notitie

FORUM STANDAARDISATIE 16 december 2014
Agendapunt 5. Open standaarden, lijsten
Stuknummer 5A. Intake-advies DMARC

## Advies

Het Forum Standaardisatie wordt geadviseerd om DMARC, een standaard voor de verificatie van de authenticiteit van e-mailberichten, in procedure te nemen voor opname op de 'pas uit of leg toe'-lijst.

Over de standaard
Domeinnamen zijn veelal beperkt beveiligd waardoor het voor anderen mogelijk is namens de domeinnaam van een organisatie e-mailberichten te sturen. Via deze e-mails kunnen bijvoorbeeld gevoelige gegevens zoals creditcardnummers of inloggegevens voor DigiD en eHerkenning worden ontfutseld (zogenaamde phishing). Ook is het mogelijk om virussen te verspreiden. 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.

Er zijn standaarden op de markt die tot doel hebben om spam- en phishing-mails beter te kunnen filteren, zoals SPF en DKIM. Dit gebeurt in het geval van DKIM door de toevoeging van een elektronische sleutel in het e-mailbericht en in het geval van SPF door het controleren en verifiëren van het IP-adres van uitgaande e-mailservers. Hoewel door het gebruik van deze standaarden het aantal ontvangen spam- en phishing-e-mails zal verminderen, stelt het de eigenaar van de domeinnaam nog niet in staat inzicht te krijgen in het mogelijk misbruik van de eigen domeinnaam. Evenmin hebben zij invloed op de actie die een ontvangende e-mailprovider neemt op een e-mail waarvan is vastgesteld dat het niet voldoet aan het SPF- en/of DKIM-beleid. Zonder gebruik van DMARC bepalen e-mailproviders namelijk zelf wat gebeurt met e-mailberichten die als onrechtmatig worden beschouwd.

DMARC is een open standaard die het voor organisaties mogelijk maakt om te bepalen hoe e-mailproviders, die DMARC ondersteunen, omgaan met e-mail waarvan niet kan worden vastgesteld dat deze afkomstig is van het

eigen domein. Hierdoor kunnen organisaties voorkomen dat anderen e-mails versturen namens het e-maildomein van de organisatie. Hierbij kan gedacht worden aan phishing e-mails en spam. Het gebruik van 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 e-mailproviders onterecht voor spam worden aangezien.

De standaard voldoet aan de criteria voor inbehandelname. Mede door de toepasbaarheid van de standaard en de relatie tot de al op de lijst opgenomen standaard DKIM (DomainKeys Identified Mail) is de kansrijkheid van de procedure voldoende.

De standaard kent naast samenhang met DKIM ook samenhang met SPF (Sender Policy Framework). Via SPF kan worden aangegeven welke e-mailservers e-mail namens een domein mogen versturen. DMARC maakt in haar toepassing gebruik van SPF en DKIM. DMARC kan zodoende alleen gebruikt worden wanneer een organisatie SPF en/of DKIM toepast. Daarnaast kent de standaard een nauwe relatie met DNSSEC een standaard voor het beveiligen van domeinnamen en de netwerkstandaard IPv6.

De standaard is ingediend door Measuremail en wordt naar verwachting ondersteund door de Dienst Publiek en Communicatie (onderdeel van het ministerie van Algemene Zaken), de gemeente Den Bosch en de gemeente Heerlen.

*Over het toepassingsgebied*
Geadviseerd wordt om tijdens de expertsessie stil te staan bij een goede definiëring van het functioneel toepassingsgebied van de standaard. De standaard zou in ieder geval verplicht gesteld moeten worden voor alle domeinnamen (van partijen in het organisatorisch werkingsgebied) die burgers en bedrijven vertrouwen als zij daar e-mail van zouden ontvangen (uitgaande mail). Het is de vraag of het functioneel toepassingsgebied ook gericht moet zijn op het toepassen van DMARC op alle inkomende e-mail.

# Toelichting

### 1. Aanmelding, intakegesprek en toetsingsprocedure

Op 30 oktober 2014 is door Martijn Groeneweg van Measuremail BV een melding ingediend, betreffende de aanmelding van DMARC versie Base05 voor de 'pas toe of leg uit'-lijst.

Op 14 november 2014 heeft een intakegesprek plaatsgevonden met de aanmelder. Hierbij is gekeken of alle basisinformatie aanwezig is en of de standaard voldoet aan de criteria voor inbehandelname. Daarnaast is vooruitgeblikt op de procedure.

