Forum Standaardisatie

Expertadvies DKIM

Datum 13 februari 2012

Colofon

Projectnaam	Expertadvies DKIM
Versienummer	1.0
Locatie	
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag forumstandaardisatie@logius.nl

Auteurs	Dr. B. Hulsebosch Ir. M. van Bekkum

Inhoud

Managementsamenvatting

Waar gaat het inhoudelijk over?
Onderwerp van dit expertadvies is de standaard Domain Keys Identified Mail (DKIM). DKIM maakt het mogelijk om 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. DKIM maakt door gebruik van een digitale handtekening validatie door de ontvanger mogelijk. Verificatie van de handtekening vindt plaats via het publieke deel van de private sleutel waarmee de handtekening gezet is. Deze publieke sleutel wordt in het DNS domein geplaatst dat eigendom is van de organisatie.

DKIM biedt overheidsorganisaties zo de mogelijkheid misbruik van de eigen Internet domeinnaam door derden via e-mail te detecteren en de gevolgen van dergelijk misbruik te beperken.

Hoe is het proces verlopen?
Om tot een goed advies te komen is een groep van 18 experts uit de overheid, bedrijfsleven en academische wereld verzameld. Verschillende leden uit deze groep zijn in twee bijeenkomsten bij elkaar gekomen om over het toepassingsgebied van DKIM te discussiëren en om de standaard te toetsen tegen een de criteria van Forum en College standaardisatie. Een tweede bijeenkomst bleek nodig om tot een goede definitie van het functionele toepassingsgebied te komen. De experts is gevraagd naar hun mening ten aanzien van de standaard; dit expertadvies is een weergave daarvan. In dit 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.

Hoe scoort de standaard op de toetsingscriteria?
- 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: DKIM zal bijdragen aan het verbeteren van de interoperabiliteit. 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.
- 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: de verzendende overheidspartij houdt hiervoor verantwoordelijkheid. Het maatschappelijk vertrouwen in de overheid als afzender van berichten zal echter toenemen. Verder kan DKIM worden beschouwd als een relatief laagdrempelige en kosteneffectieve authenticatiemethode met betrekking tot e-mail. Er dient opgemerkt te worden dat DKIM geen totaaloplossing voor e-mail beveiliging is; het moet gezien worden als een van de bouwstenen.

Wat is de conclusie van de expertgroep en de consultatie?
Een meerderheid van de expertgroep adviseert het college in meerderheid 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

Naar mening van deze groep worden met de adoptie van de DKIM standaard problemen met misbruik van overheidsdomeinnamen voor ongewenste e-mail activiteiten verminderd. De meerderheid van 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 wordt gezien als een van de basale bouwstenen hiervoor en wordt daarom aangeraden voor opname op de lijst.

De meerderheid van de expertgroep is verder van mening dat een goed voorbeeld goed doet volgen. Dit 'leading by example' argument wordt op zichzelf al als voldoende valide geacht om toetreding tot de lijst te rechtvaardigen. Andere partijen zullen gestimuleerd worden om ook DKIM te gaan gebruiken of om ermee door te gaan waardoor het effect van DKIM vergroot zal worden, namelijk een betrouwbaarder e-mail verkeer.

De focus voor gebruik van DKIM ligt op uitgaande e-mail; het verifiëren van inkomende mail wordt gezien als nuttig maar niet noodzakelijk.

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
- De genoemde probleemstelling met betrekking tot e-mail verkeer en de overheid onvoldoende wordt onderschreven.
- 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.
- DNaast 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.

Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaard?

Concreet doet de expertgroep in meerderheid de volgende aanvullende aanbevelingen:

- Informeer als Forum Standaardisatie burgers over het veilig gebruik van e-mail ten aanzien van overheids e-mail (b.v. m.b.t. het uitvragen van DigiD gegevens).
- Wijs specifiek partijen als DigiD en MijnOverheid op het gebruik van aanvullende maatregelen als DKIM om e-mail notificaties vanuit deze organisaties beter te beveiligen.
- Wijs overheidspartijen op het nut van DKIM verificatie door de overheid zelf, om phishing en spoofing gericht tegen overheidspartijen en ambtenaren zichtbaar te maken: opname op de lijst richt zich uitsluitend op uitgaand e-mail verkeer
- Stel als Forum Standaardisatie in samenwerking met GovCERT en NCSC een handreiking op voor overheidspartijen voor veilig en betrouwbaar e-mail verkeer. Benoem daarin de relaties met de andere standaarden.
- Beveel voor domein authenticatie naast DKIM gebruik van SPF aan bij implementaties.

