FS-20101011.05B

Forum Standaardisatie

Wilhelmina v Pruisenweg 104
2595 AN Den Haag
Postbus 84011
2508 AA Den Haag
www.forumstandaardisatie.nl

notitie

FORUM STANDAARDISATIE
Concept COLLEGE NOTITIE

Agendapunt:	05 Lijst open standaarden		
Bijlagen:	Expertadvies + verzamelde reacties		
Aan:	College Standaardisatie		
Van:	Forum Standaardisatie		
Datum:	November 2010	**Versie**	0.2
Betreft:	Advies over opname PKIoverheid op lijst met open standaarden voor 'pas toe of leg uit'		

Waarom is een keuze belangrijk?
Het programma van eisen van PKIoverheid (PvE PKIoverheid) is een standaard op basis waarvan namens de Staat der Nederlanden digitale certificaten uitgegeven kunnen worden. Het sluit aan bij breed geaccepteerde, internationale standaarden. De certificaten kunnen gebruikt worden als elektronisch authenticatiemiddel door personen, bedrijven of autonome apparaten. Voorbeelden van dit gebruik zijn onder meer de elektronische identiteitskaart, taximeters, beveiliging van websites en beveiligde elektronische berichtenuitwisseling.

Het PvE PKIoverheid heeft alleen betrekking op de uitgifte van certificaten. Vier commerciële en twee publieke organisaties geven momenteel conform het PvE PKIoverheid certificaten uit. Het PvE PKIoverheid geeft dus geen richtlijnen aan overheidsorganisaties wanneer zij welke authenticatiemiddelen zouden moeten inzetten en draagt daarmee als zodanig onvoldoende bij aan de interoperabiliteit. Daarom dient het PvE PKIoverheid niet opgenomen te worden op de "pas toe of leg uit"-lijst. Om de interoperabiliteit van het stelsel van PKIoverheid te benutten is een kader noodzakelijk waarin staat wanneer overheidsorganisaties welk authenticatiemiddel dienen in te zetten in hun onderlinge berichtenverkeer en in hun berichtenverkeer met burgers en bedrijven. Dat kader kan worden aangemeld voor de "pas toe of leg uit"-lijst.

Kunt u met een gerust hart akkoord gaan met het voorgestelde advies?
Het voorliggende advies is het resultaat van een uitgebreid expertonderzoek, een publieke consultatie en bespreking in het Forum Standaardisatie. Van de 12 consultatiereacties onderschrijven er 11 grotendeels het expertadvies. De uitgebreide reactie van BZK / DRI bevat een andersluidende zienswijze.

Zijn er risico's verbonden aan de keuze?
Het niet opnemen van het PvE PKIoverheid kan worden gezien als een afwijzing van het stelsel en de organisatie PKIoverheid. Dat is geenszins het geval. Door zijn aard komt het PvE PKIoverheid als zodanig niet in aanmerking voor opname. Het beoogde, nog te ontwikkelen kader is mede bedoeld om ook PKIoverheid scherper te positioneren.

Doel

Datum
1 oktober 2010

Het College Standaardisatie wordt gevraagd in te stemmen met het volgende:

1. het Programma van Eisen van PKIoverheid (hierna: PvE PKIoverheid) niet op te nemen op de lijst met open standaarden voor 'pas toe of leg uit'.
2. te constateren dat het stelsel PKIoverheid wel kan bijdragen aan de interoperabiliteit. Daartoe moet voor de Nederlandse overheid een kader ontwikkeld worden waarin staat wanneer overheidsorganisaties welk authenticatiemiddel dienen in te zetten in hun onderlinge berichtenverkeer en in hun berichtenverkeer met burgers en bedrijven. Het beoogde kader zou onder andere eenduidig gedefinieerd de betrouwbaarheidsniveaus moeten bevatten, die zijn gekoppeld aan beschikbare authenticatiemiddelen (zoals commerciële PKI en PKIoverheid).
3. BZK op te roepen om een dergelijk kader te ontwikkelen en vervolgens aan te melden voor opname op de "pas toe of leg uit"-lijst.
4. Logius op te roepen om de gesignaleerde punten m.b.t. het beheer van PKIoverheid op te pakken.

