FS-20150610.02F

Forum Standaardisatie

Aanvullend onderzoek beoordeling SPF bij Forumadvies DMARC en SPF – addendum bij Forumadvies DMARC en SPF

Datum 29 april 2015

FS-20150610.02F

Colofon

Projectnaam	Aanvullend onderzoek beoordeling SPF aan toetsingscriteria open standaarden
Versienummer	1.0
Locatie	Den Haag
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag forumstandaardisatie@logius.nl
Auteur	Onno de Kamper

FS-20150610.02F

Inhoud

Advies & Managementsamenvatting

Advies aan het Forum
Aan de hand van onderliggend aanvullend onderzoek wordt geconcludeerd dat SPF voldoet aan de toetsingscriteria. Hiermee wordt voldaan aan de voorwaarde die de expertgroep DMARC stelt aan de opname van SPF op de 'pas toe of leg uit'-lijst. SPF kan samen met DKIM en DMARC (die in procedure van toelating op de 'pas toe of leg uit'-lijst is) de adoptie van een complete set van e-mailbeveiligingsstandaarden bevorderen.

Hoe is het advies tot stand gekomen?
Gedurende de toetsingsprocedure voor DMARC is gebleken dat er een nauwe relatie bestaat tussen de standaard en SPF. Uit de expertgroepsessie DMARC is gebleken dat experts tevens voorstander zijn van toepassing SPF, mits deze zou voldoen aan de toetsingscriteria. In de reacties van de openbare consultatie is geen reden gezien om dit expertadvies te herzien of om aanvullende adviezen te geven. Conform het expertadvies is SPF beoordeeld aan de hand van de toetsingscriteria. Het resultaat van deze toetsing is weergegeven in dit advies.

Hoe scoort de standaard op de toetsingscriteria?

<u>Toegevoegde waarde</u>
Met SPF kan de e-mailverzender geauthenticeerd worden, door te controleren of een apparaat dat e-mail verstuurt e-mail mag versturen voor een bepaalde domeinnaam. SPF is met name relevant voor (semi-)overheidsorganisaties waarvan het essentieel is dat burgers e-mails van deze afzenders vertrouwen, met als doel te voorkomen dat burgers, bedrijven en andere (semi-)overheidsorganisaties ongeauthenticeerde (valse) e-mails ontvangen. Via deze e-mails kunnen gevoelige gegevens zoals creditcardnummers of inloggegevens voor DigiD en het eHerkenning worden ontfutseld (zogenaamde phishing). Dit kan niet alleen leiden tot kosten voor burgers en bedrijven die in deze nep e-mails trappen. Het is ook schadelijk voor de 'merknaam' van het domein en het vertrouwen in de overheid.

Als grootste nadeel van SPF wordt genoemd dat SPF als op zichzelf staande standaard (zonder DMARC en/of DKIM) te weinig nauwkeurig is en teveel 'false positives' oplevert. Dit zijn e-mails die onterecht geweigerd worden. Dit komt voornamelijk voor bij het forwarden van e-mail, waarbij SPF van de uiteindelijke ontvanger op het afzenderadres van de tussenliggende provider controleert, en niet op het afzenderadres van de oorspronkelijke zender. Men kan SPF wel configureren als 'soft fail', zodat deze mails wel doorlaat maar markeert als spam.

Als op zichzelf staande standaard biedt SPF zodoende geringe bescherming, alhoewel SPF inmiddels wel een bekende 'best practice' genoemd kan worden. De werkelijke toegevoegde waarde van SPF zit voornamelijk in de complementaire werking in combinatie met de standaard DMARC en de reeds op de 'pas toe of leg uit'-lijst opgenomen standaard DKIM.
Geconcludeerd wordt dat SPF voldoende toegevoegde waarde heeft binnen het gekozen functioneel toepassingsgebied en organisatorisch werkingsgebied.

Open standaardisatieproces
SPF is in beheer bij IETF, een internationale standaardisatieorganisatie. IETF heeft naast SPF ook de standaard DKIM in beheer en voert op dit moment een opnameprocedure voor DMARC.
SPF is vrij implementeerbaar te gebruiken. Documentatie over het ontwikkel- en beheerproces van IETF is gratis te downloaden op de website van IETF. Belanghebbenden kunnen zich ook kosteloos aanmelden voor de verschillende groepen die werken aan de (door)ontwikkeling van standaarden die bij IETF in beheer zijn.
Geconcludeerd wordt dat het standaardisatieproces van IETF voldoende open is.

