Forum Standaardisatie

Wilhelmina v Pruisenweg 52
2595 AN Den Haag
Postbus 96810
2509 JE Den Haag
www.forumstandaardisatie.nl

notitie

Opname DKIM op de lijst voor 'pas toe of leg uit'

FORUM STANDAARDISATIE CS 12-06-06A

Agendapunt:	6. Open Standaarden		
Bijlagen:	Expertadvies en consultatiereacties		
Aan:	College Standaardisatie		
Van:	Forum Standaardisatie		
Datum:	23 mei 2012	**Versie**	1.0
Betreft:	Opname DKIM op de lijst voor 'pas toe of leg uit'		

Waarom is een keuze belangrijk?
De overheid verstuurt niet alleen digitale post via de beveiligde berichtenbox(en). De bulk van digitale overheidspost verloopt via 'normale' e-mail (bijv. voor wachtwoordherstel DigiD). Domain Keys Identified Mail (DKIM) wordt gezien als een belangrijke bouwsteen om beveiliging van e-mail te verbeteren. DKIM stelt de ontvanger in staat om te controleren of e-mail legitiem vanaf een bepaald internetdomein (bijv. rijksoverheid.nl) is verstuurd. Een spamfilter kan DKIM-informatie gebruiken waardoor spam beter kan worden geweerd en phishing kan worden voorkomen. Bovendien kan de eindgebruiker zelf in zijn e-mailprogramma de DKIM-handtekening controleren. DKIM maakt identiteitsfraude, waarbij een internetcrimineel in naam van een overheidsorganisatie een mail verstuurd, moeilijker. Zoals het NCSC onlangs heeft geconstateerd, vormt dit soort fraude voor de overheid in toenemende mate een risico. DKIM is al breed omarmd door e-mailproviders en wordt door veel software ondersteund. Een opname op de 'pas toe of leg uit'-lijst voor uitgaande e-mail van de overheid draagt bij aan de adoptie.

Hoe is het advies tot stand gekomen?
Een expertgroep is tweemaal bij elkaar gekomen om toetsing van de standaard uit te voeren. Tijdens de tweede bijeenkomst op 17 januari 2011 is door een ruime meerderheid van de experts een positief advies gegeven voor opname op de 'pas toe of leg uit'-lijst. Twee van de negentien betrokken experts waren van mening dat DKIM niet op de lijst moet worden geplaatst. Dit advies is publiek geconsulteerd hetgeen geleid heeft tot zeven reacties. (5 positief)

Zijn er risico's verbonden aan de keuze?
De standaard is weliswaar een belangrijke, maar niet de enige bouwsteen voor veilig en betrouwbaar mailverkeer met de overheid. DKIM garandeert niet de vertrouwelijkheid van de e-mail en geeft ook geen garantie van de authentieke herkomst tot op persoonsniveau. In aanvulling op DKIM kunnen daarvoor eventueel andere standaarden worden gebruikt. Forum Standaardisatie wordt geadviseerd om de beveiliging van mailverkeer in samenhang met ander standaarden te (blijven) beschouwen.

Beslispunt

Datum
23 mei 2012

Het College Standaardisatie wordt gevraagd in te stemmen met:

1. de opname van DKIM op de lijst voor 'pas toe of leg uit';
2. het functionele toepassingsgebied *"Het faciliteren van het vaststellen van organisatorische herkomst voor e-mail afkomstig van overheidsdomeinen, als deze over een onbeveiligde, publieke internetverbinding wordt verstuurd wanneer verdere authenticatie ontbreekt."*;
3. het organisatorische werkingsgebied *"Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector";*
4. de additionele adviezen ten aanzien van de adoptie van de standaard:
    a. het oproepen van Digivaardig & Digiveilig om burgers te informeren over het veilig gebruik van e-mail die afkomstig is van overheden (bijv. m.b.t. het uitvragen van DigiD-gegevens).
    b. het oproepen van Nationaal Cyber Security Centrum (NCSC) om via Waarschuwingsdienst.nl melding te doen van relevante spam- en phishingactiviteiten die in naam van overheidsorganisaties worden uitgevoerd.
    c. het oproepen van NCSC om een richtlijn (analoog aan en in aanvulling op de "ICT-Beveiligingsrichtlijnen voor webapplicaties") over veilig en betrouwbaar e-mailverkeer op te stellen voor overheidsorganisaties. Laat daarin ook de aanbeveling opnemen om, naast DKIM, additioneel SPF voor e-mailverzending in te zetten en beschouw de samenhang met andere standaarden. Laat hierin ook wijzen op het nut van DKIM verificatie door de overheid zelf, om phishing en spoofing gericht tegen overheidspartijen en ambtenaren zichtbaar te maken.
    d. het oproepen van beheerders (o.a. ICTU, Logius) van domeinen met een hoog risico op phishing/spam activiteiten (bijv. DigiD, Overheid.nl, MijnOverheid.nl, etc.) om DKIM te gebruiken bij het uitsturen van e-mails.

