notitie

FORUM STANDAARDISATIE 22 april 2015
Agendapunt 2: Open standaarden, lijsten
Stuk 2A: Advies opname DMARC en SPF op de 'pas toe of leg uit'-lijst

Aanleiding en achtergrond
DMARC is een open standaard die het mogelijk maakt om beleid in te stellen over de manier waarop ontvangende e-mailproviders, die DMARC ondersteunen, om zouden moeten gaan met e-mail waarvan niet kan worden vastgesteld dat deze afkomstig is van het vermelde afzenderdomein. Het doel van DMARC is om, in combinatie met DKIM en/of SPF, misbruik van de domeinnaam middels e-mail te verminderen en/of te voorkomen. Daarnaast kan met DMARC worden voorkomen dat e-mailmailingen door ontvangende e-mailproviders onterecht voor spam worden aangezien.

DMARC maakt gebruik van SPF en DKIM. SPF controleert of de mailserver die een e-mail wil versturen namens het e-maildomein e-mail mag verzenden. DKIM koppelt een e-mail aan een domeinnaam met behulp van een digitale handtekening. DMARC gebruikt DKIM en SPF om de authenticiteit van een e-mail te verifiëren. Wanneer deze verificatie niet mogelijk is wordt het DMARC-beleid in werking gezet.

Geadviseerd wordt om zowel DMARC als SPF op te nemen zodat samen met DKIM de adoptie van een complete set van e-mailbeveiligingsstandaarden wordt bevorderd.

Betrokkenen en proces
DMARC is ingediend door Measuremail met steun vanuit de gemeente Den Bosch en de gemeente Heerlen. Vervolgens heeeft een intake en experttoets plaatsgevonden. De uitkomst van de expertgroep was om naast DMARC ook SPF op de lijst op te nemen, onder voorwaarde dat de standaard voldoet aan de toetsingscriteria. Vervolgens heeft voor zowel DMARC als SPF een openbare consultatie plaatsgevonden.

Het expertadvies is gepubliceerd ten behoeve van de openbare consultatie. Tijdens de consultatie zijn er 11 reacties en vragen ontvangen. Het waren overwegend aanvullingen op het expertadvies en positief over opname van DMARC en SPF. Wel is het advies om voor SPF een aanvullende check uit te voeren op basis van de toetsingscriteria. De reacties zijn in overleg met de betrokken partijen verwerkt in

dit forumadvies.

Consequenties en vervolgstappen
DMARC is nog niet in beheer genomen bij IETF. De standaard zelf is stabiel en de beheerprocedures zijn geheel afgestemd op IETF. De conclusie uit de expertgroep is om DMARC op te nemen op de 'pas toe of leg uit'-lijst onder voorwaarde dat DMARC minimaal een *proposed standard*[1] is en wordt beheerd door IETF of een andere, gelijkwaardige, standaardisatieorganisatie. Op dit moment is een werkgroep van IETF bezig om, conform de standaardisatieprocedure van IETF, de specificaties van DMARC op te stellen. De verwachting is dat deze specificaties in het derde kwartaal van 2015 definitief zijn en dat de standaard als gevolg hiervan in beheer wordt genomen door IETF.

SPF heeft een positief advies vanuit zowel de expertgroep als de openbare consultatie. SPF is niet vooraf apart getoetst aan de toetsingscriteria van het Forum omdat alleen DMARC is ingediend voor de toetsing. Om 'verrassingen' te voorkomen is een voorwaarde voor opname dat SPF nog apart getoetst wordt tegen de criteria van het Forum. Deze toets vindt momenteel plaats en is eind april afgerond zodat het geen openstaand punt is op het moment dat het besluit voorligt in het Nationaal Beraad.

Tot slot kan het DMARC-beleid dat een organisatie kiest impact hebben het uitwisselen van privacy gevoelige gegevens. Het advies is om bij de invulling van DMARC-beleid een Privacy Impact Assessment (PIA) uit te voeren om te kunnen bepalen of er privacyrisico's zijn en of deze acceptabel zijn. Overheidsorganisaties kunnen hierbij gebruik maken van het Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst[2].