Draagvlak
SPF wordt op dit moment door verscheidene en diverse (semi-)overheidsorganisaties gebruikt. Met name overheidsorganisaties die als betrouwbaar ervaren worden door burgers en die veel reputatieschade kunnen ondervinden bij spoofing (misbruik van domeinnaam door anderen) zoals de Belastingdienst, ministeries, inspectiediensten, en tevens een significant aantal (121) gemeenten hebben SPF al als standaard geïmplementeerd. Op dit moment gebruiken bijvoorbeeld gemeenten Heerlen, Den Bosch en verscheidene domeinen die vallen onder de Rijksoverheid (attendering.rijksoverheid.nl, persbericht.rijksoverheid.nl) DMARC in combinatie met SPF en DKIM. Veel overheidsinstellingen zijn momenteel DMARC aan het invoeren (‘under construction’) en hebben reeds SPF ingevoerd (en soms ook DKIM). Bijvoorbeeld de Belastingdienst, Ministerie van Binnenlandse Zaken, Ministerie van Infrastructuur en Milieu, Inspectie SZW, Platform Internetstandaarden en diverse gemeenten. Toekomstige gebruikers kunnen hierbij rekenen op voldoende marktondersteuning voor de implementatie en bij het gebruik van de standaard.

Opname bevordert adoptie
Opname van de standaard op de ‘pas toe of leg uit’-lijst is een passend middel om een bredere adoptie van de standaard binnen de (semi)overheid te bevorderen. Het gebruik van de standaard is nog niet in alle gevallen vanzelfsprekend.

SPF vormt een feitelijke drie-eenheid met DMARC en DKIM. DKIM is sinds 2012 opgenomen op de ‘pas toe of leg uit’-lijst. Door zowel SPF als DMARC toe te voegen aan de ‘pas toe of leg uit’-lijst versterkt het belang van deze drie-eenheid van e-mailbeveiligingsstandaarden. Of een domeinnaam voldoet aan deze drie standaarden kan via www.internet.nl worden getoetst.

1 Achtergrond van aanvullend onderzoek SPF

1.1 Doelstelling aanvullend onderzoek SPF

Doel van dit advies is om vast te stellen of SPF voldoet aan de toetsingscriteria open standaarden. Hiermee wordt invulling gegeven aan het Forumadvies DMARC en SPF, waarbij als voorwaarde voor opname van SPF op de 'pas toe of leg uit'-lijst is gesteld dat de standaard moet voldoen aan de toetsingscriteria.

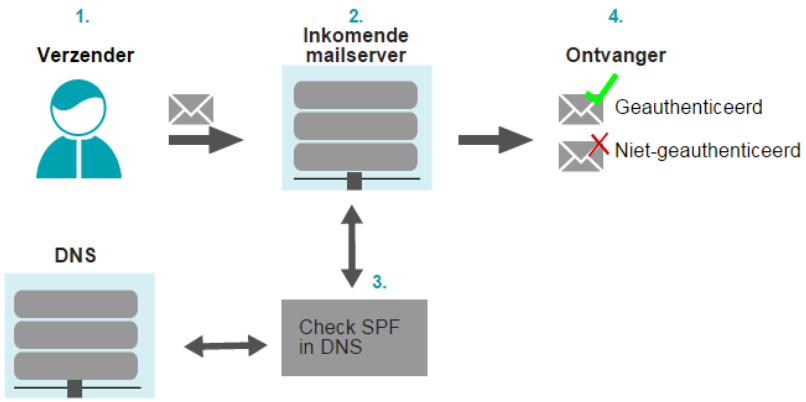
1.2 Doorlopen proces

Voor het opstellen van dit advies is de volgende procedure doorlopen:

- Gedurende de toetsingsprocedure voor DMARC is gebleken dat er een grote afhankelijkheid bestaat met SPF.
- Uit de expertgroepsessie DMARC is gebleken dat experts tevens voorstander zijn van opname van SPF op de 'pas toe of leg uit'-lijst, onder voorwaarde dat de standaard voldoet aan de toetsingscriteria.
- In de reacties van de openbare consultatie zijn geen redenen gezien om het expertadvies te herzien of om aanvullende adviezen te geven.
- Conform het forumadvies is SPF beoordeeld aan de hand van de toetsingscriteria. Het resultaat van deze toetsing is weergegeven in dit advies.

1.3 Toelichting SPF

Sender Policy Framework (SPF) is een open standaard die een technische methode specificeert om afzenderadres-vervalsing detecteerbaar te maken. SPF biedt de mogelijkheid te controleren of een bericht aangeleverd wordt vanaf een server die daartoe gerechtigd is. Dit doet SPF door de authenticiteit van de domeinnaam in het afzenderadres van de ontvangen mail herleidbaar te maken via de in DNS gepubliceerde IP-adressen van de verzendende mailserver(s). Indien een mailserver niet in de lijst met gepubliceerde IP-adressen staat (de zogeheten SPF-records) maar toch mail verstuurt met het betreffende domein als afzender, dan wordt de mail als niet geauthenticeerd beschouwd. Zie figuur 1 voor de procesmatige werking van SPF.



Figuur 1. Procesmodel werking SPF.

