

FORUM STANDAARDISATIE

Aanmelding PKloverheid



-----Oorspronkelijk bericht-----

Van: Survey [mailto:Website.Forum.Standaardisatie@[xxx].nl]

Verzonden: di 29-12-2009 20:51

Aan: GBO Forumstandaardisatie

CC: Joris Gresnigt

Onderwerp: Formulier open standaarden

#1 :

Geslacht

1 - Man

#2 :

Voornaam

[...]

#3 :

Achternaam

[...]

#4 :

Organisatie

GBO.Overheid

#5 :

Functie

[...]

#6 :

Telefoonnummer

[...]

#7 :

E-mailadres

[...]

#8 :

Welke relatie bestaat er tussen uw organisatie en de aangemelde standaard?

2 - Beheerder



#9 :

Wat voor soort melding wilt u doen?

1 - Voorstel om een geheel nieuwe standaard aan te melden

#10 :

Meldt u n standaard aan of een set van bij elkaar horende standaarden?

4 - een set van 4 bij elkaar horende standaarden

#11 :

Volledige naam

PKloverheid PvE deel 3a Certificate Policy - Domeinen Overheid/Bedrijven en Organisatie

#12 :

Afkorting

PKloverheid PvE deel 3a

#13 :

Versie

2.0 -

#14 :

Toepassingsgebied

Overheid en Bedrijven

#15 :

Beheerorganisatie

GBO.Overheid

#16 :

Locatie (Website)

<http://www.pkioverheid.nl/voor-certificaatverleners/programma-van-eisen/programma-van-eisen-2009/>

#17 :

FORUM STANDAARDISATIE

Aanmelding PKIoverheid



Volledige naam

PKIoverheid PvE deel 3b Certificate Policy - Services Bijlage bij CP Domeinen
Overheid/Bedrijven en Organisatie

#18 :

Afkorting

PKIoverheid PvE deel 3b

#19 :

Versie

2.0 -

#20 :

Toepassingsgebied

Overheid en Bedrijven

#21 :

Beheerorganisatie

GBO.Overheid

#22 :

Locatie (Website)

<http://www.pkioverheid.nl/voor-certificaatverleners/programma-van-eisen/programma-van-eisen-2009/>

#23 :

Volledige naam

PKIoverheid PvE deel 3c Certificate Policy - Domein Burger

#24 :

Afkorting

PKIoverheid PvE deel 3c

#25 :

Versie

2.0 -

#26 :

FORUM STANDAARDISATIE

Aanmelding PKloverheid



Toepassingsgebied

Burgers

#27 :

Beheerorganisatie

GBO.Overheid

#28 :

Locatie (Website)

<http://www.pkioverheid.nl/voor-certificaatverleners/programma-van-eisen/programma-van-eisen-2009/>

#29 :

Volledige naam

PKloverheid PvE deel 3d Certificate Policy - Domein Autonome Apparaten

#30 :

Afkorting

PKloverheid PvE deel 3d

#31 :

Versie

2.0 -

#32 :

Toepassingsgebied

Autonome Apparaten

#33 :

Beheerorganisatie

GBO.Overheid

#34 :

Locatie (Website)

<http://www.pkioverheid.nl/voor-certificaatverleners/programma-van-eisen/programma-van-eisen-2009/>

#35 :



In hoeverre neemt de interoperabiliteit toe door voor deze standaard een pas toe of leg uit beleid te hanteren of om de standaard op de lijst met veelgebruikte standaarden te zetten?

