FS-20101011.05B

Forum Standaardisatie

Expertadvies
PvE PKIoverheid deel 3a t/m 3d, versie 2.1

Datum 6 augustus 2010
Definitief

FS-20101011.05B

Colofon

Projectnaam	Expertadvies Programma van Eisen PKIoverheid, deel 3a t/m 3d, versie 2.1
Versienummer	1.0
Locatie	-

Organisatie	Logius Postbus 84011 2508 AA Den Haag forumstandaardisatie@logius.nl

Bijlage(n)

Auteurs	dr. J.H. Hoepman ir. L.M. Punter

FS-20101011.05B

Inhoud

Managementsamenvatting

Dit document omvat het advies van de expertgroep PKIoverheid. De expertgroep is gevraagd te toetsen in hoeverre het Pakket van Eisen PKIoverheid (deel 3a t/m 3d) voldoet aan de criteria voor de lijst met open standaarden voor het 'pas toe of leg uit' principe. Ook is de expertgroep gevraagd een uitspraak te doen over het eventuele functionele toepassingsgebied en organisatorische werkingsgebied van de standaard.

De expertgroep heeft als toepassings- en werkingsgebied vastgesteld: "*Het uitgeven van elektronische certificaten ten behoeve van een gekwalificeerde elektronische handtekening*" door "*Overheden en instellingen in de (semi-)publieke sector*".

Daarbij wordt dus uitgegaan van het *uitgeven* van certificaten en niet van het *gebruik* daarvan. De belangrijkste overwegingen hierbij zijn:

- Er zijn naar mening van de expertgroep op dit moment onvoldoende handvatten om een (voor "pas toe of leg uit") duidelijk toepassingsgebied af te bakenen m.b.t. het gebruik van een gekwalificeerde elektronische handtekening.
- Het verplichten van het gebruik van PKIoverheid-certificaten voor een gekwalificeerde handtekening zou een aanscherping van de wet betekenen. Deze aanscherping zou het gebruik van certificaten van andere (bij de OPTA geregistreerde) partijen voor die toepassing onmogelijk maken, terwijl de wet deze mogelijkheid duidelijk biedt.

Met betrekking tot de toetsingscriteria constateert de expertgroep de volgende zaken:

- *Openheid*: de standaard is op dit moment onvoldoende open. Er is geen sprake van een open besluitvormingsprocedure op basis van consensus of meerderheidsbesluitvorming. Daarnaast is (hoewel er in de praktijk geen beperkingen worden ervaren) onvoldoende vast komen te staan dat het (onderliggende) intellectueel eigendom onherroepelijk en royalty-free beschikbaar is gesteld.
- *Bruikbaarheid*: de standaard is goed bruikbaar voor het implementeren van een gekwalificeerde elektronische handtekening. De ervaring met de deelstandaard voor burger-certificaten is nog beperkt, dit deel (3c) zou dan ook uitgezonderd moeten worden. De expertgroep stelt dat niet in alle gevallen een gekwalificeerde handtekening nodig is, ook lichtere vormen zijn mogelijk. Daarvoor komen ook andere vormen van PKI in aanmerking. Een gekwalificeerde elektronische handtekening is wettelijk bovendien mogelijk met een commercieel beschikbaar certificaat.

- *Potentieel*: de opname van PKIoverheid op de lijst met open standaarden zou naar mening van de expertgroep met het gedefinieerde toepassingsgebied onvoldoende bijdragen aan de doelen van de lijst. Dit laat onverlet dat PKIoverheid wel degelijk kan bijdragen aan het realiseren van een digitale vertrouwensinfrastructuur binnen de overheid. Hoewel vanuit dat oogpunt het stimuleren van PKIoverheid gewenst kan zijn, zou dit beter op andere manieren dan via de lijst met open standaarden gedaan kunnen worden.
- *Impact*: er zijn geen specifieke voordelen of risico's verbonden aan opname van PKIoverheid op de lijst met open standaarden.

Op basis van deze constateringen adviseert de expertgroep PKIoverheid niet op te nemen op de lijst met open standaarden voor 'pas toe of leg uit', maar te zoeken naar andere manieren waarop PKI in het algemeen en PKIoverheid in het bijzonder gestimuleerd kunnen worden.

1 Doelstelling expertadvies

1.1 Achtergrond

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 standaard 'PKIoverheid' is aangemeld voor deze procedure.

In opdracht van het Forum Standaardisatie zijn daarom experts gevraagd deel te nemen aan een expertgroep, om de standaard te beoordelen aan de hand van een aantal criteria. Deze criteria - en de uitwerking ervan in de vorm van concrete vragen - worden in het hier voorliggende expertadvies genoemd en behandeld en zijn overgenomen uit het op 14 mei 2008 door het College Standaardisatie geaccordeerde rapport "Open standaarden: het proces om te komen tot een lijst met open standaarden", te vinden op de website van het Forum Standaardisatie.

De expertgroep is gevraagd om – op basis van een beoordeling aan de hand van de genoemde criteria – te adviseren over het wel of niet opnemen van PKIoverheid op de lijst met open standaarden, al dan niet onder bepaalde voorwaarden.

1.2 De standaard PKIoverheid

1.2.1 Public Key Infrastructure

Het is niet gemakkelijk om bij digitale communicatie de betrouwbaarheid van de verzonden en ontvangen gegevens te kunnen waarborgen. Het netwerk tussen verzender en ontvanger bevat immers veel schakels, waar gegevens potentieel gemanipuleerd kunnen worden. Bovendien is het moeilijk te controleren of de afzender daadwerkelijk degene is die hij/zij stelt te zijn.

Eén van de mogelijke oplossingen voor deze problematiek is de inrichting van een zogenaamde Public Key Infrastructure (PKI). In een dergelijke infrastructuur kan door middel van certificaten de betrouwbaarheid van de uitgewisselde gegevens worden vastgesteld. Een dergelijk certificaat kan bijvoorbeeld geïnstalleerd worden op een webserver, in een e-mailclient, op een chipkaart of in een losstaand apparaat (bijvoorbeeld een taximeter die periodiek uitgelezen wordt).