1 Doelstelling expertadvies

1.1 Achtergrond

Het kabinet stelt via de Digitale Agenda.nl [1] en i-NUP [2] open standaarden als norm. Doel van dit ICT-beleid is om informatievoorziening toegankelijker te maken, om elektronische dienstverlening van de overheid te verbeteren, om onafhankelijkheid van ICT-leveranciers te vergroten, en om een krachtige impuls te geven aan economische groei en innovatie.

Eén van de maatregelen van het actieplan is het gebruik van een lijst met standaarden, die vallen onder het principe "pas toe of leg uit" (comply-or-explain) [3]. Het College Standaardisatie, dat in 2006 door het kabinet is ingesteld, spreekt zich uit over de standaarden die op de lijst zullen worden opgenomen, o.a. op basis van een expertbeoordeling van de standaard [4]. Het College Standaardisatie wordt geadviseerd door het Forum Standaardisatie. Bureau Forum Standaardisatie ondersteunt beide instellingen.

Onderwerp van dit expertadvies is DKIM. Deze standaard is aangemeld door dhr. Rolf Sonneveld van Sonnection voor opname op de lijst met open standaarden voor 'pas toe of leg uit'. De opdracht aan de expertgroep was om een advies op te stellen over het wel of niet opnemen van deze standaard op de lijst met open standaarden, al dan niet onder bepaalde voorwaarden.

Een achttiental experts heeft zich in twee groepsessies gebogen over de standaard om deze te beoordelen aan de hand van een aantal criteria. Deze criteria – vooraf vastgesteld door het College Standaardisatie [3] en uitgewerkt in de vorm van concrete vragen - worden in het hier voorliggende expertadvies genoemd en behandeld.

1.2 Proces

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

- Door het Bureau Forum Standaardisatie is een intakegesprek gevoerd met de indiener. Hierin is de standaard getoetst op uitsluitingscriteria ('criteria voor in behandel-name') en is een eerste inschatting gemaakt van de kansrijkheid voor opname.
- Op basis van de intake is besloten tot het instellen van een expertgroep. Op basis van dit besluit is door het Bureau Forum Standaardisatie een groep samengesteld en een voorzitter aangezocht. Op basis van de aanmelding en de intake is een voorbereidingsdossier opgesteld voor leden van de expertgroep.
- De expertgroep is begonnen met het individueel scoren van de DKIM standaard op basis van het voorbereidingsdossier. Op basis van de verkregen antwoorden hebben voorzitter en begeleider van de expertgroep de verschillende knelpunten geïdentificeerd.
- Vervolgens is de expertgroep op 14 juli 2011 bijeengekomen om de bevindingen in het algemeen en de geïdentificeerde knelpunten in het bijzonder te bespreken. In de discussie met de expertgroep is

gepoogd het toepassingsgebied van de standaard vast te stellen. Binnen de beschikbare tijd kon hierover echter geen consensus worden bereikt.
- Naar aanleiding van de bijeenkomst is door voorzitter en begeleider een draft expertadvies op gesteld, met vermelding van de discussiepunten. Tijdens de review bleek dat er te veel bespreekpunten overeind bleven m.b.t. het toepassingsgebied om op een goede manier de discussie af te handelen via e-mail. Daarnaast bleek de beschikbaarheid van een aantal experts en de voorzitter gedurende de reviewperiode beperkt.
- Op basis van bovenstaande argumenten heeft het Forum Standaardisatie besloten tot het organiseren van een tweede bijeenkomst. In de tweede bijeenkomst van de expertgroep (bestaande uit een aantal experts die ook bij de eerste sessie aanwezig waren en een aantal nieuwe experts) op 17 januari 2012 is het toepassingsgebied verder vastgesteld.

De uitkomsten van de expertgroep zijn door de voorzitter en begeleider verwerkt in dit advies rapport. Een eerste conceptversie is aan de leden van de expertgroep gestuurd met verzoek om reactie. Na verwerking van de reacties is het rapport afgerond en ingediend voor de publieke consultatieronde.

1.3 Vervolg

Dit expertadvies zal ten behoeve van een publieke consultatie openbaar worden gemaakt door het Bureau Forum Standaardisatie. Alle belanghebbenden kunnen gedurende de consultatieperiode op dit expertadvies hun 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 College Standaardisatie opstellen. Het College Standaardisatie bepaalt uiteindelijk op basis van het advies van het Forum of de standaard op de lijst met gangbare open standaarden of de 'pas toe of leg uit'-lijst komt.

