Forum Standaardisatie

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

notitie

FORUM STANDAARDISATIE FS32-06-04

Agendapunt:	04 Authenticatie & autorisatie - betrouwbaarheidsniveaus		
Bijlagen:	Handreiking + achtergrondinformatie		
Aan:	Forum Standaardisatie		
Van:	BFS		
Datum:	mei 2011	**Versie**	0.3
Betreft:	Handreiking betrouwbaarheidsniveaus		

1. Gevraagde beslissing

a. Instemmen met de handreiking Classificatie van overheidsdiensten en bepaling van het daarvoor vereiste betrouwbaarheidsniveau;
b. Vaststellen dat deze handreiking een voldoende basis biedt voor het bepalen van het toepassingsgebied van het Programma van Eisen PKIoverheid.
c. Besluiten dat deze handreiking de weg vrijmaakt voor het op de pas toe of leg uit-lijst zetten van het PvE PKIoverheid.

2. Toelichting

Aanleiding
Door de overheid gebruikte authenticatiemiddelen kennen verschillende graden van betrouwbaarheid. Die varieert van laag (gebruikersnaam-wachtwoord) via DigiD basis (idem maar met verificatie van de identiteit van de aanvrager) en DigiD midden (met sms authenticatie) naar hoog (PKIoverheid).
Voor overheidsdienstverleners is vaak niet helder welk betrouwbaarheidsniveau voor hun dienst het meest geëigend is. Deze onduidelijkheid maakte dat het Forum Standaardisatie in oktober 2010 adviseerde het Programma van Eisen (PvE) PKIoverheid niet op te nemen op de lijst met open standaarden.

In termen van het Forumadvies: "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."

Om het stelsel van PKIoverheid optimaal te benutten achtte het Forum een kader noodzakelijk op basis waarvan kan worden bepaald welk authenticatiemiddel overheidsorganisaties moeten inzetten in hun onderlinge berichtenverkeer en in hun berichtenverkeer met burgers en bedrijven.

Naar aanleiding van de discussie in de Forumvergadering hebben Logius en het programma eHerkenning in samenwerking met verschillende uitvoerings-organisaties[1] die elektronische diensten verlenen, bijgaande handreiking voor het classificeren van diensten en de daarbij behorende betrouwbaarheidsniveaus opgesteld. De handreiking stelt overheidsdienstverleners in staat om te bepalen welk betrouwbaarheidsniveau voor hun diensten nodig is, zodat zij hun klanten gericht kunnen informeren welk betrouwbaarheidsniveau's de door hen aan te schaffen middelen moeten hebben om deze diensten af te nemen.

In de bijlage bij deze notitie wordt een aantal aspecten van de handreiking toegelicht.

Aard van de handreiking en relatie tot (open) standaarden
In het eerdere Forumadvies over PKIoverheid werd BZK opgeroepen om het te ontwikkelen kader voor bepaling van betrouwbaarheidsniveaus aan te melden voor opname op de pas toe of leg uit-lijst.

Geconstateerd moet echter worden dat de handreiking geen standaard is, in elk geval niet van het type dat zich laat toepassen bij de inkoop van ICT-producten en – diensten (waar het pas toe of leg uit beginsel op ziet). De handreiking is een hulpmiddel bij de toepassing van wat elders gestandaardiseerd is. Voorbeelden: het PKIoverheid-stelsel, het afsprakenstelsel eHerkenning, een generieke authenticatievoorziening als DigiD.[2]

De handreiking maakt het echter juist nodig om standaarden op het gebied van identificatie en authenticatie op de pas toe of leg uit-lijst op te nemen. Zonder die standaarden is het realiseren en implementeren van (op open standaarden gebaseerde) identificatie- en authenticatievoorzieningen op het vereiste betrouwbaarheidsniveau in e-overheidsdiensten niet mogelijk. Bovendien kunnen overheidsdienstverleners en hun klanten zonder die standaarden geen heldere keuze maken voor een bepaald betrouwbaarheidsniveau.

Discussiepunt
Gelet op het voorgaande zou het voor de hand liggen dat Logius het PvE PKIoverheid opnieuw aanmeldt bij het Forum, met een indicatie (op basis van de handreiking) van het toepassingsgebied. Na beoordeling van dit deelaspect (een hernieuwde integrale beoordeling lijkt niet nodig) zou het PvE op basis van een aanvullend Forumadvies op de lijst kunnen worden geplaatst.

De handreiking en een procedurevoorstel in deze zin zijn ter voorbereiding van de Forumvergadering voorgelegd aan de stuurgroep Open standaarden. Daarbij bleek dat de stuurgroep van mening was dat PKIoverheid zich q.q. niet leent voor opname op de lijst en dat alleen een gebruikskader (de handreiking) daarvoor in aanmerking zou komen. Langs deze lijn heeft het Forum in de visie van de stuurgroep eerder ook besloten.

---

[1] Belastingdienst, KvK, AgentschapNL, IND, Dienst Regelingen, Gemeente Amsterdam, Ministeries van BZK, EL&I en I&M. Voorts is er contact geweest met en gebruik gemaak van inbreng van SZW, RDW en IPO/Provincie Utrecht.
[2] De situatie ten aanzien van DigiD ligt uiteraard iets anders dan ten aanzien van PKI en eHerkenning. Hiervoor zou opname op een basisvoorzieningenlijst mogelijk ook uitkomst bieden.

De betrokkenen bij de opstelling van de handreiking hebben echter een ander beeld van het besluit dat het Forum in oktober 2010 over het PvE PKIoverheid nam en over de gewenste vervolgacties. Het Forum wordt daarom gevraagd – gezien de handreiking en de hierboven gegeven toelichting over de aard hiervan – zich uit te spreken over de gewenste koers voor PKIoverheid wat betreft het aspect van het toepassingsgebied van deze standaard.

