Datum
21 september 2010

notitie

Verzamelde reacties publieke consultatie PKI.Overheid

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). Het College Standaardisatie spreekt zich uit over de standaarden die op de lijst zullen worden opgenomen, o.a. op basis van een expertbeoordeling van de standaard. De expertbeoordeling van PKI.Overheid plaatsgevonden tijdens een bijeenkomst op donderdag 15 juli 2010. Conform procedure is het expertadvies vijf weken publiek geconsulteerd. Dit document bevat alle ontvangen reacties op de consultatieronde van PKI.Overheid.

In dit document vindt u achtereenvolgens de reacties van:

- Kadaster
- Ministerie van EZ
- Ministerie van VWS
- Gemeente Enschede
- Inspectie Verkeer en Waterstaat
- Kamer van Koophandel
- Ministerie van Financiën
- Belastingdienst
- Ministerie van BZK
- Ministerie van BZK
- Ministerie van LNV
- Ministerie van Justitie
- Ministerie van OCW

Reactie Kadaster

Datum
21 september 2010

Van: Mekking, Steven
Aan: Logius Forumstandaardisatie
CC: Groothedde, Arco
Onderwerp: Consultatieprocedure PKIoverheid, reactie namens het Kadaster.

Geachte heer, mevrouw,

Wij hebben kennis genomen van het Expertadvies PvE PKIoverheid deel 3a t/d, versie 2.1 en geven hierbij een reactie op de voor het Kadaster van toepassing zijnde vragen uit het consultatiedocument:

1. Aanvullingen of wijzigingen
Alhoewel we het met de strekking van het advies eens zijn, missen we in het document de internationale aspecten. Steeds vaker zullen Nederlandse overheden diensten (moeten) leveren aan buitenlandse burgers en bedrijven, waarbij in principe ook sprake kan zijn van het gebruik van PKI-toepassingen. Het is nu onduidelijk in hoe de Nederlandse PKI-overheid standaard dit soort internationale overheidsdienstverlening bevordert of wellicht belemmert. Er wordt nu heel kort in paragraaf 2.1. naar het STORK-project verwezen, maar een wat explicietere toelichting van de internationale of EU-aspecten (bijvoorbeeld in een afzonderlijke paragraaf) zou verhelderend zijn. In een dergelijke paragraaf zou ook een relatie met het Europese interoperabiliteitsraamwerk kunnen worden gelegd.

2 Het geadviseerde functionele toepassingsgebied
De mening, en de daaraan ten grondslag liggende argumenten, van de expertgroep dat het niet mogelijk is om een toepassingsgebied voor het gebruik vast te stellen, onderschrijven we volledig. Bij de inrichting van de elektronische aktenverwerking van het Kadaster is het een bewuste keuze geweest om niet zelf certificaten te gaan uitgeven en alleen kwaliteitseisen (conform de Wet Elektronische Handtekening) te stellen aan het gebruik van gekwalificeerde elektronische handtekeningen. Dit om aanleverende private partijen de vrijheid te geven zelf een voor hun bedrijfsvoering optimale oplossing te kiezen. Dit beleid is ook in de Kadasterwet verankerd. Een verplichting om aanbieders te dwingen PKI-oveheidscertificaten te gebruiken, past hier niet bij. We zijn blij dat de expertgroep dit heeft onderkend.

Met vriendelijke groet,
Steven Mekking

S. Mekking, senior adviseur
Kadaster, Strategie en Beleid

Reactie Ministerie van EZ

Datum
21 september 2010

Van: Haasnoot drs A.
Aan: Bart Knubben
CC: Brand drs R.; Wijnen drs E.L.
Onderwerp: PKI-overheid op lijst met open standaarden

Goedemiddag Bart,

Momenteel wordt de haalbaarheid onderzocht om PKI-Overheid op de pas-toe-of-leg-uit lijst met open standaarden te plaatsen. Er is inmiddels een expertcommissie geweest die geadviseerd heeft om PKI-Overheid niet op te nemen op de pas-toe-of-leg-uit lijst. Momenteel loopt de openbare consultatie over IPv6 op basis van dit advies. In het kader van de consultatie van IPv6 is het belangrijk om het onderstaande punt mee te nemen bij het doorgeleiden van het expertadvies naar het Forum Standaardisatie.