Toelichting

Ad 1. Opname PvE PKIoverheid
Het PvE PKIoverheid heeft alleen betrekking op de uitgifte van certificaten. Het PvE PKIoverheid richt zich daarmee niet zozeer op overheidsorganisaties als gebruikers van PKI-certificaten, maar op partijen binnen en buiten de overheid die PKI-certificaten willen gaan uitgeven. Het PvE PKIoverheid geeft dus geen richtlijnen aan overheidsorganisaties wanneer zij welke authenticatiemiddelen zouden moeten inzetten en draagt daarmee als zodanig onvoldoende bij aan de interoperabiliteit.

Ad 2 en 3. Ontwikkeling kader authenticatiemiddelen
Het stelsel PKIoverheid is volwassen[1], wordt gebruikt door diverse overheidspartijen en is gebaseerd op breed geaccepteerde internationale standaarden voor PKI. Het stelsel PKIoverheid is een belangrijke bouwsteen van de elektronische vertrouwensinfrastructuur binnen de overheid. PKIoverheid waarborgt door zijn opzet leveranciersonafhankelijkheid. Meerdere commerciële en publieke organisaties geven certificaten uit conform PKIoverheid. PKIoverheid geeft uniforme eisen voor PKI, uitgaande van een hoog betrouwbaarheidsniveau.

Echter, de situaties waarvoor PKIoverheid het meest passende middel is, zijn niet eenduidig bepaald. Ook de verhouding van PKIoverheid tot andere authenticatiemiddelen is niet eenduidig vastgelegd. BZK zou als beleidsopdrachtgever van PKIoverheid hiervoor een kader moeten ontwikkelen. Dit kader kan een belangrijk bijdrage leveren aan de interoperabiliteit van authenticatiemiddelen en kan worden aangemeld voor de "pas toe of leg uit"-lijst.

Ad 4. Aandachtspunten beheer
Er is door de expertgroep en in de consultatie een aantal punten m.b.t. de openheid van het beheer gesignaleerd die verbeterd kunnen worden.

[1] *Het gaat hierbij om "Deel 3a: Overheid, Bedrijven en Organisaties"en "Deel 3b: Services. Met "Deel 3c: Burger"en "Deel 3d: Autonome apparaten" is op dit moment onvoldoende ervaring.*

Datum
1 oktober 2010

Waar gaat het inhoudelijk over?
Het 'Programma van Eisen PKIoverheid (deel 3a t/m 3d)' (hierna te noemen: PvE PKI Overheid) beschrijft aan welke eisen een uitgever van digitale certificaten moet voldoen om certificaten te mogen uitgeven namens de Staat der Nederlanden. Een deel van de eisen heeft betrekking op de inhoud van de certificaten, een deel heeft betrekking op de procedures voor uitgifte en het toezicht daarop.

PKI is een afkorting voor Public Key Infrastructure. Dit is een generiek concept (op basis van internationale standaarden) waarin door middel van digitale certificaten de identiteit van een persoon of systeem kan worden geverifieerd. Een dergelijk certificaat kan toegevoegd worden aan een breed scala van elektronische systemen, zoals een elektronische identiteitskaart, een website, een gegevensverwerkend systeem, etc.

Overheden en commerciële dienstverleners kunnen digitale certificaten uitgeven namens de Staat der Nederlanden indien het PvE PKIoverheid wordt gevolgd.

Met PKIoverheid uitgegeven certificaten voldoen aan de eisen die de Wet Elektronische Handtekening stelt aan een (zogeheten) *gekwalificeerd certificaat*. Indien een gekwalificeerd certificaat wordt gebruikt voor een elektronische handtekening, dan is deze handtekening daardoor rechtsgeldig. Het is echter ook mogelijk om met een gekwalificeerd certificaat dat niet namens de Staat der Nederlanden, maar namens een commerciële partij (zoals Verisign) is uitgegeven te voldoen aan de Wet Elektronische Handtekening.

Welke bezwaren zijn er tegen opname op de lijst?
Er zijn op dit moment onvoldoende handvatten om te kunnen vaststellen in welke situaties PKI of PKIoverheid moet worden toegepast als authenticatiemiddel. Verschillende partijen geven aan PKIoverheid een zwaar middel te vinden.

In verschillende gevallen voldoen commerciële PKI-certificaten. Veel overheidsorganisaties kiezen hiervoor, omdat dit vaak lagere kosten met zich meebrengt en het gebruik van PKIoverheid certificaten geen specifiek voordeel voor hen oplevert. In andere gevallen, zoals Digikoppeling, de Defensiepas en het Elektronisch Patiëntendossier, wordt juist bewust gekozen voor PKIoverheid vanwege de vereiste hoge betrouwbaarheidsniveaus.