Een SPF-)record is een TXT-record in het DNS zone van het verzendende domein, waarin staat welke hosts en/of IP-adressen namens dat domein e-mail mogen versturen en wat er met een verstuurd bericht moet

gebeuren als hieraan niet wordt voldaan. Een ontvanger van e-mail van dat domein kan in het SPF-record controleren of de server waarvan de e-mail afkomstig is, is opgenomen in dat SPF-record. Om SPF goed te laten functioneren is vereist dat SPF wordt ondersteund door zowel zender als ontvanger, aangezien bij ontbreken van SPF-recordinformatie het resultaat van een SPF-evaluatie als antwoord 'none' op zal leveren (waarbij de e-mail zal worden geaccepteerd). SPF kan worden geconfigureerd als 'HardFail', (afwijzen van e-mails wiens IP-adres niet in SPF-records zijn gedefinieerd) en als 'SoftFail' (waarbij e-mails wiens afzenderadres niet in SPF-records zijn gedefinieerd wel worden doorgelaten, maar gemarkeerd worden als spam). Voor de meeste organisaties valt aan te raden SPF niet op 'HardFail' te zetten vanwege de grote kans op false positives, en voor veel organisaties geldt dat het risico op en negatieve effect van false positives groter is dan het risico op en negatieve effect van spoofing.
Om een indruk te krijgen van de resultaten op evaluatie van een SPF-record, zie tabel 1.

SPF-result	Uitleg	Actie
Pass	Het SPF-record machtigt de host tot versturen	accept
Fail	Het SPF-record staat de host NIET toe om te versturen	reject
SoftFail	Het SPF-record stelt dat de host niet is toegestaan om te versturen, maar in acceptatieovergang zit	accept but mark
Neutral	Het SPF-record specificeert expliciet dat er niets gemeld kan worden over validiteit	accept
None	Het domein heeft geen SPF-record, of het SPF-record kan niet worden beoordeeld op resultaat	accept
PermError	Er is een permanente fout opgetreden (bijv. slecht beschreven SPF-record)	unspecified
TempError	Een tijdelijke fout is opgetreden	accept or reject

Tabel 1. Mogelijke resultaten bij de evaluatie van een SPF-record

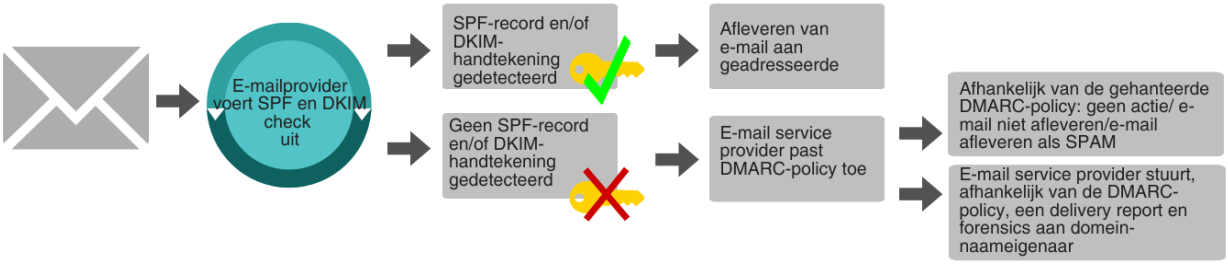
SPF is verder relatief simpel te implementeren en te onderhouden. Implementatie van SPF is voornamelijk een kwestie van goed voorbereiden, en mits kundig uitgevoerd is het toevoegen van IP-adressen in het DNS een relatief eenvoudige opgave. Verder wordt SPF al gebruikt door verschillende overheden, zoals Logius, de Belastingdienst, inspectiediensten, enkele ministeries, het CBS en door verscheidene grote en kleine gemeenten, zoals Amsterdam, Bussum, Castricum (in totaal 121 gemeenten).

1.4 Relatie met andere standaarden

Samenhang met reeds opgenomen standaarden op de lijst voor 'pas toe of leg uit' of 'gangbare lijst'
SPF biedt, net als DKIM, een vorm van e-mail authenticatie op organisatieniveau. Daar waar DKIM authenticatie biedt voor het e-mailbericht, biedt SPF dit voor een deel van het transmissiekanaal. DKIM en SPF zijn in deze zin aanvullend op elkaar.

DMARC maakt gebruik van SPF en DKIM. DMARC gebruikt het SPF-mechanisme om de authenticiteit van het domein in het afzenderadres van een e-mail te verifiëren. Wanneer de authenticiteitscontrole een

negatief resultaat heeft wordt het DMARC-beleid in werking gezet. De DMARC-regels kunnen de 'HardFail'- en 'SoftFail'-settings van SPF overrulen via alignment met de zichtbare 'from'-header (het zichtbare afzenderadres in e-mails) in plaats van enkel de onzichtbare SPF-envelope sender address (ook wel 'return path' genoemd). DMARC kan zo helpen om 'false positives' van SPF te voorkomen. Opname van de DMARC-standaard op de 'pas toe of leg uit'-lijst kan verder gezien worden als een aanvulling op de al opgenomen DKIM-standaard. Zie figuur 2 voor de samenhang tussen DMARC, SPF en DKIM.