Mijnsinziens is pas-toe-of-leg-uit lijst met open standaarden bedoeld om interoperabiliteit en leveranciersonafhankelijkheid te bevorderen en niet om concurrentievoordeel voor een bepaalde groep aanbieders ten opzichte van aanbieders van gelijkwaardige oplossingen te bewerkstelligen. Door eventuele opname van PKI-Overheid op de pas-toe-of-leg-uit lijst kan sprake zijn van marktverstoring doordat Nederlandse overheidspartijen die iets met certificaattechnologie willen, geacht worden voor PKI-overheidcertificaten te kiezen. Anders hebben ze iets uit te leggen. Dit kan aanbieders van andere certificaten met hetzelfde veiligheidsniveau benadelen.

Momenteel wordt gewerkt aan een afsprakenstelsel eHerkenning. Op het hoogste niveau van eHerkenning (veiligheidsniveau 4) wordt gewerkt met certificaattechnologie. PKI-overheid past hier prima in maar is niet de enige oplossing. Er zijn in Nederland ook aanbieders van certificaten die niet aan PKI-overheid voldoen maar die wel veiligheidsniveau 4 kunnen bieden. Daarnaast zijn er in Europa ook andere aanbieders van certificaten op niveau 4 die niet aan PKI-overheid voldoen. Het is goed mogelijk dat deze niet PKI-overheidoplossingen wel voldoen aan eHerkenning waarmee interoperabiliteit is gewaarborgd. Hier volgt een voorbeeld. Stel de inspectie Verkeer en Waterstaat wil certificaten inkopen voor de taximeter. Ze hebben het betrouwbaarheidsniveau vastgesteld op 4 en hebben er 10.000 nodig. Dan ligt het voor de hand dat ze kijken bij wie de certificaten het goedkoopste zijn, eventueel ook over de grens heen. De inspectie zou niet min of meer gedwongen moeten worden om te kiezen voor PKI-overheidcertificaten maar voor de goedkoopste die aan het vereiste veiligheidsniveau voldoet.

Mijn zorg/ vraag is wat de consequenties zijn voor niet PKI-overheidoplossingen (die wel het benodigde veiligheidsniveau hebben en ook voldoen aan eHerkenning) wanneer PKI-overheid op de lijst met open standaarden wordt geplaatst.

Met vriendelijke groet,
Arjen Haasnoot

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) - IVW **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 Kamer van Koophandel

Datum
21 september 2010

Geachte leden forum standaardisatie,

Consultatie vraag 11

Ondergetekende kan het niet eens zijn met het expertadvies ten aanzien van het enkelvoudig stimuleren van het gebruik van PKIOverheid certificaten. Er is meer behoefte aan een totaal beeld en mogelijke daarbij behorende standaarden over het toepassen van beveiligde en ondertekende overheidsdienstverlening. Het gebruik van PKIOverheid certificaten valt dan vanzelf wel of niet op zijn plaats.

Mogelijk dat het Expertadvies in de Managementsamenvatting wel kan pleiten voor het scheppen van duidelijk onderscheid in de verschillende typen standaarden die nu gezamenlijk met de standaard PKIOverheid worden benoemd. Door hieraan de (mogelijke) achterliggende behoeften te formuleren ontstaat ook meer duidelijkheid over nut en noodzaak.

Mogelijke advies aanvulling - inhoud
Leidraad: vanuit de wettelijke kaders
vanuit de bestaande papieren overheidsbedrijfsprocessen
vanuit de reeds opgestelde programma's van eisen van overheidsprocessen die via elektronische weg verlopen

Mogelijke te onderkennen gebieden voor het definieren van standaards:

1. processen van CSP's rondom de uitgifte en het gebruik van certificaten, zodat CSP's een PKI kunnen opzetten die certificaten oplevert die te gebruiken zijn binnen de elektronische overheidsdienstverlening
2. technische producten die dienstverlening over PKI mogelijk maken, zodat leveranciers en overheidsafnemers weten waar producten en toepassingen aan moeten voldoen binnen de elektronische overheidsdienstverlening
3. processen van elektronische overheidsdienstverlening, zodat overheidsdienstverleners op (wettelijk) verantwoorde wijze de met PKI geboden faciliteiten kunnen toepassen in hun bedrijfsprocessen
4. de overheid PKI CA, zodat er bij het gebruik van PKI binnen de eigen techniek een aan de overheid gelieerd beveiligingscontrole middel ontstaat binnen de implementaties van de overheidsdienstverleners.
5. de relatie tussen het GBA en de PKI certificaten, zodat bestaande papieren dienstverlening correct overgezet kan worden naar een elektronische variant.

