Forum Standaardisatie

Expertadvies DMARC

Datum 12 februari 2015

Colofon

Projectnaam	Expertadvies DMARC
Versienummer	1.0
Locatie	Den Haag
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag forumstandaardisatie@logius.nl
Auteurs	Jasmijn Wijn Marc Gill'ard

Inhoud

Colofon 2

Inhoud 3

Advies & Managementsamenvatting 4

1 Doelstelling expertadvies 7

1.1 Achtergrond 7

1.2 Doelstelling expertadvies 7

1.3 Proces 7

1.4 Vervolg 8

1.5 Samenstelling expertgroep 8

1.6 Toelichting DMARC 9

1.7 Relatie met andere standaarden 10

1.8 Leeswijzer 10

2 Toepassings– en werkingsgebied 11

2.1 Functioneel toepassingsgebied 11

2.2 Organisatorisch werkingsgebied 11

3 Toetsing van standaard aan criteria 12

3.1 Toegevoegde waarde 12

3.2 Open standaardisatieproces 15

3.3 Draagvlak 18

3.4 Opname bevordert adoptie 19

3.5 Adoptieactiviteiten 20

Advies & Managementsamenvatting

Advies aan het Forum
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 standaard is en wordt beheerd door IETF of een andere, gelijkwaardige standaardisatieorganisatie.

Als functioneel toepassingsgebied 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 wordt geadviseerd:
Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-)publieke sector.

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

Waar gaat het inhoudelijk over?
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 vermelde afzender domein. Gebruik van DMARC biedt echter geen volledige zekerheid dat de ontvangende e-mailprovider het beleid ook daadwerkelijk toepassen.

Organisaties kunnen door het gebruik van DMARC in combinatie met DKIM en/of SPF voorkomen dat anderen e-mails versturen namens (de domeinnaam van) de organisatie. Hierbij kan gedacht worden aan phishing e-mails en spam. DMARC maakt hierbij misbruik zichtbaar.

DMARC kan daarmee ingezet worden voor het verminderen en/of voorkomen van misbruik van de domeinnaam middels e-mail. Ook kan door het gebruik van de standaard worden voorkomen dat e-mailmailingen door ontvangende e-mailproviders onterecht voor spam worden aangezien.

Hoe is het proces verlopen?
Om tot dit advies te komen is op 22 januari een groep van 16 experts bijeengekomen om over het toepassings- en werkingsgebied van DMARC te discussiëren en om de standaard te toetsen tegen de toetsingscriteria. Dit expertadvies vat de uitkomsten van de discussie en toetsing samen.

Hoe scoort de standaard op de toetsingscriteria?

Toegevoegde waarde
De toepassing van DMARC maakt het mogelijk om misbruik van de domeinnaam van (semi-)overheidsorganisaties zoveel mogelijk tegen te gaan. In combinatie met DKIM en/of SPF wordt het domein van de afzender van een e-mailbericht geverifieerd. Hierdoor kan bij ontvangst van een e-mail door de ontvanger 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 voor de wijze waarop e-mailproviders omgaan met de verwerking van ongeauthenticeerde e-mailberichten. De eigenaar van de domeinnaam kan daarmee terugkoppeling krijgen over e-mailstromen die de domeinnaam gebruiken en misbruiken.

Afhankelijk van het DMARC-beleid dat een organisatie kiest voor het terugkoppelen van (mogelijk) ongeauthenticeerde e-mailberichten kan DMARC privacy impact hebben. Bij de invulling van 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[1].

De expertgroep concludeert zodoende dat DMARC voldoende toegevoegde waarde heeft binnen het gekozen functioneel toepassingsgebied en organisatorisch werkingsgebied.

Open standaardisatieproces
De expertgroep concludeert dat het standaardisatieproces van IETF voldoende open is. Voorwaarde voor opname van DMARC op de 'pas toe of leg uit'-lijst is echter wel dat DMARC minimaal een proposed standaard is en wordt beheerd door IETF, of een andere, vergelijkbare standaardisatieorganisatie.

Draagvlak
De expertgroep concludeert dat het draagvlak voor DMARC voldoende is. 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. Toekomstige gebruikers kunnen hierbij rekenen op voldoende marktondersteuning voor de implementatie en bij het gebruik van de standaard.

Opname bevordert de adoptie
De expertgroep concludeert dat de 'pas toe of leg uit'-lijst het passende middel is om de adoptie van de standaard binnen de (semi)overheid te bevorderen.