Het Forum plaatste destijds overigens nog twee kanttekeningen bij opneming van het PvE PKI overheid op de lijst, namelijk de mogelijk marktverstorende werking van verplichtstelling van PKIoverheid (dat private PKI's hun positie in de markt voor overheidsdiensten zou ontnemen en daarom ook op Europeesrechtelijke bezwaren zou stuiten) en het feit opneming geen echt toegevoegde waarde heeft voor gebruik van PKIoverheid (er zijn nu vier leveranciers, dat zouden er op zijn best zes worden).

Wat betreft het punt over mogelijke marktverstoring: het lijkt aangewezen dat naar aanleiding van de mededingingsrechtelijke analyse die EL&I heeft gemaakt over het op de pas toe of leg uit lijst plaatsen van het PvE PKIoverheid overleg plaatsvindt tussen EL&I en BZK en dat daarbij de juridische analyses worden betrokken die waarschijnlijk bij ontwikkeling van het PKIoverheidstelsel over dit aspect zijn gemaakt.

Wat betreft het tweede punt geldt dat het aannemelijk lijkt dat de komende jaren een flinke groei zal ontstaan in de vraag naar PKIoverheidcertificaten. Dit niet alleen in het verlengde van de verplichtingstelling van SBR als enige kanaal voor Vpb- en IB-aangiftes van ondernemers, maar ook vanwege ontwikkelingen in de B2B-omgeving. Als ondernemers eenmaal elektronisch zaken doen met de overheid, hoeven ze niet meer te investeren in de infrastructuur, de protocollen, het certificaat etc. Dat verlaagt de drempel voor elektronische diensten in het B2B-domein verlaagt.

In het licht van eventuele nadere besluitvorming over PKIoverheid in het Forum (naar aanleiding van de in het voorgaande gevraagde positiebepaling) zal een nadere analyse van deze punten gemaakt worden.

Bijlage: achtergrondinformatie over de handreiking

Onderstaand wordt nader ingegaan op de scope, wijze van gebruik en beheer en doorontwikkeling van de handreiking.

Scope
De handreiking ziet op e-diensten van de overheid aan burgers en bedrijven, die deze afnemen via internet. Het gaat dus primair om diensten die via een online portaal worden aangeboden, of waarbij de afnemer in een lokale applicatie handelingen verricht en de uitkomst daarvan aan de overheidsorganisaties toestuurt (bv. de elektronische belastingaangifte voor particulieren). De scope is vooralsnog beperkt tot degene die een dienst voor zichzelf afneemt. Ik zou dit niet vooralsnog noemen. Het gaat steeds om de betrouwbaarheid van de identificatie (door een authenticatieproces), machtigingen staan daar los van. Het hier weer opnemen als beperking (die het niet is) leidt weer tot onnodige discussie.
Ook processen waarbij machine-machine communicatie plaatsvindt zijn nog niet meegenomen in de handreiking. Aangeven dat we dat nog wel gaan doen!
Dit geldt tot slot ook voor verkeer tussen overheidsorganisaties onderling (bijvoorbeeld het raadplegen van basisregistraties, het uitwisselen van informatie die nodig is voor het beoordelen van een vergunningaanvraag). Dit is het domein dat (in elk geval waar het de ministeries en daaronder direct ressorterende diensten betreft) wordt bestreken door het Besluit voorschrift informatiebeveiliging rijksdienst (VIR), en voor decentrale overheden door standaarden als ISO27002, NEN7510 en wettelijke bepalingen in het kader van de Wet GBA en Wbp. Staan die dan gebruik van de handreiking in de weg? Volgens mij niet….
De administratieve organisatie en interne controle en het beveiligingsbeleid van de overheidsorganisaties moeten op basis van die regels in de nodige waarborgen voor de betrouwbaarheid en vertrouwelijkheid van gegevensstromen voorzien, onder meer door verlening van autorisaties binnen de organisatie en voorzieningen voor het traceren van handelingen in een beslisproces. Op dit vlak wordt op dit moment ook door DGOBR beleid ontwikkeld (fysieke en logische toegang).
Met deze handreiking wordt ten aanzien van dienstverlening door de overheid aan burgers en bedrijven tegemoetgekomen aan de door het Forum in relatie tot het PvE PKIoverheid gesignaleerde gebrek. De handreiking classificeert de overheidsdiensten waarvoor het hoogste betrouwbaarheidsniveau aangewezen is. Overigens zal de handreiking worden doorontwikkeld voor de andere genoemde situaties.

Wijze van totstandkoming, gebruik en beheer/doorontwikkeling
De handreiking is een product van nauwe samenwerking tussen gebruikers (aanbieders van overheidsdiensten) en beleid. Hij is tot stand gekomen in een aantal intensieve bijeenkomsten met gebruikers, voorgezeten door Cor Franke (lid van het Forum en tevens voorzitter van het Launching Customer Overleg in eHerkenning).
De handreiking stelt overheidsorganisaties in staat om eenduidig betrouwbaarheidsniveaus vast te stellen, met volledig behoud van hun eigen verantwoordelijkheid daarvoor. Het ligt in de rede dat overheidsorganisaties de handreiking verankeren in hun uitvoeringsbeleid rond elektronische dienstverlening aan burgers en bedrijven.
Logius zal het beheer en de doorontwikkeling van de handreiking blijven faciliteren. Daartoe wordt beoogd de huidige gebruikersgroep uit te bouwen tot een community, waar ervaringen met gebruik van de handreiking en ontwikkelingen op het vlak van e-dienstverlening gedeeld kunnen worden en waar nodig verwerkt worden in de handreiking.