## Aanmelding van een nieuwe standaard voor de 'pas toe of leg uit'-lijst

Voor dit type aanmelding geldt dat alle criteria van toepassing zijn en alle vragen beantwoord dienen te worden. U wordt als eerst gevraagd uw persoonsgegevens en de basisinformatie van de standaard te geven. Vervolgens dienen de criteriavragen beantwoord te worden. De criteria vallen uiteen in *criteria voor inbehandelname* en *inhoudelijke criteria*.

### 0. Persoonsgegevens indiener & relatie tot standaard

Deze gegevens worden door het Forum gebruikt om met u in contact te kunnen treden. De gegevens worden vertrouwelijk behandeld.

| **0.** | **Persoonsgegevens en relatie tot de standaard** |
|---|---|
| 0.1 | Naam: |
| | |
| 0.2 | Organisatie: |
| | Measuremail |
| 0.3 | Functie: |
| | |
| 0.4 | Telefoonnummer: |
| | |
| 0.5 | E-mailadres |
| | |
| 0.6 | Welke relatie bestaat er tussen uw organisatie en de standaard? |
| | Measuremail is e-mail service provider en past de DMARC standaard reeds toe in combinatie met de standaarden SPF en DKIM in het kader van e-mail deliverability en e-mail authenticatie. Measuremail verstuurt onder andere voor Rijksoverheid en de Europese Unie diverse mailstromen, waar de standaarden DMARC, DKIM en SPF ook al op worden toegepast. Tevens hebben we de Gemeente Heerlen ondersteunt om DMARC, DKIM en SPF te implementeren. |
| 0.7 | Zijn er (andere) overheidsorganisaties die de aanmelding van deze standaard ondersteunen? |
| | Ik ga dit nog even navragen om bevestigd te krijgen, maar ik denk dat de volgende 2 overheidsorganisaties de aanmelding ondersteunen:<br>1. Dienst Publiek en Communicatie (onderdeel van het Ministerie van Algemene Zaken<br>2. Gemeente Heerlen<br>3. Mogelijk ook nog de Gemeente Den Bosch |

#### I. Basisinformatie aanmelding standaard

De basisinformatie van de standaard vormt de basis voor de toetsing tegen de criteria. Probeer hier zo volledig mogelijk in te zijn.

| | |
|---|---|
| **1.** | **Basisinformatie standaard(en)**<br>(In geval van een set van standaarden, meerdere malen invullen) |
| 1.1 | Volledige naam van de standaard |
| | Domain-based Message Authentication, Reporting & Conformance |
| 1.2 | Verkorte naam van de standaard |
| | DMARC |
| 1.3 | Versie van de standaard, vaststellingsdatum en status |
| | Base05 vastgesteld op 28-10-2014 met status: informational |
| 1.4 | Oudere en aanstaande versies van de standaard inclusief (verwachte) publicatiedata en ondersteuningsstatus |
| | Zie https://datatracker.ietf.org/doc/draft-kucherawy-dmarc-base/ |
| 1.5 | Naam en vindplaats specificatiedocument (bij voorkeur URL of bijvoegen bij aanmelding) |
| | https://datatracker.ietf.org/doc/draft-kucherawy-dmarc-base/ |
| 1.6 | Naam van de standaardisatieorganisatie |
| | IETF |
| 1.7 | Kosten van deelname aan het standaardisatieproces (bijv. voor lidmaatschap) |
| | 0 euro |
| 1.8 | Kosten voor het verkrijgen van het specificatiedocument |
| | 0 euro |
| 1.9 | Andere standaarden die genoemd worden in het specificatiedocument van de standaard |
| | DomainKeys Identified Mail (DKIM)<br>Sender Policy Framework (SPF) |
| 1.10 | Hoe werkt de standaard?<br>(graag op een bondige en voor een buitenstaander duidelijke manier beschrijven hoe de standaard werkt en wat deze mogelijk maakt) |
| | DMARC zorgt ervoor dat anderen niet namens jouw domein een e-mail kunnen sturen. |

| | |
|---|---|
| **2.** | **Toepassings- en werkingsgebied van opname** |
| 2.1 | Wat is het beoogde functioneel toepassingsgebied voor de standaard? |

| | |
|---|---|
| | Iedereen kan namens ieder domein een e-mail sturen naar iedereen. DMARC zorgt voor e-mail authenticatie, waardoor anderen niet namens jouw domein een e-mail kunnen sturen. Valse e-mails (phishing) kunnen hiermee voorkomen worden. |
| 2.2 | Wat is het beoogde organisatorisch werkingsgebied voor de standaard?<br>(*hoeft alleen ingevuld te worden als de standaard op de 'pas toe of leg uit' –lijst is opgenomen)* |
| | |

**II. Criteria voor inbehandelname**

De criteria voor inbehandelname worden gebruikt tijdens de intake om te bepalen of een aanmelding correct is en binnen de scope van de lijsten valt. U kunt voor het beantwoorden van deze vraag de tekstvlakken bij de betreffende criteriavragen gebruiken.