1.4 Samenstelling expertgroep

Voor de expertgroep zijn personen uitgenodigd die vanuit hun persoonlijke expertise of werkzaamheden bij een bepaalde organisatie direct of indirect betrokken zijn bij de standaard. Daarnaast is een onafhankelijke voorzitter aangesteld om de expertgroep te leiden en als verantwoordelijke op te treden voor het uiteindelijke expertadvies.

Als voorzitter is opgetreden de heer Bob Hulsebosch, senior onderzoeker en projectleider bij Novay. Daarnaast is hij certified information systems security professional (CISSP). Bij Novay houdt hij zich vooral bezig met (gefedereerd) identity management en authenticatie-oplossingen voor consumenten.

De expertgroep is in opdracht van het Forum Standaardisatie begeleid door ir. Michael van Bekkum, adviseur standaarden en interoperabiliteit bij TNO.

Aan de expertgroep hebben deelgenomen:

- Dhr. Rolf Sonneveld (Sonnection, indiener)
- Dhr. Willem Kossen (BKWI)
- Dhr. Erik Holkers (Ministerie van EL&I)
- Dhr. Rob Weemhoff (IBM)
- Dhr. Tom Peelen (Logius)
- Dhr. Bart Kerver (ICTU, Antwoord voor Bedrijven)
- Dhr. Fred van Blommestein (Universiteit Groningen)
- Dhr. Harrie Biersteker (Ministerie van Justitie)
- Dhr. Marco Davids (SIDN)
- Dhr. Martijn Groeneweg (Measuremail)
- Dhr. Roelof Vredeveld (Rabobank Nederland)
- Dhr. Olaf Kolkman (IAB / NLnetLabs)
- Dhr. Dick Batenburg (Diginotar)
- Dhr. Carel Bitter (Primerelay)
- Dhr. Joris Joosten (Logius)
- Dhr. Rinus Braak (Ministerie van EL&I)
- Dhr. Brian Joseph (Zarafa)
- Dhr. Maarten Oelering (Suremail)

Daarnaast is door één persoon voorafgaand aan de expertgroepbijeenkomst een inhoudelijke bijdrage geleverd door het individueel scoren van de standaard of door het geven van een reactie in algemene zin:

- Dhr. Martijn Grooten (Virus Bulletin Ltd.)

Hun bijdrage is meegenomen in de discussie in de expertgroep.

1.5 Toelichting DKIM

Dit advies betreft de internet standaard DomainKeys Identified Mail (DKIM) Signatures (hierna afgekort tot DKIM). De standaard DKIM kan worden beschouwd als een verzamelnaam voor een tweetal samenhangende standaarden, die zijn vastgelegd in zogenaamde RFC's[1] . Onderstaande twee RFC's zijn door de expertgroep in beschouwing genomen:

Hoofd RFC
RFC 6376 DomainKeys Identified Mail (DKIM) Signatures

Relatie tussen DKIM en Internet mail messaging technologie
RFC 5585 DomainKeys Identified Mail (DKIM) Service Overview

DKIM is een set van RFC's die in samenhang met elkaar een authenticatiemiddel specificeren, waarmee zekerheid over de organisatorische herkomst van e-mail kan worden geboden.

1 Request for Comments, het standaard publicatieformaat voor de Internet Standaarden van de IETF (http://tools.ietf.org/html/rfc2026).

De DKIM standaard wordt beheerd en onderhouden door de Internet Engineering Task Force (IETF)[2], een orgaan dat Internet standaarden ontwikkelt en daarbij nauw samenwerkt met o.a. W3C. Werk aan DKIM is gestart in 1994. Werk aan de huidige versie van de standaard in de IETF DKIM working group is gestart in 2006.

DKIM maakt het mogelijk om 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 organisatie die de e-mail heeft verzonden ook daadwerkelijk verantwoordelijk is (of kan worden gehouden) voor de mail.

DKIM biedt organisaties de mogelijkheid misbruik van de eigen Internet domeinnaam door derden via e-mail te detecteren en de gevolgen van dergelijk misbruik te beperken. Daarnaast biedt DKIM door gebruik van een digitale handtekening de mogelijkheid de integriteit van de e-mail te beoordelen door na te gaan of deze is verstuurd vanuit het e-maildomein dat de private sleutel bezit en of de e-mail na versturen niet is veranderd. DKIM maakt validatie van de geldigheid van de handtekening dus mogelijk. Het is vervolgens aan degene die de validatie uitvoert (of de eindontvanger van de e-mail) om de uitkomst van deze validatie te interpreteren.