Daarnaast moet binnen de standaards onderscheid gemaakt worden in:

- beveiligingsniveaus (bv. hoog, midden, laag)
- identificatie, ondertekening, verzegeling (taximeter), vertrouwelijkheid

Met vriendelijke groet,

Reeuward Bousema
ICT-infrastructuur architect
Afdeling IM&O

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: Nee, er zijn geen aanvullingen of wijzigingen nodig op par. 1.1. – 1.7 van het document
Vraag 2: Ja
Vraag 3: Ja
Vraag 4: Ja, mits rekening gehouden wordt met het feit dat implementatie van een bepaalde versie binnen een bedrijf een bepaalde doorlooptijd kent. Wanneer halverwege de implementatie van een versie een nieuwe versie verschijnt, moet er een mogelijkheid zijn om 'door te gaan', al dan niet met de oude versie, totdat de update naar de nieuwe versie ingepland kan worden. Dit 'rekening houden met' zou b.v. betekenen dat ruim van te voren bij de aanvrager van certificaten bekend is dat er een nieuwe versie op komst is, zodat dit kan worden ingepland.
Vraag 5: Ja
Vraag 6: Ja
Vraag 7: Ja
Vraag 8: Ja, als toevoeging zie ik wel een positief effect op de bedrijfsvoering, n.l. die van eenduidigheid en efficiënt werken.
Vraag 9: Ja, merkwaardig is wel dat niet achterhaald kan worden hoe het precies zit met het intellectueel eigendom van de onderliggende technische standaarden, t.a.v. het beschikking stellen daaraan aan uitgevers van de certificaten.
Vraag 10 Ja.
Vraag 11 Ja. Aanvullend op het verplicht stellen helpt het ook om organisaties te assisteren bij het migreren van de bestaande (niet PKI-O) naar PKI-Overheidscertificaten, voor zover dit nog niet gedaan wordt. Zoals in het expertadvies is aangegeven is deze migratie niet eenvoudig.
Vraag 12 Nee.

Voor toelichting op bovenstaande contact opnemen met:

J.E. (Jaap) van der Veen
Strategisch architect Informatiebeveiliging

Reactie Ministerie van BZK

Datum
21 september 2010

Van: Luijten, Carlo
Aan: Logius Forumstandaardisatie
CC: Guus Bronkhorst; Adamse, Carl; Mark Janssen
Onderwerp: Consultatieprocedue PKIoverheid
Urgentie: Hoog

Bureau Forum Standaardisatie,

Bijgaand treft u de reactie van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties aan, betreffende de consultatieprocedure PKIoverheid.

Heeft u vragen of opmerkingen, dan verneem ik die graag van u.

Gr. Carlo Luijten

Programmadirectie Dienstverlening Regeldruk en Informatiebeleid (DRI)
Cluster Informatiebeleid Basisvoorzieningen Overheid (IBO)

Vraag:
1. Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig, bezien vanuit het doel van het document (het Forum en College Standaardisatie voorzien van een inhoudelijk relevante toelichting op PKIoverheid). [paragraaf 1.1 t/m 1.7 van het expertadvies].

Antwoord:
Geen opmerkingen.

Vraag:
2. Bent u het eens met het door de expertgroep geadviseerde functionele toepassingsgebied van PKIoverheid? [paragraaf 2.1 van het expertadvies]

Antwoord:
Neen. Hieronder volgen puntsgewijs de argumenten waarom het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (hierna aangeduid als BZK) zich niet kan vinden in het geadviseerde functionele toepassingsgebied van PKIoverheid:

- Het Programma van Eisen (PvE) van PKIoverheid heeft niet uitsluitend en alleen als toepassingsgebied het uitgeven van elektronische certificaten ten behoeve van een gekwalificeerde elektronische handtekening. Ergo veruit de meeste certificaten die onder de PKI voor de overheid worden uitgegeven, worden gebruikt voor andere toepassingen zoals beveiliging van websites, system to system communicatie en authenticeren van personen, organisaties en middelen langs elektronische weg. Het geadviseerde functionele toepassingsgebied is veel te beperkt. Het gaat niet alleen om elektronische certificaten ten behoeve van een gekwalificeerde elektronische handtekening maar om vele PKI oplossingen c.q. toepassingen;
- De Expertgroep heeft in haar advies ten onrechte als uitgangspunt het *uitgeven* van certificaten gehanteerd terwijl het moet gaan om het *gebruik* daarvan. De Expertgroep heeft als uitgangspunt het uitgeven van certificaten genomen omdat zij geen mogelijkheden zag om een toepassingsgebied vast te stellen voor het gebruik van elektronische certificaten. Zij geeft aan dat het daarom beter zou zijn wanneer de overheid als geheel of binnen specifieke domeinen vastlegt welke betrouwbaarheidsniveaus voor welke toepassingen behaald moeten worden. BZK herkent deze problematiek. Deze problematiek is ook

reeds eerder geconstateerd en beschreven in de notitie van het Forum Standaardisatie met als kenmerk FS22-10-07 en als onderwerp "Indeling van authenticatiemiddelen".

Anticiperend hierop stelt BZK voor om onduidelijkheid over welke betrouwbaarheidsniveaus voor welke toepassingen gelden, niet blokkerend te laten zijn voor de opname van het PvE van PKIoverheid op de pas toe of leg uit lijst. BZK stelt verder voor dat de volgende overgangssituatie zal gelden voor wat betreft het toepassen van het PvE van PKIoverheid:

> "Als gebruik wordt gemaakt van het product PKI certificaten in de elektronische communicatie met (door burgers en bedrijven) én tussen overheden en instellingen in de (semi-) publieke sector, deze dan de facto gebaseerd is op de normen uit het Programma van Eisen van PKIoverheid.
>
> Wanneer overheden en instellingen in de (semi-) publieke sector, o.b.v. een door hen uitgevoerde risicoanalyse naar de gewenste betrouwbaarheid voor de elektronische communicatie, besluiten om een PKI product of dienst af te nemen, dan dient deze gebaseerd te zijn op de normen uit het PvE van PKIoverheid."

Deze uitgangspunten zullen niet leiden tot "marktvervuiling/verstoring". Als uitgegaan wordt van het *gebruik* van certificaten als toepassingsgebied dan kan dit bijdragen aan een grotere leveranciersonafhankelijkheid. Afnemers kunnen dan immers kiezen uit meerdere commerciële aanbieders (van PKIoverheid certificaten).

Als het Programma van Eisen van PKIoverheid (PvE deel 3a en 3b) wordt opgenomen op de pas toe of leg uit lijst, dan moeten overheden en instellingen uit de (semi-)publieke sector bij ICT-opdrachten (inkoop en aanbestedingen) i.h.k.v. nieuwbouw, verbouw of contractverlenging waarbij PKI een rol speelt, het 'comply-or-explain and commit'-principe toepassen. Dit betekent b.v. dat als een overheidsorgaan een e-overheid voorziening wil bouwen en daarbij PKI wil gebruiken zij de *plicht* heeft om PKIoverheid te gebruiken (of zij moet kunnen uitleggen waarom zij dit bewust niet doet).

Burgers en bedrijven zijn niet gecommitteerd aan het 'comply-or-explain and commit'-principe. Zij kunnen echter wel *rechten* ontlenen aan het 'comply-or-explain and commit'-principe. Dit betekent b.v. dat als een (medewerker van een) bedrijf zich authenticeert met een PKIoverheid certificaat bij een overheidsorgaan, dit geaccepteerd moet (kunnen) worden (of het overheidsorgaan moet kunnen uitleggen waarom zij dit bewust niet accepteert).

Vraag:
3. Bent u het eens met het door de expertgroep geadviseerde organisatorische werkingsgebied van PKIoverheid? [paragraaf 2.2 van het expertadvies]

Antwoord:
Ja. Geen opmerkingen.

In het verlengde van het antwoord op vraag 2 en 3 kan het toepassings- en werkingsgebied nu als volgt vastgesteld worden:
"*Het gebruiken van PKI oplossingen bij nieuwbouw, verbouw of contractverlenging"* door *"Overheden en instellingen in de (semi-) publieke sector"*.