Het vaststellen van een eenduidig functioneel toepassingsgebied aan de *gebruikerskant* (bijvoorbeeld: authenticatie op websites, elektronische identiteitskaarten, autonome apparaten, etc.) is voor de expertgroep niet mogelijk gebleken. Er zijn te weinig richtlijnen vanuit de wet of anderszins die eenduidig aangeven wanneer PKI vereist is en (meer specifiek) wanneer het hoge betrouwbaarheidsniveau van PKIoverheid noodzakelijk is.

Hierdoor kan enkel een functioneel toepassingsgebied worden gedefinieerd dat uitgaat van het verplichten van PKIoverheid voor het *uitgeven* van gekwalificeerde certificaten (*aanbiederskant*). Op basis hiervan is de standaard door de expertgroep beoordeeld tegen de vier criteria voor opname op de "pas toe of leg uit"-lijst.

De belangrijkste uitkomsten van de toetsing, uitgaande van het verplichten van PKIoverheid voor het *uitgeven* van certificaten, zijn als volgt:

- Openheid: De standaard is onvoldoende open. Het beheerproces geschiedt niet op basis van open besluitvorming (consensus of meerderheidsbesluitvorming).

Hoewel dit past bij de aard van PKIoverheid (hiërarchische vertrouwensrelatie Staat der Nederlanden), is dit wel vereist voor opname op de lijst.

- Bruikbaarheid: De standaard is goed bruikbaar voor het uitgeven van zogenaamde gekwalificeerde elektronische certificaten. Het door de Wet Elektronische Handtekening vereiste hoge betrouwbaarheidsniveau kan echter ook worden gerealiseerd door certificaten uit te geven die niet onder de Staat der Nederlanden vallen. Daarnaast is dit hoge betrouwbaarheidsniveau niet in alle gevallen noodzakelijk.

- Potentieel: Het potentieel van opname van PKIoverheid voor het uitgeven van certificaten op de lijst is nihil. Er zijn op dit moment ca. 6 partijen (4 commercieel en 2 publiek) die certificaten uitgeven namens de Staat der Nederlanden. De verwachting is dat hier in de komende jaren nog 2 of 3 partijen bijkomen. Deze groei wordt niet of nauwelijks beïnvloed door opname van de standaard op de lijst. Aan de gebruikerszijde lijkt de adoptie wel bevorderd te kunnen worden, zo vloeit voort uit de nadere overwegingen van de expertgroep.

- Impact: Er is geen specifieke positieve of negatieve impact te verwachten indien de standaard wordt opgenomen op de lijst.

Op basis van het voorgaande is de expertgroep tot de conclusie gekomen om PKIoverheid niet op te nemen op de lijst met open standaarden voor "pas toe of leg uit".

Aanvullende mogelijkheden?

Het belang van PKI en PKIoverheid moet worden onderkend. In het rapport van de expertgroep worden twee alternatieve mogelijkheden genoemd om het gebruik van PKI en PKIoverheid te stimuleren:

- Door het eenduidig vastleggen van betrouwbaarheidsniveaus en het koppelen hiervan aan authenticatiemiddelen

  Als het mogelijk is om eenduidig bepaalde betrouwbaarheidsniveaus te definiëren dan zou per betrouwbaarheidsniveau bepaald kunnen worden welk (of welke) authenticatiemiddelen gebruikt moeten worden. Helaas zijn deze betrouwbaarheidsniveaus nog onvoldoende scherp gedefinieerd. Wel wordt hier in Europees verband (STORK) aan gewerkt. Binnen Nederland wordt o.a. in het programma eHerkenning gewerkt aan authenticatiemiddelen voor verschillende toepassingen. Binnen het Forum Standaardisatie is dit ook een terugkerend onderwerp.

- Door het verplichten van PKIoverheid voor individuele voorzieningen

  Voor een aantal ICT-voorzieningen moet verplicht gebruik gemaakt worden van elektronische certificaten volgens het PvE PKIoverheid. Een voorbeeld hiervan is Digikoppeling (standaard voor gegevensuitwisseling tussen overheden). Het is een optie om voor meer toepassingen het gebruik van PKIoverheid te verplichten. Dit zou dan per toepassing bekeken moeten worden.

Deze mogelijkheden zijn ook voorgelegd in de consultatieronde.

Schets van de expertgroep en de consultatie
De expertgroep bestond uit 15 personen uit wetenschap, overheid, adviesbureaus en uitgevers van certificaten. De indiener maakte deel uit van de expertgroep. Het advies van de expertgroep is vervolgens gepubliceerd ten behoeve van de publieke consultatie.