***Criteria:*** De aanmelding is correct en valt binnen scope van de lijsten, d.w.z. de standaard:

- Is toepasbaar voor elektronische gegevensuitwisseling tussen en met (semi-)overheidsorganisaties;
- Draagt binnen het beoogde opnamegebied substantieel bij aan de interoperabiliteit van de (semi-)overheid;
- Is niet reeds wettelijke verplicht.

| **1.** | **Valt de aangemelde standaard binnen de scope van de lijsten?** |
|---|---|
| 1.1 | Is de standaard toepasbaar voor elektronische gegevensuitwisseling tussen (semi-) overheidsorganisaties en bedrijven, tussen (semi-)overheidsorganisaties en burgers of tussen (semi-)overheidsorganisaties onderling? |
| | Ja, omdat de standaard betrekking heeft betrekking op e-mail. |
| 1.2 | 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, omdat iedere dag bijna 4x meer legitieme e-mails worden verstuurd dan het aantal Facebook/Twitter updates, Google searches en website bezoeken bij elkaar. |
| 1.3 | 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 |

**III. Inhoudelijke criteria**

De inhoudelijke criteria worden gebruikt voor het expertonderzoek om te adviseren over het al dan niet opnemen van de standaard op één van de lijsten. U kunt voor het beantwoorden van deze

vragen de tekstvlakken bij de betreffende criteriavragen gebruiken. De vragen dienen beantwoord te worden met Ja, Nee of Onbekend en altijd te worden voorzien van een toelichting op het antwoord.

**III. Inhoudelijke criteria**

**1. Inhoudelijk criterium: Toegevoegde waarde**

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

***Vragen:***

| **1.1** | **Verhoudt de standaard zich goed tot andere standaarden?** |
|---|---|
| 1.1.1 | 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, de standaard vormt een feitelijke 3-eenheid samen met DKIM en SPF. Verder is er een nauwe relatie met DNSSEC en IPv6. |
| 1.1.2 | 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.)* |
| | Ja, je kan zelfs stellen dat je aan de huidige DKIM standaard relatief weinig hebt zonder de combinatie met SPF en DMARC. |
| 1.1.3 | Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname? |
| | Ja, DMARC wordt wereldwijd voor inkomende e-mail al toegepast voor zo'n 60% van alle e-mail boxen. |
| 1.1.4 | Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden? |
| | Ja, het is een internationale standaard, die voortbouwt op de open standaarden SPF en DKIM. |
| 1.1.5 | Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn? |
| | Ja, de standaard wordt al dagelijks wereldwijd voor meer dan 80.000 actieve domeinnamen toegepast zonder enige aanvullende standaardisatie afspraak. Van belang is wel dat zowel verzenders als ontvangers van e-mail DMARC toe gaan passen. |

| | |
|---|---|
| **1.2** | **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?** |
| 1.2.1 | Draagt de adoptie van de standaard bij aan de oplossing van een bestaand, relevant interoperabiliteitsprobleem? |
| | Ja, omdat phishing e-mails namens bijvoorbeeld de domeinnaam @belastingdienst.nl bij zo'n 45% van de Nederlandse burgers simpelweg niet meer aan zal komen. KPN zal ook inkomend DMARC toe gaan passen, waarmee dit percentage naar zo'n 60% zal gaan. |
| 1.2.2 | Draagt de standaard bij aan het voorkomen van een vendor lock-in (leveranciersafhankelijkheid)? |
| | Ja, er zijn leveranciers op de markt die bilaterale afspraken maken met ISP's. Middels DMARC kan je als eigenaar van een domeinaam zelf aangeven aan ISP's wat zij moeten doen, als ze een valse e-mail namens jouw domeinnaam ontvangen. |
| 1.2.3 | Wegen de overheidsbrede en maatschappelijke baten voor de informatievoorziening en de bedrijfsvoering op tegen de kosten? |
| | Ja, ik durf zelfs te stellen, dat deze standaard bovenaan de prioriteitenlijst van bijvoorbeeld Belastingdienst, DigID, etc zouden moeten staan om te implementeren gezien de bestaande phishing problematiek. |
| 1.2.4 | Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel? |
| | Ja, feitelijk is het een standaard ter bevordering van de veiligheid van e-mail verkeer. |
| 1.2.5 | Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel? |
| | Ja, omdat in de zogeheten DMARC reports alleen IP-adressen zijn opgenomen van SMTP servers. Bij de forensic reports ontvangt een domeinnaam eigenaar vrijwel realtime een kopie van een valse e-mail. Die ontvangt hij nu ook, echter veelal met vertraging via de abuse desk. |