Vraag:

4. Herkent u zich in de door de expertgroep gemaakte opmerking dat certificaten altijd op basis van de laatste versie van PKIoverheid moeten worden uitgegeven? [paragraaf 2.3 van het expertadvies]

Antwoord:
Neen. Bepalend moet zijn of een nieuwe versie van het PvE van PKIoverheid gevolgen heeft voor de interoperabiliteit en/of de leveranciersonafhankelijk met betrekking tot het gebruik van certificaten. In dat kader zou het onzinnig zijn om elke nieuwe versie van het PvE van PKIoverheid voor te leggen aan het Forum. Zo is b.v. begin dit jaar, zoals de Expertgroep zelf ook al aangeeft, de versie van het PvE van PKIoverheid van versie 2.0 naar 2.1 gegaan enkel en alleen omdat de documenten in overeenstemming zijn gebracht met de nieuwe huisstijl van de Rijksoverheid.

Om aan het bezwaar van de Expertgroep tegemoet te komen stelt BZK voor om de change advisory board (zie antwoord op vraag 5) te laten beoordelen of de voorgestelde wijzigingen van het PvE van PKIoverheid negatieve gevolgen hebben voor interoperabiliteit en/of de leveranciersonafhankelijk met betrekking tot het gebruik van certificaten. Als dit wordt geconstateerd dan zou voorlegging aan het Forum aan de orde zijn.

Vraag:
5. Bent u het eens met de conclusie van de expertgroep inzake de openheid van PKIoverheid? [paragraaf 3.1 van het expertadvies]

Antwoord:
BZK wil benadrukken dat er te allen tijde gestreefd wordt naar consensus in het Afnemersoverleg tussen de Policy Authority PKIoverheid en haar certificatiedienstverleners. Desalniettemin liggen de uiteindelijke beslissingen bij BZK.

Om die reden wil BZK de suggestie, van de Expertgroep, om een change advisory board op te richten verder uitwerken. Deelnemers aan deze board kunnen dan b.v. bestaan uit de ministeries die thans al gebruik maken van PKIoverheid oplossingen (of dit in de zeer nabije toekomst gaan doen). Het betreft Defensie, VWS, VenW, Justitie en BZK zelf.

Vraag:
6. Bent u het eens met de conclusie van de expertgroep inzake de bruikbaarheid van PKIoverheid? [paragraaf 3.2 van het expertadvies]

Antwoord:
Ja. De suggesties van de Expertgroep bij paragraaf 3.2.3 worden ter kennisgeving aangenomen.

Vraag:
7. Bent u het eens met de conclusie van de expertgroep inzake het potentieel van opname van PKIoverheid op de lijst met open standaarden? [paragraaf 3.3 van het expertadvies]

Antwoord:
Neen. BZK is het niet eens met het gegeven toepassingsgebied. Zie hiervoor ons antwoord op vraag 2. Echter als uitgegaan wordt van het *gebruik* van certificaten als toepassingsgebied dan kan dit bijdragen aan een grotere leveranciersonaf-hankelijkheid. Afnemers kunnen dan immers kiezen uit meerdere commerciële

aanbieders van PKIoverheid certificaten. Daarnaast constateert de Expertgroep zelf dat het *gebruik* van certificaten die allemaal volgens dezelfde manier zijn uitgegeven kan bijdragen aan interoperabiliteit – het vertrouwensniveau is immers gelijk.

Vraag:
8. Bent u het eens met de conclusie van de expertgroep inzake de impact van PKIoverheid? [paragraaf 3.4 van het expertadvies]

Antwoord:
Geen opmerkingen.

Vraag:
9. Bent u het eens met de samenvatting van de overwegingen van de expertgroep? [paragraaf 4.1 van het expertadvies]

Antwoord:
Neen. De bezwaren tegen, en de aanvullingen op, de overwegingen zijn al geadresseerd in onze antwoorden op vraag 2, 4, 5 en 7.