Gevraagd besluit

Het Forum Standaardisatie wordt gevraagd om in te stemmen met onderstaande advies.

Het Forum Standaardisatie adviseert het Nationaal Beraad Digitale Overheid om:

1. in te stemmen met de opname van DMARC op de 'pas toe of leg uit'-lijst onder voorwaarde dat het beheer van DMARC is geformaliseerd door IETF of een andere, gelijkwaardige, standaardisatieorganisatie.

2. in te stemmen met de opname van SPF op de 'pas toe of leg uit'-lijst. *Voorwaarde voor het SPF advies is dat uit de controle op de toetsingscriteria geen aandachtspunten naar voren komen. Dit moet duidelijk zijn voor 29 april 2015 zodat het geen openstaand punt is op het moment dat het besluit voorligt in het Nationaal Beraad.*

Zodra het Forum Standaardisatie vaststelt dat aan bovenstaande punten is voldaan kunnen de standaarden op de lijst worden opgenomen.

3. de additionele adviezen ten aanzien van de adoptie van DMARC en SPF.

[1] De status 'proposed standard' is het eerste (instap)niveau van de volwassenheid van een standaard, conform de standaardisatieprocedure van IETF.
[2] *Zie http://www.rijksoverheid.nl/documenten-en-publicaties/publicaties/2013/06/24/toetsmodel-privacy-impact-assessment-pia-rijksdienst.html.*

Ad 1 Opname van DMARC op de 'pas toe of leg uit'-lijst

DMARC is op dit moment nog niet in beheer bij een standaardisatieorganisatie. Dit advies is onder de voorwaarde dat DMARC minimaal een *proposed standard* is en wordt beheerd door IETF of een andere, gelijkwaardige, standaardisatieorganisatie. Op dit moment is een werkgroep van IETF bezig om, conform de standaardisatieprocedure van IETF, de specificaties van DMARC op te stellen. De verwachting is dat deze specificaties in het derde kwartaal van 2015 definitief zijn en dat de standaard als gevolg hiervan in beheer wordt genomen door IETF.

Als functioneel toepassingsgebied voor DMARC wordt geadviseerd:
Het instellen van beleid voor alle domeinnamen, waarvan de overheid de houder is, om betrouwbare e-mailcommunicatie met burgers, bedrijven en (semi)overheidsorganisaties te bevorderen, alsmede de bescherming van de overheid zelf tegen e-mail van ongeauthenticeerde afzenders te bevorderen.

Als organisatorisch werkingsgebied voor DMARC wordt geadviseerd
Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.

Ad 2 Opname van SPF op de 'pas toe of leg uit'-lijst

DKIM is sinds 2012 opgenomen op de 'pas toe of leg uit'-lijst. Geadviseerd wordt om naast DMARC ook SPF op te nemen om zo de adoptie van een complete set van e-mailbeveiligingsstandaarden te bevorderen. Opname op de lijst kan ervoor zorgen dat de toegevoegde waarde van het gebruik van e-mailbeveiligingsstandaarden zoals DMARC, DKIM en SPF ook op bestuurlijk niveau aandacht krijgt.

SPF is niet vooraf apart getoetst aan de toetsingscriteria omdat alleen DMARC is ingediend voor de toetsingsprocedure. Om 'verrassingen' te voorkomen is een voorwaarde voor opname dat SPF nog apart getoetst moeten worden tegen de criteria van het Forum. De uitkomsten moeten worden voorgelegd aan de expertgroep. Als SPF voldoet aan de criteria kan de standaard worden opgenomen op de 'pas toe of leg uit'-lijst.

Als functioneel toepassingsgebied voor SPF wordt geadviseerd:
Het controleren of een e-mailserver gerechtigd is om namens een domeinnaam e-mail te mogen verzenden.

