**Forum Standaardisatie**

Wilhelmina v Pruisenweg 104
2595 AN Den Haag
Postbus 84011
2508 AA Den Haag

www.forumstandaardisatie.nl

# notitie

Aanpassing functioneel toepassingsgebieden
Internet veiligheidstandaarden

## FORUM STANDAARDISATIE 11 oktober 2017

| | |
|---|---|
| **Agendapunt:** | FS 20171011.3E |
| **Bijlagen:** | Expertadvies functioneel toepassingsgebieden internet veiligheidstandaarden en overzicht reacties consultatieronde |
| **Aan:** | Forum Standaardisatie |
| **Van:** | Stuurgroep Standaardisatie |
| **Datum:** | 20 september 2017 |

**Aanleiding en achtergrond**
Van iedere verplichte standaard op de lijst met open standaarden is het functioneel toepassingsgebied omschreven. Dit functioneel toepassingsgebied bepaalt voor welke ICT-producten en -diensten een standaard relevant is en wanneer de standaard dus moet worden toegepast.

Niet alle functioneel toepassingsgebieden zijn even duidelijk omschreven. Dit kan adoptie van standaarden in de weg staan. Om deze reden zijn de huidige omschrijvingen geanalyseerd, zijn voorstellen gedaan voor nieuwe omschrijvingen en zijn instrumenten ontwikkeld om de omschrijvingen te helpen verduidelijken en uniformeren.

De voorgestelde omschrijvingen van de functioneel toepassingsgebieden van SPF, DKIM, DMARC, HTTPS en HSTS, TLS en DNSSEC zijn in procedure genomen. Dit zijn standaarden voor de beveiliging van internetverbindingen, websites en e-mail. Het gebruik ervan levert een belangrijke bijdrage aan de betrouwbaarheid van het Nederlandse internet. De standaarden worden genoemd in de memorie van toelichting bij de Wet GDI en in het Nationaal Beraad Digitale Overheid (hierna Nationaal Beraad) van 2 februari 2016 zijn aanvullende resultaatafspraken gemaakt over de adoptie van de standaarden.

**Betrokkenen en proces**
In opdracht van het Forum Standaardisatie heeft Verdonck, Klooster & Associates een onderzoek uitgevoerd naar de omschrijvingen van de functioneel toepassingsgebieden van de verplichte (‘pas toe of leg uit’) standaarden op de lijst met open standaarden. De resultaten van dit onderzoek zijn vastgelegd in een eindrapport, met daarin een analyse van de huidige omschrijvingen, voorstellen voor nieuwe omschrijvingen en instrumenten om de omschrijvingen te verduidelijken en te uniformeren.

Op basis van het onderzoek heeft het Forum Standaardisatie op 14 juni 2017 besloten de voorgestelde omschrijvingen van de functioneel toepassingsgebieden van de internet veiligheidstandaarden SPF, DKIM, DMARC, HTTPS en HSTS, TLS en DNSSEC in procedure te nemen. Hierop volgend is een expertgroep samengesteld en een voorzitter aangesteld.

De leden van de expertgroep hebben voorafgaand aan de expertbijeenkomst het onderzoeksrapport ontvangen en zijn in de gelegenheid gesteld om dit rapport door te nemen en aandachtspunten te identificeren.

De expertgroep is op 6 juli 2017 bijeengekomen om de voorgestelde omschrijvingen van de functioneel toepassingsgebieden te bespreken en verder te verduidelijken. Op basis hiervan is een concept expertadvies opgesteld en aan de leden van de expertgroep gestuurd met verzoek om commentaar. Na verwerking van de reacties uit de expertgroep is het rapport nogmaals toegestuurd aan de experts en afgerond.

Het Bureau Forum Standaardisatie (het secretariaat van het Forum Standaardisatie) heeft het expertadvies openbaar gemaakt ten behoeve van een publieke consultatie. Deze publieke consultatie heeft plaatsgevonden van 1 augustus 2017 tot en met 13 september 2017.