Het Programma van Eisen van PKI-overheid (<http://www.pkioverheid.nl/voor-certificaatverleners/programma-van-eisen/programma-van-eisen-2009/>) 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). Dit is een samenstel van architectuur, techniek, organisatie, procedures en regels, gebaseerd op public key cryptografie. Het doel is het hiermee mogelijk maken van betrouwbare elektronische communicatie en betrouwbare elektronische dienstverlening. Het Programma van Eisen van PKI-overheid kan onder meer gebruikt worden voor de beveiliging van websites door uitgifte van SSL certificaten (https) die op dit normenstelsel zijn gebaseerd. Daarnaast kunnen b.v. PDF documenten worden voorzien van een gekwalif!

iceerde elektronische handtekening door middel van een certificaat gebaseerd op de normen uit het Programma van Eisen van PKI-overheid. Het beheer van het Programma van Eisen van PKI-overheid valt onder verantwoordelijkheid van de Nederlandse overheid. Daarmee is afhankelijkheid van (buitenlandse) commerciële partijen niet aan de orde. Indien voor het Programma van Eisen een pas toe of leg uit beleid wordt gehanteerd, zullen partijen binnen de overheid voor hun processen hetzelfde betrouwbare mechanisme, gebaseerd op internationale open standaarden, hanteren voor elektronische communicatie en elektronische dienstverlening binnen de overheid. Dit betekent dat partijen niet zelf steeds de betrouwbaarheid hoeven te definiëren c.q. vast te stellen. Hierdoor wordt interoperabiliteit binnen de overheid, bijvoorbeeld op het gebied van het beveiligen van websites, gerealiseerd en bevorderd.

#36 :

In hoeverre neemt de leveranciersafhankelijkheid toe door voor deze standaard een pas toe of leg uit beleid te hanteren of om de standaard op de lijst met veelgebruikte standaarden te zetten?

Het Programma van Eisen is een standaard die gebaseerd is op internationale open standaarden, waardoor interoperabiliteit is gerealiseerd. Verschillende Certificate Service Providers (CSP's) kunnen producten aanbieden binnen de PKI voor de overheid, waardoor proceseigenaren niet afhankelijk zijn van een partij. Momenteel leveren vier private CSP's en twee publieke CSP's certificaten gebaseerd op de eisen uit het Programma van Eisen PKI-overheid. Naar verwachting zullen in 2010 nog twee private CSP's en een publieke CSP worden aangesloten.



#37 :

Waaruit blijkt de behoefte voor het gebruik van deze standaard door de verschillende (semi) publieke organisaties?

De Nederlandse overheid heeft hoge ambities op het gebied van elektronische dienstverlening. Een essentiële voorwaarde voor elektronische dienstverlening is de betrouwbaarheid van de elektronische communicatie. Zo vraagt bijvoorbeeld een elektronische subsidieaanvraag in het algemeen om de identiteitsvaststelling van de betrokkenen, de wilsverklaring dat er daadwerkelijk een overheidsdienst wordt gevraagd en om vertrouwelijkheid van de communicatie van de aanvrager met de subsidieverstrekende instantie. Dit alles kan mogelijk worden gemaakt door toepassing van generieke mechanismen zoals identificatie en een elektronische handtekening op basis van Public Key Cryptografie. Public Key Cryptografie kan op verschillende manieren worden toegepast om betrouwbare elektronische communicatie te realiseren, waarbij men wel spreekt over een PKI. PKI is een zeer effectieve basis voor het cryptografische deel van de informatiebeveiliging.

Concrete toepassingen van het Programma van Eisen zijn:

- CIBG hanteert als CSP het Programma van Eisen voor uitgifte van PKI-overheid certificaten binnen de Zorg;
- Defensie hanteert als CSP het Programma van Eisen voor uitgifte van PKI-overheid certificaten op de Defensiepas.

Concrete ontwikkelingen in het gebruik van het Programma van Eisen zijn:

- Inspectie Verkeer en Waterstaat gaat het Programma van Eisen hanteren voor uitgifte van PKI-overheid certificaten voor de taxiboordcomputer;
- Justitie gaat het Programma van Eisen hanteren voor uitgifte van PKI-overheid certificaten voor de Justitiepas;
- Rijkswaterstaat is voornemens het Programma van Eisen te hanteren voor uitgifte van PKI-overheid certificaten voor Kilometerbeprijzing.