Reikwijdte 'pas toe of leg uit' regime

Het 'pas toe of leg uit' regime heeft betrekking op de aanschaf van producenten of diensten waarbij de betreffende standaarden toegepast kunnen worden. Dit betekent concreet dat overheidsorganisaties worden opgeroepen om bij de aanschaf van nieuwe hard- en software (en eventuele bijbehorende diensten) tenminste die producten aan te schaffen die geschikt zijn voor het gebruik van de DKIM standaard. Het besluit over wanneer deze standaard het best kan worden toegepast, ligt daarmee alsnog bij de individuele organisaties.

In het geval van DKIM wordt voor een aantal partijen een uitzondering gemaakt op deze regel. Voor deze partijen geldt dat het Forum hen adviseert actief DKIM te gaan implementeren (zie bovenstaande additionele adviezen 4d). Daarnaast wordt NCSC opgeroepen om voor veilig en betrouwbaar e-mailverkeer en daarmee o.a. voor het gebruik van DKIM een heldere richtlijn op te stellen.

Toelichting

Datum
23 mei 2012

Waar gaat het inhoudelijk over?
Onderwerp van dit expertadvies is de standaard Domain Keys Identified Mail (DKIM). Deze standaard is vastgelegd in RFC 6376 van standaardisatieorganisatie IETF.

DKIM maakt het mogelijk om met behulp van een digitale handtekening het afzendadres van een e-mail te koppelen aan een domein/organisatie op een manier die is te valideren door de ontvanger van de e-mail. Het gebruik van DKIM biedt een willekeurige ontvanger dus de mogelijkheid om na te gaan of de (overheids)organisatie die de e-mail heeft verzonden ook daadwerkelijk verantwoordelijk is (of kan worden gehouden) voor de mail.

Omdat burgers en bedrijven op grote schaal gewend zijn aan het gebruik van e-mail als communicatiemiddel, verwacht men van de overheid analoog aan betrouwbare – https – websites dat deze (ook) per betrouwbare e-mail communiceert met burgers en bedrijven. De overheid biedt voor communicatie met burger en bedrijfsleven diensten aan als Berichtenbox (voor ontvangen van overheidsberichten) en Digipoort. In de praktijk bestaat er tussen overheid enerzijds en bedrijven en burgers anderzijds ook veel e-mail communicatie buiten deze diensten om: het doorsturen van bekendmakingen van besluiten, bevestigingen en indicaties over de status van een (digitale) aanvraag (bijvoorbeeld bouwvergunning, paspoort), herinneringen om een aangevraagde DigiD te activeren, informatie vanuit de Belastingdienst richting ondernemers over aangifte BTW of het kenbaar maken van toekenning van subsidievoorstellen aan bedrijven.

Mailactiviteiten in het algemeen en die van de overheid in het bijzonder vormen een potentieel doelwit voor domeinnaam misbruik, spam of phishing aanvallen richting ontvangende burgers en bedrijven. Prominente voorbeelden bij overheidsinstellingen zijn gevallen van phishing naar DigiD gegevens.

Burgers en bedrijven moeten echter uit kunnen gaan van de betrouwbaarheid van de overheid. Van burgers kan niet verwacht worden dat ze een e-mail kunnen kwalificeren als malafide omdat de overheid voor berichten met een bepaalde inhoud, zoals een verzoek om ergens in te loggen, normaliter alleen haar Berichtenbox gebruikt. De overheid zal er als afzender dus voor moeten zorgen dat ze een herkenbare en betrouwbare e-mail partij is in haar communicatie richting burgers en bedrijven.