Gedurende de consultatieperiode is één reactie gegeven op het expertadvies. Het Bureau Forum Standaardisatie heeft deze reactie na afsluiting van de openbare consultatie gedeeld met de expertgroep. Met het expertadvies en de relevante inzichten uit de openbare consultatie is dit advies aan het Nationaal Beraad opgesteld.

**Consequenties en vervolgstappen**
Het Nationaal Beraad besluit met dit advies om de omschrijvingen van de functioneel toepassingsgebieden van de internet veiligheidstandaarden SPF, DKIM, DMARC, HTTPS en HSTS, TLS en DNSSEC wel of niet aan te passen op de lijst met open standaarden.

**Gevraagd besluit**

Het Forum Standaardisatie wordt gevraagd om in te stemmen met onderstaand advies:

Het Forum Standaardisatie adviseert het Nationaal Beraad om:
1. de omschrijving van het functioneel toepassingsgebied van SPF aan te passen op de lijst met open standaarden;
2. de omschrijving van het functioneel toepassingsgebied van DKIM aan te passen op de lijst met open standaarden;
3. de omschrijving van het functioneel toepassingsgebied van DMARC aan te passen op de lijst met open standaarden;
4. de omschrijving van het functioneel toepassingsgebied van HTTPS en HSTS aan te passen op de lijst met open standaarden;
5. de omschrijving van het functioneel toepassingsgebied van TLS aan te passen op de lijst met open standaarden;
6. de omschrijving van het functioneel toepassingsgebied van DNSSEC aan te passen op de lijst met open standaarden.

<u>Ad 1) Aanpassen van de omschrijving van het functioneel toepassingsgebied van SPF op de lijst met open standaarden</u>

Als functioneel toepassingsgebied voor SPF wordt geadviseerd:
*SPF moet worden toegepast op alle overheidsdomeinnamen, ook op domeinen waarvan niet wordt gemaild, én op alle mailservers waarmee de overheid e-mail ontvangt.*

Ad 2) Aanpassen van de omschrijving van het functioneel toepassingsgebied van DKIM op de lijst met open standaarden
Als functioneel toepassingsgebied voor DKIM wordt geadviseerd:
*DKIM moet worden toegepast op alle overheidsdomeinnamen waarvandaan wordt gemaild én op alle mailservers waarmee de overheid e-mail verstuurt en ontvangt.*

Ad 3) Aanpassen van de omschrijving van het functioneel toepassingsgebied van DMARC op de lijst met open standaarden
Als functioneel toepassingsgebied voor DMARC wordt geadviseerd:
*DMARC moet worden toegepast op alle overheidsdomeinnamen, ook op domeinen waarvan niet wordt gemaild, én op alle mailservers waarmee de overheid e-mail ontvangt.*

Ad 4) Aanpassen van de omschrijving van het functioneel toepassingsgebied van HTTPS en HSTS op de lijst met open standaarden
Als functioneel toepassingsgebied voor HTTPS en HSTS wordt geadviseerd:
*HTTPS en HSTS moeten worden toegepast op de communicatie tussen clients (zoals webbrowsers) en servers voor alle websites en webservices.*

Ad 5) Aanpassen van de omschrijving van het functioneel toepassingsgebied van TLS op de lijst met open standaarden
Als functioneel toepassingsgebied voor TLS wordt geadviseerd:
*TLS moet worden toegepast op de uitwisseling van gegevens tussen clients en servers, inclusief machine-to-machine communicatie.*

Ad 6) Aanpassen van de omschrijving van het functioneel toepassingsgebied van DNSSEC op de lijst met open standaarden
Als functioneel toepassingsgebied voor DNSSEC wordt geadviseerd:
*DNSSEC moet worden toegepast op alle overheidsdomeinnamen én op DNS-resolvers die clients van overheidsorganisaties direct of indirect van DNS-antwoorden voorzien.*

**Toelichting**

1. Waar gaat het inhoudelijk over?
SPF, DKIM, DMARC, HTTPS en HSTS, TLS en DNSSEC zijn standaarden voor de beveiliging van internetverbindingen, websites en e-mail. Het gebruik ervan levert een belangrijke bijdrage aan de betrouwbaarheid van het Nederlandse internet. De standaarden worden genoemd in de memorie van toelichting bij de Wet GDI en in het Nationaal Beraad van 2 februari 2016 zijn aanvullende resultaatafspraken gemaakt over de adoptie van de standaarden.