#38 :

Voor welke doeleinden zou de standaard het beste toegepast kunnen worden? (zie de lijst met open standaarden voor voorbeelden van toepassingsgebieden van standaarden)

Het Programma van Eisen kan het beste worden toegepast voor public key infrastructure binnen en met de overheid. De PKI voor de overheid maakt het mogelijk dat communicerende partijen waarborgen krijgen omtrent:

- de identiteit van een persoon die een dienst afneemt of de dienst zelf (identificatie en authenticiteit);
- de (juridische) zekerheid dat een bericht door een bepaalde persoon is verzonden of een document door een bepaalde persoon is ondertekend en dit ook niet achteraf kan worden ontkennd (elektronische handtekening, onweerlegbaarheid);



- de mogelijkheid om communicatie te beschermen tegen ongewenste inzage (vertrouwelijkheid, privacy) of wijziging (integriteit) door derden.

#39 :

Voor welke doeleinden wordt de standaard al toegepast?

- Het Programma van Eisen van PKloverheid kan onder meer gebruikt worden voor de beveiliging van websites door uitgifte van SSL certificaten (https) die op dit normenstelsel zijn gebaseerd;
- PDF documenten kunnen worden voorzien van een gekwalificeerde elektronische handtekening door middel van een certificaat gebaseerd op de normen uit het Programma van Eisen van PKloverheid;
- De integriteit en authenticiteit van programmatuur kan worden gewaarborgd (code signing) door middel van een certificaat gebaseerd op de normen uit het Programma van Eisen van PKloverheid.

#40 :

Indien er al een open standaard voor het beoogde toepassingsgebied is opgenomen op de lijst met open standaarden, is de aangemelde standaard interoperabel met de desbetreffende standaard op de lijst?

De volgende open standaarden (lijst met veelgebruikte standaarden) voor het beoogde toepassingsgebied zijn reeds opgenomen op de lijst en interoperabel met het Programma van Eisen van PKloverheid:

- HTTPS
- FTPS / SFTP
- IPsec
- TLS
- UTF-8

De Overheidsservicebus (OSB) schrijft het gebruik van PKloverheid certificaten, gebaseerd op het Programma van Eisen, dwingend voor.

Het MD5 message-digest algorithm (MD5) is niet interoperabel met met het Programma van Eisen van PKloverheid omdat daar het SHA-1 en SHA-256 dwingend wordt voorgeschreven.

#41 :

Binnen welke organisaties zou de standaard het beste gebruikt kunnen worden?



De standaard kan het beste gebruikt worden tussen overheid en overheid, overheid en bedrijven en overheid en burgers.

#42 :

Binnen welke organisaties wordt de standaard al gebruikt?
Binnen overheidsorganisaties en bedrijven.

#43 :

Wat is de mate waarin de standaard al gebruikt wordt?
2 - Enkele organisaties gebruiken de standaard

#44 :

De standaard dient kosteloos of tegen nominale kosten beschikbaar te worden gesteld.
Waaruit blijkt dat dit voor uw standaard het geval is?

In het Certificate Practice Statement (CPS) Policy Authority PKI-overheid v3.1 (<http://www.pkioverheid.nl/voor-certificaatverleners/cps/>) is vermeld dat geen kosten worden berekend voor:

- het raadplegen van de certificaten;
- het raadplegen van de revocation status information (CRL's);
- het raadplegen van het CPS.

#45 :

Het intellectueel eigendomsrecht van de standaard moet vrijelijk beschikbaar zijn (geen royalty). Waaruit blijkt dat dit voor uw standaard het geval is?

Het Programma van Eisen PKI-overheid kan kosteloos worden benaderd en is gebaseerd op de volgende lijst van internationale open standaarden:

- 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?.

#46 :

Zijn er beperkingen voor hergebruik van de standaard?

Neen. In het Programma van Eisen van PKloverheid is geen voorbehoud gemaakt m.b.t. het auteursrecht. In beginsel kunnen derden het Programma van Eisen PKloverheid verder openbaarmaken of verveelvoudigen zonder dat dat als inbreuk op het auteursrecht wordt beschouwd. Overigens zullen derden dit wel met in achtneming van bronvermelding moeten doen.