Ad 3 Additionele adviezen ten aanzien van de adoptie van DMARC en SPF

Ten aanzien van de adoptie worden de volgende oproepen gedaan:

1. Het NCSC wordt opgeroepen om (in samenwerking met de expertgroep) een handreiking/ICT-richtlijnen voor de beveiliging van e-mail op te stellen, zoals ook is gedaan voor Transport Layer Security (TLS). Het is hierbij niet alleen van belang om de technologie van de standaarden toe te lichten (waaronder aandachtspunten bij de implementatie), maar ook het bestuurlijke belang van de standaarden.
2. Het Forum Standaardisatie wordt opgeroepen om bij (semi)overheidsorganisaties het gebruik van DMARC, SPF en DKIM onder de aandacht te brengen via de leden van het Forum. Het gaat hier met name om (semi)overheidsorganisaties waarvan het aannemelijk is dat burgers, bedrijven en andere overheidsorganisaties e-mails met deze afzenders vertrouwen.
3. Veilige e-mail is een belangrijke basis voor het realiseren van de ambities van de Digitale Overheid 2017 uit het regeerakkoord. De minister van BZK wordt opgeroepen om adoptie van de standaarden voor veilig e-mailverkeer vanuit de

overheid richting burgers en bedrijven op de agenda van de Digitale Overheid 2017 te zetten. [3]

4. Het Forum Standaardisatie wordt opgeroepen om de CTO-raad, het platform internetstandaarden en het ECP (Platform voor de InformatieSamenleving) te betrekken bij activiteiten ter bevordering van de adoptie van de standaard.
5. Het Forum Standaardisatie wordt opgeroepen om in samenwerking met het College bescherming persoonsgegevens (CBP) te onderzoeken of het mogelijk is om een (voorbeeld) Privacy Impact Assessment uit te (laten) voeren. De uitkomsten uit dit assessment kunnen als voorbeeld gebruikt worden door andere (semi)overheidsorganisaties.
6. De eigenaren van informatiebeveiligingsbaselines binnen de overheid, zoals de Baseline Informatiebeveiliging Rijksdienst (BIR), Baseline Informatiebeveiliging Gemeenten (BIG) en de Baseline Informatiebeveiliging Waterschappen (BIWA), worden opgeroepen om de standaarden voor veilige e-mailcommunicatie, zoals DMARC, DKIM en SPF, op te nemen in deze baselines.

De opgeroepen partijen worden gevraagd om één jaar na opname van de standaard over de voortgang van deze punten te rapporteren aan het Forum Standaardisatie.

Toelichting

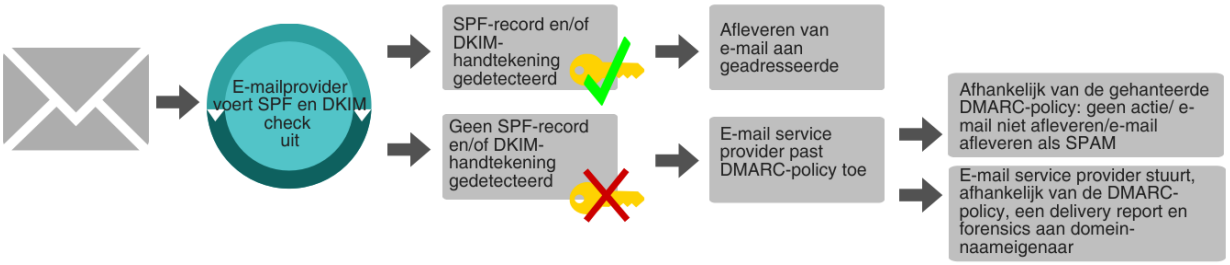
1. Waar gaat het inhoudelijk over?