PKI is gebaseerd op een stelsel van internationaal geldende afspraken over de inhoud en het gebruik van dergelijke certificaten en het bijbehorende proces van uitgifte en controle. In hoofdlijnen definiëren deze afspraken de volgende zaken:

- Autoriteit wordt vastgesteld op basis van hiërarchische vertrouwensrelaties. Er is dus altijd een hoofdpartij die vertrouwd wordt. Dit wordt een root *certificate authority* genoemd. Daaronder kunnen zich weer meerdere *certificate authorities* bevinden.
- Via een vastgesteld proces kan een certificate authority (CA) certificaten uitreiken aan eindgebruikers. Er zijn meerdere mogelijkheden waarop dit proces vormgegeven kan worden. Afhankelijk van de inrichting van het proces (bijvoorbeeld: volledig geautoriseerd of door tussenkomst van een notaris) kan het certificaat meer of minder zekerheid bieden. De CA bepaalt de inhoud en de maximale geldigheidsduur van een certificaat. Ook kan een CA certificaten intrekken.
- De eindgebruiker kan het certificaat vervolgens gebruiken in zijn of haar toepassing. Aan de hand van het certificaat van de CA kan vervolgens worden gecontroleerd of het certificaat van de eindgebruiker correct is. Ook kan aan de hand van de lijst van ingetrokken certificaten (CRL) de geldigheid worden geverifieerd.

De gebruiker is vrij om te kiezen van welke certificate authority hij certificaten koopt. Het betrouwbaarheidsniveau verschilt potentieel wel tussen de diverse CA's. Dit hangt als gezegd vooral af van de manier waarop de certificaten worden uitgegeven.

1.2.2 Het programma PKIoverheid

Het programma PKIoverheid heeft tot doel deze infrastructuur in te richten onder de vlag van de Nederlandse overheid, met een hoog en uniform betrouwbaarheidsniveau:

- Hierbij is de Nederlandse overheid een root certificate authority – de hoogst vertrouwde instantie. De infrastructuur maakt het daarmee mogelijk om hiërarchisch vertrouwen te garanderen onder de vlag van de Nederlandse overheid.
- Dit wordt gegarandeerd door middel van specifieke procedures en technische voorwaarden voor het uitgeven van certificaten.

Certificaten kunnen worden uitgeven door overheidsorganisaties of commerciële dienstverleners die dit namens de overheid doen (Third Trusted Parties, TTP's). Deze partijen worden samen *Certificate Service Providers* genoemd (CSP's).

De uitgifteprocedure volgt de vereisten uit de Wet Elektronische Handtekening voor de *gekwalificeerde elektronische handtekening*[1]. De juridische status hiervan is gelijkwaardig aan de 'papieren' handtekening.

Hoewel het programma ten doel heeft een gekwalificeerde elektronische handtekening vanuit de overheid mogelijk te maken, zijn er ook gekwalificeerde elektronische handtekeningen mogelijk die niet onder het root certificate van de overheid vallen, maar onder die van een

1 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).

commerciële partij. De wet stelt o.a. de verplichting dat de certificaataanbieder zich moet registreren bij de OPTA.

1.2.3 De aangemelde standaard

De standaard PKIoverheid is aangemeld door Logius. Logius fungeert als beheerder van de standaard.

Aangemeld zijn de volgende documenten:
- PKIoverheid PvE deel 3a Certificate Policy - Domeinen Overheid/Bedrijven en Organisatie
- PKIoverheid PvE deel 3b Certificate Policy - Services Bijlage bij CP Domeinen Overheid/Bedrijven en Organisatie
- PKIoverheid PvE deel 3c Certificate Policy - Domein Burger
- PKIoverheid PvE deel 3d Certificate Policy - Domein Autonome Apparaten

Van deze documenten is versie 2.0 aangemeld. Deze versie vormde het onderwerp van toetsing. Inmiddels is er een nieuwe versie beschikbaar, versie 2.1. Deze nieuwe versie heeft betrekking op de naamswijziging van GBO.Overheid in Logius.

Naast de genoemde documenten is ook een deel 3e in ontwikkeling. Dit deel is echter buiten beschouwing gelaten, aangezien dit nog niet definitief is vastgesteld.

De documenten zijn programma's van eisen waaraan voldaan moet worden bij het uitgeven van certificaten voor de respectievelijke toepassingen. Het merendeel van de opgenomen eisen heeft betrekking op het proces van uitgifte. Dit proces is ingericht conform de vereisten in o.a. de Wet Elektronische Handtekening.

Auditors controleren periodiek of de PvE's nog voldoen aan de wettelijke vereisten. Uitgevers van certificaten worden daarnaast ook periodiek gecontroleerd door auditors. Hierdoor kunnen gebruikers van de certificaten een hoog niveau van betrouwbaarheid afleiden. Dit maakt PKIoverheid zeer geschikt voor toepassingen waar dit aspect een grote rol speelt.

1.3 Relatie met andere standaarden

Volgens opgave van de indiener wordt in PKIoverheid verwezen naar verschillende onderliggende standaarden.

<u>Gangbare standaarden</u>
- HTTPS
- FTPS / SFTP
- IPsec
- TLS
- UTF-8

Er wordt door de indiener opgemerkt dat in plaats van MD5 (opgenomen op de lijst met gangbare standaarden) een zwaardere vorm van encryptie wordt gebruikt, nl. op basis van SHA2 / SHA256. Naar mening van de expertgroep is dit gegeven de toepassing een goede keuze.