Vraag:
10. Bent u het eens met het advies van de expertgroep aan het Forum en College Standaardisatie? [paragraaf 4.2 van het expertadvies]

Antwoord:
Neen. Hierbij wij refereren wij aan de bovenstaande antwoorden op vraag 2 en 7. De Expertgroep heeft in haar advies ten onrechte als uitgangspunt het *uitgeven* van certificaten gehanteerd terwijl het moet gaan om het *gebruik* daarvan. Als uitgegaan wordt van het *gebruik* van certificaten als toepassingsgebied dan kan dit bijdragen aan een grotere leveranciersonafhankelijkheid. Afnemers kunnen dan immers kiezen uit meerdere commerciële aanbieders van PKIoverheid certificaten. Daarnaast constateert de Expertgroep zelf dat het *gebruik* van certificaten die allemaal volgens dezelfde manier zijn uitgegeven kan bijdragen aan interoperabiliteit – het vertrouwensniveau is immers gelijk.

M.b.t. de openheid van de standaard: BZK is bereid de suggestie van de Expertgroep, om een change advisory board op te richten, verder uit te werken. Deelnemers aan deze board kunnen dan bestaan uit de ministeries die thans al gebruik maken van PKIoverheid oplossingen (of dit in de zeer nabije toekomst gaan doen). Het betreft Defensie, VWS, VenW, Justitie en BZK zelf.

Vraag:
11. Bent u het eens met de nadere overwegingen van de expertgroep ten aanzien van het stimuleren van PKI binnen de overheid? Heeft u eventueel nadere suggesties of overwegingen? [paragraaf 4.3 van het expertadvies]

Antwoord:
Met name de marktpartijen maar ook de Policy Authority van PKIoverheid doen zelf al veel aan het stimuleren van PKIoverheid. Dit blijven zij ook doen. De wens van BZK is echter om de standaard meer afdwingbaar te laten zijn. Met het promoten c.q. stimuleren wordt het meer afdwingen van de standaard onvoldoende bereikt. Dit is naar de mening ban BZK wel het geval als de standaard op de pas toe of leg uit lijst wordt opgenomen.

Vraag:

12. Is/zijn er volgens u nog andere informatie of overwegingen omtrent PKIoverheid die aan het Forum en College Standaardisatie zou moeten worden meegegeven voor een besluit over het opnemen van PKIoverheid op de lijst met standaarden?

Antwoord:

In het advies van de Expertgroep wordt voorbijgegaan aan de doelstelling van het kabinet (http://www.ikregeer.nl/document/kst-28600-VII-7?format=pdf) met de PKI voor de overheid. Daaruit blijkt dat het met name gaat om het *gebruik* van PKIoverheid. Met de PKI voor de overheid is er namelijk één niveau van betrouwbaarheid (interoperabiliteit). Partijen kunnen zo op een eenduidige en gebruiksvriendelijke wijze met elkaar en met hun klanten communiceren. Hiermee wordt vermeden dat gebruik moet worden gemaakt van meerdere elektronische handtekeningen (de digitale sleutelbos).

Daarnaast wordt niet of heel summier ingegaan op PKI ontwikkelingen binnen Europa. Een klein onderzoekje geeft als resultaat dat de PKI van de overheid in Noorwegen en Denemarken wel verplicht is gesteld. In dat kader is het opnemen van het PvE van PKIoverheid op de Nederlandse pas toe of leg uit lijst, gezien de Europese ontwikkelingen, geen bijzonderheid.

Als laatste kan nog worden opgemerkt dat enkele ministeries, zoals Justitie, Defensie, VenW en VWS, PKIoverheid, met als onderliggende standaard het Propgramma van Eisen, al gebruiken in het kader van PKI oplossingen c.q. toepassingen.

Reactie Ministerie van BZK

Datum
21 september 2010

Van: Wierda, Hylke
Aan: Logius Forumstandaardisatie; Bart Knubben
CC: Raad, Hans de; Zeeuw, Erik van der; Goey, Michel de; Stolk, Nicole
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

PKIOverheid

Public Key Infrastructure biedt faciliteiten voor de digitale ondertekening van documenten/berichten die tussen verschillende partijen worden uitgewisseld.
De toepassing van dergelijke faciliteiten is zeer veel voorkomend, alle hedendaagse (netwerk)communicatiemiddelen (zoals webbrowsers en emailapplicaties) kunnen dergelijke certificaten afhandelen.

PKIOverheid is volgens haar eigen website:
"Een betrouwbare elektronische dienstverlening is pas mogelijk als vertrouwelijkheid, authenticatie en elektronische handtekeningen zijn gewaarborgd. Met een PKI zijn deze waarborgen goed te realiseren. PKIoverheid gaat nog een stapje verder."

