# Aanbiedingsformulier

**Betreft**
Notitie adoptieafspraken open standaarden

**Contactpersoon**
Patrick Rinzema
patrick.rinzema@digicommissaris.nl
06-38825659

**Datum**
18 maart 2015

**Kenmerk**

**Bijlagen**
Notitie adoptieafspraken open standaarden

## Aanleiding

Het Forum Standaardisatie ziet verschillende aanleidingen (de resultaten van de monitor open standaarden 2014, de bevindingen van de commissie Elias en signalen van leveranciers) voor het maken van adoptieafspraken in het Nationaal Beraad rondom standaarden.

Het Digiprogramma staat over standaarden onder meer het volgende:
- "Daarom worden in de Regieraad Interconnectiviteit bindende adoptie afspraken met betrekking tot overheidsbrede standaarden gemaakt" (p.27);
- "(…) De Regieraad Interconnectiviteit stimuleert beleidsontwikkeling voor toezicht op, en juiste implementatie van standaarden en (verplicht) gebruik van voorzieningen. In een later stadium ziet de Regieraad ook toe op de daadwerkelijke uitvoering van het ontwikkelde beleid." (p.28).

In onderliggende notitie van het Forum Standaardisatie staat een voorstel (onder C) om:
C-1 *aanvullende (meetbare) adoptieafspraken te maken omtrent informatieveiligheid-standaarden;* en
C-2 *de bestaande overheidsbrede 'pas toe of leg uit'-afspraak te herbevestigen en daarmee te verlengen tot eind 2017.*

Ad. C-1 *meetbare adoptieafspraken*
Het voorstel is om - naast de reeds geldende 'pas toe of leg uit' afspraken – rondom een paar standaarden van de lijst automatisch meetbare adoptieafspraken te maken over het gebruik.

De keuze voor de voorgestelde standaarden rond informatieveiligheid is gemaakt omdat:
- een betrouwbare GDI van belang is voor het vertrouwen van burgers en bedrijven in de (elektronische) overheid;
- de standaarden bestuurlijk goed uit te leggen zijn;
- de kosten van de implementatie van voorgestelde standaarden te overzien zijn.

Voor de brede adoptie van deze standaarden is de adoptiekracht van het Nationaal Beraad onontbeerlijk. Het zijn immers de partijen uit het Nationaal Beraad die verantwoordelijk zijn voor de dienstverlening aan burgers en bedrijven, en voor de adoptie van deze standaarden bij hun organisaties.

## De regieraad Interconnectiviteit wordt gevraagd:

1. in te stemmen met bijgaande voorstellen (C-1 en C-2), of anders aan te geven welke planning of standaarden in de optiek van de regieraad haalbaar zijn;
2. te bespreken op welke wijze dit advies in het Nationaal Beraad wordt voorgelegd (ter bespreking of als hamerstuk?);
3. te overleggen op welke wijze ervoor kan worden gezorgd dat de afspraken ook daadwerkelijk worden uitgevoerd. Bijvoorbeeld door een adoptiegroepje rond deze standaardenafspraak te vormen onder de regieraad. Daar kan dan ook de kennis van succesvolle implementaties van deze standaarden worden hergebruikt (onder meer bij de Belastingdienst, DigiD, MijnOverheid, gemeenten Heerlen en Den Bosch (DKIM) en het ministerie van AZ /DPC en SSC-ICT (DNSSEC)).

# notitie

## Van: Forum Standaardisatie
## Aan: regieraad Interconnectiviteit

**A. Aanleiding**

Het Forum Standaardisatie monitort jaarlijks de naleving van de afspraken over adoptie van open standaarden door overheden. Uit de Monitor Open Standaarden 2014[1] blijkt dat de adoptie van open standaarden in de centrale e-overheids-voorzieningen van de GDI redelijk op orde is. Voor het derde jaar op rij blijkt evenwel dat in meer dan de helft van de ICT-aanbestedingen ten onrechte niet naar de relevante open standaarden wordt gevraagd. De parlementaire commissie ICT-projecten (commissie Elias) beveelt aan dat er daadwerkelijk wordt toegezien op de naleving van het 'pas toe of leg uit'-beleid rondom open standaarden (aanbeveling negen)[2]. Daarnaast signaleren ook leveranciers dat de overheid – ook nu ze de open standaarden in hun producten aanbieden - niet om de standaarden vraagt.

In het Nationaal Beraad van 10 februari is daarom aangekondigd dat het Forum Standaardisatie in mei 2015 – in afstemming met de regieraad Interconnectiviteit – een uitgewerkt advies (ter besluitvorming) zal uitbrengen aan het Nationaal Beraad.