DMARC
Domain-based Message Authentication, Reporting, and Compliance (DMARC) is een open standaard die het voor organisaties mogelijk maakt om beleid op te stellen over de manier waarop ontvangende e-mailproviders, die DMARC ondersteunen, om zouden moeten gaan met e-mail waarvan niet kan worden vastgesteld dat deze afkomstig is van het eigen domein. Bij ongeauthenticeerde e-mailberichten kan gedacht worden aan phishing e-mails en spam. Door middel van een DMARC-beleid, ook wel DMARC-record genoemd, kunnen organisaties aangeven wat er met ongeauthenticeerde e-mailberichten zou moeten gebeuren (geen actie vereist van de e-mailserviceprovider, e-mail beschouwen als 'verdacht' of de ongeauthenticeerde e-mail niet afleveren).

Verder kan een organisatie in een DMARC-record aangeven op welke manier zij hierover gerapporteerd wil worden; periodieke geaggregeerde rapportage met de IP-adressen van de SMTP-servers (aggregate report) of een kopie van de valse e-mail (failure report).

Zonder de toepassing van DMARC bepalen e-mailproviders geheel zelf wat met ongeauthenticeerde e-mailberichten gebeurt. Organisaties waarvan de domeinnaam is 'misbruikt' hebben zodoende geen invloed op en inzicht in misbruik van de domeinnaam. De toegevoegde waarde van DMARC is dat organisaties ook zicht krijgen op dit misbruik door middel van bovengenoemde reports.

[3] *Er ligt nu ook een notitie in het Nationaal Beraad van april 2015 Digitale Overheid om meer te sturen op de adoptie van DMARC en DKIM*

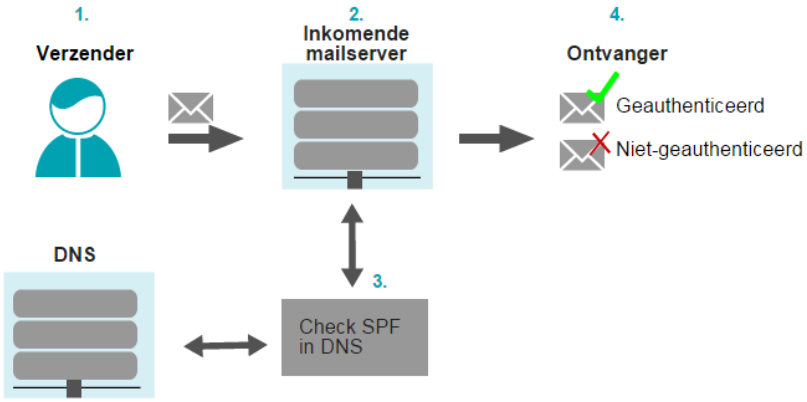


Figuur 1. Procesmodel werking DMARC in combinatie van SPF en DKIM.

Belangrijk om te vermelden is dat vanuit ieder domeinnaam e-mail kan worden verstuurd. Zo kan er bijvoorbeeld een e-mailbericht gestuurd worden vanuit de naam forumstandaardisatie.nl terwijl deze domeinnaam zelf niet gebruikt wordt als e-mailextensie. Gebruik van DMARC maakt in dit geval inzichtelijk dat er vanuit een domeinnaam ongewenst mail wordt verstuurd.

SPF
Sender Policy Framework (SPF) is een internationale standaard die wordt beheerd door IETF. SPF stelt vast of de mailserver van een e-mailbericht gerechtigd is om namens het opgegeven e-maildomein e-mail te verzenden.

Binnen het SPF-protocol wordt aan het DNS-record (Domain Name System) een extra informatieveld van een domein toegevoegd. In dit record is vermeld welke mailservers namens dit domein e-mail mogen verzenden. Wanneer een mailserver niet in dit record opgenomen is, en toch e-mail verzendt met de desbetreffende domeinnaam als afzender kan de e-mail niet worden geauthenticeerd. Als gevolg hiervan wordt de e-mail als onrechtmatig beschouwd. De standaard levert hiermee een bijdrage aan de vermindering van spam.



Figuur 2. Procesmodel werking SPF.

2. Hoe is het proces verlopen?

Om tot dit forumadvies te komen, hebben achtereenvolgens een intakegesprek, experttoetsing en openbare consultatie plaatsgevonden. Naar aanleiding van de intake is besloten om DMARC in behandeling te nemen. Aan de experttoetsing hebben (toekomstig) eindgebruikers, leveranciers, adviseurs en andere kennishebbers deelgenomen.