De aan het Forum Standaardisatie voorgelegde elementen behelzen "het stapje extra", namelijk het raamwerk van normenkaders waarin de eisen beschreven staan waaraan een mogelijke verstrekker van PIKIOverheid cerficaten moet voldoen.

Het doel van de voordracht van deze normenkaders/Programma van Eisen lijkt te zijn de tot standaard verheffing van PKIOverheid certificaten voor de digitale ondertekening van documenten/berichten binnen het bereik van de Pas-Toe-Of-Leg-Uit Rijksinstructie.

Zie bijlage 2 voor de beantwoording van de door het Forum Standaardisatie gestelde vragen.

Bijlage 2: Beantwoording vragen PKIOverheid

Links:
Consultatiedocument
Expertadvies

1. Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig, bezien vanuit het doel van het document (het Forum en College Standaardisatie voorzien van een inhoudelijk relevante toelichting op PKIoverheid). [paragraaf 1.1 t/m 1.7 van het expertadvies].

    a. Nee
2. Bent u het eens met het door de expertgroep geadviseerde functionele toepassingsgebied van PKIoverheid? [paragraaf 2.1 van het expertadvies]
    a. Ja
3. Bent u het eens met het door de expertgroep geadviseerde organisatorische werkingsgebied van PKIoverheid? [paragraaf 2.2 van het expertadvies]
    a. Ja
4. Herkent u zich in de door de expertgroep gemaakte opmerking dat certificaten altijd op basis van de laatste versie van PKIoverheid moeten worden uitgegeven? [paragraaf 2.3 van het expertadvies]
    a. Ja
5. Bent u het eens met de conclusie van de expertgroep inzake de openheid van PKIoverheid? [paragraaf 3.1 van het expertadvies]
    a. Ja
6. Bent u het eens met de conclusie van de expertgroep inzake de bruikbaarheid van PKIoverheid? [paragraaf 3.2 van het expertadvies]
    a. Ja
7. Bent u het eens met de conclusie van de expertgroep inzake het potentieel van opname van PKIoverheid op de lijst met open standaarden? [paragraaf 3.3 van het expertadvies]
    a. Ja
8. Bent u het eens met de conclusie van de expertgroep inzake de impact van PKIoverheid? [paragraaf 3.4 van het expertadvies]
    a. Ja
9. Bent u het eens met de samenvatting van de overwegingen van de expertgroep? [paragraaf 4.1 van het expertadvies]
    a. Ja
10. Bent u het eens met het advies van de expertgroep aan het Forum en College Standaardisatie? [paragraaf 4.2 van het expertadvies]
    a. Ja
11. Bent u het eens met de nadere overwegingen van de expertgroep ten aanzien van het stimuleren van PKI binnen de overheid? Heeft u eventueel nadere suggesties of overwegingen? [paragraaf 4.3 van het expertadvies]
    a. Ja en nee
12. Is/zijn er volgens u nog andere informatie of overwegingen omtrent PKIoverheid die aan het Forum en College Standaardisatie zou moeten worden meegegeven voor een besluit over het opnemen van PKIoverheid op de lijst met standaarden?
    a. Nee

Reactie Ministerie van LNV

Datum
21 september 2010

Van: Rood, drs. P.H. (Pieter)

Aan: Bart Knubben; Logius Forumstandaardisatie
CC: Standaardisatie; Middeljans, F.K. (Karin); Braak, M.M.W. (Rinus); Tolido, E.C.P. (Edwin)
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

PKI-Overheid

1. Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig, bezien vanuit het doel van het document (het Forum en College standaardisatie voorzien van een inhoudelijk relevante toelichting op PKI-overheid). [paragraaf 1.1 t/m 1.7 van het expertadvies].

Pagina 7, voetnoot stelt:
Formeel: een geavanceerde handtekening, waarvan het certificaat een z.g.n. gekwalificeerd certificaat is. Het certificaat a) voldoet aan de eisen uit de Telecommunicatiewet en b) is gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen (bijv. een smartcard).

Dit is (technisch) niet correct. Het public / private keypair wordt gegenereerd op / door b.v. een smartcard, maar het certificaat zelf door de CSP.