Er zijn in totaal 12 reacties ontvangen in de consultatieperiode op het expertadvies. 11 respondenten geven aan het geheel of grotendeels eens te zijn met het expertadvies en onderschrijven het advies PKIoverheid nu niet op te nemen. Dit betreft het Ministerie van Binnenlandse Zaken & Koninkrijksrelaties (CIO-office, directie PRIO), Ministerie van Onderwijs, Cultuur & Wetenschappen, Ministerie van Justitie, Ministerie van Landbouw Natuurbeheer & Voedselkwaliteit, Ministerie van Volksgezondheid, Welzijn & Sport, Ministerie van Financiën (DG Belastingdienst), Ministerie van Financiën (Bedrijfsvoering/ICT), Gemeente Enschede (mede namens het Overleg Open Gemeenten), Kadaster, Inspectie Verkeer & Waterstaat, InformatieDesk Standaarden Water (mede namens Het Waterschapshuis).

Op een aantal punten zijn door deze respondenten specifieke opmerkingen gemaakt:
- Het ministerie van Justitie is voorstander van het gebruik van PKIoverheid, maar is het niet eens met de opname hiervan op de lijst omdat PKIoverheid "al van andere zijdes een verplichtend karakter" heeft.
- De Kamer van Koophandel is het niet eens met het enkelvoudig stimuleren van PKIoverheid. Er zou beter gekeken moeten worden naar de achterliggende nut en noodzaak (vanuit wettelijk kaders en de praktijk) en vervolgens geanalyseerd moeten worden hoe en welke standaarden gebruikt zouden moeten worden. Het definiëren van betrouwbaarheidsniveaus kan daar een middel bij zijn. Vervolgens zou e.e.a. in samenhang bekeken moeten worden.
- De InformatieDesk Standaarden Water en het Ministerie van Economische Zaken wijzen op de eventuele marktverstoring die verplichte opname van PKIoverheid zou kunnen betekenen.
- IDsW ziet wel graag stimuleringsmaatregelen voor de toepassing van PKIoverheid. En nadere definitie van het werkingsgebied (bijv. basisregistraties) kan volgens IDsW veel onduidelijkheid wegnemen.
- Het Ministerie van Economische Zaken wijst ook op het stelsel eHerkenning. Op niveau 4 (het hoogste betrouwbaarheidsniveau) moet PKI worden toegepast. Niet-PKIoverheid-toepassingen (d.w.z. commerciële PKI-certificaten) kunnen volgens hen ook aan dat niveau voldoen.
- Het Kadaster vindt dat een aantal internationale aspecten nader moet worden belicht. Het advies geeft volgens hen onvoldoende weer in hoeverre PKIoverheid internationale overheidsdienstverlening bevordert of wellicht belemmert. Daarnaast vindt men dat PKIoverheid certificaten niet verplicht opgelegd moeten worden. Men wijst op de Kadasterwet waarin private partijen de vrijheid worden gegeven zelf voor hun bedrijfsvoering optimale oplossingen te kiezen.
- Het Ministerie van Financiën (DG-Belastingdienst) wijst op de problemen die bij migratie naar andere (nieuwere) versies of andere certificaten kunnen ontstaan. Het zou wenselijk zijn dat daar een vorm van ondersteuning voor zou komen.

Deze opmerkingen zijn in hoofdzaak aanvullend op het expertadvies. Wel geeft een aantal organisaties aan dat het vooral gewenst is om te kijken naar stimulering van elektronische authenticatie in de breedte en niet specifiek gericht op PKIoverheid.

Eén respondent geeft aan zich niet volledig te kunnen vinden in het expertadvies. Dit betreft het Ministerie van Binnenlandse Zaken & Koninkrijksrelaties (Dienstverlening, Regeldruk en Informatiebeleid; DRI). BZK (DRI) is opdrachtgever van PKIoverheid.

- BZK (DRI) stelt dat wel degelijk een toepassingsgebied gekozen kan worden dat uitgaat van het *gebruik* van PKIoverheid. Men stelt voor als toepassingsgebied te kiezen *"het gebruiken van PKI oplossingen bij nieuwbouw, verbouw of contractverlenging"*. Dit zou betekenen dat bij iedere toepassing van PKI binnen de overheid, gebruik gemaakt zou moeten worden van certificaten op basis van PKIoverheid.