## 2. Inhoudelijk criterium: Open standaardisatieproces

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

***Vragen:***

| **2.1** | **Is de documentatie voor eenieder drempelvrij beschikbaar?** |
|---|---|
| 2.1.1 | Is het specificatiedocument beschikbaar zonder dat er sprake is van onacceptabele belemmeringen (zoals te hoge kosten en te hoge lidmaatschapseisen)? |
| | Ja, zie https://datatracker.ietf.org/doc/draft-kucherawy-dmarc-base |
| 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)? |
| | Ja, zie https://datatracker.ietf.org/doc/draft-kucherawy-dmarc-base |

| **2.2** | **Is het intellectuele eigendomsrecht voor eenieder beschikbaar, zodat de standaard vrij implementeerbaar en te gebruiken is** |
|---|---|
| 2.2.1 | Stelt de standaardisatieorganisatie het intellectueel eigendomsrecht op de standaard m.b.t. bijvoorbeeld eventuele patenten- onherroepelijk royalty-free voor eenieder beschikbaar? |
| | Ja, zie https://datatracker.ietf.org/doc/draft-kucherawy-dmarc-base |
| 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? |
| | Ja, zie https://datatracker.ietf.org/doc/draft-kucherawy-dmarc-base |

| **2.3** | **Is de inspraak van eenieder in voldoende mate geborgd?** |
|---|---|
| 2.3.1 | Is het besluitvormingsproces toegankelijk voor alle belanghebbenden (bijv. gebruikers, leveranciers, adviseurs, wetenschappers)? |
| | Ja, IETF |
| 2.3.2 | Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen? |
| | Ja, IETF |
| 2.3.3 | Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde procedure? |
| | Ja, IETF |

## III. 2. Inhoudelijk criterium: Open standaardisatieproces (vervolg)

*Let op: ook de grijs gemarkeerde vragen dienen positief beantwoord te worden wil een organisatie in aanmerking komen voor de status uitstekend beheerproces.*

| | |
|---|---|
| 2.3.4 | Organiseert de standaardisatieorganisatie regelmatig overleggen met belanghebbenden over doorontwikkeling en beheer van de standaard? |
| | Ja, IETF |
| 2.3.5 | Organiseert de standaardisatieorganisatie een publieke consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld? Zie ook bijlage 3 uit de toetsingsprocedure en criteria. |
| | Ja, IETF |

| **2.4** | **Is de standaardisatieorganisatie onafhankelijk en duurzaam?** |
|---|---|
| 2.4.1 | Is de ontwikkeling en het beheer van de standaard belegd bij een onafhankelijke non-profit standaardisatieorganisatie? |
| | Ja, IETF |
| 2.4.2 | Is de financiering van de ontwikkeling en het onderhoud van de standaard voor tenminste drie jaar gegarandeerd? |
| | Ja, IETF |

| **2.5** | **Is het (versie) beheer van de standaard goed geregeld?** |
|---|---|
| 2.5.1 | Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot versiebeheer van de standaard? (met o.a. aandacht voor migratie van gebruikers) |
| | Ja, IETF |
| 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? |
| | Ja, IETF |
| 2.5.3 | Is het belang van de Nederlandse overheid voldoende geborgd bij de ontwikkeling en het beheer van de standaard? |
| | Ja, IETF |
| 2.5.4 | Is de vertegenwoordiging van belanghebbenden bij het beheer van de standaard een goede representatie van het werkingsgebied en functioneel toepassingsgebied van de standaard? |
| | Ja, IETF |