Internationale standaarden op het gebied van PKI

- ETSI TS 101 456, 'Policy requirements for certification authorities issuing qualified certificates', ESI;
- ETSI TS 102 042, 'Policy requirements for certification authorities issuing public key certificates', ESI.
- EN 45012:1998; 'Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures', CEN/ISSS WS/E-Sign (CWA 14167-1);
- ETSI TS 102 176-1 v2.0.0 (2007-11), 'Electronic Signatures and Infrastructures (ESI) & Security Requirements For Cryptographic Modules'; NIST (FIPS PUB 140-2);
- Secure signature-creation devices EAL 4+, CEN/ISSS WS/E-Sign (CWA 14169);
- EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes, CEN/ISSS WS/E-Sign (CWA 14172-2);
- Cryptographic module for CSP Signing Operations Protection Profile CEN/ISSS WS/ESign (CWA 14167-2);
- EESSI Conformity Assessment Guidance Part 3: Trustworthy systems managing certificates for electronic signatures, CEN/ISSS WS/E-Sign (CWA 14172-3);
- Cryptographic module for CSP Signing Operations Protection Profile CEN/ISSS WS/ESign (CWA 14167-4);
- ETSI TS 101 862: Qualified certificate profile;
- ETSI TS 102 280 : X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons;
- ITU-T Aanbeveling X.509 (1997)
- ISO/IEC 9594-8: Information Technology Open Systems Interconnection The directory: Public-key and attribute certificate frameworks;
- ITU-T Aanbeveling X.520 (2001)
- ISO/IEC 9594-6: Information Technology Open Systems Interconnection ?The directory: Selected Attribute Types;
- RFC 2560: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol OCSP;
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile;
- RFC 3739: Internet X.509 Public Key Infrastructure Qualified Certificates Profile;
- ISO 3166 English country names and code elements.

De vraag kan gesteld worden in hoeverre PKIoverheid zelf een ICT-standaard is. Het is immers een programma van eisen dat (in hoofdzaak) beschrijft hoe bedrijfsprocessen – die gebruik maken van de onderliggende ICT-standaarden – moeten worden ingericht.

Hier is in de expertgroep kort bij stilgestaan. Er kon geen consensus over worden bereikt. Ten behoeve van de behandeling is er gemakshalve vanuit gegaan dat er sprake is van een standaard.

1.4 Proces

Voor het opstellen van dit advies is de volgende procedure doorlopen:
In opdracht van het Forum Standaardisatie zijn experts benaderd om deel te nemen aan de expertgroep. Getracht is de experts een goede afspiegeling te laten zijn van het veld (gebruikers, certificaat uitgevers, overheden, indiener, etc.).

Aan alle leden is gevraagd individueel de standaard te scoren op basis van de vastgestelde criteria. Op basis van de reacties zijn door de procesbegeleider de mogelijke knelpunten in kaart gebracht.
Op 15 juli 2010 is de expertgroep bijeen gekomen. De standaard en de aanmelding zijn hier door Logius toegelicht. Tijdens deze bijeenkomst is gesproken over de ingediende versie, het toepassings- en werkingsgebied en de score op de toetsingscriteria. Tevens is de hoofdlijn van het advies vastgesteld.

Door de voorzitter en procesbegeleider is tenslotte dit adviesrapport opgesteld, dat is rondgestuurd naar alle leden van de expertgroep. Op basis van hun reacties is het document aangepast en gereed gemaakt voor de publieke consultatieronde.

1.5 Samenstelling expertgroep

Voor de expertgroep zijn personen uitgenodigd die vanuit hun persoonlijke expertise of werkzaamheden bij een bepaalde organisatie direct of indirect betrokken zijn bij de standaard. Daarnaast is een onafhankelijke voorzitter aangesteld om de expertgroep te leiden en als verantwoordelijke op te treden voor het uiteindelijke expertadvies.

Als voorzitter heeft opgetreden dr. Jaap-Henk Hoepman, senior scientist bij TNO op het gebied van security en privacy. Daarnaast is hij als universitair hoofddocent ‘security and applied cryptography’ verbonden aan de Radboud Universiteit Nijmegen. Vanuit die rol is hij tevens coördinator van het Kerckhoffs Instituut, dat een masteropleiding verzorgt in computerbeveiliging.

De expertgroep is begeleid door ir. Matthijs Punter, adviseur open standaarden en interoperabiliteit bij TNO.

Aan de expertgroep hebben deelgenomen:
- Luitenant Kolonel ing. Fekke Bakker, programmamanager bij de Afdeling Informatievoorziening, Ministerie van Defensie
- Mr. Dick Batenburg, notaris, directeur van DigiNotar Internet Trust Services
- Maarten de Boer MSc., adviseur bij KPMG.
- Harry Dragstra, ICT-security manager, Ministerie van Onderwijs, Cultuur en Wetenschappen, Dienst Uitvoering Onderwijs
- drs. Arjen Haasnoot, adviseur bij het Ministerie van Economische Zaken
- Ir. Geert Kleinhuis, senior security specialist, TNO
- Harld Röling, consultant PKI Overheid, Logius (namens de indiener)
- Sander Steenbergen, adviseur bij Getronics CSP.
- Dr. Frank Terpstra, adviseur implementatie Digikoppeling, Renoir
- Harold Teunissen, vertegenwoordiger van Surfnet.
- Drs. Lilian Theunissen, senior procesadviseur, CIBG, uitvoeringsorganisatie van het ministerie van Volksgezondheid, Welzijn en Sport.
- Lex Samuel, adviseur bij QuoVadis Trustlink
- Michael Stoelinga, adviseur bij ICTU
- Kees Uijl, coördinator Informatiebeveiliging en als organisatie : (BPR) Agentschap Basisadministratie Persoonsgegevens en Reisdocumenten; Ministerie van Binnenlandse Zaken.
- Benne de Weger, onderzoeker op het gebied van IT-beveiliging en cryptografie, Technische Universiteit Eindhoven

1.6 Vervolg

Het expertadvies zoals in dit document tot stand is gekomen, zal ten behoeve van een publieke consultatie openbaar worden gemaakt door het Bureau Forum Standaardisatie. Alle belanghebbenden kunnen gedurende de consultatieperiode van 5 weken op dit expertadvies reactie geven. Het Bureau Forum Standaardisatie legt vervolgens de reacties voor aan de voorzitter en indien nodig aan de expertgroep.

Het Forum Standaardisatie zal op basis van het expertadvies en relevante inzichten uit de openbare consultatie een advies aan het College Standaardisatie opstellen. Het College Standaardisatie bepaalt uiteindelijk op basis van het advies van het Forum of de standaard op de lijst met gangbare open standaarden of de 'pas toe of leg uit'-lijst komt.