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

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 te doen:

- 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.
- Het Forum Standaardisatie wordt opgeroepen om bij (semi)overheidsorganisaties het gebruik van DMARC (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.
- 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.
- 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.
- 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.
- 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.

1 Doelstelling expertadvies

1.1 Achtergrond

Het gebruik van open standaarden en het voorkomen van vendor lock-in is een van de doelstellingen van de Nederlandse overheid. Dit beleid wordt herbevestigd in actieplan "Open overheid", de digitale agenda 2011-2015, de digitale agenda 2017 en de kabinetsreactie op het rapport Elias. Deze plannen onderstrepen de noodzaak van het zoveel mogelijk meenemen van open standaarden bij het ontwerpen van informatiesystemen.

Een van de maatregelen om de adoptie van standaarden te bevorderen is het beheren van een lijst met standaarden, die vallen onder het principe 'pas toe of leg uit'. Het Nationaal Beraad Digitale Overheid spreekt zich uit over de standaarden die op de lijst zullen worden opgenomen, o.a. op basis van een expertbeoordeling van de standaard. Het Nationaal Beraad wordt geadviseerd door het Forum Standaardisatie. Het Bureau Forum Standaardisatie ondersteunt beide instellingen.

1.2 Doelstelling expertadvies

Onderwerp van dit expertadvies is DMARC. Deze standaard is aangemeld voor opname op de 'pas toe of leg uit'-lijst door Martijn Groeneweg, managing director van Measuremail.

Doel van dit advies is om, aan de hand van de criteria vast te stellen of DMARC moet worden opgenomen op de 'pas toe of leg uit'-lijst, al dan niet onder bepaalde voorwaarden.

1.3 Proces

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

- Door het Bureau Forum Standaardisatie is een intakegesprek gevoerd met de indiener op 14 november 2014. Tijdens de intake is de standaard getoetst op uitsluitingscriteria ('criteria voor in behandelname') en is een eerste inschatting gemaakt van de kansrijkheid van de procedure.
- Op basis van de intake is besloten de aanmelding in procedure te nemen. Op basis van dit besluit is een expertgroep samengesteld en een voorzitter aangesteld. Op basis van de aanmelding en de intake is een voorbereidingsdossier opgesteld voor de leden van de expertgroep.
- De expertgroep heeft voorafgaand aan de expertbijeenkomst DMARC individueel gescoord aan de hand van een spreadsheet met vragen in het voorbereidingsdossier. Op basis van de verkregen antwoorden hebben de voorzitter en de begeleider van de expertgroep de verschillende aandachtspunten geïdentificeerd.
- Tot slot is de expertgroep op 22 januari 2015 bijeengekomen om de bevindingen in het algemeen en de geïdentificeerde aandachtspunten in het bijzonder te bespreken. Tijdens deze bijeenkomst zijn ook het toepassings- en werkingsgebied vastgesteld.

De uitkomsten van de expertgroep zijn door de voorzitter en begeleider verwerkt in dit adviesrapport. Een eerste conceptversie is aan de leden van de expertgroep gestuurd met het verzoek om een reactie. Na verwerking van deze reacties is het rapport afgerond, nogmaals toegestuurd aan de experts en ingediend bij het Bureau Forum Standaardisatie ten behoeve van de publieke consultatieronde.

1.4 Vervolg

Dit expertadvies zal ten behoeve van een publieke consultatie openbaar worden gemaakt door het Bureau Forum Standaardisatie. Eenieder kan gedurende de consultatieperiode op dit expertadvies zijn/haar reactie geven. Het Bureau Forum Standaardisatie legt vervolgens de reacties voor aan de voorzitter en indien nodig aan de expertgroep.

Het Forum Standaardisatie zal op basis van het expertadvies en relevante inzichten uit de openbare consultatie een advies aan het Nationaal Beraad opstellen. Het Nationaal Beraad bepaalt uiteindelijk op basis van het advies van het Forum of de standaard op de 'pas toe of leg uit'-lijst komt.

1.5 Samenstelling expertgroep

Het Forum streeft naar een zo representatief mogelijke expertgroep, met een evenwichtige vertegenwoordiging van (toekomstige) gebruikers (zowel publiek als privaat), leveranciers, wetenschappers en andere kennishebbers. Daarnaast wordt een onafhankelijke voorzitter aangesteld om de expertgroep te leiden en als verantwoordelijke op te treden voor het uiteindelijke expertadvies.