Figuur 2. Procesmodel werking DMARC in combinatie van SPF en DKIM

Daarnaast kent de standaard samenhang met DNSSEC en IPv6. SPF conflicteert niet met deze standaarden. SPF is afhankelijk van een Domain Name Server (DNS) aangezien SPF een TXT-record in het DNS-zone van het verzendende domein toevoegt, waarin staat welke hosts en/of IP-adressen namens dat domein e-mail mogen versturen. Door SPF's gebruik van DNS is DNSSEC als DNS-beveiliging een logisch gevolg. DNSSEC staat tevens op de 'pas toe of leg uit'-lijst. Verder leggen IPv4 en IPv6 de basis voor de werking van SPF, aangezien deze ervoor zorgen dat ieder ICT-systeem binnen een netwerk een uniek IP-adres heeft.

Samenhang met standaarden die mogelijk in aanmerking komen voor opname op één van de lijsten
Zoals in figuur 2 valt af te lezen heeft SPF grote samenhang met DMARC en DKIM die tevens in aanmerking is opname op de 'pas toe of leg uit'-lijst.

1.5 Leeswijzer

In hoofdstuk 2 wordt beschreven in welke gevallen de standaard functioneel gezien gebruikt zou moet worden (functioneel toepassingsgebied) en door welke organisaties deze gebruikt zou moeten worden (organisatorisch werkingsgebied).

Om te bepalen of de standaard opgenomen moet worden op de lijst met standaarden voor 'pas toe of leg uit', is deze getoetst aan een viertal vastgestelde criteria. In hoofdstuk 3 staat het resultaat van deze toetsing.

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'-regime. 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 de standaard functioneel gezien gebruikt zou moeten worden (functioneel toepassingsgebied), en door welke organisaties deze gebruikt zou moeten worden (organisatorisch werkingsgebied).

2.1 Functioneel toepassingsgebied

Als functioneel toepassingsgebied wordt, conform Forumadvies, voorgesteld:
Het controleren of een e-mailserver gerechtigd is om namens een domeinnaam e-mail te mogen verzenden.

2.2 Organisatorisch werkingsgebied

Conform het Forumadvies wordt geadviseerd om het organisatorisch werkingsgebied van de standaard overeen te laten komen met het werkingsgebied waarop het 'pas toe of leg uit' principe van toepassing is, te weten:
Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.

3 Toetsing van standaard aan criteria

Om te bepalen of de standaard opgenomen moet worden op de lijst met open standaarden is deze getoetst aan een aantal criteria. Er zijn vier hoofdcriteria:

1. Toegevoegde waarde
2. Open standaardisatieproces
3. Draagvlak
4. Opname bevordert adoptie

Deze criteria staan beschreven in het rapport, *"Toetsingprocedure en criteria voor indieners en experts"* en staan op de website www.forumstandaardisatie.nl/open-standaarden. Het resultaat van de toetsing zal in dit hoofdstuk per criterium beschreven worden. Voor de volledigheid is tevens de definitie van elk criterium opgenomen.

3.1 Toegevoegde waarde

De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de risico's en nadelen.

3.1.1 Is het toepassings- en werkingsgebied van de aanmelding goed gedefinieerd?

3.1.1.1 *Is het functioneel toepassingsgebied goed gedefinieerd?*
Ja, zie paragraaf 2.1.

3.1.1.2 *Is het organisatorisch werkingsgebied goed gedefinieerd?*
Ja, zie paragraaf 2.2.

3.1.1.3 *Is de standaard generiek toepasbaar en niet alleen bedoeld voor gegevensuitwisseling met één of een beperkt aantal specifieke voorzieningen? (toelichtende vraag)*
Ja, de standaard is algemeen toepasbaar. Ook binnen het werkgebied van de (semi-)overheid. SPF kan zowel toegepast worden voor elektronische gegevensuitwisseling tussen (semi-)overheidsorganisaties en bedrijven, (semi-)overheidsorganisaties en burgers, en (semi-) overheidsorganisaties onderling.

3.1.2 Verhoudt de standaard zich goed tot andere standaarden?

3.1.2.1 *Kan de standaard naast of in combinatie met reeds opgenomen standaarden worden toegepast (d.w.z. de standaard conflicteert niet met reeds opgenomen standaarden)?*
Ja, in combinatie met DMARC en naast DKIM. DMARC maakt in zijn toepassing gebruik van SPF en DKIM. DMARC gebruikt SPF en DKIM om de authenticiteit van de domeinnaam in het afzenderadres van een e-mail te verifiëren. Wanneer de authenticiteitscontrole een negatief resultaat heeft wordt het DMARC-beleid in werking gezet. Opname van SPF op de 'pas toe of leg uit'-lijst kan daarmee gezien worden als een aanvulling op DKIM, en tevens bij DMARC die op dit moment in procedure is voor opname.