De conclusie uit de expertgroep was om DMARC op te nemen op de 'pas toe of leg uit'-lijst onder voorwaarde dat – en niet eerder dan nadat – DMARC minimaal een *proposed standard* is en wordt beheerd door IETF of een andere, gelijkwaardige, standaardisatieorganisatie. De expertgroep heeft tevens geadviseerd om ook SPF op te nemen op de 'pas toe of leg uit'-lijst, onder voorwaarde dat SPF – en niet eerder dan nadat – voldoet aan de gestelde toetsingscriteria voldoet.

Het expertadvies is gepubliceerd ten behoeve van een openbare consultatie waarbij gevraagd is naar DMARC en SPF. Naar aanleiding hiervan zijn nog een aantal aandachtspunten naar voren gekomen. Deze reacties zijn in overleg met de betrokken partijen verwerkt in dit forumadvies.

3. Hoe scoort de standaard op de toetsingscriteria?

Open standaardisatieproces

DMARC is op dit moment nog niet in beheer bij een standaardisatieorganisatie. Verwacht wordt dat DMARC in het derde kwartaal van 2015 in beheer wordt genomen door de Internet Engineering Task Force (IETF). Bij de toetsing is om deze reden door de experts gekeken hoe IETF scoort op het criteria *Open standaardisatieproces.*

IETF is internationale standaardisatieorganisatie die onder andere ook DKIM en SPF in beheer heeft. DMARC is vrij implementeerbaar en 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. De experts zijn van mening dat wanneer DMARC in beheer wordt genomen door IETF het standaardisatieproces niet nogmaals hoeft te worden getoetst.

Toegevoegde waarde
Door de toepassing van DMARC kan misbruik van de domeinnaam van (semi-)overheidsorganisaties zoveel mogelijk tegen worden te gaan. In combinatie met DKIM en/of SPF wordt het domein van het afzenderadres van een e-mailbericht geauthenticeerd. Hierdoor 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. Daarnaast geeft de toepassing van de standaard de mogelijkheid om zelf beleid te vormen omtrent de verwerking van ongeauthenticeerde e-mailberichten door e-mailproviders.

DMARC en SPF zijn met name relevant voor (semi-)overheidsorganisaties waarvan het aannemelijk is dat burgers e-mails met deze afzenders vertrouwen, met als doel te voorkomen dat burgers, bedrijven en andere (semi-)overheidsorganisaties ongeauthenticeerde e-mails ontvangen. Via deze e-mails kunnen bijvoorbeeld 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.

Geconcludeerd wordt dat de standaarden hierdoor voldoende toegevoegde waarde

hebben binnen het gekozen functioneel toepassingsgebied en organisatorisch werkingsgebied. Te meer omdat door de toepassing van DMARC de eigenaar van de domeinnaam ook een middel in handen heeft om terugkoppeling te krijgen over e-mailstromen die de domeinnaam misbruiken.

Draagvlak
Aanbieders en gebruikers hebben voldoende ervaring met het ondersteunen, implementeren en gebruiken van de standaard. Hoewel het gebruik van de standaard door (semi-)overheidsorganisaties op dit moment nog beperkt is zijn er voldoende signalen dat dit in de toekomst zal toenemen.

Opname bevordert de 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.

DMARC vormt een feitelijke drie-eenheid met SPF en DKIM. DKIM is sinds 2012 opgenomen op de 'pas toe of leg uit'-lijst. Door zowel DMARC als SPF toe te voegen aan de 'pas toe of leg uit'-lijst versterkt het belang van deze drie-eenheid van e-mailbeveiligingsstandaarden. De additionele adviezen in dit Forumadvies zijn dan ook gericht op de verdere bevordering van een bredere aandacht voor en adoptie van e-mailbeveiligingsstandaarden zoals DMARC, SPF en DKIM binnen de (semi)overheid.