Als voorzitter is opgetreden Marc Gill’ard, directeur bij Verdonck, Klooster & Associates. Jasmijn Wijn, adviseur bij Verdonck, Klooster & Associates, heeft de expertgroep in opdracht van het Bureau Forum Standaardisatie begeleid.

Aan de expertbijeenkomst hebben deelgenomen:
- Martijn Groeneweg, Measuremail (indiener)
- Carl Adamse, ministerie van BZK
- Sebastiaan Assink, Oxilion
- Alwin de Bruin, Measuremail
- John Dautzenberg, Gemeente Heerlen
- Marco Davids, SIDN
- Paul Dekkers, SURFnet
- Onno Hoogeveen, ministerie van BZK
- Willem Kossen, BKWI
- Maarten Oelering, Postmastery
- Pieter Rogaar, NCSC
- Rolf Sonneveld, Sonnection
- Tony van der Togt, ministerie van BZK
- Willem Toorop, NLnet Labs
- Paddy Verberne, Gemeente ‘s-Hertogenbosch
- Wijbren de Vries, UWV

Lancelot Schellevis van het Bureau Forum Standaardisatie was als toehoorder bij de expertbijeenkomst aanwezig. Martijn van Rooijen (Belastingdienst) heeft een schriftelijke bijdrage geleverd.

1.6 Toelichting DMARC

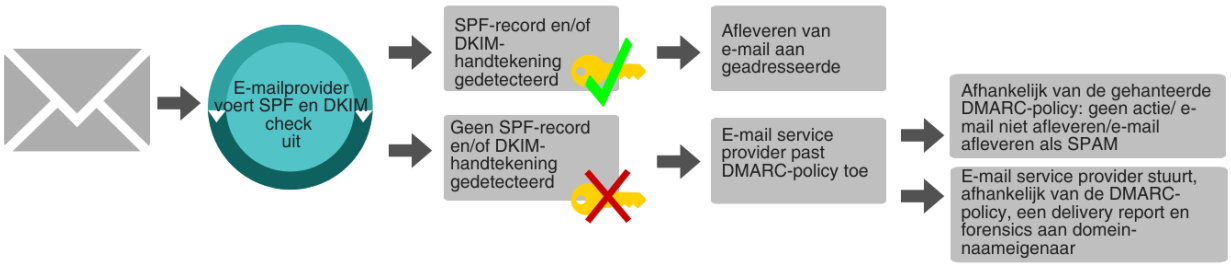
Domain-based Message Authentication, Reporting, and Compliance (DMARC) is een open standaard die het voor organisaties mogelijk maakt om beleid op te stellen over de manier waarop ontvangende e-mailproviders, die DMARC ondersteunen, om zouden moeten gaan met e-mail waarvan niet kan worden vastgesteld 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, zie figuur 1.

DMARC-record	Gevraagde actie van de ontvangende e-mailprovider
P=none	Geen actie van e-mailserviceprovider vereist. De e-mail kan als 'gewone' e-mail worden behandeld.
P=quarantine	Beschouw de mail als 'verdacht'. Dit kan betekenen dat mail aan extra controles/filtering wordt onderworpen, of als spam wordt aangemerkt of als verdacht wordt aangemerkt.
P=reject	Weiger de ongeauthenticeerde e-mail. De e-mail wordt niet afgeleverd aan de geadresseerde partij.

Figuur 1. Verschillende DMARC-records en gevraagde actie.

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.



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

DMARC kan worden ingezet voor het verminderen en/of voorkomen dat anderen e-mails kunnen versturen met gebruik making van het e-maildomein van de organisatie, en zo misbruik kunnen maken. De toepassing van DMARC bevordert de veiligheid van e-mailverkeer vanuit de (semi-)overheid. 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.

1.7 Relatie met andere standaarden

Samenhang met reeds opgenomen standaarden op de lijst voor 'pas toe of leg uit' of 'gangbare lijst'
DMARC maakt gebruik van DKIM. DKIM koppelt een e-mail aan een domeinnaam met behulp van een digitale handtekening. DMARC gebruikt het DKIM-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. Opname van de DMARC-standaard op de 'pas toe of leg uit'-lijst kan daarmee gezien worden als een aanvulling op de al opgenomen DKIM-standaard.