Daarnaast kent de standaard samenhang met DNSSEC en IPv6. SPF conflicteert niet met deze standaarden. SPF is afhankelijk van een Domain Name Server (DNS) aangezien SPF een TXT-record in het DNS-zone van het verzendende domein toevoegt, waarin staat welke hosts en/of IP-adressen namens dat domein e-mail mogen versturen. Door SPF's gebruik van DNS is DNSSEC als DNS-beveiliging een logisch gevolg. DNSSEC staat tevens op de 'pas toe of leg uit'-lijst. Verder legt IPv6 de basis voor de werking van SPF, aangezien deze ervoor zorgt dat ieder ICT-systeem binnen een netwerk een uniek IP-adres heeft.

3.1.2.2 *Biedt de aangemelde standaard meerwaarde boven reeds opgenomen standaarden met een overlappend functioneel toepassings- en organisatorisch werkingsgebied? (Dit kan ook om een nieuwe versie van dezelfde standaard gaan.)*
Er zijn geen standaarden met een overlappend functioneel toepassingsgebied die reeds opgenomen zijn op één van de lijsten.

3.1.2.3 *Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname? (toelichtende vraag)*
SPF vertoont gelijkenis met de Sender-ID standaard, aangezien beiden e-mails authenticeren door records toe te voegen aan DNS. De IETF heeft, na beide standaarden zes jaar gevolgd te hebben, een memo geschreven over beide standaarden[1], waarin ze concluderen dat '*het ontbreken van significante adoptie van Sender-ID een sterke aanwijzing is dat er geen community is die deze standaard uitrolt en gebruikt'*, terwijl voor SPF geldt dat deze *'wijdverbreide implementatie kent, vergelijkbaar met vele Standards Track Protocols'.*

3.1.2.4 *Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden? (toelichtende vraag)*
SPF wordt internationaal toegepast en sluit aan bij het tevens internationaal toegepaste DMARC en DKIM. SPF is in 2014 in beheer genomen door de Internet Engineering Task Force (IETF). IETF is een internationale standaardisatieorganisatie voor internetstandaarden. IETF beheert onder andere ook DKIM en DNSSEC. Voor DMARC geldt dat er op dit moment een werkgroep van IETF bezig is om, conform de standaardisatieprocedure van IETF, de specificaties van DMARC op te stellen.

3.1.2.5 *Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn? (toelichtende vraag)*
SPF-records kunnen in het DNS worden toegevoegd zonder dat hiervoor aanvullende standaardisatieafspraken noodzakelijk zijn. Aangezien SPF op verschillende manieren ingevuld kan worden zijn richtlijnen/best practices (net als bij DMARC) wel aan te raden. Het controleren van SPF-records voor inkomende mail is meestal een gratis toevoeging die beschikbaar is voor de meest gebruikte (web)mailproviders.

3.1.3 Wegen de kwantitatieve en kwalitatieve voordelen van adoptie van de standaard, voor de (semi-)overheid als geheel en voor de maatschappij, op tegen de nadelen?

1 https://tools.ietf.org/html/rfc6686.

3.1.3.1 *Draagt de adoptie van de standaard bij aan de oplossing van een bestaand, relevant interoperabiliteitsprobleem?*
Ja. De toepassing van SPF biedt (beperkt) bescherming tegen misbruik van de domeinnaam van (semi-)overheidsorganisaties. De standaard vormt een drie-eenheid met DMARC en DKIM. Waar SPF controleert op het IP adres waar een bericht vandaan komt, voegt DKIM een digitale handtekening toe aan de inhoud van een bericht. DMARC maakt het mogelijk om beleid in te richten dat richting geeft voor serviceproviders hoe zij zouden willen dat omgegaan wordt met e-mails waarvan de afzender niet door SPF en/of DKIM geauthenticeerd kan worden. DMARC rapporteert tevens door SPF en DKIM-resultaten inzichtelijk te maken aan de organisaties die zich willen beschermen. Zo kan bij ontvangst van een e-mail door de ontvangende partij met redelijke zekerheid worden aangenomen dat een e-mail ook daadwerkelijk vanuit het desbetreffende domein is verzonden. Als op zichzelf staande standaard biedt SPF geringe bescherming, het is voornamelijk de complementaire werking met DMARC en DKIM die SPF waardevol maakt.

3.1.3.2 *Draagt de standaard bij aan het voorkomen van een vendor lock-in (leveranciersafhankelijkheid)?*
Ja. De standaard is vrij beschikbaar. Op de phishing scorecard[2] is helder inzichtelijk gemaakt welke organisaties de standaard ondersteunen.

3.1.3.3 *Wegen de overheidsbrede en maatschappelijke baten voor de informatievoorziening en de bedrijfsvoering op tegen de kosten?*
Voordat de standaard volledig in gebruik kan worden genomen moet een inventarisatie worden gemaakt wie op organisatieniveau namens de domeinnaam e-mail mag verzenden. De tijdsinspanning die hiervoor nodig is verschilt per organisatie. Het vervolgens opnemen van deze IP-adressen in het DNS is een relatief eenvoudige operatie. De kosten voor het invoeren van deze standaard is hiermee (relatief) gering.