DomainKeys Identified Mail (DKIM), een authenticatietechniek voor e-mail, wordt gezien als één van de bouwstenen voor het invullen van het bredere thema van veiliger en betrouwbaarder e-mail, zoals authenticatie, integriteit, onweerlegbaarheid en vertrouwelijkheid. Een middel, dat de ontvanger de mogelijkheid geeft om vast stellen of en zo ja van welke overheidspartij deze mail afkomstig is (en of de ontvanger deze mail dus wel of niet kan vertrouwen).

Hoe is het proces verlopen?
Na aanmelding van de standaard door dhr. Rolf Sonneveld van Sonnection, heeft ene intakegesprek plaatsgevonden. Dit gesprek leidde tot een positief advies voor het in procedure nemen van DKIM. Op 14 juli is een achttiental experts uit de overheid, bedrijfsleven en academische wereld bijeengekomen om de standaard te toetsen. Tijdens deze expertmeeting kon over het toepassingsgebied

geen overeenstemming worden bereikt. Het Forum Standaardisatie heeft daarop besloten een tweede expertsessie te organiseren. Op 17 januari 2012 is de expertgroep in iets andere samenstelling voor de tweede maal bijeengekomen. De expertgroep adviseerde in meerderheid, maar niet unaniem voor opname op de lijst: twee expertgroepleden waren tegen opname op de lijst.

Het expertadvies is publiekelijk geconsulteerd en hierop zijn 7 reacties binnengekomen. Vijf respondenten (Proxy Laboratories, BKWI, Belastingdienst, Ministerie van EL&I en KvK) onderschreven het advies van de expertgroep om DKIM op de lijst voor pas toe of leg op te nemen. Twee respondenten (Logius en UWV) zijn tegen opname op de lijst.

De belangrijkste opmerkingen uit de consultatie zijn:

- BKWI onderschrijft het advies, maar geeft aan de standaard nog stricter te willen toepassen, namelijk voor alle e-mail verkeer. De expertgroep heeft na uitgebreid overleg besloten om het toepassingsgebied zo te formuleren , dat dit niet overlapt met bestaande standaarden op de lijst (o.a. Digikoppeling).
- BKWI geeft aan dat een ambassadeur/sponsor binnen de overheid nodig is om adoptie van DKIM tot een succes te maken. Dit is een zinvolle aanvulling op de adviezen aan het Forum uit het expertadvies.
- KVK onderschrijft het advies, maar is van mening dat het niet van toepassing verklaren van DKIM op inkomende mail voor de overheid een tekortkoming is in het expertadvies. De expertgroep is echter van mening dat op binnenkomende mail geen plicht van de overheid richting maatschappij ligt en een verplichting dus minder noodzakelijk is.
- KVK geeft aan dat overheid-overheid communicatie ten onrechte niet wordt afgedekt in het expertadvies. Voor overheid-overheid e-mail verkeer heeft de expertgroep echter vastgesteld, dat deze onder een koppelvlak valt, dat al op transportniveau is beveiligd (en dus buiten het vastgestelde toepassingsgebeid valt).
- UWV onderschrijft de noodzaak voor een meer betrouwbaar e-mail verkeer vanuit de overheid en het nut van de standaard DKIM. UWV vindt de scope (alleen uitgaande e-mail, uitsluitend gericht op verzendende organisatie en geen versleuteling) echter te beperkt om DKIM zelfstandig op de lijst te plaatsen. In plaats daarvan ziet UWV graag een groeipad geschetst voor een samenhangend geheel van standaarden (waar DKIM een onderdeel van kan zijn). De expertgroep ziet het nut van aanvullende standaarden om het onderwerp van betrouwbaar e-mail verkeer nog vollediger af te dekken, maar ziet DKIM ook als een bouwsteen die zelfstandig op de lijst kan worden geplaatst.
- Logius onderschrijft het advies niet en geeft als belangrijkste reden aan, dat er onvoldoende toegevoegde waarde lijkt voor het zelfstandig opnemen van DKIM op de lijst als afzonderlijke standaard, gegeven de functionaliteit van aanpalende standaarden als bijv. S/MIME en SPF. De expertgroep ziet in DKIM een zelfstandige bouwsteen voor plaatsing op de lijst en beschouwt o.m. S/MIME en SPF als standaarden die ingezet kan worden als er aanvullende eisen en wensen op het gebied van betrouwbaarheid en vertrouwelijkheid zijn. De expertgroep gaat daarbij uit van het standpunt dat DKIM een (eerste) logische stap is, laagdrempelig is en de inzet ervan geen organisatie ervan weerhoudt om aanvullende standaarden in te zetten. Logius onderschrijft wel het belang van en de behoefte aan betrouwbaarheid en vertrouwelijkheid van berichtenverkeer met en door de overheid. Er zou dan wel nadrukkelijker moet worden bekeken op welke wijze de overheid in generieke zin betrouwbaarheid