1.7 Leeswijzer

In hoofdstuk 2 wordt beschreven in welke gevallen PKIoverheid functioneel gezien gebruikt moet worden (functioneel toepassingsgebied) en door welke organisaties PKIoverheid gebruikt zou moeten worden (organisatorisch werkingsgebied). Om te bepalen of PKIoverheid opgenomen moet worden op de lijst met open standaarden is deze getoetst aan een viertal door het College vastgestelde criteria. In hoofdstuk 3 staat het resultaat van deze toetsing. Hoofdstuk 4 bevat een samenvatting van de toetsresultaten op hoofdlijnen en het advies van de expertgroep aan het Forum.

2 Toepassings- en werkingsgebied

Van overheidsorganisaties wordt verwacht dat zij de lijst met open standaarden hanteren bij aanbestedingstrajecten volgens het "pas toe of leg uit" principe. Afhankelijk van de aan te schaffen functionaliteit zal bepaald moeten worden welke koppelvlakken geïmplementeerd moeten worden, en welke standaarden uit de lijst hiervoor ingezet dienen te worden. Om dit te kunnen doen heeft de expertgroep gekeken in welke gevallen PKIoverheid functioneel gezien gebruik moet worden (toepassingsgebied), en door welke organisaties PKIoverheid gebruikt zou moeten worden (werkingsgebied)

2.1 Functioneel toepassingsgebied

In de aanmelding van PKIoverheid werd bij het toepassingsgebied verwezen naar de scope van de verschillende delen van het Programma van Eisen ('Overheid en Bedrijven', 'Services', 'Burgers' en 'Autonome apparaten'). Er is echter niet bij vermeld welke functionele toepassingen die dan zou moeten betreffen.

In de expertgroep is hier daarom lang bij stil gestaan.

Er is een aantal mogelijkheden overwogen om het functionele toepassingsgebied te classificeren, die zich grofweg verdelen in twee groepen:

- Op basis van *gebruik* van certificaten: hierbij zouden toepassingen gedefinieerd moeten worden waarvoor én PKI gebruikt moet worden én PKIoverheid het uitgangspunt zou moeten zijn.
- Op basis van het *uitgeven* van certificaten: hierbij zou gedefinieerd moeten worden in welke gevallen de richtlijnen van PKIoverheid gevolgd zouden moeten worden voor het uitgeven van een certificaat.

De expertgroep ziet geen mogelijkheden om een toepassingsgebied vast te stellen voor het *gebruik* van elektronische certificaten:

- Het is niet gemakkelijk om eenduidig te definiëren wanneer een PKI-infrastructuur gebruikt moet worden (wanneer verplicht / wanneer optioneel / wanneer niet). Er zijn immers ook andere methoden om de betrouwbaarheid van gegevens te waarborgen.
- Europese richtlijnen voor betrouwbaarheidsniveaus zijn nog in ontwikkeling (onder andere vanuit het STORK project, zie: https://www.eid-stork.eu/). In lang niet alle gevallen is een certificaat nodig (pas vanaf STORK niveau 4). In het Nederlandse programma eHerkenning wordt dit overgenomen.
- Er is niet precies vastgelegd in wet- en regelgeving voor welke toepassing welk betrouwbaarheidsniveau geldt. Hoewel er wel enkele handreikingen zijn, blijft het uiteindelijk aan de aanbieder van een dienst om te bepalen welk niveau gekozen wordt.
- De Wet Elektronische Handtekening geeft overheden en bedrijven een hoge mate van vrijheid om zelf te bepalen op welke manier een elektronische handtekening wordt ingericht. Zo is er lange tijd de vijfcijferige elektronische handtekening in gebruik geweest bij de Belastingdienst voor het ondertekenen van een belastingaangifte. Voor bancaire toepassingen wordt vaak gebruik gemaakt van tokens

of e-readers in combinatie met een pincode. In sommige gevallen wordt zelfs volstaan met een gedigitaliseerde fysieke handtekening.
- De wet maakt onderscheid tussen een eenvoudige elektronische handtekening, een geavanceerde elektronische handtekening en een geavanceerde elektronische handtekening met een gekwalificeerd certificaat (de gekwalificeerde elektronische handtekening). Er is in de wet niet vastgelegd wanneer een gekwalificeerde elektronische handtekening moet worden gebruikt. Enkel is de juridische status ervan vastgelegd.
- Als toepassing van een gekwalificeerde elektronische handtekening door een organisatie voor een bepaalde toepassing gewenst is, biedt de wet ook de mogelijkheid een dergelijke handtekening te plaatsen op basis van een root certificaat van een commerciële aanbieder. Mits e.e.a. uiteraard voldoet aan de eisen die aan een gekwalificeerd certificaat worden gesteld.

Hoewel de expertgroep het mogelijk acht dat er meer richting wordt gegeven op dit vlak, acht zij zich niet de aangewezen partij om dit te doen. Het zou indirect immers een aanscherping kunnen betekenen van wet- en regelgeving op dit terrein (in ieder geval voor wat betreft interactie met en door de overheid). Opname op de lijst met verplichte open standaarden zou het bovendien enkel borgen binnen de inkoop van ICT-middelen, terwijl gezien de aard van de standaard ook borging van het daadwerkelijke gebruik wenselijk is.

Het zou daarom beter zijn wanneer de overheid als geheel of binnen specifieke domeinen vastlegt welke betrouwbaarheidsniveaus voor welke toepassingen behaald moeten worden. Aan de hand daarvan kan dan worden bepaald of achtereenvolgens PKI, een gekwalificeerde elektronische handtekening en een gekwalificeerde elektronische handtekening op basis van PKIoverheid toegepast moeten worden.

De expertgroep constateert dat binnen delen van de overheid deze keuze inmiddels is gemaakt. Voorbeelden zijn o.a.:
- Digikoppeling, waarbij PKIoverheid certificaten verplicht zijn voor uitwisseling met zowel de WUS als ebMS koppelvlakstandaard.
- CIBG gebruikt PKIoverheid certificaten binnen de zorg;
- Defensie geeft certificaten op basis van PKIoverheid uit voor de Defensiepas.