**B. Digicommissaris erkent belang standaarden in Digiprogramma**

Het essentieel belang van standaardisatie en standaarden voor de GDI, wordt expliciet onderkend door de Digicommissaris. In het Digiprogramma[3] schrijft hij:

- p.26: ' Zonder (…) standaarden kan er geen eOverheid zijn. De (...) standaarden zijn dus vitaal voor de BV Nederland.';
- p.27: 'Daarom worden in de Regieraad Interconnectiviteit bindende adoptie afspraken met betrekking tot overheidsbrede standaarden gemaakt';
- 'Prioriteit 3: meer en beter gebruik standaarden inclusief (…)adoptie afspraken';
- P. 28: 'Een aantal standaarden ('pas toe of leg uit'-lijst) en voorzieningen is voor de overheid verplicht. Het toezicht op juistheid van standaarden en de adoptie/implementatie van standaarden of (verplicht) gebruik van voorzieningen is nog niet goed geregeld. De Regieraad Interconnectiviteit stimuleert beleidsontwikkeling voor toezicht op, en juiste implementatie van standaarden en (verplicht) gebruik van voorzieningen. In een later stadium ziet de Regieraad ook toe op de daadwerkelijke uitvoering van het ontwikkelde beleid.'

[1] *Monitor Open Standaarden beleid, https://www.forumstandaardisatie.nl/open-standaarden/beleid-en-monitoring/*
[2] *Rapport Commissie Elias, 'Parlementair onderzoek naar ICT-projecten bij de overheid', https://zoek.officielebekendmakingen.nl/dossier/33326/kst-33326-5*
[3] *Zie bijlage FS 150225.3C2 (Standaarden in) Digiprogramma versie 1.0, en voor de volledige tekst: http://www.digicommissaris.nl/files/2015-01/20150210_03b_01_Oplegger_en_Digiprogramma.pdf*

De positionering van de Digicommissaris en het Nationaal Beraad, inclusief de overheidsbrede samenstelling met beleid én uitvoering op hoogambtelijk niveau, biedt grote doorzettingsmacht en implementatiekracht, en daarmee een uitzonderlijke kans om de daadwerkelijke adoptie en het gebruik van de standaarden van de 'pas toe of leg uit'-lijst verder te brengen.



## C. Uitgewerkt advies

***C-1.*** *Aanvullende adoptieafspraken standaarden informatieveiligheid*
Om de doelstellingen van Digitaal 2017 te verwezenlijken is het ondermeer noodzakelijk ervoor te zorgen dat burgers en bedrijven vertrouwen hebben en houden in de Digitale overheid.

Om dat te laten welslagen is nodig dat de informatieveiligheid op orde is. Burgers en bedrijven moeten er op kunnen rekenen dat een website of e-mail daadwerkelijk van de overheid is, voordat ze erop inloggen en betaal en/of persoonsgegevens prijs geven. Het gebeurt nu nog te vaak dat mensen in *Phishing*-mails en nepsites trappen. Dat kan worden voorkomen door het gebruik van standaarden die de echtheid van overheidswebsites en overheidsmail zichtbaar maken (TLS, DKIM/DMARC en DNSSEC).

Het is evenwel cruciaal dat deze standaarden door ***alle*** overheidsorganisaties worden toegepast. Want net als bij echtheidskenmerken van papiergeld (het watermerk) is het zinloos indien het echtheidskenmerk is opgenomen bij 60% van de echte bankbiljetten. Je hebt er pas echt wat aan, als je ervan uit kunt gaan dat in elk écht bankbiljet een watermerk zit. Dat geldt ook voor de echtheidskenmerken van websites. Banken begrijpen dat, en daarom hebben ook al hun websites dezelfde echtheidskenmerken (o.a. 'het slotje' zie www.veiligbankieren.nl). Dit beginsel van eenduidigheid geldt ook voor de overheid: ook een overheidswebsite moet je telkens op eenzelfde manier als echt kunnen herkennen.

Daarom is het voorstel in het Digiprogramma rondom de volgende set standaarden aanvullende adoptieafspraken te maken:

*Betrouwbare overheid: standaarden informatieveiligheid*
Eind 2016 heeft de overheid als geheel op orde dat burgers en bedrijven haar websites en e-mails op een eenduidige wijze als echte overheidswebsite kunnen herkennen.
Meer specifiek: dat doet de overheid door adoptie van de volgende standaarden:

| Standaard | Adoptieafspraken en fasering (meetbaar resultaat) |
|---|---|
| TLS:<br>het slotje op een website | - eind 2015 zijn alle (transactie) websites en voorzieningen van de GDI van een echtheidskenmerk voorzien (TLS), en<br>- eind 2016 alle overheidswebsites met transacties/persoonsgegevens |
| DKIM/DMARC:<br>anti-email-phishing | - eind 2015 zijn alle domeinnamen[4] van de GDI voorzien van DKIM/DMARC, en<br>- eind 2016 alle overheidsdomeinen |

