uitkomsten van de expertgroep
Hierbij het ingevulde consultatie document op de nieuwe
standaard SHA-2 ingevuld met behulp van Justitie achterban.

Mvg

Roland Groustra
ICT-adviseur/EA-architect

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].
=> JA
2. Bent u het eens met het geadviseerde functionele toepassingsgebied van SHA_2? [paragraaf 3.1 van het expertadvies]
=> JA
3. Bent u het eens met de conclusie van de experts ten aanzien van de uitsluitingscriteria? [paragraaf 3.2 van het expertadvies]
=> JA
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]
=> JA
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]
=> JA

Reactie Ministerie van OCW

Datum
21 september 2010

From: Gaakeer, Bram

To: Bos, Marianne; Bart Knubben
Subject: RE: REMINDER: Openbare consultatie IPv6, PKIoverheid en SHA-2 standaarden

Beste Bart,

Bij deze laat ik je weten dat OCW akkoord gaat met de voorgestelde standaarden.

Vriendelijke groeten,

Bram Gaakeer

IDsW
InformatieDesk standaarden Water

Postbus 17
8200 AA, Lelystad

Forum Standaardisatie
Postbus 84011
2508 AA Den Haag

Onze referentie:	Uw referentie: Consultatie IPv6; PKI; SHA-2	Datum: 13-09-2010

L.S.,

In reactie op de openbare consultatie aangaande:
A: IPv6
B: PKI Overheid
C: SHA-2
het volgende:

Ad a: IPv6

Wij vinden het advies voor IPv6 tweeslachtig, enerzijds wordt voorgesteld deze standaard op de 'pas toe of leg uit' lijst op te nemen, anderzijds is de verwachting dat niemand op korte termijn over zal gaan.

Met name omdat IPv4 momenteel de de-facto standaard is kan niet van 'pas toe of leg uit' worden gesproken zonder substantiële investeringen. Het lijkt daarmee dan ook alleen mogelijk om IPv6 op korte termijn toe te passen door het maken van grote investeringen. Ook binnen de waterwereld zien we deze ontwikkeling en wordt voorzien dat de ontwikkeling in lopende ontwikkelingen wordt meegenomen.

Vanuit dit oogpunt zien we het gebruik van IPv6 als sterke aanbeveling voor toekomstige ontwikkelingen maar zien we ook dat de standaard niet als zodanig op de 'pas toe of leg uit' lijst thuis hoort aangezien dit onvermijdelijk zal leiden tot veel uitleg en geen significant grotere toepassing. Een mogelijk alternatief is opname van zowel IPv4 als IPv6 tot het moment dat voldoende organisaties IPv6 hebben geïmplementeerd.

Ad b: PKI Overheid
Rondom PKI Overheid hebben we een tweeslachtige reactie. Enerzijds juichen wij het vaststellen van standaard methoden voor een betrouwbare communicatie toe. Het voordeel hiervan voor de afnemer is groot doordat deze nog slechts me één methode wordt geconfronteerd.

Anderzijds zien we hiermee ook een keuze die potentieel marktverstorend kan werken doordat het leveranciers niet meer is toegestaan om eigen certificaten etc toe te passen (gedwongen winkelnering). Een nadere definitie van het werkingsgebied (bv basisregistraties) kan hier veel onduidelijkheid wegnemen.

Vanuit deze optiek onderschrijven wij de conclusie van de expertgroep (niet opnemen) maar zien we graag stimuleringsmaatregelen voor de toepassing van PKI Overheid.

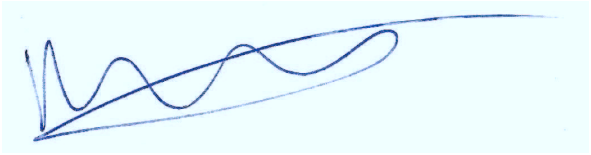
Ad c: SHA-2

De keuze voor SHA-2 tav de huidige standaarden wordt door ons onderschreven.

Met vriendelijke groet,

Myriam de Jong,
Programma manager IDsW

Namens deze,



Huibert-Jan Lekkerkerk
Sr. Projectleider standaarden IDsW