Ten behoeve van de experttoetsing is daarom uitgegaan van het volgende functionele toepassingsgebied:

Het uitgeven van elektronische certificaten ten behoeve van een gekwalificeerde elektronische handtekening.

Concreet betekent dit dat:
- Ook andere methoden van elektronische handtekeningen / elektronische authenticatie zijn toegestaan;
- Voor het uitgeven van certificaten voor niet-gekwalificeerde toepassingen, niet noodzakelijkerwijs het PvE PKIoverheid gevolgd dient te worden. Denk hierbij aan het uitgeven van certificaten voor eenvoudige websites, testservers etc., waarvoor naar mening van de ontwikkelaar/eigenaar niet de vereisten voor gekwalificeerde certificaten gevolgd hoeven te worden.

- De ruimte die de wet biedt om ook certificaten te gebruiken c.q. te accepteren voor een gekwalificeerde elektronische handtekening van commerciële aanbieders die niet onder het root certificate van de Nederlandse overheid vallen behouden blijft.
- Enkel indien een organisatie zelf gekwalificeerde certificaten gaat uitgeven of dit door een andere partij (namens hen) laat doen PKIoverheid moet worden gebruikt.

2.2 Organisatorisch werkingsgebied

Er is gekozen het werkingsgebied van de standaard niet in te perken en vast te stellen als zijnde:

Overheden en instellingen in de (semi-)publieke sector

In combinatie met het functionele toepassingsgebied betekent dit dat – als de standaard zou worden opgenomen op de lijst voor 'pas toe of leg uit' – overheden en instellingen in de semi-publieke sector, die certificaten willen uitgeven ten behoeve van een gekwalificeerde elektronische handtekening, dit zouden moeten doen conform de specificaties van PKIoverheid.

Deze verplichting zou dan gelden bij de aanschaf van ICT-middelen (producten én diensten) die ten doel hebben de uitgifteprocedure te faciliteren.

2.3 Versie

Initieel is versie 2.0 voorgesteld van de verschillende documenten. Het Pakket van Eisen wordt echter gemiddeld één maal per jaar aangepast. Inmiddels is versie 2.1 van de documenten beschikbaar. Zoals reeds eerder aangegeven is de wijziging tussen versie 2.0 en 2.1 beperkt (naamswijziging GBO.Overheid in Logius).

De expertgroep hecht er aan dat altijd de laatste versie van de standaard wordt gebruikt. Opname van een standaard op de lijst voor 'pas toe of leg uit' betekent dat een nieuwe versie weliswaar kan worden uitgebracht door de beheerder, maar pas opgenomen kan worden na nadere toetsing door het Forum Standaardisatie. Hierdoor zijn er gedurende een zekere periode meerdere versies 'in omloop'. Er worden dan gedurende een bepaalde periode PKIoverheid certificaten uitgegeven met verschillende versies. Dat is gezien de aard van de standaard (processtandaard) naar mening van de expertgroep niet wenselijk.

Overigens moet opgemerkt worden dat certificaten die zijn uitgegeven conform een oude versie wel geldig blijven (gedurende hun geldigheidstermijn). Er is op dat punt dus geen migratieproblematiek te verwachten.

3 Toetsing aan de criteria

3.1 Openheid

3.1.1 Goedkeuring en handhaving

Is de standaard goedgekeurd en wordt zij gehandhaafd door een non-profit organisatie?

De standaard wordt beheerd door Logius in opdracht van het Ministerie van Binnenlandse Zaken. Er is daarmee sprake van een non-profit organisatie als beheerder.

Gebeurt de lopende ontwikkeling op basis van een open besluitvormingsprocedure die toegankelijk is voor alle belanghebbende partijen (consensus of meerderheidsbeschikking enz.)?

Logius biedt de mogelijkheid om meldingen en wijzigingsverzoeken in te dienen. Er is echter geen open besluitvormingsprocedure. Hoewel er sprake is van een Afnemersoverleg waarin advies kan worden gegeven, ligt de uiteindelijke beslissing bij de programmaorganisatie en de opdrachtgever daarvan (BZK).

Onafhankelijke certificaatuitgevers geven aan dat de ervaringen wisselend zijn. Het is onduidelijk of en zo ja wat er met hun inbreng gebeurt. De oprichting van een 'change advisory board' zou al een verbetering zijn.

Voordat de standaard opgenomen kan worden op de lijst van open standaarden zou het beheerproces verbeterd moeten worden, bijvoorbeeld op basis van het Beheer en Ontwikkelmodel Open Standaarden (BOMOS) van het programma Nederland Open in Verbinding.

Tegelijkertijd vraagt de expertgroep zich af of een consensus-/meerderheidsmodel goed past bij een standaard als PKIoverheid. Inherent aan PKIoverheid is immers een hiërarchisch vertrouwensmodel, met de Nederlandse overheid (het Ministerie van Binnenlandse Zaken) als meest vertrouwde partij in de keten.

3.1.2 Beschikbaarheid

Is de standaard gepubliceerd en kan over de specificatie vrijelijk worden beschikt of is deze te verkrijgen tegen een nominale bijdrage? Is het voor eenieder mogelijk de standaard te kopiëren, beschikbaar te stellen en te gebruiken om niet of tegen een nominale prijs?

Het programma van eisen is gepubliceerd op de website van Logius (http://www.logius.nl/producten/toegang/pkioverheid/aansluiten/programma-van-eisen/) en kan gratis worden gedownload.

De onderliggende internationale standaarden zijn volgens de expertgroep verkrijgbaar via de betreffende standaardisatieorganisaties. In een aantal gevallen moet hiervoor een nominale prijs worden betaald (ISO)

3.1.3 Intellectueel eigendom

Is het intellectuele eigendom (m.b.t. evt. aanwezige patenten) van (delen) van de standaard onherroepelijk "royalty-free" ter beschikking gesteld?

In het programma van eisen zijn bepalingen opgenomen rondom het intellectueel eigendom. Deze eisen beschermen de afnemer van certificaten: de CSP vrijwaart de abonnee ten aanzien van aanspraken door derden vanwege schendingen van intellectuele eigendomsrechten door de CSP.

