

**Forum Standaardisatie**

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

notitie

COLLEGE STANDAARDISATIE Concept

Agendapunt:	04		
Bijlagen:	-		
Aan:	College Standaardisatie		
Van:	Forum Standaardisatie		
Datum:	april 2010	Versie	
Betreft:	5) resultaten intake PKIoverheid		

Advies

U wordt gevraagd in te stemmen met het volgende advies:

- De ingediende delen van het Programma van Eisen (PvE) van PKIoverheid worden niet verder in behandeling genomen, omdat dit grotendeels geen betrekking heeft op informatie-uitwisseling
- Met de aanmelder wordt nader bekeken of onderdelen van het PvE zijn te isoleren die wel in aanmerking komen voor opname, en daarnaast of achterliggende internationale standaarden in aanmerking komen voor opname.

Toelichting

Inleiding

Na een vooroverleg met PKIoverheid¹ (onderdeel van Logius) op 15 december 2009, is op 29 december 2009 een deel van het Programma van Eisen (PvE) van PKIoverheid aangemeld voor opname op de lijst met open standaarden voor 'pas toe of leg uit'. Ingediend zijn de volgende delen:

- deel 3a Certificate Policy - Domeinen Overheid/Bedrijven en Organisatie
- deel 3b Certificate Policy - Services Bijlage bij CP Domeinen Overheid/Bedrijven en Organisatie
- deel 3c Certificate Policy - Domein Burger
- deel 3d Certificate Policy - Domein Autonome Apparaten

Naast bovengenoemde delen bevat het PvE de volgende delen (die niet ingediend zijn voor opname op de lijst):

¹ Voluit: Public Key Infrastructure voor de overheid.

- deel 1: Introductie
- deel 2: Toetreding tot en toezicht binnen de PKI voor de overheid,
- deel 4: Definities en Afkortingen

Deze memo beschrijft de resultaten van de intake.

Achtergrond

Het Programma van Eisen (PvE) van PKIoverheid deel 3a t/m deel 3d is een normenstelsel, dat generiek en grootschalig gebruik van de elektronische handtekening, identificatie op afstand en vertrouwelijke communicatie mogelijk maakt tussen overheid en overheid, overheid en bedrijven en overheid en burgers. Voor deze communicatie wordt gebruik gemaakt van Public Key Infrastructure (PKI).

Het PvE beschrijft aan welke eisen een organisatie dient te voldoen als deze wil optreden als Certificate Service provider. De delen 3a t/m 3d zijn met name gebaseerd op internationale standaarden van ETSI en IETF.

Toelichting advies

Om te bepalen of het PvE in aanmerking komt voor opname op één van de lijsten, is het getoetst aan de uitsluitingcriteria. Per criterium zal hieronder beschreven worden hoe PKIoverheid hierop scoort.

- Eenmalige opname
Aan deze eis wordt voldaan, PKIoverheid staat niet de lijst met open standaarden voor 'pas toe of leg uit', en ook niet op de lijst met gangbare open standaarden.
- Betrekking op informatie-uitwisseling
Aan deze eis wordt niet voldaan (dat wil zeggen, het PvE PKIoverheid gaat grotendeels niet over informatie-uitwisseling). De ingediende delen van het PvE gaan grotendeels over eisen die aan een organisatie gesteld worden. Veel van de eisen hebben namelijk betrekking op de inrichting van de Certificate Service Provider en procedures die hij moet hanteren. Er staan wel een paar eisen in die betrekking hebben op informatie-uitwisseling tussen organisaties, maar dit is slechts beperkt. Daarnaast bevat het PvE een aantal referenties naar internationale standaarden die wel primair op informatie-uitwisseling tussen organisaties betrekking lijken te hebben.
- Geen beperkt werkingsgebied
Aan deze eis wordt voldoende voldaan. Het PvE is over het algemeen redelijk generiek in te zetten. Wel worden in deel 2 (dat niet ingediend is voor opname op de lijst) veel rollen expliciet toegewezen aan partijen (zoals de Raad v/d Accreditatie, eigenaar van het root certificaat, etc). Voor de ingediende delen is dit veel beperkter het geval. In deel 3b worden nog wel een aantal partijen genoemd, zoals PKIoverheid en het ministerie van BZK, maar dit hoeft niet perse een belemmering te zijn om de standaard in procedure te nemen. Strikt genomen is het feit dat deze partijen bij naam genoemd worden strijdig met het uitgangspunt dat een standaard niet organisatie- of implementatiespecifiek mag zijn, maar het PvE is wel generiek opgezet voor de Nederlandse overheid. Onduidelijk is of er mogelijk belemmeringen gaan ontstaan bij internationale gegevens-uitwisseling.

- Wettelijk verplicht
Het PvE wordt niet vastgelegd in wet- of regelgeving. Op basis van dit criterium kan het PvE dus niet worden uitgesloten van opname op de lijsten met open standaarden.

Samenvattend wordt geconcludeerd dat het PvE als zodanig niet in aanmerking komt om in procedure te nemen, aangezien dit slechts in beperkte mate over informatie-uitwisseling gaat. Wel bevat het PvE onderdelen en referenties naar standaarden die wel in aanmerking zouden kunnen komen voor opname.