en vertrouwelijkheid van mailverkeer in de vorm van een groeiscenario zou moeten regelen.

Hoe scoort de standaard op de toetsingscriteria?

NB: In het expertadvies heeft toetsing aan de 'oude' set met criteria plaatsgevonden (openheid, bruikbaarheid, potentieel en impact), omdat deze ten tijde van de eerste expertsessie de op dat moment geldige criteria waren.

- *Openheid*
  De standaard voldoet aan de criteria van openheid. DKIM is in beheer bij IETF en zonder kosten te gebruiken. De standaard is in hoge mate stabiel en aan weinig veranderingen onderhevig.

- *Bruikbaarheid*
  DKIM is een volwassen standaard, waarmee vooral in het commerciële domein voldoende praktijkervaring is opgedaan. Er is verder ruim voldoende ondersteuning bij productleveranciers en bij een aantal grote ISP's.

- *Potentieel*
  De expertgroep is van mening dat de interoperabiliteit tussen partijen die e-mail uitwisselen verbetert (zij het in beperkte mate), door het vergroten van de zekerheid die DKIM biedt om de afzender te herleiden. Hierdoor kan het vertrouwen in de samenwerkingsrelatie tussen partijen toenemen.
  De onbetrouwbaarheid van e-mail vormt in de praktijk een steeds groter probleem, ook voor de overheid. GOVCERT.NL (nu NCSC) schrijft in zijn Cybersecuritybeeld Nederland van december 2011 het volgende: "In het begin van 2011 hebben een paar incidenten plaatsgevonden waarbij uit naam van de overheid phishingmails verstuurd zijn. Dit is voor de overheid, maar zeker ook voor de burger een zorgelijke ontwikkeling. De kans op dit soort phishingaanvallen en de belangstelling voor DigiD, neemt toe naarmate steeds meer diensten digitaal door de overheid verleend worden." DKIM draagt ertoe bij dat dit type misbruik kan worden voorkomen.

  Voor bedrijven
  Net als overheden zijn bedrijven (bijvoorbeeld banken) gebaat bij een standaard die helpt de afkomst van email te valideren om zo bijvoorbeeld schadelijke activiteiten zoals phishing te ondervangen. Door als overheid DKIM de 'pas toe of leg uit' status te verlenen, en actief te gaan gebruiken, wordt de adoptie van deze standaard, naar verwachting aanzienlijk versneld en wordt het voor bedrijven eenvoudiger om deze standaard effectief in te zetten.

- *Impact*
  De impact van DKIM is vooral gelegen in de veiligheidsaspecten. DKIM kan een bepaalde schijnveiligheid creëren omdat de herleidbaarheid van de afzender nog steeds geen waarborg is op de intenties van de afzender en de inhoud van het mailbericht zelf.

  Het gebruik van DKIM is naadloos in te passen in het huidige mailverkeer, in de zin dat het complementair is aan bestaande maatregelen en als zodanig op elk moment toegevoegd kan worden aan mailstromen. Het is in die zin niet disruptief, zowel aan de kant van de verzender als de ontvanger. Wel zullen aan de kant van de ontvanger maatregelen (zoals activering in de mailsoftware) moeten worden genomen om gebruik te maken van de aanwezige handtekening, anders maakt het toevoegen geen verschil voor de ontvanger.

Implementatie van DKIM betekent voor de verzender concreet:

- Aanpassing DNS records (met specifieke DKIM velden).
- Laten ondertekenen van uitgaande mail met een (elektronische) handtekening. In de meerderheid van de gevallen is dit een bestaande optie op de bestaande mail servers.