Toelichting van eventuele risico's
Er worden geen specifieke beveiligingsrisico's gezien. Wel kan afhankelijk van het DMARC-beleid dat een organisatie kiest voor het terugkoppelen van (mogelijk) ongeauthenticeerde e-mailberichten impact hebben op de privacy. Bij de rapportage ontvangt de domeineigenaar, afhankelijk van de invulling van het DMARC-beleid, een periodieke geaggregeerde rapportage met de IP-adressen van de SMTP-servers of een kopie van de valse e-mail. In deze kopie van de e-mail kunnen persoonsgegevens van de ontvangende partij zichtbaar zijn. Ook de IP-adressen van SMTP-servers zijn mogelijk gevoelig wanneer deze worden aangemerkt als persoonsgegeven. Deze discussie is overigens door het CBP nog niet beslecht. Bij de invulling van he DMARC-beleid dienen organisaties een Privacy Impact Assessment (PIA) uit te (laten) voeren om te kunnen bepalen of er privacyrisico's zijn en, indien dit het geval is, of deze acceptabel zijn. Overheidsorganisaties kunnen hierbij gebruik maken van het Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst[4].

4. Wat is de conclusie van de expertgroep en de consultatie?

Conclusie van de expertgroep
De expertgroep adviseert het Forum Standaardisatie en het Nationaal Beraad Digitale Overheid om DMARC op te nemen op de 'pas toe of leg uit'-lijst. Opname van DMARC is wel gebonden aan de voorwaarde dat DMARC minimaal een *proposed standard* is en wordt beheerd door IETF of een andere, gelijkwaardige standaardisatieorganisatie.

Voor DMARC wordt als functioneel toepassingsgebied geadviseerd: *Het instellen van beleid voor alle domeinnamen, waarvan de overheid de houder is, om betrouwbare e-mailcommunicatie met burgers, bedrijven en (semi)overheidsorganisaties te*

[4] *Zie http://www.rijksoverheid.nl/documenten-en-publicaties/publicaties/2013/06/24/toetsmodel-privacy-impact-assessment-pia-rijksdienst.html.*

bevorderen, alsmede de bescherming van de overheid zelf tegen e-mail van ongeauthenticeerde afzenders te bevorderen.

Geadviseerd wordt om ook SPF op te nemen op de 'pas toe of leg uit'-lijst, onder voorwaarde dat SPF ook aan de gestelde toetsingscriteria voldoet. Geadviseerd wordt om dit middels een onderzoek op de criteria vast te stellen.

Voor SPF wordt als functioneel toepassingsgebied geadviseerd: *Het controleren of een e-mailserver gerechtigd is om namens een domeinnaam e-mail te mogen verzenden.*

Eventuele aanvullingen vanuit de consultatie
Op de openbare consultatie van het expertadvies zijn reacties ontvangen van SIDN, ministerie van BZK, Kolab Systems AG en OpenNovations, CROW, ministerie van Veiligheid & Justitie, DICTU, DHPA, Logius, DUO (in combinatie met Kennisnet en ministerie van OCW) en Kamer van Koophandel.

Deze partijen hebben positief gereageerd op het expertadvies en onderschrijven het belang van de standaard en opname op de 'pas toe of leg uit'-lijst:
- ministerie van Veiligheid en Justitie,
- DICTU,
- DHPA,
- Logius.