Het is onduidelijk in hoeverre het intellectuele eigendom m.b.t. de onderliggende (internationale) (technische) standaarden onherroepelijk aan de certificaatverlener ter beschikking zijn gesteld. De aanwezige certificaatverleners in de expertgroep geven aan dat men in de praktijk niet te maken heeft met eventuele patentclaims.

Hoewel een vrijgaveonderzoek geen deel uitmaakte van het expertonderzoek is er een steekproef gedaan onder de onderliggende technische standaarden. Daarbij is gebleken dat o.a. op de certificaatstandaard X.509 een patent is gevestigd (in dat geval door Nortel/Entrust Technologies) waarbij niet duidelijk is of deze onherroepelijk en royalty-free ter beschikking zijn gesteld aan alle gebruikers[2].

3.1.4 Hergebruik

Zijn er beperkingen omtrent het hergebruik van de standaard?

Er zijn geen beperkingen omtrent het hergebruik van de standaard bekend.

Wel is aan de standaard een auditverplichting gekoppeld (feitelijk maakt deze verplichting onderdeel uit van de standaard).

2 Het patent is overigens wel in 2007 royalty-free ter beschikking gesteld aan Sun Microsystems voor opnamen in internetbrowser Mozilla.

Om gekwalificeerde elektronische certificaten uit te geven dient de certificaatverlener geregistreerd te zijn bij de OPTA[3] – dit is een wettelijke verplichting. Hiervoor zijn (beperkte) registratiekosten verschuldigd.

3.2 Bruikbaarheid

3.2.1 Volwassenheid

Is de standaard voldoende uitgekristalliseerd?
Is er voldoende praktijkervaring met het gebruik van de standaard?

Naar mening van de expertgroep is de standaard voldoende uitgekristalliseerd. Wel zijn er nog wensen vanuit commerciële certificaataanbieders voor vereenvoudiging (zonder dat dit de betrouwbaarheid hoeft aan te tasten).

Regelmatig wordt de standaard bijgewerkt, dit gebeurt vooral naar aanleiding van wijzigingen in de omgeving (bijvoorbeeld aanpassingen in wet of regelgeving of nieuwe toepassingsgebieden).

Wel moet er onderscheid worden gemaakt tussen de verschillende delen van het Programma van Eisen. Met het onderdeel 3c, dat betrekking heeft op het uitgeven van certificaten aan individuele burgers, is nog geen ervaring. Deze certificaten zouden bijvoorbeeld gebruikt kunnen worden in het kader van eNIK. Mocht PKIoverheid op de lijst met open standaarden opgenomen worden, dan zou onderdeel 3c daarom vooralsnog uitgezonderd moeten worden. Pas nadat meer uitvoerig praktijkervaring is opgedaan met 3c zou dit deel opgenomen kunnen worden.

Hetzelfde geldt voor het onderdeel 3e, ten behoeve van *extended verification*. Dit is nu nog in ontwikkeling en zou nog niet opgenomen moeten worden (deel 3e maakt overigens ook geen deel uit van de aanmelding).

Is verdere ontwikkeling en het onderhoud van de standaard verzekerd?

Ontwikkeling en onderhoud is belegd bij Logius en wordt gefinancierd door het Ministerie van Binnenlandse Zaken. Via deze weg zijn ontwikkeling en onderhoud voldoende verzekerd.

Is er een methode waarmee conformiteit aan de standaard bepaald kan worden?

Aan de standaard is een verplichte audit gekoppeld. Via deze audit wordt conformiteit aan de standaard afgedwongen.

Is er nu en in de toekomst voldoende ondersteuning door (meerdere) marktpartijen voor de standaard?

Er zijn meerdere partijen die op commerciële basis certificaten verstrekken namens de overheid (QuoVadis, Getronics en Diginotar). Daarnaast kunnen overheidspartijen ook zelf certificaatverlener zijn.

3 De lijst van partijen is te vinden via https://www.opta.nl/download/bestand/current-tsl.pdf

De aan de standaard gekoppelde audit wordt op dit moment uitgevoerd door KPMG namens PriceWaterhouseCoopers en BSI Management (geaccrediteerde auditpartijen). Ook andere partijen zijn echter vertrouwd met de eisen die de Wet Elektronische Handtekening stelt aan gekwalificeerde elektronische handtekeningen.

Naar mening van de expertgroep is de marktondersteuning nu en in de toekomst hiermee voldoende.

Is de verwachting van het toekomstige gebruik van de standaard positief?

Deze verwachting is positief. Naar verwachting van de expertgroep neemt het gebruik van PKI toepassingen in de toekomst toe. Wel gaat de toepassing van PKI tot nu toe minder snel dan in de jaren '90 werd verwacht. Voor de overheid ligt – ten behoeve van het uitgeven van certificaten voor een gekwalificeerde elektronische handtekening – het gebruik van (het door de overheid opgezette) PKIoverheid voor de hand.

Een voorbeeld wordt gegeven door Defensie, dat PKIoverheid naar verwachting gaat gebruiken in de elektronische uitwisseling met bepaalde toeleveranciers. Ook kijkt men naar harmonisatie van PKI in NAVO-verband.

3.2.2 Functionaliteit

Voldoet de standaard aan de functionele eisen die aan de werking van de standaard gesteld worden binnen het voorgestelde toepassingsgebied?

Ja, de standaard implementeert de eisen die de wet stelt aan een gekwalificeerde elektronische handtekening. Daarnaast is de standaard toe te passen binnen meerdere functionele domeinen (beveiliging van websites, e-mail, ondertekening PDF-documenten, gebruikersauthenticatie, etc.).

Wel is het zo dat soms certificaten nodig kunnen zijn van meerdere certificaatverleners. Dit wordt veroorzaakt doordat verschillende certificaatverleners verschillende gegevens in een certificaat kunnen opnemen. Zo zal de Belastingdienst in een certificaat voor bedrijven wellicht een BTW-nummer willen opnemen en de Kamer van Koophandel een KvK-nummer, ondanks dat het vertrouwensniveau gelijk is. Het zou wenselijk zijn dat men kan werken met één certificaat, waarbij een identity-makelaar (bijvoorbeeld zoals voorgesteld in eHerkenning) dit koppelt aan identiteiten bij verschillende partijen.