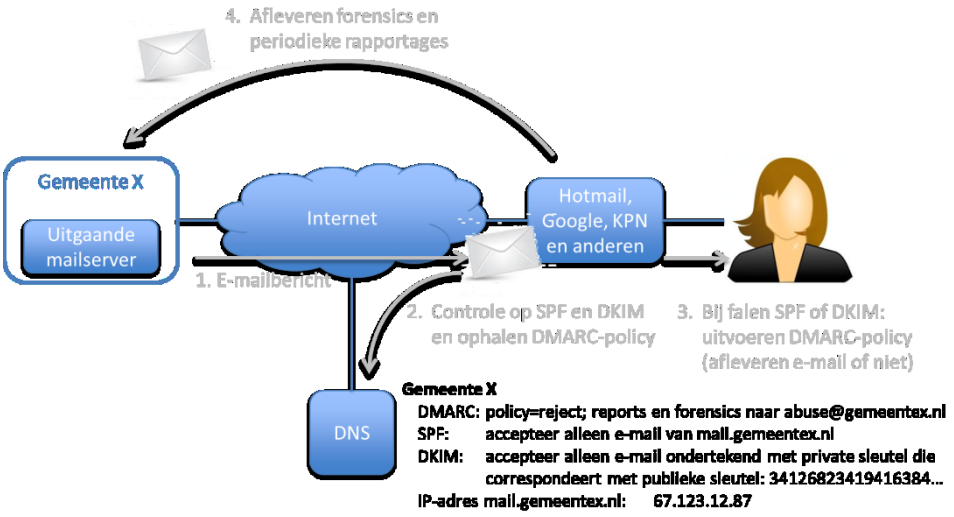
### 2. Korte beschrijving standaard

*Waar gaat de standaard over?*
Domain-based Message Authentication, Reporting, and Compliance (DMARC) is een open standaard die het voor organisaties mogelijk maakt om te bepalen hoe e-mailproviders, die DMARC ondersteunen, omgaan met ongeauthenticeerde e-mail die 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 kunnen organisaties aangeven wat er met een ongeauthenticeerd e-mailbericht moet gebeuren (blokkeren of toch verzenden naar een ontvanger). Verder kan een organisatie aangeven op welke manier de organisatie hierover gerapporteerd wil worden (real time een rapportage met het IP-adres van de SMTP-server of een kopie van de valse e-mail). Daarnaast is periodieke geaggregeerde rapportage mogelijk.

Zonder de toepassing van DMARC bepalen e-mailproviders zelf wat met ongeauthenticeerde e-mailberichten gebeurt. Organisaties waarvan de domeinnaam is 'misbruikt' hebben hier geen invloed op en inzicht in.

DMARC kan ingezet worden in het verminderen en/of voorkomen dat anderen e-mails kunnen versturen namens 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 emailextensie. Gebruik van DMARC maakt in dit geval inzichtelijk dat er vanuit een domeinnaam ongewenst mail wordt verstuurd.

Bij het toepassen van DMARC wordt gebruikt gemaakt van SPF- en DKIM-mechanismen (zie ook 5. Samenhang).




*Wie beheert de standaard?*

De standaard wordt beheerd door de Internet Engineering Task Force (IETF).

*Waarom is de standaard aangemeld voor pas toe of leg uit?*
Door de nauwe relatie tussen DKIM en DMARC is tijdens de behandeling van DKIM voor opname op de 'pas toe of leg uit'-lijst al gesproken over DMARC. Omdat de DMARC-standaard destijds nog in ontwikkeling was is alleen DKIM in procedure genomen. DMARC is in de tussentijd dermate ontwikkeld dat dit heeft geleid tot aanmelding van de standaard voor opname op de lijst voor 'pas toe of leg uit'. Gebruik van de standaard is groeiende, maar kent op dit moment nog niet de omvang die nodig is om te kunnen worden beschouwd als gangbare standaard. Opname van de standaard op de 'pas toe of leg uit'-lijst kan zodoende helpen om de adoptie van de standaard verder te bevorderen.

(zie ook: *7. Functionele use case*)

## 3. Criteria voor inbehandelname

Om een standaard in behandeling te nemen moet de standaard vallen binnen de scope van de lijsten. Hiervoor gelden drie criteria:

*1. Is de standaard toepasbaar voor elektronische gegevensuitwisseling tussen (semi-)overheidsorganisaties en bedrijven, tussen (semi-)overheidsorganisaties en burgers of tussen (semi-)overheidsorganisaties onderling?*
Ja. De standaard heeft namelijk betrekking op veilige elektronische gegevensuitwisseling, e-mail, vanuit (semi-)overheidsorganisaties richting burgers, bedrijven en andere (semi-)overheidsorganisaties.

*2. Is het beoogde functioneel toepassingsgebied en het organisatorisch werkingsgebied van de standaard, voldoende breed om substantieel bij te dragen aan de interoperabiliteit van de (semi-)overheid?*
Ja. De standaard is algemeen toepasbaar, ook binnen het werkgebied van de (semi-)overheid.