Het is voor elke partij mogelijk om het Programma van Eisen PKloverheid als standaard volledig te implementeren. Een partij kan echter pas overgaan tot uitgifte van PKloverheid certificaten als zij een audit, met een positief resultaat, hebben ondergaan. Deze audit moet worden uitgevoerd door een onafhankelijke geaccrediteerde auditor. Na deze audit moet de betreffende partij dan, d.m.v. een sleutelceremonie, worden opgenomen in de PKloverheid hirarchie.

#47 :



Hoe worden besluiten genomen in de beheerorganisatie?

De Policy Authority (PA), o.a. verantwoordelijk voor ontwikkeling en beheer van het Programma van Eisen, en is defacto beslissingsbevoegd. De PA-rol is belegd bij de Directeur van GBO.Overheid, Steven Luitjens en is gedelegeerd aan het Hoofd Servicemanagement van GBO.Overheid, Hans Verweij. De PA wordt binnen GBO.Overheid ondersteund en geadviseerd door het Productteam PKloverheid. Het Productteam bereidt beslissingen voor. Beslispunten worden ter kennisname of advies besproken met aangesloten Certificate Service Providers tijdens het reguliere halfjaarlijkse CSP-overleg.

De PA is qua beleidsvorming en financiering afhankelijk van Dienstverlening Regeldruk en Informatiebeleid (DRI) van BZK.

#48 :

Welke organisaties hebben inspraak in de besluitvorming?
DRI en aangesloten CSP?s hebben inspraak in de besluitvorming.

#49 :

Is het mogelijk om zelf inspraak te krijgen in de ontwikkeling van de standaard?
Ja, aangesloten en aspirant-CSP?s kunnen inspraak krijgen in de ontwikkeling van de standaard.

#50 :

Welke standaarden concurreren met uw standaard?
De programma?s van eisen van commercile Certificate Service Providers. Deze programma?s van eisen bieden echter geen ruimte aan leveranciersafhankelijkheid, maar aan leveranciersafhankelijkheid. Het nadeel van de concurrerende standaarden is ook dat afnemende partijen steeds zelf de betrouwbaarheid moeten definiëren c.q. vaststellen.

#51 :

Wat zijn voorbeelden van implementaties van de standaard?
PKloverheid, Defensiepas en UZI-pas. De beveiliging van b.v. de websites van DigiD Burger, DigiD Machtigen en Mijnoverheid.

#52 :

Is het beheer van de standaard structureel geregeld?
Ja. Het beheer van de standaard is belegd bij GBO.Overheid, dat onderdeel uitmaakt van het Ministerie van Binnenlandse zaken en Koninkrijksrelaties.



#53 :

Welke impact (zowel positief als negatief) zou het opnemen van deze standaard als aanbevolen standaard hebben voor organisaties die deze standaard moeten invoeren? Denk hierbij aan technische, financile en organisatorische aspecten.

Voordelen:

- het Programma van Eisen is een volledig interoperabele open standaard;
- momenteel maken vier private CSP?s en twee publieke CSP?s gebruik van het Programma van Eisen;
- toekomstige CSP?s/afnemers kunnen leunen op de ervaringen van eerder aangesloten CSP?s/afnemers.

Nadelen:

- back-end applicaties moeten mogelijk compatibel worden gemaakt met deze standaard. Dit brengt voor een organisatie migratiekosten met zich mee.

#54 :

Welke andere organisatie(s) en/of expert(s) zou(den) betrokken kunnen worden bij de beoordeling van de standaard op grond van hun expertise of anderszins?

De private CSP?s DigiNotar, QuoVadis en Getronics (namens VeriSign) en publieke CSP?s (CIBG/UZI-register en Defensie). Vanuit ECP-EPN de voorzitter van het College van Belanghebbenden TTP.NL dhr Jans Sauer. Uit de wetenschap: Bart Jacobs Hoogleraar computerbeveiliging, in Nijmegen & Eindhoven.

#55 :

Wordt de standaard al voorgeschreven in wet en/of regelgeving? Zo ja, in welke wet of regelgeving
N.v.t.