SIDN
SIDN heeft opmerkingen gemaakt over:
1. De beperkte toepasbaarheid van DMARC voor bepaalde domeinen, met name voor domeinen waarbij e-mailcontact plaatsvindt tussen de overheid en burgers.
   Reactie: Wanneer het noodzakelijk is dat met zekerheid kan worden gesteld dat e-mail tussen de overheid en burgers aan komt kan er voor gekozen worden om het DMARC-record 'p=none' te hanteren. Met dit record is er geen actie van de e-mailserviceprovider verwacht en kunnen deze e-mails als 'gewone' e-mail worden behandeld.
2. Over de standaardisatieprocedure van IETF, in relatie tot in beheer name van DMARC. De specificatie van DMARC staat nu op de Informational track, en niet op de Standards track.
   Reactie: Van de voorzitter van de Working Group DMARC van IETF is vernomen dat DMARC uiterlijk in juni 2015 opgenomen zal worden op de standards track, en daarmee de status 'proposed standard' krijgt.
3. De situatie waarbij DMARC alleen in combinatie met SPF wordt gebruikt.
   Reactie: DKIM staat al opgenomen op de 'pas toe of leg uit'-lijst, waardoor verwacht wordt dat organisaties die DMARC en SPF gaan implementeren al gebruik maken van DKIM. Er is dan ook niet aannemelijk dat organisaties alleen gebruik zullen maken van de combinatie SPF en DMARC.

In de opmerkingen van SIDN wordt geen reden gezien om het expertadvies te herzien of om aanvullende adviezen te geven.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, directie Burgerschap & Informatiebeleid vindt het noodzakelijk om SPF afzonderlijk te toetsen aan de toetsingscriteria, alvorens het Forum en Nationaal Beraad Digitale Overheid een besluit kan nemen over de plaatsing van de standaard op de lijst.

Reactie: Er wordt een verkort onderzoek worden gedaan naar de standaard, waarin gekeken wordt of SPF voldoet aan alle toetsingscriteria (toegevoegde waarde, open standaardisatieproces, draagvlak en opname bevorderd adoptie).

Kolab Systems AG en OpenNovations
Kolab Systems AG en OpenNovations hebben aanbevolen om het Forum Standaardisatie tevens een referentie implementatie aan te laten wijzen om de correcte implementatie van de standaard te kunnen toetsen.
Reactie: Er zijn al verschillende websites[5] waar de conformiteit van de implementatie getoetst kan worden. Na invoering van de domeinnaam wordt getoetst of er een DMARC-record is toegevoegd aan de domeinnaam. Er bestaat (nog) geen losstaande tooling waarmee gecontroleerd kan worden of de ontvangende mailserver correcte afhandeling conform het gekozen DMARC-beleid biedt. Ontvangende mailservers zijn niet verplicht om het DMARC-beleid van een domeineigenaar toe te passen. Het gebruik van DMARC biedt dan ook geen volledige zekerheid dat de ontvangende mailserver het DMARC-beleid daadwerkelijk toepast. Daarentegen krijgen organisaties die DMARC hebben geïmplementeerd wel zicht op het 'misbruik' van de domeinnaam door de rapportages.

In de aanbeveling van Kolab Systems AG en OpenNovations wordt geen reden gezien om het expertadvies te herzien of om aanvullende adviezen te geven.

CROW
CROW heeft opmerkingen gemaakt over het mogelijke raakvlak en/of overlap van DMARC en SPF met de VISI-standaard.
Toelichting op de opmerking: VISI staat op de 'pas toe of leg uit'-lijst en richt zich op digitale communicatie tussen partijen in een bouwproject. VISI wordt gebruikt in de bouw bij het geven van opdrachten, het aanleveren van tijdschema's, het opleveren van resultaten en het melden van afwijkingen.
Reactie: In nader overleg met CROW is geconcludeerd dat er geen raakvlak of overlap is tussen DMARC en de VISI-standaard in relatie tot het werkingsgebied van de standaarden.

In de vraag van CROW wordt geen reden gezien om het expertadvies te herzien of om aanvullende adviezen te doen.

DUO, Kennisnet en Ministerie OCW
DUO, Kennisnet en het ministerie van Onderwijs, Cultuur en Wetenschap hebben aangegeven dat het advies voor alle typen organisaties uit het instellingsbesluit van het Forum Standaardisatie zou moeten gelden. En hiermee dus ook voor onderwijs- en zorginstellingen.
Reactie: Het geadviseerde organisatorisch werkingsgebied komt overeen met het werkingsgebied waarop het 'pas toe of leg uit' principe van toepassing is. Daarmee worden, conform het instellingsbesluit, ook onderwijs- en zorginstellingen mee bedoeld.