Verificatie van de handtekening vindt plaats via het publieke deel van de private sleutel waarmee de handtekening gezet is. Deze publieke sleutel wordt in het DNS domein geplaatst dat eigendom is van de organisatie. Gebruik van een techniek als DNSSEC kan de zekerheid omtrent integriteit daarbij verder verhogen.

Samenvattend, DKIM biedt de volgende functionaliteit:

- Het vormt een baseline voor authenticiteit van e-mail bij het versturen van e-mail via SMTP en over openbaar internet, met gebruik van het Internet Message Format (RFC 5321/5322).
- De authenticiteit van de e-mail heeft betrekking op het e-mail object zelf.
- Het kunnen vaststellen van de organisatie die verantwoordelijk is voor verzending van de e-mail.
- DKIM wordt op organisatieniveau ingezet en is daarmee een schaalbare technologie.

Functionaliteit die DKIM niet biedt is:

- Versturen van e-mail over een vooropgezette, beveiligde verbinding point-to-point systeemkoppelingen): bij gebruik van authenticatiemiddelen op transmissieniveau biedt de verbinding al afdoende maatregelen om authenticiteit tussen organisaties vast te stellen.
- Waarborg op vertrouwelijkheid van de inhoud: DKIM geeft geen garanties over de aard van de inhoud en biedt geen additionele privacy maatregelen.
- Garantie op data integriteit: DKIM biedt data integriteit van e-mail (geen primaire functie).

2 http://www.ietf.org/

De standaard wordt momenteel gebruikt door diverse financiële instellingen en banken[3], door een aantal grote e-mail service providers (Yahoo, Gmail, America Online e.d.) en daarnaast door bedrijven die zich bezighouden met verkoop via Internet (marktplaats, eBay e.d.). Bij de Nederlandse providers is ondersteuning van DKIM aanwezig (bij het ontvangen van e-mail) bij o.m. Freeler, HetNet, KPN Planet, XS4ALL en Ziggo[4].

1.6 Relatie met andere open/gangbare standaarden

DKIM kent een relatie met de volgende standaarden die voorkomen op de lijst met gangbare standaarden, door verwijzing in de specificatie:

- Domain Name System (DNS)
- Simple Mail Transfer Protocol (SMTP)
- Multipurpose Internet Mail Extensions (MIME)
- Secure Hash Algorithm 2 (SHA-2)

Overige standaarden die een raakvlak hebben met het toepassingsgebied van DKIM, worden benoemd in 3.2.3.

1.7 Leeswijzer

In hoofdstuk 2 wordt beschreven in welke gevallen de standaard functioneel gezien gebruikt moet worden (functioneel toepassingsgebied) en door welke organisaties deze gebruikt zouden moeten worden (organisatorisch werkingsgebied). Daarnaast geeft hoofdstuk 2 achtergrond bij de noodzaak om DKIM te gebruiken.

Om te bepalen of de standaard opgenomen moet worden op de lijst met open standaarden zijn deze getoetst aan een viertal door het College Standaardisatie vastgestelde criteria. In hoofdstuk 3 staat het resultaat van deze toetsing. Hoofdstuk 4 bevat een samenvatting van de toetsresultaten op hoofdlijnen en het advies van de expertgroep aan het Forum Standaardisatie.

---

3 BITS email security toolkit: Protocols and Recommendations for reducing the Risks, BITS security Working group, April 2007, http://bitsinfo.org/downloads/Publications%20Page/BITSSecureEmailFINALAPRIL1507.pdf

4 http://returnpath.net/internetserviceprovider/receivermap/

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 gebruik moeten worden (functioneel toepassingsgebied), en door welke organisaties deze gebruikt zouden moeten worden (organisatorisch werkingsgebied).

2.1 Noodzaak

De expertgroep acht het belangrijk dat de noodzaak en probleemstelling voor e-mail beveiliging worden beschreven, met een toelichting voor de rol van DKIM daarin als een van de bouwstenen. Deze paragraaf zal een achtergrond schetsen bij deze problematiek.

2.1.1 Overheid en mailverkeer

In Nederland wordt Internet e-mail op grote schaal gebruikt door personen, bedrijven en overheid.

Door de relatief lage kosten van het verzenden van e-mail en door het ontbreken van beveiligingsoplossingen in de basisstandaarden voor e-mail (RFC5321, RFC5322) wordt e-mail dan ook op grote schaal misbruikt voor het verzenden van ongewenste mail, in de vorm van spam en phishing mail. Daarbij wordt misbruik gemaakt van e-mail adresgegevens, zowel voor ontvanger adressen als voor afzenderadressen.