  De expertgroep geeft in het advies aan dat het gebruik van PKIoverheid door de overheid (als 'eigen' ontwikkeling) weliswaar voor de hand ligt, maar dat:
  - Niet altijd de 'zware' vorm van PKI van PKIoverheid noodzakelijk is; dit leidt in een aantal gevallen tot onnodige extra inspanningen en kosten;
  - De wettelijke vereisten op het gebied van de gekwalificeerde handtekening ook met niet-PKIoverheid certificaten ingevuld kunnen worden en de Wet Elektronische Handtekening deze mogelijkheid zelfs expliciet biedt.

  Dit wordt onderschreven door de andere partijen in de consultatie.

- In het advies wordt gesteld dat - zo mogelijk - altijd de laatste versie van PKIoverheid op de lijst opgenomen zou moeten worden. BZK (DRI) is het hier niet mee eens. Men vindt het niet noodzakelijk elke nieuwe versie voor te leggen aan het Forum Standaardisatie.

  Hoewel er begrip op te brengen is voor deze positie hangt dit feit samen met de beheerprocedure voor de lijst en niet met PKIoverheid. Wel hoeft niet in alle gevallen bij een nieuwe versie de gehele toetsingsprocedure te worden doorlopen (in de praktijk zal vaak een melding volstaan).

- BZK (DRI) stelt voor een nieuwe *change advisory board* op te richten, waarin (bijvoorbeeld) ministeries die gebruik maken van PKIoverheid zitting kunnen nemen. Hiermee zou volgens BKZ (DRI) tegemoet gekomen kunnen worden aan de huidige gesignaleerde aandachtspunten op het gebied van beheer/openheid.

- Ten aanzien van de eventuele alternatieven om PKI en PKIoverheid te stimuleren geeft BZK (DRI) aan vooral te zoeken naar methoden met een afdwingbaar karakter. De lijst voor open standaarden zou volgens hen dan een geschikte methode zijn. Adoptiemiddelen op het gebied van promotie en stimulering zouden tot nu toe onvoldoende effect sorteren.

- Tenslotte geeft men nog een aantal nadere overwegingen:
  - Het advies zou voorbijgaan aan de doelstellingen van het kabinet op het gebied van PKI. Hierbij verwijst men naar een brief van de Minister van BZK aan de Kamer uit 2003, waarin de minister aangeeft te willen toewerken naar een uitrol van PKI binnen de overheid en waarin hij het gebruik tot dan toe evalueert.

    Het advies doet hier echter niets aan af. Sterker nog: het advies geeft aan duidelijk een rol te zien voor PKI en PKIoverheid. De overheid kiest voor een groot aantal toepassingen (Defensiepas, EPD, etc.) specifiek voor

PKIoverheid. Dit laat echter onverlet dat er ook situaties kunnen zijn waarvoor dit een te zwaar middel is. In het programma eHerkenning (onderdeel van de strategische ICT agenda 2008-2011) wordt dan ook nadrukkelijk gekeken naar verschillende authenticatiemiddelen in verschillende situaties.

- BZK (DRI) wijst op ontwikkelingen in Noorwegen en Denemarken waar de overheid PKI verplicht heeft gesteld.

  In het advies is inderdaad vooral ingegaan op de Nederlandse situatie. Hierbij geldt dat in Nederland 'pas toe of leg uit' primair een inkoopmiddel is. In veel andere landen worden ICT standaarden echter per wet afgedwongen.

  Een vergelijkbare situatie, waarbij in Nederland via een regeling afgedwongen wordt welke authenticatiemiddelen verplicht zijn in bepaalde situaties is voorstelbaar. Zo definieert eHerkenning bijvoorbeeld 4 niveaus van zeer lage tot zeer hoge betrouwbaarheid (in dat laatste geval stelt eHerkenning PKI verplicht). Er zou in een richtlijn mogelijk bindend vastgelegd kunnen worden welk niveau in welke situatie moet worden toegepast (met andere woorden: wanneer is een zeer hoge betrouwbaarheid benodigd?).

- BZK (DRI) wijst op het feit dat de ministeries van Justitie, Defensie, Verkeer en Waterstaat en Volksgezondheid, Welzijn en Sport al gebruik maken van PKIoverheid toepassingen.

  Deze organisaties waren allen vertegenwoordigd in de expertgroep en/of hebben gereageerd in de consultatieronde.

Communicatie
Het Forum Standaardisatie zal via haar website communiceren over het besluit.