In de aanbeveling van DUO, Kennisnet en het ministerie van OCW wordt geen reden gezien om het expertadvies te herzien of om aanvullende adviezen te doen.

De volledige reacties van SIDN, ministerie van Binnenlandse Zaken en Koninkrijksrelaties, OpenNovations, CROW, ministerie van Veiligheid en Justitie, DICTU, DHPA, Logius, DUO (in combinatie met Kennisnet en ministerie van

[5] Zie *http://dmarc.org/resources/products-and-services/.*

Onderwijs, Cultuur en Wetenschap en Kamer van Koophandel zijn terug te vinden in bijlage 2 Overzicht reacties consultatie.

5. Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaard?
De expertgroep doet het Nationaal Beraad de aanbeveling om bij de opname op de lijst voor 'pas toe of leg uit' de volgende oproepen ten aanzien van de adoptie van DMARC en SPF te doen:

1. NCSC wordt opgeroepen om (in samenwerking met de expertgroep) een handreiking/ICT-richtlijnen voor de beveiliging van e-mail op te stellen, zoals ook is gedaan voor Transport Layer Security (TLS). Het is hierbij niet alleen van belang om de technologie van de standaarden toe te lichten (waaronder aandachtspunten bij de implementatie), maar ook het bestuurlijke belang van de standaarden.
2. Het Forum Standaardisatie wordt opgeroepen om bij (semi)overheidsorganisaties het gebruik van DMARC en SPF (en e-mailbeveiligingsstandaarden) onder de aandacht te brengen via de leden van het Forum. Het gaat hier met name om (semi)overheidsorganisaties waarvan het aannemelijk is dat burgers, bedrijven en andere overheidsorganisaties e-mails met deze afzenders vertrouwen.
3. Veilige e-mail is een belangrijke basis voor het realiseren van de ambities van de Digitale Overheid 2017 uit het regeerakkoord. De minister van BZK wordt opgeroepen om adoptie van de standaarden voor veilig e-mailverkeer vanuit de overheid richting burgers en bedrijven op de agenda van de Digitale Overheid 2017 te zetten.[6]
4. Het Forum Standaardisatie wordt opgeroepen om de CTO-raad, het platform internetstandaarden en het ECP (Platform voor de InformatieSamenleving) te betrekken bij activiteiten ter bevordering van de adoptie van de standaard.
5. Het Forum Standaardisatie wordt opgeroepen om in samenwerking met het College bescherming persoonsgegevens (CBP) te onderzoeken of het mogelijk is om een (voorbeeld) Privacy Impact Assessment uit te (laten) voeren. De uitkomsten uit dit assessment kunnen als voorbeeld gebruikt worden door andere (semi)overheidsorganisaties.
6. De eigenaren van informatiebeveiligingsbaselines binnen de overheid, zoals de Baseline Informatiebeveiliging Rijksdienst (BIR), Baseline Informatiebeveiliging Gemeenten (BIG) en de Baseline Informatiebeveiliging Waterschappen (BIWA), worden opgeroepen om de standaarden voor veilige e-mailcommunicatie, zoals DMARC, DKIM en SPF, op te nemen in deze baselines.

De opgeroepen partijen worden gevraagd om één jaar na opname van de standaard over de voortgang van deze punten te rapporteren aan het Bureau Forum Standaardisatie.

Aanvullende informatie

1. Expertadvies DMARC:
   https://www.forumstandaardisatie.nl/fileadmin/os/Consultatiedocumenten/Expertadvies_DMARC_1.0.pdf

2. Overzicht reacties consultatieronde:
   https://www.forumstandaardisatie.nl/fileadmin/os/Consultatiedocumenten/20150326_Reacties_uit_openbare_consultatie_DMARC_1_0.pdf

[6] *Er ligt nu ook een notitie in het Nationaal Beraad Digitale Overheid om meer te sturen op de adoptie van DMARC en DKIM*