Daarnaast kent de standaard samenhang met DNSSEC en IPv6 (en diens voorganger IPv4). DMARC conflicteert niet met deze standaarden.

Samenhang met standaarden die mogelijk in aanmerking komen voor opname op één van de lijsten
DMARC maakt, naast DKIM, ook gebruik van SPF. SPF staat voor Sender Policy Framework. Dit is een internationale standaard die wordt beheerd door IETF. De standaard controleert in het DNS of de mailserver die een e-mail wil versturen namens het e-maildomein een e-mail mag verzenden.

Geadviseerd wordt om naast DMARC ook SPF op te nemen op de 'pas toe of leg uit'-lijst, onder voorwaarde dat SPF ook aan de gestelde toetsingscriteria voldoet. Als functioneel toepassingsgebied wordt geadviseerd:
Het controleren of een e-mailserver gerechtigd is om namens een domeinnaam e-mail te mogen verzenden.

1.8 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 voorgesteld:
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.

Belangrijk om te vermelden is dat vanuit iedere domeinnaam e-mail kan worden verstuurd. De standaard is daarom ook van waarde voor domeinnamen waarvandaan geen e-mails worden gestuurd, zoals 'parked domains'[2]. Het is voor de ontvangende partij (burgers, bedrijven en andere semi-overheidsorganisaties) veelal niet mogelijk om te kunnen beoordelen of een (semi-)overheidsorganisatie vanuit een bepaalde domeinnaam e-mail verstuurt.

2.2 Organisatorisch werkingsgebied

De expertgroep adviseert 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.

2 Er wordt gesproken van een parked domain wanneer een domein is geregistreerd zonder dat het direct wordt gebruikt voor een website of e-mailadres.

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. DMARC kan zowel toegepast worden voor elektronische gegevensuitwisseling tussen (semi-)overheidsorganisaties en bedrijven, (semi-)overheidsorganisaties en burgers, en (semi-) overheidsorganisaties onderling. De standaard kan voor zowel uitgaande als inkomende e-mailberichten worden gebruikt.

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)?
DMARC maakt in zijn toepassing gebruik van DKIM. DKIM koppelt een e-mail aan een domeinnaam met behulp van een elektronische handtekening. DMARC gebruikt het DKIM-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. Opname van de DMARC-standaard op de 'pas toe of leg uit'-lijst kan daarmee gezien worden als een aanvulling op de al opgenomen DKIM-standaard.

Daarnaast kent de standaard samenhang met DNSSEC en IPv6 (en diens voorganger IPv4). DMARC conflicteert niet met deze standaarden. DMARC is afhankelijk van een Domain Name Server (DNS) en het gebruik van DNSSEC is daarom aan te bevelen in combinatie met DMARC. IPv6 zorgt er voor dat ieder ICT-systeem binnen een netwerk een uniek IP-adres heeft en is hiermee de basis voor het gebruik van SPF (zie hieronder). Het gebruik van IPv6 doet mogelijk de noodzaak voor het gebruik van DMARC stijgen.

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 gevonden 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)
Er zijn geen concurrerende standaarden gevonden.

3.1.2.4 Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden? (toelichtende vraag)
DMARC wordt internationaal toegepast. Op dit moment is de standaard nog niet in beheer bij een standaardisatieorganisatie. De verwachting is dat DMARC op korte termijn in beheer wordt genomen door de Internet Engineering Task Force (IETF). IETF is een internationale standaardisatieorganisatie voor internetstandaarden. IETF beheert onder andere ook DKIM, SPF en DNSSEC.

3.1.2.5 Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn? (toelichtende vraag)
Organisaties die gebruik willen maken van DMARC moeten afspraken maken met bijvoorbeeld partijen die namens de overheid e-mail versturen. Het gebruik van de standaard vereist verder geen aanvullende standaardisatieafspraken. Het gebruik van DMARC is alleen mogelijk wanneer de e-mailserviceprovider van de ontvangende partij DMARC ondersteunt. Op dit moment wordt DMARC ondersteund door een aantal grote (web)mailproviders, waaronder Google (Gmail), Microsoft (Outlook en Hotmail) en XS4ALL. KPN werkt momenteel aan de ondersteuning van DMARC. Op de phishing scorecard[3] is helder inzichtelijk gemaakt welke organisaties de standaard ondersteunen.

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

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?