2. Hoe is het proces verlopen?
In opdracht van het Forum Standaardisatie heeft Verdonck, Klooster & Associates een onderzoek uitgevoerd naar de omschrijvingen van de functioneel toepassingsgebieden van de verplichte (‘pas toe of leg uit’) standaarden op de lijst met open standaarden. De resultaten van dit onderzoek zijn vastgelegd in een eindrapport, met daarin een analyse van de huidige omschrijvingen, voorstellen voor nieuwe omschrijvingen en instrumenten om omschrijvingen te verduidelijken en te uniformeren.

Op basis van het onderzoek heeft het Forum Standaardisatie op 14 juni 2017 besloten de voorgestelde omschrijvingen van de functioneel toepassingsgebieden van de internet veiligheidstandaarden SPF, DKIM, DMARC, HTTPS en HSTS, TLS en DNSSEC in procedure te nemen. Hierop volgend is een expertgroep samengesteld en een voorzitter aangesteld.

De leden van de expertgroep hebben voorafgaand aan de expertbijeenkomst het onderzoeksrapport ontvangen en zijn in de gelegenheid gesteld om dit rapport door te nemen en aandachtspunten te identificeren.

De expertgroep is op 6 juli 2017 bijeengekomen om de voorgestelde omschrijvingen van de functioneel toepassingsgebieden te bespreken en verder te verduidelijken. Op basis hiervan is een concept expertadvies opgesteld en aan de leden van de expertgroep gestuurd met verzoek om commentaar. Na verwerking van de reacties uit de expertgroep is het rapport nogmaals toegestuurd aan de experts en afgerond.

Het Bureau Forum Standaardisatie (het secretariaat van het Forum Standaardisatie) heeft het expertadvies openbaar gemaakt ten behoeve van een publieke consultatie. Deze publieke consultatie heeft plaatsgevonden van 1 augustus 2017 tot en met 13 september 2017.

Gedurende de consultatieperiode is één reactie gegeven op het expertadvies. Het Bureau Forum Standaardisatie heeft deze reactie na afsluiting van de openbare consultatie gedeeld met de expertgroep.

Met het expertadvies en de relevante inzichten uit de openbare consultatie is dit advies aan het Nationaal Beraad opgesteld.

## 3. Wat is de conclusie van de expertgroep en de consultatie?

*Conclusie van de expertgroep*
De expertgroep adviseert het Forum Standaardisatie en het Nationaal Beraad om:

1. de omschrijving van het functioneel toepassingsgebied van SPF aan te passen op de lijst met open standaarden;
2. de omschrijving van het functioneel toepassingsgebied van DKIM aan te passen op de lijst met open standaarden;
3. de omschrijving van het functioneel toepassingsgebied van DMARC aan te passen op de lijst met open standaarden;
4. de omschrijving van het functioneel toepassingsgebied van HTTPS en HSTS aan te passen op de lijst met open standaarden;
5. de omschrijving van het functioneel toepassingsgebied van TLS aan te passen op de lijst met open standaarden;
6. de omschrijving van het functioneel toepassingsgebied van DNSSEC aan te passen op de lijst met open standaarden.