3.2.3 Concurrerende standaarden

Verhoudt de standaard zich goed ten opzichte van eventuele concurrerende standaarden?

Er zijn ook commerciële aanbieders van root-certificaten. Getronics biedt gekwalificeerde certificaten aan op basis van het VeriSign root certificaat. De Wet Elektronische Handtekening biedt deze mogelijkheid. Op basis van de wet moet o.a. de aanbieder van de gekwalificeerde certificaten bij de OPTA worden geregistreerd. De wet biedt daarmee de mogelijkheid voor bijvoorbeeld een bedrijf dat zaken wil doen met de overheid gebruik te maken van een dergelijk commercieel certificaat om zich te authenticeren.

Voor de overheid zelf ligt het gebruik van PKIoverheid voor de hand (als 'eigen' ontwikkeling van de overheid).

Naar mening van een aantal deelnemers implementeert PKIoverheid de vereisten uit de wet relatief 'zwaar' ten opzichte van een aantal commerciële aanbieders van root-certificaten. Dit brengt voor de certificaatverlener en de afnemers extra inspanningen en kosten met zich mee.

De expertgroep wijst bij dit punt opnieuw op de mogelijkheid om ook 'lichtere' vormen van PKI toe te passen of andere vormen van betrouwbaarheidsverificatie (zoals Web of Trust). OCW-DUO noemt het voorbeeld van basisscholen aan wie zij certificaten uitgeven. Het zou te veel kosten met zich meebrengen en te weinig voordelen om dit te laten verlopen via PKIoverheid. Zo verplicht PKIoverheid een 'fysieke' overdracht van het certificaat (langsgaan bij een notaris of andere door de certificaatverlener vertrouwde persoon).

3.3 Potentieel

Gegeven het gedefinieerde toepassingsgebied kan het opnemen van de standaard zorgen voor een toename van het aantal certificaataanbieders dat gebruik maakt van de PKIoverheid-specificatie voor de certificaten en het uitgifteproces.

Concrete alternatieven die er zouden zijn indien PKIoverheid niet met het gedefinieerde toepassingsgebied zijn:
- Het gebruik maken van een eigen root certificaat. Dit beperkt echter de toepassingsmogelijkheden en maakt het lastig een gekwalificeerde elektronische handtekening te bieden.
- Het gebruik maken van een commercieel root certificaat.

Er zijn op dit moment 6 partijen die PKIoverheid certificaten uitgeven; vier daarvan zijn commerciële partijen. De verwachting van de expertgroep is dat het aantal overheidsorganisaties (reikwijdte van de lijst voor 'pas toe of leg uit') dat zelf certificaten gaat uitgeven beperkt zal blijven (in de komende jaren 2 tot hooguit 3 partijen). Overheidspartijen die certificaten willen gebruiken hebben immers de mogelijkheid gebruik te maken van de reeds beschikbare (al dan niet commerciële) aanbieders van certificaten.

Draagt het opnemen van de standaard op de lijst bij aan het vergroten van de leveranciersonafhankelijkheid?

Opname van de standaard op de lijst kan zoals geschetst zorgen voor een toename van het aantal uitgevers van certificaten. Het aantal zal echter zeer beperkt zijn. Daarbij is het bovendien de vraag of deze overheidspartijen zonder opname van PKIoverheid zullen kiezen voor een commercieel root-certificaat. De expertgroep denkt dat kans daarop zeer gering is.

Op basis hiervan is de expertgroep van mening dat opname van PKIoverheid op de lijst met open standaarden niet of nauwelijks bijdraagt aan het vergroten van leveranciersonafhankelijkheid.

Draagt het opnemen van de standaard op de lijst bij aan het vergroten van de interoperabiliteit?

Het *gebruik* van certificaten die allemaal volgens dezelfde manier zijn uitgegeven kan bijdragen aan interoperabiliteit – het vertrouwensniveau is immers gelijk. Daarbij moet wel opgemerkt worden dat door de Wet Elektronische Handtekening interoperabiliteit al wordt bevorderd door het stellen van wettelijke eisen aan een gekwalificeerde elektronische handtekening.

Het verplichten van de standaard voor het *uitgeven* van certificaten kan voordelen bieden, maar draagt als zodanig naar mening van de expertgroep niet specifiek bij aan het vergroten van interoperabiliteit.

3.4 Impact

3.4.1 Bedrijfsvoering

Brengt de toepassing van de standaard risico's met zich mee op het gebied van de bedrijfsvoering?
Brengt de toepassing van de standaard positieve effecten met zich mee op het gebied van de bedrijfsvoering?

Er zijn geen specifieke risico's verbonden aan het gebruik van PKIoverheid voor de bedrijfsvoering. Ook zijn er geen specifieke positieve effecten voor de bedrijfsvoering.

3.4.2 Informatievoorziening

Brengt de toepassing van de standaard risico's met zich mee op het gebied van de informatievoorziening?
Brengt de toepassing van de standaard positieve effecten met zich mee op het gebied van de informatievoorziening?

Er zijn geen specifieke risico's voor de informatievoorziening.
Als positief effect van het gebruik van PKIoverheid certificaten kan het verhoogde betrouwbaarheidsniveau van elektronische communicatie worden genoemd.

3.4.3 Technologie

Brengt de toepassing van de standaard technologische risico's met zich mee?
Brengt de toepassing van de standaard positieve technologische effecten 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. Ook zijn er geen specifieke positieve technologische effecten aan de standaard verbonden (anders dan de generieke voordelen van een PKI-infrastructuur op het gebied van beveiligde communicatie).

3.4.4 Beveiliging en privacy

Brengt de toepassing van de standaard risico's met zich mee op het gebied van beveiliging of privacy?
Brengt de toepassing van de standaard positieve technologische effecten met zich mee op het gebied van de beveiliging en privacy?

Gekoppeld aan de introductie van PKI (en in het bijzonder PKIoverheid) is de verhoging van het betrouwbaarheidsniveau van elektronische communicatie. Dit is een positief technologisch effect.