DMARC kan toegepast worden voor zowel inkomende als uitgaande e-mailberichten. Bij de behandeling van de standaard door de experts dient nagedacht te worden over de reikwijdte van het toepassingsgebied.

*3. Is het zinvol de standaard op te nemen, gezien het feit dat deze niet al wettelijk verplicht is voor het beoogde functioneel toepassingsgebied en organisatorisch werkingsgebied?*
Ja. De standaard is niet wettelijk verplicht en opname van de standaard op de 'pas toe of leg uit'-lijst kan helpen om de adoptie van de standaard verder te bevorderen.

<u>Conclusie</u>
De standaard voldoet aan de criteria voor inbehandelname.

## 4. Toetsing kansrijkheid procedure

Het Forum Standaardisatie wil voorkomen dat er standaarden in procedure worden genomen, waarvan bij voorbaat al bekend is dat deze in de expertronde of consultatieronde zullen stranden op één van de inhoudelijke criteria. Daarom heeft de procedurebegeleider de beantwoording van de criteriavragen nagelopen, waar mogelijk zelf aangevuld en vervolgens besproken met de indiener.

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

IETF is een internationale beheerorganisatie met open beheerprocessen. Naast DMARC beheert het ook andere standaarden waaronder DKIM en SPF. Het specificatiedocument en documentatie over het ontwikkel- en beheerproces zijn kosteloos en voor een ieder te downloaden van de website van IETF (www.ietf.org). Nieuwe versies van de standaard zijn backwards compatible met oude versies.

Het gebruik van de standaard is gratis. Verschillende werkgroepen werken aan de (door)ontwikkeling van standaarden. Samenwerking binnen deze werkgroepen gebeurt veelal via e-mail. Gebruikers kunnen zich via de website van IETF kosteloos aanmelden voor de werkgroepen.

*2. Toegevoegde waarde*
De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de kosten, de risico's en nadelen. Voor elk van de te onderscheiden stakeholders (overheid, bedrijven en burgers) afzonderlijk zouden de baten voor de informatievoorziening en de bedrijfsvoering op moeten wegen tegen de kosten. Verder moeten de risico's aan overheidsbrede adoptie van de standaard (beveiliging, privacy) acceptabel zijn.

De toepassing van DMARC maakt het mogelijk om misbruik van de domeinnaam van (semi-)publieke organisaties zoveel mogelijk tegen te gaan. In combinatie met DKIM en/of SPF wordt de afzender van een e-mailbericht geverifieerd. Hierdoor kan bij ontvangst van een e-mail door de ontvanger met redelijke zekerheid aangenomen worden dat de identiteit van de verzender van e-mails juist is. Dit is met name van belang bij e-mail uit grotere verzendingen (zogeheten bulk-mails). Deze e-mails worden door spamfilters snel voor spam aangezien. Wanneer dit een e-mail betreft waaraan consequenties voor de ontvangende partij zitten (bijvoorbeeld burgers), is het noodzakelijk dat de afzender geverifieerd kan worden.

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 (de zender) een middel in handen om terugkoppeling te krijgen over e-mailstromen die de domeinnaam misbruiken bij onder andere phishing pogingen.

*3. Draagvlak*

Aanbieders en gebruikers moeten voldoende ervaring hebben met de implementatie en het gebruik van de standaard.

De standaard wordt momenteel in combinatie met de standaarden SPF en DKIM gebruikt door de gemeente Heerlen en het Forum Standaardisatie. De Rijksoverheid (onderdeel van het ministerie van Algemene Zaken) gebruikt DMARC voor een aantal domeinnamen in combinatie met SPF en DKIM. Een aantal andere gemeenten werken momenteel aan de implementatie van de standaard. Deze gemeenten maken al gebruik van SPF en/of DKIM, maar nog niet van DMARC. Het ministerie van Veiligheid en Justitie werkt aan de implementatie van DMARC, maar heeft SPF en DKIM (nog) niet geïmplementeerd.

Een aantal grote (web)mailproviders ondersteunen DMARC, waaronder Google (Gmail), Microsoft (Outlook en Hotmail) en Xs4all. KPN werkt momenteel aan de ondersteuning van DMARC. Op de phishing scorecard (https://www.phishingscorecard.com) is helder inzichtelijk gemaakt welke organisaties de standaard ondersteunen.

*4. Opname bevordert adoptie*
De opname op de lijst moet een geschikt middel zijn om de adoptie van de standaard te bevorderen.

DMARC versie base05 is aangemeld voor opname op de lijst voor 'pas toe of leg uit'. Het gebruik van de standaard kent op dit moment nog niet de omvang die nodig is om te kunnen worden beschouwd als gangbare standaard. Opname van de standaard op 'pas toe of leg uit'-lijst kan zodoende helpen om de adoptie van de standaard verder te bevorderen.