3.1.3.4 *Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel?*
Er zijn geen specifieke beveiligingsrisico's geïdentificeerd.

3.1.3.5 *Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel?*
Er zijn geen specifieke privacyrisico's geïdentificeerd.

3.1.4 Conclusie criteria 'Toegevoegde waarde'
De toepassing van SPF biedt bescherming tegen misbruik van de domeinnaam van (semi-)overheidsorganisaties. Als op zichzelf staande standaard biedt SPF geringe bescherming. De standaard vormt een drie-eenheid met DMARC en DKIM. Waar SPF controleert op het afzenderadres van een bericht, voegt DKIM een digitale handtekening toe aan de inhoud van een bericht. DMARC kan resultaten van SPF en DKIM inzichtelijk maken aan de organisaties die zich willen beschermen door resultaten te rapporteren. Zo kan bij ontvangst van een e-mail door de ontvangende partij met redelijke zekerheid worden aangenomen dat een e-mail ook daadwerkelijk vanuit het desbetreffende domein is verzonden. De complementaire werking van SPF met DMARC en DKIM maakt SPF waardevol.

2 Zie https://www.phishingscorecard.com.

3.2 Open standaardisatieproces

De ontwikkeling en het beheer van de standaard zijn op een open, onafhankelijke, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze ingericht.

3.2.1 Is de documentatie voor een ieder drempelvrij beschikbaar?

3.2.1.1 *Is het specificatiedocument beschikbaar zonder dat er sprake is van onacceptabele belemmeringen (zoals te hoge kosten en te hoge lidmaatschapseisen)?*
Het specificatiedocument is gratis te downloaden via de website van IETF[3]. Ook niet-gebruikers kunnen de specificatie downloaden.

3.2.1.2 *Is de documentatie over het ontwikkel- en beheerproces (bijv. het voorlopige specificatiedocument, notulen en beschrijving besluitvormingsprocedure) beschikbaar zonder dat er sprake is van onacceptabele belemmeringen (zoals te hoge kosten en te hoge lidmaatschapseisen)?*
De documentatie over het ontwikkel- en beheerproces is gratis en voor iedereen te downloaden via de website van IETF. De documentatie heeft public review doorstaan en is goedgekeurd voor publicatie door de Internet Engineering Steering Group (IESG).

Specificaties doorlopen in het standaardisatieproces van IETF twee stadia van volwassenheid; 'proposed standard', en 'internet standard'. SPF bevindt zich op het moment in het 'proposed standard' -stadium. Een 'proposed standard'-specificatie is over het algemeen stabiel, wordt verondersteld te goed worden begrepen, en geniet van voldoende belangstelling van de IETF standards community om als waardevol te worden beschouwd. Echter, toekomstige ervaring kan alsnog leiden tot een wijziging of zelfs terugtrekking van de specificatie voor deze doorstroomt naar 'internet standard'. Overige documentatie zoals notulen van bijeenkomsten en besluiten zijn ook kosteloos beschikbaar op de website van IETF.

3.2.2 Is het intellectuele eigendomsrecht voor eenieder beschikbaar, zodat de standaard vrij implementeerbaar en te gebruiken is?

3.2.2.1 *Stelt de standaardisatieorganisatie het intellectueel eigendomsrecht op de standaard m.b.t. bijvoorbeeld eventuele patenten- onherroepelijk royalty-free voor eenieder beschikbaar?*
De Intellectual Property Rights (IPR) van IETF is vastgelegd in RFC3979. Hierin staat dat leden van de werkgroep van een specifieke standaard bestaande en relevante IPR moeten bekendmaken. Met de IPR-zoekfunctie van IETF[4] kan worden ingezien dat dit proces tevens bij SPF is doorlopen.

3 Zie https://tools.ietf.org/html/rfc7208
4 Zie https://www.phishingscorecard.com.

3.2.2.2 *Garandeert de standaardisatieorganisatie dat partijen die bijdragen aan de ontwikkeling van de standaard hun intellectueel eigendomsrecht onherroepelijk royalty-free voor eenieder beschikbaar stellen?*
Partijen die hebben meegewerkt aan de SPF-standaard hebben verklaard dat zij *geen* IPR-rechten claimen, hoewel dit geen garantie is dat dit in de toekomst niet alsnog kan gebeuren.

3.2.3 Is de inspraak van eenieder in voldoende mate geborgd?

3.2.3.1 *Is het besluitvormingsproces toegankelijk voor alle belanghebbenden (bijv. gebruikers, leveranciers, adviseurs, wetenschappers)?*
Verschillende werkgroepen werken aan de (door)ontwikkeling van IETF-standaarden. Samenwerking binnen deze werkgroepen vindt veelal plaats via e-mail. Belanghebbenden zoals gebruikers, leveranciers, adviseurs en wetenschappers kunnen zich via de website van IETF aanmelden voor werkgroepen. Hier zijn geen (lidmaatschaps)kosten aan verbonden. Zo was de SPF Update Working Group (ook wel SPFbis genoemd) vrij toegankelijk.