3.1.3.1 Draagt de adoptie van de standaard bij aan de oplossing van een bestaand, relevant interoperabiliteitsprobleem?
Ja. De toepassing van DMARC maakt het mogelijk om misbruik van de domeinnaam van (semi-)overheidsorganisaties zoveel mogelijk tegen 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. Dit is met name van belang bij e-mail uit grotere verzendingen, zogeheten bulk e-mail.

3.1.3.2 Draagt de standaard bij aan het voorkomen van een vendor lock-in (leveranciersafhankelijkheid)?
Ja. De standaard is vrij beschikbaar. Een aantal leveranciers biedt ondersteuning bij de implementatie van DMARC.

3.1.3.3 Wegen de overheidsbrede en maatschappelijke baten voor de informatievoorziening en de bedrijfsvoering op tegen de kosten?
De kosten die gemaakt worden om de standaard te gebruiken zitten voornamelijk in het analyseren van de feedback van DMARC. Voordat de standaard volledig in gebruik kan worden genomen moet een inventarisatie worden gemaakt wie namens de domeinnaam mag e-mailen. De tijdsinspanning die hiervoor nodig is verschilt per organisatie. Ook het interpreteren van en reageren op het DMARC-beleid van andere partijen kost tijd.

De experts adviseren organisaties om een kosten-batenanalyse te maken op het moment dat de DMARC policy moet worden ingericht om een inschatting van de tijdsinspanning te kunnen maken.

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?
Afhankelijk van de toegepaste policy ontvangen domeineigenaren bij het gebruik van DMARC *aggregate reports* en *failure reports.* Een aggregate report geeft een periodiek overzicht van de IP-adressen waarvandaan frauduleuze e-mail is verstuurd namens de domeinnaam. Een failure report is een kopie van de vermoedelijke phishing e-mail. Bij de invulling van het 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 Zie http://www.rijksoverheid.nl/documenten-en-publicaties/publicaties/2013/06/24/toetsmodel-privacy-impact-assessment-pia-rijksdienst.html.

3.1.4 Conclusie criteria 'Toegevoegde waarde'

De toepassing van DMARC maakt het mogelijk om misbruik van de domeinnaam van (semi-)overheidsorganisaties zoveel mogelijk tegen 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. Daarmee heeft de eigenaar van de domeinnaam een middel in handen om terugkoppeling te krijgen over e-mailstromen die de domeinnaam misbruiken.

Bij de invulling van het 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[5].

De expertgroep concludeert zodoende dat DMARC voldoende toegevoegde waarde heeft binnen het gekozen functioneel toepassingsgebied en organisatorisch werkingsgebied.

3.2 Open standaardisatieproces

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

DMARC is op dit moment nog niet in beheer bij een standaardisatieorganisatie (zie paragraaf 3.1.2.4). De verwachting is dat DMARC op korte termijn in beheer wordt genomen door de Internet Engineering Task Force (IETF). Hier is bij de beantwoording van onderstaande vragen vanuit gegaan. Wanneer er gesproken wordt over het beheer van de standaard en/of de standaardisatieorganisatie wordt hiermee IETF bedoeld.

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. 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. Er wordt op dit moment

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

gewerkt aan een draftdocument om DMARC te beschrijven als *Informational RFC*. Het huidige werkdocument en voorgaande versies zijn gepubliceerd op de website van IETF.

Specificaties doorlopen in het standaardisatieproces van IETF een twee stadia van volwassenheid; 'proposed standard', en 'internet standard'. De voortgang van de standaard in dit proces is transparant en kosteloos te volgen via de website van IETF.

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. Dit zal moeten gebeuren op het moment dat IETF DMARC in beheer neemt.

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?
Dat er bij inbeheername van de standaard door IETF geen IPR zijn geclaimd geeft geen garantie over toekomstige claims met betrekking tot het intellectueel eigendom.

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.

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[6] is kosteloos. De eerstvolgende IETF-bijeenkomst vindt plaats in Dallas, Texas (Amerika) van 22 t/m 27 maart 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[7], 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?*
IETF is een onafhankelijke organisatie zonder winstoogmerk.

3.2.4.2 *Is de financiering van de ontwikkeling en het onderhoud van de standaard voor tenminste drie jaar gegarandeerd?*
De financiering van de ontwikkeling en het onderhoud van de standaard wordt verzorgd door de leden van de werkgroep waar DMARC onder valt. Omdat DMARC nog niet in beheer is bij IETF kan hier specifiek voor DMARC op dit moment geen uitspraak over worden gedaan.