### Ad 1) Aanpassen van de omschrijving van het functioneel toepassingsgebied van SPF op de lijst met open standaarden

Als functioneel toepassingsgebied voor SPF wordt geadviseerd:
*SPF moet worden toegepast op alle overheidsdomeinnamen, ook op domeinen waarvan niet wordt gemaild, én op alle mailservers waarmee de overheid e-mail ontvangt.*

De expertgroep maakt de (algemene) kanttekening dat de lijst met open standaarden ook informatie moet bieden over de manier waarop SPF en de andere internet veiligheidstandaarden moeten worden toegepast (het 'hoe'). De lijst zou bijvoorbeeld duidelijk moeten maken dat de toepassing van SPF zonder beperking

van de toegestane mailverzenders (zoals bij gebruik van het '+all'-mechanisme in het SPF record) weinig beveiligingswaarde heeft. Hiertoe zou ook verwezen kunnen worden naar richtlijnen van het NCSC. Deze informatie dient direct te relateren te zijn aan (delen van) het functioneel toepassingsgebied. Deze informatie hoort echter niet thuis in de omschrijving van het functioneel toepassingsgebied (het 'wanneer'). De lijst met open standaarden kent hiervoor andere velden, zoals 'Hulpmiddelen' en 'Community en Organisaties' (beide onder 'Implementatie'). Deze velden hebben bovendien als voordeel dat zij zonder voorafgaande procedure kunnen worden aangepast. Een mogelijkheid is om in toekomstige procedures met toekomstige expertgroepen expliciet bij deze velden stil te staan.

De expertgroep maakt de (algemene) kanttekening dat de lijst met open standaarden ook informatie moet bieden over het doel waarmee SPF en de andere internet veiligheidstandaarden moeten worden toegepast (het 'waarom'). Een voorbeeld van een dergelijk gebruiksdoel is het verifiëren van de identiteit van de verzender. Ook deze informatie hoort niet thuis in de omschrijving van het functioneel toepassingsgebied. De lijst met open standaarden kent hiervoor de velden 'Nut' en 'Werking' (beide onder 'Uitleg'). Ook hier geldt dat deze velden zonder voorafgaande procedure kunnen worden aangepast en dat in toekomstige procedures met toekomstige expertgroepen expliciet bij deze velden kan worden stilgestaan.

De expertgroep maakt de (algemene) kanttekening dat overheidsorganisaties onderling ook gegevens uitwisselen via besloten (overheids)netwerken. Door hun besloten karakter zijn deze netwerken veiliger dan het open internet. Als een organisatie er om deze reden voor kiest om SPF of een andere internet veiligheidstandaard met 'pas toe of leg uit'-verplichting niet toe te passen, dan dient zij dit gemotiveerd aan te geven in haar jaarverslag ('leg uit').

<u>Ad 2) Aanpassen van de omschrijving van het functioneel toepassingsgebied van DKIM op de lijst met open standaarden</u>
Als functioneel toepassingsgebied voor DKIM wordt geadviseerd:
*DKIM moet worden toegepast op alle overheidsdomeinnamen waarvandaan wordt gemaild én op alle mailservers waarmee de overheid e-mail verstuurt en ontvangt.*

De expertgroep maakt geen (nieuwe) kanttekeningen bij het functioneel toepassingsgebied van DKIM.

<u>Ad 3) Aanpassen van de omschrijving van het functioneel toepassingsgebied van DMARC op de lijst met open standaarden</u>
Als functioneel toepassingsgebied voor DMARC wordt geadviseerd:
*DMARC moet worden toegepast op alle overheidsdomeinnamen, ook op domeinen waarvan niet wordt gemaild, én op alle mailservers waarmee de overheid e-mail ontvangt.*

De expertgroep maakt de kanttekening dat DMARC nog niet is opgenomen op de lijst met open standaarden, omdat deze standaard formeel nog in beheer moet worden genomen door IETF. Ook is er discussie over de geschiktheid van DMARC voor brede toepassing. Met name domeinen waarop veel met e-mailverspreidingslijsten wordt gewerkt, kunnen problemen krijgen indien DMARC wordt toegepast. Het ARC-protocol (zie http://arc-spec.org) moet dit gaan oplossen. Aan de standaardisatie hiervan wordt nog hard gewerkt. Het expertadvies betreft alleen de omschrijving van het functioneel toepassingsgebied van DMARC, niet de beantwoording van de vraag of deze standaard wel of niet moet worden opgenomen op de lijst met open standaarden.