2. Bent u het eens met het door de expertgroep geadviseerde functionele toepassingsgebied van PKIoverheid? [paragraaf 2.1 van het expertadvies]

Niet volledig. De beperking tot de uitgifte van certificaten i.p.v. het gebruik van certificaten is begrijpelijk maar lost tevens het probleem niet op. Indien niet eenduidig aangegeven kan worden wanneer welk soort certificaat gebruikt moet worden zijn eisen aan de uitgifte niet toepasbaar.

3. Bent u het eens met het door de expertgroep geadviseerde organisatorische werkingsgebied van PKIoverheid? [paragraaf 2.2 van het expertadvies]

Ja

4. Herkent u zich in de door de expertgroep gemaakte opmerking dat certificaten altijd op basis van de laatste versie van PKIoverheid moeten worden uitgegeven? [paragraaf 2.3 van het expertadvies]

Ja

5. Bent u het eens met de conclusie van de expertgroep inzake de openheid van PKIoverheid? [paragraaf 3.1 van het expertadvies]

Ja

6. Bent u het eens met de conclusie van de expertgroep inzake de bruikbaarheid van PKIoverheid? [paragraaf 3.2 van het expertadvies]

Het antwoord is ons inziens onvolledig omdat alleen het uitgifte proces en niet de bruikbaarheid van certificaten zelf in scope is.

7. Bent u het eens met de conclusie van de expertgroep inzake het potentieel van opname van PKIoverheid op de lijst met open standaarden? [paragraaf 3.3 van het expertadvies]

Ja

8. Bent u het eens met de conclusie van de expertgroep inzake de impact van PKIoverheid? [paragraaf 3.4 van het expertadvies]

Niet volledig eens. H 3.4.2. :
Brengt de toepassing van de standaard risico's met zich mee op het gebied van de informatievoorziening?
Er zijn geen specifieke technologische risico's verbonden aan het uitgeven van certificaten door middel van PKIoverheid.

Dit is ons inziens wel zo. Mogelijk b.v. issues voor ondersteuning SHA-2 bij legacy applicaties binnen of buiten LNV.

9. Bent u het eens met de samenvatting van de overwegingen van de expertgroep? [paragraaf 4.1 van het expertadvies]

Kleine aanvulling.

Er wordt gesteld:
De expertgroep heeft als toepassingsgebied gedefinieerd: "Het uitgeven van elektronische certificaten ten behoeve van een gekwalificeerde elektronische handtekening.".
Het is niet gezegd dat in alle gevallen een gekwalificeerde elektronische handtekening moet worden gebruikt. De wet specificeert niet welke toepassingen hier gebruik van moeten maken.

Bovenstaande ondergraaft het genoemde *potentieel*.

10. Bent u het eens met het advies van de expertgroep aan het Forum en College Standaardisatie? [paragraaf 4.2 van het expertadvies]

Ja

11. Bent u het eens met de nadere overwegingen van de expertgroep ten aanzien van het stimuleren van PKI binnen de overheid? Heeft u eventueel nadere suggesties of overwegingen? [paragraaf 4.3 van
het expertadvies]

Ja

12. Is/zijn er volgens u nog andere informatie of overwegingen omtrent PKIoverheid die aan het Forum en College Standaardisatie zou moeten worden meegegeven voor een besluit over het opnemen van
PKIoverheid op de lijst met standaarden?

Nee

Reactie Ministerie van Justitie

Datum
21 september 2010

Van: Groustra F.R. - BD/DI

Aan: Logius Forumstandaardisatie
Onderwerp: PKI-overheid

Beste Bart,

Justitie is het NIET eens met de opneming van PKI-overheid als een openstandaard PKI-Overheid heeft al van andere zijdes een verplichtend karakter: het is niet nodig om dit alsnog als openstandaard te bekrachtigen

Justitie is het voor een groot deel eens met het expertadvies met een andere conclusie: hoofdpunt blijft dat Justitie voorstander is van gebruik PKI overheid

Mvg

Roland Groustra
ICT-adviseur/EA-architect

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.

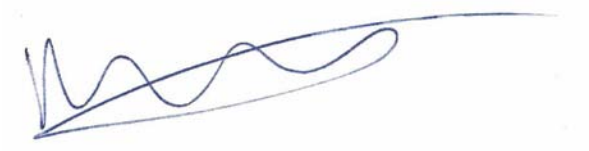
Ad c: SHA-2

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