3.2.3.2 *Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen?*
Het standaardisatieproces van IETF maakt gebruik van een besluitvormingsprocedure via het principe van 'rough consensus', waarbij de dominante mening van een groep, zoals door de voorzitter vastgesteld, de basis voor een beslissing vormt.

3.2.3.3 *Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde procedure?*
Binnen de werkgroepen kunnen belanghebbenden bezwaren kenbaar maken. Buiten de werkgroepen kan bezwaar worden aangetekend bij de leden van de Internet Engineering Steering Group (IESG).

3.2.3.4 *Organiseert de standaardisatieorganisatie regelmatig overleggen met belanghebbenden over doorontwikkeling en beheer van de standaard?*
IETF organiseert jaarlijks een aantal bijeenkomsten. Deze bijeenkomsten worden wereldwijd georganiseerd en zijn voor een ieder, tegen betaling, toegankelijk. Remote attendance[5] is kosteloos. De eerstvolgende IETF-bijeenkomst vindt plaats in Praag, Tsjechië van 19 t/m 24 juli 2015.

3.2.3.5 *Organiseert de standaardisatieorganisatie een publieke consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld?*
IETF werkt met RFC's[6], het standaard publicatieformaat voor Internet Standaarden van IETF. Voordat een nieuwe RFC van een standaard wordt geaccordeerd, wordt door een werkgroep van deze standaard een zogeheten *open comments proces* georganiseerd waarbij belanghebbenden commentaar kunnen leveren over de (nieuwe versie van de) standaard.

3.2.4 Is de standaardisatieorganisatie onafhankelijk en duurzaam?

3.2.4.1 *Is de ontwikkeling en het beheer van de standaard belegd bij een onafhankelijke non-profit standaardisatieorganisatie?*
SPF is in beheer bij IETF. De IETF is een onderneming zonder winstoogmerk.

5 Remote attendance is mogelijk door bijvoorbeeld een livestream vanaf de bijeenkomst.
6 RFC staat voor Request for comments.

3.2.4.2 *Is de financiering van de ontwikkeling en het onderhoud van de standaard voor tenminste drie jaar gegarandeerd?*
IETF bestaat bijna 30 jaar en heeft zich in het verleden bewezen als stabiele standaardisatieorganisatie. De expertgroep is om deze reden van mening dat de continuïteit van de financiering voor IETF-standaarden hierdoor voldoende is gewaarborgd.

3.2.5 Is het (versie) beheer van de standaard goed geregeld?

3.2.5.1 *Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot versiebeheer van de standaard? (met o.a. aandacht voor migratie van gebruikers)*
De inhoud van eerdere versies van IETF-standaarden is terug te lezen op de website van IETF. In de verschillende RFC's van een standaard is aandacht voor de implementatie van een standaard.

3.2.5.2 *Is het standaardisatieproces van de standaardisatieorganisatie zodanig goed geregeld dat het Forum zich kan onthouden van aanvullende toetsing bij de aanmelding van een nieuwe versie van de standaard?*
Iedere nieuwe versie van een standaard doorloopt een vaste set van stappen in het standaardisatieproces van IETF. De experts zijn daarom van mening dat nogmaals toetsen van een nieuwe versie van de standaard geen meerwaarde zal hebben.

3.2.5.3 *Is het belang van de Nederlandse overheid voldoende geborgd bij de ontwikkeling en het beheer van de standaard?*
SPF is in beheer bij het IETF, wat betekent dat de Nederlandse overheid zich, indien gewenst, kosteloos kan aanmelden voor deelname aan een van de werkgroepen voor SPF.

3.2.6 *Conclusie criteria 'Open standaardisatieproces'*
De expertgroep concludeert dat het standaardisatieproces van IETF voldoende open is. SPF voldoet aan de voorwaarden voor opname op de 'pas toe of leg uit'-lijst, het is een proposed standaard die wordt beheerd door IETF.

3.3 Draagvlak

Aanbieders en gebruikers moeten voldoende ervaring hebben bij het ondersteunen, implementeren en gebruiken van de standaard.

3.3.1 Bestaat er voldoende marktondersteuning voor de standaard?

3.3.1.1 *Bieden meerdere leveranciers ondersteuning voor de standaard?*
Ja, waarbij op het internet tevens meerdere aanbieders te vinden die (gratis) producten en diensten aanbieden ter ondersteuning van de implementatie van de standaard.[7]

7 Zie http://www.openspf.org/

3.3.1.2 *Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen?*
Er zijn verschillende websites waar de conformiteit van de implementatie van SPF-records kan worden getoetst (inclusief syntaxcontrole, een check of de syntax geen fouten oplevert) waaronder http://www.kitterman.com/spf/validate.html en http://mxtoolbox.com/spf.aspx en www.internet.nl.