Wel zijn er een aantal risico's:

- Bij het werken met PKI moeten er inherent (persoonlijke) gegevens van de houder van een certificaat worden verwerkt en opgeslagen. Deze verwerking en opslag moet veilig gebeuren en recht doen aan de privacy van gebruikers. Hiervoor kunnen aanvullende maatregelen noodzakelijk zijn.
- Op dit moment wordt nog gebruik gemaakt van SHA1 voor de beveiliging (encryptie) van het root-certificaat van de Nederlandse overheid. Per 1-1-2011 moeten alle partijen overstappen naar het sterkere SHA256 (de z.g.n. G2-root). Dit is nodig om ook op termijn de beveiliging te kunnen garanderen. Deze overstap wordt door PKIoverheid verplicht gesteld.

3.4.5 Migratie

Kan er gemakkelijk naar de standaard toe worden gemigreerd?

Een migratie naar de standaard is niet eenvoudig. Dit is echter inherent aan het karakter van de standaard. Het uitgeven van certificaten volgens PKIoverheid vergt een groot aantal technische en organisatorische maatregelen.

4 Advies aan Forum en College Standaardisatie

4.1 Samenvatting van de toetsingscriteria

De expertgroep heeft als toepassingsgebied gedefinieerd: *"Het uitgeven van elektronische certificaten ten behoeve van een gekwalificeerde elektronische handtekening.".* Er is nadrukkelijk niet gekozen voor het definiëren van een toepassingsgebied dat betrekking heeft op het gebruik van certificaten. Voor een nadere duiding hiervan wordt verwezen naar hoofdstuk 2.

Op basis van dit toepassingsgebied is de standaard beoordeeld op de vastgestelde toetsingscriteria.

Openheid
De standaard is nog onvoldoende open. Het beheerproces geschiedt niet op basis van open besluitvorming (consensus of meerderheidsbesluitvorming). Hoewel dit een vereiste is voor opname op de lijst met open standaarden, stelt de expertgroep wel de vraag of een dergelijke open besluitvorming past bij de aard van de standaard (hiërarchisch vertrouwensmodel onder de Nederlandse overheid).

Niet vastgesteld kan worden of het intellectueel eigendom van alle onderliggende technische standaarden onherroepelijk en royalty-free beschikbaar is gesteld aan uitgevers van certificaten. Hoewel dit in de praktijk niet tot problemen heeft geleid, is dit een aandachtspunt.

Bruikbaarheid
De standaard is goed bruikbaar voor het uitgeven van certificaten die voldoen aan de eisen voor een gekwalificeerde elektronische handtekening. De standaard implementeert hiertoe de wettelijke vereisten uit de Wet Elektronische Handtekening. Dit maakt de standaard geschikt voor het geschetste toepassingsgebied.

De expertgroep maakt hierbij enkele kanttekeningen:
- De ervaring met de standaard verschilt per 'verschijningsvorm'. Zo is er ruime ervaring met het uitgeven van certificaten aan bedrijven en voor het gebruik op computersystemen (b.v. websites). De ervaring met het uitgeven van certificaten aan individuele burgers is echter nihil. Het gedeelte van de standaard dat hier betrekking op heeft (deel 3c) zou bij opname uitgezonderd moeten worden.
- 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. Enkel de vereisten voor en rechtsgevolgen van een gekwalificeerde elektronische handtekening worden gedefinieerd in de wet. Vaak voldoen daarom ook 'lichtere' methoden (met minder betrouwbaarheid).

Voor een gekwalificeerde elektronische handtekening kan op basis van de Wet Elektronische Handtekening ook gebruik worden gemaakt van commerciële certificaten (niet op basis van het hoofdcertificaat (*root certificate*) van de Nederlandse overheid). Indien men zelf certificaten gaat uitgeven, ligt het gebruik van het overheidscertificaat uiteraard wel voor de hand. Dit laat echter onverlet dat partijen die zaken doen met de overheid (wettelijk gezien) gebruik kunnen maken van een commercieel certificaat.

Potentieel
Er is duidelijk een potentieel om met PKIoverheid de betrouwbaarheid van elektronische gegevensuitwisseling te verbeteren.

Het potentieel van opname van de standaard op de lijst is echter nihil. Het zal waarschijnlijk niet leiden tot een forse vergroting van het aantal aanbieders van certificaten.

Impact
Er is geen specifieke positieve of negatieve impact te verwachten indien de standaard wordt opgenomen op de lijst met open standaarden.

4.2 Advies

PKIoverheid kan goed worden gebruikt voor het uitgeven van gekwalificeerde elektronische certificaten.

Opname van PKIoverheid met dit toepassingsgebied op de lijst met open standaarden draagt echter onvoldoende bij aan interoperabiliteit en leveranciersonafhankelijkheid (de doelen van de lijst). Ook is er een aantal aandachtspunten m.b.t. de openheid.

De expertgroep adviseert op basis van deze overwegingen PKIoverheid niet op te nemen op de lijst met open standaarden.

4.3 Nadere overweging: stimuleren van PKIoverheid via voorzieningen

Ondanks het feit dat de expertgroep van mening is dat PKIoverheid niet op de lijst met open standaarden opgenomen zou moeten worden, wil de expertgroep wel het belang van PKIoverheid als zodanig duidelijk onderstrepen. Het uitgeven en gebruiken van certificaten conform de specificaties van PKIoverheid kan duidelijk bijdragen aan verbetering van de betrouwbaarheid van elektronische communicatie. PKIoverheid vormt daarmee een belangrijke bouwsteen van de elektronische vertrouwensinfrastructuur binnen de overheid.

Het gebruik van PKIoverheid zou volgens de expertgroep op andere manieren beter gestimuleerd kunnen worden, ondermeer door:
- door nadere richtlijnen te formuleren voor het verplichte gebruik van een gekwalificeerde elektronische handtekeningen bij elektronische toepassingen door de overheid.
- binnen specifieke voorzieningen het gebruik van PKIoverheid te verplichten (vergelijkbaar met de huidige praktijk in (o.a.) Digikoppeling)