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.

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

3.2.5.3 *Is het belang van de Nederlandse overheid voldoende geborgd bij de ontwikkeling en het beheer van de standaard?*
Omdat DMARC nog niet in beheer is bij IETF zijn er ook nog geen werkgroepen actief bezig met de (door)ontwikkeling van de standaard. Op het moment dat DMARC in beheer wordt genomen door IETF kan de Nederlandse overheid zich, indien gewenst, aanmelden voor deelname aan een van de werkgroepen voor DMARC.

3.2.6 *Conclusie criteria 'Open standaardisatieproces'*
De expertgroep concludeert dat het standaardisatieproces van IETF voldoende open is. Voorwaarde voor opname van DMARC op de 'pas toe of leg uit'-lijst is echter wel dat DMARC minimaal een proposed standaard is en wordt beheerd door IETF, of een andere, vergelijkbare standaardisatieorganisatie.

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?*
Er zijn meerdere leveranciers die ondersteuning bieden voor de implementatie van DMARC. Ook zijn er op het internet meerdere aanbieders te vinden die (gratis) producten en diensten aanbieden ter ondersteuning van de implementatie van de standaard en tools voor analyse van rapportages.[8]

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 DMARC kan worden getoetst, waaronder https://dmarcian.com/dmarc-inspector/ en https://www.dmarcanalyzer.com/. Na invoering van de domeinnaam wordt getoetst of er een DMARC-record is toegevoegd aan de domeinnaam.

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?*
DMARC wordt op dit moment binnen de (semi)overheid gebruikt door de Dienst Publiek en Communicatie (onderdeel van het ministerie van Algemene Zaken), de gemeente Heerlen, de gemeente Voerendaal en het Veiligheidshuis Limburg. Voor de domeinnamen forumstandaardisatie.nl en internet.nl (Platform Internetstandaarden) zijn DMARC-records toegevoegd. Een aantal organisaties is momenteel bezig met de implementatie van DMARC, zie paragraaf 3.3.2.4.

3.3.2.2 *Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt?*
Dit is niet van toepassing, aangezien er geen eerdere versie van DMARC is.

8 Zie http://www.dmarc.org/resources.html.

3.3.2.3 Is de aangemelde versie backwards compatible met eerdere versies van de standaard?
Dit is niet van toepassing, aangezien er geen eerdere versie van DMARC is.

3.3.2.4 Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?
DMARC wordt op dit moment door een aantal organisaties binnen de (semi-)overheid geïmplementeerd, waaronder het ministerie van Veiligheid en Justitie, de Belastingdienst en de gemeenten 's-Hertogenbosch, Heerlen, Landgraaf en Kerkrade.

3.3.3 Conclusie criteria 'Draagvlak'
De expertgroep concludeert dat het draagvlak voor DMARC voldoende is. 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. Toekomstige gebruikers kunnen hierbij rekenen op voldoende marktondersteuning voor de implementatie en bij het gebruik van de standaard.

3.4 Opname bevordert adoptie

De opname op de lijst is een geschikt middel om de adoptie van de standaard te bevorderen.

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 DMARC binnen de (semi)overheid 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 e-mailbeveiligingsstandaarden zoals DMARC, DKIM en SPF ook op bestuurlijk niveau 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 DMARC heeft nog niet de omvang die nodig is om de standaard als gangbaar te kunnen beschouwen.

3.4.3 Conclusie criteria 'Opname bevordert adoptie'
De expertgroep concludeert dat de 'pas toe of leg uit'-lijst het passende middel is om de adoptie van de standaard binnen de (semi)overheid te bevorderen.

3.5 Adoptieactiviteiten

Gebruik van de standaard is het einddoel van het Forum en College. Plaatsing op de lijsten is hiervoor een goede stap, maar voor het daadwerkelijk adopteren (implementeren en gebruiken) van de standaard is vaak aanvullende actie benodigd. Aanvullend kan Forum Standaardisatie dan ook bijdragen aan adoptie van de standaard door het actief inzetten van adoptie-instrumenten of ondersteunende acties. Welke kansen zijn er om de adoptie te versnellen en welke drempels bestaan er die de adoptie van de standaard hinderen?

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 te doen:

- 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.
- Het Forum Standaardisatie wordt opgeroepen om bij (semi)overheidsorganisaties het gebruik van DMARC (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.
- 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.
- 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.
- 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.
- 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.