Ad 4) Aanpassen van de omschrijving van het functioneel toepassingsgebied van HTTPS en HSTS op de lijst met open standaarden
Als functioneel toepassingsgebied voor HTTPS en HSTS wordt geadviseerd:
*HTTPS en HSTS moeten worden toegepast op de communicatie tussen clients (zoals webbrowsers) en servers voor alle websites en webservices.*

De expertgroep maakt de kanttekening dat in deze omschrijving van het functioneel toepassingsgebied de begrippen 'clients' en 'servers' niet specifiek genoeg zijn. De expertgroep adviseert daarom om bij de omschrijving een duidelijke en (context)specifieke verklaring van deze begrippen op te nemen.

Ad 5) Aanpassen van de omschrijving van het functioneel toepassingsgebied van TLS op de lijst met open standaarden
Als functioneel toepassingsgebied voor TLS wordt geadviseerd:
*TLS moet worden toegepast op de uitwisseling van gegevens tussen clients en servers, inclusief machine-to-machine communicatie.*

De expertgroep maakt de kanttekening dat met TLS op applicatieniveau kan worden vastgesteld of een verbinding met voldoende beveiliging is opgebouwd. Daarmee biedt TLS een signaleringsfunctie, die applicaties in staat stelt om gebruikers te waarschuwen voor onvoldoende beveiliging of om automatisch de verbinding te verbreken indien deze onvoldoende beveiligd is. Bij versleuteling op de IP laag (met bijvoorbeeld IPsec, een aanbevolen standaard) is deze signaalfunctie richting applicaties niet aanwezig. Er zijn dus alternatieven voor versleuteling met TLS, maar deze zijn niet altijd gelijkwaardig.

Voorts maakt de expertgroep de kanttekening dat er een standaard is voor DNS over TLS (die niet op de 'pas toe of leg uit' lijst staat). Deze standaard waarborgt de authenticiteit, integriteit en vertrouwelijkheid van DNS-verkeer. DNSSEC, een internet veiligheidstandaard met 'pas toe of leg uit'-verplichting voor DNS-verkeer (zie onder), waarborgt alleen authenticiteit en integriteit. DNS over TLS is echter niet bedoeld om DNSSEC te vervangen. Dit probleem met de omschrijving van het functioneel toepassingsgebied zou ook kunnen gaan spelen bij andere, toekomstige protocolontwikkelingen. De 'leg uit'-verplichting biedt hier uitkomst en kan aanleiding zijn om nieuwe standaarden aan te dragen voor opname op de lijst met open standaarden.

Ad 6) Aanpassen van de omschrijving van het functioneel toepassingsgebied van DNSSEC op de lijst met open standaarden
Als functioneel toepassingsgebied voor DNSSEC wordt geadviseerd:
*DNSSEC moet worden toegepast op alle overheidsdomeinnamen én op DNS-resolvers die clients van overheidsorganisaties direct of indirect van DNS-antwoorden voorzien.*

De expertgroep maakt de kanttekening dat met deze omschrijving van het functioneel toepassingsgebied ook resolvers van derde partijen waarvan de overheid gebruik maakt DNSSEC moeten gebruiken.

De expertgroep maakt de kanttekening dat de lijst met open standaarden duidelijk moet maken dat validatie plaats moet vinden op een vertrouwd netwerk. Bij gebruik van DNSSEC op publieke resolvers, zoals die van internet serviceproviders, gaan gevalideerde antwoorden alsnog onbeveiligd over het internet voordat deze door clients worden gebruikt. Deze informatie over de toepassing van de standaard hoort niet thuis in de omschrijving van het functioneel toepassingsgebied. De lijst met open standaarden kent hiervoor andere velden.