**III. Inhoudelijke criteria**

**3. Inhoudelijk criterium: Draagvlak**

***Criterium:*** Aanbieders en gebruikers hebben voldoende positieve ervaring met de standaard.

***Vragen:***

| **3.1** | **Bestaat er voldoende marktondersteuning voor de standaard?** |
|---|---|
| 3.1.1 | Bieden meerdere leveranciers ondersteuning voor de standaard? |
| | Ja, Measuremail past DMARC al toe voor al haar klanten. Het betreft een DNS toevoeging in de vorm van een txt record dat door alle DNS servers standaard wordt ondersteund. Aan de ontvangende kant (bv inkomend mail verkeer naar infrastructuur Rijksoverheid), is de toepassing van DMARC nog in ontwikkeling. |
| 3.1.2 | Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen? |
| | Ja, de conformiteit is eenvoudig te toetsen. Zie https://www.phishingscorecard.com/ScoreCard/Netherlands/Government/MS0y en zie https://dmarcian.com/dmarc-inspector/measuremail.com. |

| **3.2** | **Kan de standaard rekenen op voldoende draagvlak?** |
|---|---|
| 3.2.1 | Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt? |
| | Ja, zie https://www.phishingscorecard.com/ScoreCard/Netherlands/Government/MS0y<br>Verder passen partijen als Hotmail (Microsoft), Gmail, Yahoo, AOL, mail.ru en NetEase, etc ook inkomend al bijna 3 jaar DMARC toe. Ook de grote sociale netwerken passen DMARC voor hun domeinnamen al toe, zie https://www.phishingscorecard.com/ScoreCard/International/Internet/Social/MTAtOS0zNg%3d%3d. |
| 3.2.2 | Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt? |
| | Ja, zie 3.2.1 |
| 3.2.3 | Is de aangemelde versie backwards compatible met eerdere versies van de standaard? |
| | Ja, basis is de policy binnen het DMARC record en daar is niets aan veranderd. |
| 3.2.4 | Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers? |
| | Ja, DKIM staat al op de "Pas toe of leg uit" lijst. Zo heeft het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) een document gepubliceerd, waarom organisaties met DMARC zouden moeten gaan werken, zie http://www.cip-overheid.nl/downloads/e-mailauthenticatie. |

**III. Inhoudelijke criteria**

**4. Inhoudelijk criterium: Opname bevordert adoptie**

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

***Toelichting lijsten:***

a. Met de lijsten wil het College de adoptie van open standaarden bevorderen die voldoen aan de voorgaande criteria (open standaardisatieproces, toegevoegde waarde, draagvlak);
b. Met de 'pas toe of leg uit'-lijst beoogt het College dit soort standaarden verplichten als:
    1. hun huidige adoptie binnen de (semi-)overheid beperkt is;
    2. opname op de lijst bijdraagt aan de adoptie door te stimuleren o.b.v. het 'PToLU; -regime. (functie=stimuleren).
c. Met de lijst met gangbare standaarden beoogt het College dit soort standaarden aan te bevelen als:
    1. hun huidige adoptie binnen de (semi-)overheid reeds hoog is;
    2. opname op de lijst bijdraagt aan de adoptie door te informeren en daarmee onbedoelde afwijkende keuzes te voorkomen. (functie=informeren)

***Vragen:***

| **4.1** | **Opname op de lijst bevordert de adoptie van de standaard.** |
|---|---|
| 4.1.1 | Is de "pas toe of leg uit"-lijst het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen? |
| | Ja, omdat er inmiddels al 3 jaar over de open standaard DMARC wordt gesproken en ondanks de enorme meerwaarde bijvoorbeeld de Belastingdienst, DigID, etc DMARC nog niet hebben geïmplementeerd. DMARC, DKIM en SPF behoren naar mijn mening ook opgenomen te worden in richtlijnen documenten van NCSC en IBD. |
| 4.1.2 | Is de lijst met gangbare open standaarden het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen? |
| | Nee, omdat DMARC met de policy "reject" in combinatie met DKIM en SPF echt de wereldwijde e-mail authenticatie standaard is en derhalve verplicht gesteld dient te worden. |

## Verzending

Als u het aanmeldingsformulier zo volledig mogelijk heeft ingevuld, dan kunt u deze als bijlage versturen naar forumstandaardisatie@logius.nl

Gebruikt u dan als onderwerp: "Aanmelding standaard".
Na ontvangst van het formulier ontvangt u binnen 5 dagen een ontvangstbevestiging per e-mail.

Bedankt voor uw aanmelding.