[4] *Van belang is niet zozeer òf de voorzieningen zélf daadwerkelijk gebruik maken van e-mail, maar of fraudeurs de goede naam van die voorzieningen kunnen misbruiken bij het hengelen naar inlog- en betalingsgegevens.*

| | |
|---|---|
| DNSSEC:<br>betrouwbare<br>'internetbewegwijzering' | - eind 2015 zijn alle domeinnamen van de GDI voorzien van DKIM/DMARC, en<br>- eind 2016 alle overheidsdomeinen |

**Datum**
**13 maart 2014**

Nota bene:
Deze standaarden staan allemaal al op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie. Dat blijft gehandhaafd, net zoals het 'pas toe of leg uit'-regime voor de overige standaarden op de lijst (dat ook voor de GDI-voorzieningen geldt). Het voorstel aan het Nationaal Beraad is om, ten aanzien van de hierboven genoemde standaarden, niet meer alleen te sturen op aanbesteding, maar te concretiseren waar de overheid eind 2016 qua (meetbaar) gebruik van deze standaarden wil staan.

Immers, de combinatie van:
a) de koppeling aan het moment van een ICT investering (die soms maar eens per zes jaar voorkomt),
b) de relatieve vrijblijvendheid (leg uit blijft immers mogelijk) en
c) het feit dat in 60% van de verwervingen dan nog niet om de standaard wordt gevraagd,

leidt momenteel tot achterblijvende adoptie, en afnemend vertrouwen van burgers en bedrijven in de elektronische overheid[5].

Het voorstel is om het op dit moment bij deze standaarden te houden. Later dit jaar of volgend jaar kunnen desgewenst meetbare adoptieafspraken over andere (groepen van) standaarden worden gemaakt, of een standaard voor informatieveiligheid worden toegevoegd. Momenteel wordt bijvoorbeeld onderzocht of er afspraken kunnen worden gemaakt over de standaard ISO27001/2 (standaard op het gebied van informatieveiligheidsmanagement, vertaald in BIG, BIR, BIWA, IBO).

***C-2.*** *Herbevestiging van overheidsbrede 'pas toe of leg uit'-afspraak*
'Pas toe of leg uit' betekent dat overheden bij aanschaf van ICT moeten kiezen voor de relevante open standaarden van de zogeheten 'pas toe of leg uit'-lijst. Afwijken mag alleen bij zwaarwegende reden en hierover moet via het jaarverslag worden verantwoord. Voor het Rijk is het 'pas toe of leg uit'-principe vastgelegd in een Rijksinstructie.[6] De 'pas toe of leg uit'-afspraak voor decentrale overheden komt terug in resultaatverplichting nr. 20 van i-NUP en in bestuursakkoorden.[7]

Hoewel iNUP per 31-12-2014 is afgelopen, bestaat formeel nog tot eind 2015 een formele basis voor overheidsbrede 'pas toe of leg uit'[8]. Het ligt evenwel voor de hand om deze afspraak op dit moment - in het Digiprogramma - te herbevestigen en daarmee te verlengen tot eind 2017: "Gemeenten, provincies, rijk en waterschappen maken gebruik van de open standaarden zoals vastgesteld door het Nationaal Beraad en werken hierbij volgens het principe 'pas toe of leg uit'[9]".

[5] *Zie bijlage hieronder.*
[6] *'Instructie rijksdienst bij aanschaf ICT-diensten of ICT-producten', https://zoek.officielebekendmakingen.nl/stcrt-2008-837.html*
[7] *'Pas toe of leg uit'-regime, https://www.forumstandaardisatie.nl/open-standaarden/voor-overheden/pas-toe-of-leg-uit-regime/*
[8] *Namelijk via het Bestuursakkoord 2011-2015 (zie: https://zoek.officielebekendmakingen.nl/kst-32749-1.html). Daarin staat: "Standaarden die zijn vastgesteld door het College standaardisatie dienen door alle overheidsorganen te worden toegepast volgens het principe 'pas toe of leg uit waarom niet'."*
[9] *Zoals vastgelegd in de eerdergenoemde Rijksinstructie.*

Bijlage: voorbeelden van afnemend vertrouwen als gevolg van phishing:

**Datum**
**13 maart 2014**

- https://www.waarschuwingsdienst.nl/Risicos/Actuele+dreigingen/Softwarelekken/WD-2014-007+Waarschuwing+phishing-e-mail+uit+naam+van+het+Centraal+Justitieel+Incassobureau+CJIB+in+omloop.html

- https://www.waarschuwingsdienst.nl/Risicos/Actuele+dreigingen/Virussen+en+wormen/WD-2013-014+Sterke+toename+in+nep+incasso+e-mails.html

- https://www.waarschuwingsdienst.nl/Risicos/Actuele+dreigingen/Virussen+en+wormen/WD-2013-020+Sterke+toename+in+spam+e-mail+die+van+de+Politie+lijkt+te+zijn.html

- http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/standaard_functies/prive/contact/andere_onderwerpen/phishing

- http://www.fraudehelpdesk.nl/nieuwsbericht/digid_tijdelijk_onbereikbaar_door_vereiste_verificatie