Conclusie
Er is op voorhand een mogelijk struikelblok te verwachten. Wanneer een ongeauthenticeerd e-mailbericht wordt gesignaleerd ontvangt de domeineigenaar direct een kopie van deze e-mail. Deze e-mail kan persoonsgegevens van de ontvangende partij bevatten. Tijdens de toetsingsprocedure dient onderzocht te worden of dit juridisch toelaatbaar is in verband met privacy van ontvangende partijen. Overigens is het ook mogelijk de standaard zinvol in te zetten zonder dat deze optie wordt gebruikt.

## 5. Samenhang

Forumstandaardisatie wil weten of de aangemelde standaard samenhangt met standaarden die reeds op de 'pas toe of leg uit' -lijst en gangbare lijst zijn opgenomen, of standaarden die voor toetsing in aanmerking komen. Uit de intake moet duidelijk worden of dit gevolgen heeft voor de toetsing en eventuele opname van de aangemelde standaard.

1. Bestaat er samenhang tussen de aangemelde standaard en de standaarden die reeds op de **'pas toe of leg uit' -lijst** zijn opgenomen en wat betekent dit voor de toetsing en eventuele opname van de standaard?

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 een e-mail te verifiëren. Zodra dit niet mogelijk is wordt het DMARC-beleid in werking gezet.

Opname van de DMARC-standaard op de lijst voor 'pas toe of leg uit' 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 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.

2. Bestaat er samenhang tussen de aangemelde standaard en de standaarden die reeds op de **gangbare lijst** zijn opgenomen en wat betekent dit voor de toetsing en eventuele opname van de standaard?
   Er zijn geen standaarden gevonden.

3. Bestaat er samenhang tussen de aangemelde standaard en standaarden die in aanmerking komen voor opname op één van de lijsten en wat betekent dit voor de toetsing van de standaard(en)? (Denk bijvoorbeeld ook aan een gezamenlijke toetsing met (een deel van) deze aanvullende standaarden).

   Naast DKIM maakt DMARC ook gebruik van SPF. SPF staat voor Sender Policy Framework, een internationale standaard die ook wordt beheerd door IETF. De standaard controleert in het DNS (Domain Name Server) of de mailserver die een e-mail wil versturen namens het e-maildomein een e-mail mag verzenden. Wanneer dit niet het geval is wordt de e-mail als onrechtmatig beschouwd.

   DMARC vormt een feitelijke drie-eenheid met DKIM en SPF. Gedacht kan worden om bij de toetsing van DMARC ook SPF te behandelen.

## 6. Sponsorschap

De aanmelding van standaarden voor de lijsten van Forum en College dient ondersteund of gesponsord te worden door overheids- en/of (semi)publieke organisaties die de standaard reeds in gebruik hebben (of voornemens zijn dit te doen) en die de beoogde opname op de lijsten ondersteunen. Dit draagt bij aan het draagvlak voor de standaard, geeft zich op de functionele usecase voor de overheid en helpt bovendien om tijdens de toetsing de juiste experts te benaderen.

1. Welke overheden en/of (semi) publieke organisaties ondersteunen de aanmelding van de standaard?

Dienst Publiek en Communicatie (onderdeel van het ministerie van Algemene Zaken) en de gemeente Heerlen, maken gebruik van DMARC en zijn enthousiast over het effect. Verder wordt de standaard ook voorgeschreven door het Centrum voor Informatiebeveiliging en Privacybescherming (CIP). Met deze organisatie wordt afgestemd of ze de aanmelding kunnen ondersteunen.

2. Hebben deze organisaties de standaard geïmplementeerd?
   (zie ook punt 7 voor een uitwerking)
   De Dienst Publiek en Communicatie (onderdeel van het ministerie van Algemene Zaken) en de gemeente Heerlen hebben DMARC, DKIM en SPF geïmplementeerd.

## 7. Functionele use case

Voor de standaard dient een duidelijke use case beschikbaar te zijn op basis waarvan overheden en/of instellingen uit de (semi) publieke sector kunnen bepalen of de aangemelde standaard voor hen relevant is en wie eventueel moet deelnemen aan de experttoetsing van de standaard.

DMARC is 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-)overheidsinstellingen ongeauthenticeerde e-mails ontvangen. Hierbij kan gedacht worden aan gemeenten, uitvoeringsorganisaties (zoals Belastingdienst, DUO, UWV, SVB, DNB), provincies, ministeries (waaronder de Dienst Publiek en Communicatie van het ministerie van Algemene Zaken).

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.

Daarnaast voorkomt de toepassing van de standaard dat e-mails uit grotere verzendingen (bulkmail) door spamfilters onterecht als spam worden gezien, omdat de afzender kan worden geverifieerd.