*Eventuele aanvullingen vanuit de consultatie*

Op de openbare consultatie van het expertadvies is een reactie ontvangen van Networking4all. Deze reactie wordt in het onderstaande samengevat en behandeld.

Ad 1) Aanpassen van de omschrijving van het functioneel toepassingsgebied van SPF op de lijst met open standaarden
Networking4all onderschrijft de (algemene) kanttekening van de expertgroep dat de lijst met open standaarden ook informatie moet bieden over de manier waarop SPF en de andere internet veiligheidstandaarden moeten worden toegepast (het 'hoe'). Ook de suggestie van de expertgroep om te verwijzen naar (nog op te stellen) richtlijnen van het NCSC voor het maken van een SPF record wordt door Networking4all onderschreven. In aanvulling op het gebruik van het '+all'-mechanisme, waarschuwt Networking4all voor het gebruik van het 'ptr'-mechanisme in een SPF record. Verder wijst zij erop dat SPF nadelen heeft bij het doorsturen (forwarden) van e-mailberichten.
**Reactie:** De reactie gaat vooral in op de implementatie van de standaard(en) en niet zozeer op het toepassingsgebied ervan.

Ad 2) Aanpassen van de omschrijving van het functioneel toepassingsgebied van DKIM op de lijst met open standaarden
Networking4all onderschrijft het gebruik van DKIM en wijst ook hier op het belang van een goede implementatie van de standaard.
**Reactie:** De reactie gaat vooral in op de implementatie van de standaard en niet zozeer op het toepassingsgebied ervan.

Ad 3) Aanpassen van de omschrijving van het functioneel toepassingsgebied van DMARC op de lijst met open standaarden
Networking4all onderschrijft het gebruik van DMARC en wijst, net als de expertgroep, op het ARC-protocol, dat problemen met DMARC moet gaan oplossen. Verder roept zij op om de valkuilen van DMARC, DKIM en SPF te verduidelijken.
**Reactie:** De reactie gaat vooral in op de implementatie van de standaard(en) en niet zozeer op het toepassingsgebied ervan.

Ad 4) Aanpassen van de omschrijving van het functioneel toepassingsgebied van HTTPS en HSTS op de lijst met open standaarden
De begrippen 'clients' en 'servers' mogen van Networking4all, net als van de expertgroep, worden verduidelijkt.
**Reactie:** De expertgroep adviseert om bij de omschrijving van het functioneel toepassingsgebied een duidelijke en (context)specifieke verklaring van deze begrippen op te nemen.

Ad 5) Aanpassen van de omschrijving van het functioneel toepassingsgebied van TLS op de lijst met open standaarden
Networking4all onderschrijft het gebruik van TLS. Verder waarschuwt zij voor het (onjuiste) gebruik van de alternatieve of gerelateerde standaarden IPsec en DNS over TLS, die ook door de expertgroep zijn genoemd.
**Reactie:** De reactie gaat niet zozeer in op het toepassingsgebied van TLS.

Ad 6) Aanpassen van de omschrijving van het functioneel toepassingsgebied van DNSSEC op de lijst met open standaarden
Networking4all onderschrijft het gebruik van DNSSEC. Verder merkt zij op dat niet iedereen vanzelfsprekend gebruik maakt van deze standaard.

Resterende inhoudelijke opmerkingen
Networking4all onderschrijft het gebruik van standaarden als SPF, DKIM, DMARC, HTTPS en HSTS, TLS en DNSSEC en stimulering hiervan door de overheid. Aandacht voor een goede implementatie en toepassing is hierbij volgens haar ook

nodig. Verder stelt zij voor om aankomende alternatieve of gerelateerde standaarden zoals ARC op een roadmap of iets dergelijks te zetten.

**Bijlage**

- Expertadvies functioneel toepassingsgebieden internet veiligheidstandaarden.
- Overzicht reacties consultatieronde