3.3.2 Kan de standaard rekenen op voldoende draagvlak?

3.3.2.1 *Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt?*
SPF wordt op dit moment door diverse (semi)overheidsorganisaties gebruikt, zoals Logius, de Belastingdienst, inspectiediensten, enkele ministeries, het CBS en door verscheidene grote en kleine gemeenten, zoals Amsterdam, Bussum, Castricum (in totaal 121 gemeenten. Zie https://www.phishingscorecard.com/ScoreCard/Netherlands/Government/MS0y voor een volledig overzicht.

3.3.2.2 *Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt?*
Sender ID wordt door sommigen ook wel gezien als een oude versie van SPF, en door sommigen tevens als een gemankeerde (en inmiddels overbodige) standaard, aangezien gebruikers die de aanbevelingen opvolgen in de Sender ID specificatie RFC 4406 (sectie 3.4) in overtreding zijn betreffende de SPF-specificaties van RFC 4408. Deze fout werd niet hersteld voor publicatie, ondanks officieel beroep door de Internet Architecture Board[8]. De Sender ID standaard wordt echter nauwelijks meer gebruikt.

3.3.2.3 *Is de aangemelde versie backwards compatible met eerdere versies van de standaard?*
Sender ID en SPF maken beiden records aan in het DNS. Afhankelijk van de instellingen van de ontvanger kan het voorkomen dat van deze standaarden de huidige SPF-versie v=spf1 uitgaande berichten niet aankomen (genegeerd worden) bij de ontvanger. In hoofdstuk 3.4 van RFC 4406[9] wordt hiervoor een oplossing geboden, namelijk het toevoegen van zowel v=spf1 als spf2.0 (Sender ID)-records.

3.3.2.4 *Zijn er voldoende positieve signalen over toekomstig gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?*
SPF is inmiddels door diverse organisaties binnen de (semi-)overheid geïmplementeerd. Verder wordt ook DMARC op dit moment door diverse organisaties binnen de (semi-)overheid geïmplementeerd, zoals Logius, de Belastingdienst, inspectiediensten, enkele ministeries, het CBS en door verscheidene grote en kleine gemeenten, zoals Amsterdam, Bussum, Castricum (in totaal 121 gemeenten. Aangezien DMARC gebruik maakt van SPF en DKIM ligt het voor de hand dat het invoeren van

8 https://www.iab.org/appeals/2006-2/appeal-against-iesg-decision-by-julian-mehnle-8-february-2006/
9 https://tools.ietf.org/html/rfc4406#section-3.4

DMARC tevens het invoeren SPF en DKIM verder zal stimuleren. Het CIP (Centrum Informatiebeveiliging en Privacybescherming) stelt verder over SPF en domeinverificatie dat het gebruik "zal groeien en standaard gaan worden" [10].

3.3.3 Conclusie criteria 'Draagvlak'

De expertgroep concludeert dat het draagvlak voor SPF voldoende is. Er wordt door een groot aantal overheidsorganisaties gebruik gemaakt van SPF. Toekomstige gebruikers kunnen hierbij rekenen op voldoende marktondersteuning voor de implementatie en bij het gebruik van de standaard.

3.4 Opname bevordert adoptie

Er zijn twee lijsten: de lijst met gangbare standaarden en de lijst voor 'pas toe of leg uit'. Deze laatste lijst is bedoeld om standaarden een extra stimulans te geven wanneer:

1. Hun huidige adoptie binnen de (semi-)overheid beperkt is;
2. Opname bijdraagt aan de adoptie door te stimuleren o.b.v. het 'pas toe of leg uit' regime.

De lijst met gangbare standaarden vormt een referentie voor standaarden die veel gebruikt worden. Als standaarden voldoen aan enkele basisvoorwaarden (voor o.a. openheid), er is geen discussie over en de standaarden worden breed gebruikt, dan vindt opname op die lijst plaats.

3.4.1 Is de "pas toe of leg uit"-lijst het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

Ja. Gezien het feit dat het gebruik van SPF binnen de (semi)overheid wel aanwezig maar nog beperkt is concludeert de expertgroep dat de 'pas toe of leg uit'-lijst een geschikt middel is om adoptie te bevorderen.

Daarnaast kan opname op de lijst ervoor zorgen dat de toegevoegde waarde van het gebruik van de drie e-mailbeveiligingsstandaarden SPF, DMARC en DKIM ook op bestuurlijk niveau gezamenlijk aandacht krijgt.

3.4.2 Is de lijst met gangbare open standaarden het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

Nee. Het gebruik van SPF heeft nog niet de omvang die nodig is om de standaard als gangbaar te kunnen beschouwen.

10 http://www.cip-overheid.nl/wp-content/uploads/2014/06/20140528_Emailauthenticatie_def.pdf.