De onderhoudslast is gelegen in onderhouden van sleutelpaar (of certificaten) voor de handtekening.

Wat is de conclusie van de expertgroep en de consultatie?

Een meerderheid van de expertgroep adviseert het college om DKIM op te nemen op de lijst met open standaarden voor "pas toe of leg uit".

Als functioneel toepassingsgebied wordt daarbij voorgesteld:

> *"Het faciliteren van het vaststellen van organisatorische herkomst voor e-mail afkomstig van overheidsdomeinen, als deze over een onbeveiligde, publieke internetverbinding wordt verstuurd wanneer verdere authenticatie ontbreekt."*

Als organisatorisch werkingsgebied wordt voorgesteld:

> *"Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector*

Met de adoptie van de DKIM standaard worden naar mening van de meerderheid van de expertgroep problemen met misbruik van overheidsdomeinnamen voor ongewenste e-mail activiteiten teruggedrongen. Een meerderheid in de expertgroep is van mening dat de overheid de plicht heeft om zich een 'goede' communicatiepartner te tonen, door de ontvanger de mogelijkheid te bieden na te gaan of de e-mail ook echt van de overheid komt. Het gebruik van DKIM hiervoor wordt gezien als een van de basale bouwstenen hiervoor en wordt daarom aangeraden voor adoptie.

Twee partijen uit de expertgroep kunnen zich niet vinden in het advies DKIM op te nemen op de lijst. Zowel Logius als IBM geven aan dat

- Ze de genoemde probleemstelling met betrekking tot e-mail verkeer en de overheid onvoldoende onderschrijven.
- Opname van DKIM op zichzelf te weinig bijdraagt aan de doelstelling van betrouwbaarder e-mail verkeer en de voordelen van inzet van DKIM onvoldoende duidelijk zijn in genoemde probleemstelling.
- Naast DKIM aanvullende maatregelen/afspraken nodig zijn om deze doelstelling te bereiken.
- Er alternatieve standaarden beschikbaar zijn (o.m. S/MIME) die beter invulling kunnen geven aan deze doelstelling.

Risico's

- De expertgroep heeft vastgesteld dat er een afhankelijkheid is ten opzichte van de veiligheid van DNS: als DNS gecompromitteerd raakt, zijn de DKIM sleutels niet meer betrouwbaar.
- DKIM kan een bepaalde schijnveiligheid creëren omdat de herleidbaarheid van de afzender nog steeds geen waarborg is op de intenties van de afzender en de inhoud van het mailbericht zelf: de verzendende overheidspartij houdt hiervoor verantwoordelijkheid.

Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaard?
Concreet doet de expertgroep in meerderheid de volgende aanvullende aanbevelingen:

- Laat Digivaardig & Digiveilig burgers informeren over het veilig gebruik van overheids e-mail (bijv. m.b.t. het uitvragen van DigiD gegevens). Roep NCSC op om via Waarschuwingsdienst.nl op om melding te doen van relevante spam- en phishingactiviteiten die in naam van overheidsorganisaties worden uitgevoerd.
- Laat NSCS een handreiking opstellen voor overheidspartijen voor veilig en betrouwbaar e-mail verkeer. Laat daarin de aanbeveling opnemen om naast DKIM, optioneel ook SPF voor domein authenticatie in te zetten. Laat hierin ook wijzen op het nut van DKIM verificatie door de overheid zelf, om phishing en spoofing gericht tegen overheidspartijen en ambtenaren zichtbaar te maken.
- Roep beheerders (o.a. ICTU, Logius) van domeinen met een hoog risico op phishing/spam activiteiten (bijv. DigiD, Overheid.nl, MijnOverheid.nl, etc.) uit naam van de overheid, op het gebruik van DKIM om e-mail notificaties vanuit deze organisaties beter te beveiligen.

Bijlagen
(zie https://lijsten.forumstandaardisatie.nl/open-standaard/dkim)

- Expertadvies DKIM, 13 februari 2012
- Overzicht reacties consultatieronde
    - Belastingdienst
    - BKWI
    - Logius
    - KvK
    - Ministerie van EL&I
    - Proxy Laboratories
    - UWV