De laatste jaren is er een trend dat ongewenste mail niet alleen reclameboodschappen bevat, maar steeds vaker ook malware (of verwijzingen naar websites met malware) en dat er naar vertrouwelijk informatie (zoals bankgegevens of gebruikersnamen en wachtwoorden) gevist wordt (phishing). In het bedrijfsleven en met name bij de banken is de schade van deze activiteiten inmiddels dermate groot, dat men een campagne is gestart om gebruikers bewust te maken van deze praktijken[5]. Verschillende overheden hebben inmiddels ook te maken gehad met de negatieve gevolgen van geslaagde spam en phishing praktijken.

Bovengenoemde trends ondergraven het vertrouwen in e-mail als communicatiemiddel en brengen grote maatschappelijke kosten met zich mee. Het 'Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010'[6] constateert dat deze kosten moeilijk te kwantificeren zijn, maar beschrijft wel het economisch belang dat in het geding is.

[5] *http://www.veiligbankieren.nl/index.php?p=561813*

[6] *http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/trendrapporten/trendrapport-2010.html*

Voor de overheid komt daar nog een aspect bij. 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, maar de praktijk laat zien dat er tussen overheid enerzijds en bedrijven en burgers anderzijds ook veel e-mail communicatie buiten deze diensten om bestaat[7].

De mailactiviteiten van overheden bestaan ondermeer uit het doorsturen van bekendmakingen van besluiten[8], 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. 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.

Overheden die e-mailcontact mogelijk maken, moeten dat e-mail verkeer echter ook officieel behandelen[9]. Daarbij moeten burgers en bedrijven uit kunnen gaan van de betrouwbaarheid van de overheid[10]. Deze beide verwachtingen (gebruik e-mail en betrouwbare overheid) verenigen zich echter moeilijk met het gebruik van e-mail als communicatiemiddel, wanneer voorzieningen ontbreken om eerder genoemde dreigingen tegen te gaan. Mailactiviteiten in het algemeen en die van de overheid in het bijzonder vormen namelijk 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[11,12].

2.1.2 Bouwstenen voor betrouwbaarder e-mail verkeer

In reactie op deze groei van de hoeveelheid en de veranderende aard van ongewenste mail nemen (internet) service providers (ISP) en bedrijven steeds verdergaande maatregelen om berichten te filteren.
Daarbij komt het regelmatig voor dat gewenste mail uitgefilterd wordt. Een wereldwijde studie naar commercieel mailverkeer laat zien dat inmiddels 1 op de 5 e-mails de inbox niet meer bereikt[13] en de

---

7 Een eenvoudige schatting op basis van het mailverkeer van een middelgrote gemeente als Dordrecht, leert dat er vele miljoenen (vaak geautomatiseerde) e-mails per jaar alleen al door de gemeentelijke overheden worden verstuurd.

8 http://zoekdienst.overheid.nl/ICTU_Website/Abonneren/abonneren.aspx

9 http://www.nationaleombudsman-nieuws.nl/sites/default/files/rapport_2011-204.pdf

10 Zie ook het advies van de Onderzoeksraad voor Veiligheid in het kader van het Diginotar onderzoek, http://www.onderzoeksraad.nl/index.php/pers/onderzoek-diginotar-richt-zich-op-digitale-veiligheid-overheid/.

11 http://profielen.hro.nl/nieuws/item/aangifte_van_phishing_aanval/

12 http://www.bigwobber.nl/wp-content/uploads/2011/09/1754_0001.pdf

13 http://www.returnpath.net/blog/intheknow/2011/09/email-deliverability-still-plagues-commercial-email-senders-worldwide-only-81-of-email-reaches-the-inbox/

verwachting is dat dit aantal zonder aanvullende maatregelen zal toenemen.

Om te voorkomen dat haar e-mail berichten op den duur op soortgelijke wijze in spamfilters en quarantainegebieden terecht komen, zal de overheid er als afzender voor moeten zorgen dat ze een herkenbare en betrouwbare e-mail partij is in haar communicatie richting burgers en bedrijven. Dat betekent dat de overheid middelen zal moeten inzetten, die de ontvanger de mogelijkheid geven 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). De ontvanger zal hier zelf uiteraard ook middelen tot zijn beschikking moeten hebben (via ISP/ESP) of maatregelen moeten nemen (mailclient) om van deze mogelijkheid gebruik te kunnen maken.
N.B: Logius geeft aan dat bovenstaande situatie ('in spamfilters en quarantainegebieden terecht komen') op moment van schrijven nauwelijks voorkomt en er dus geen noodzaak is de standaard in te zetten.

Om deze uitdagingen op te lossen, zijn standaarden en voorzieningen als bouwstenen beschikbaar die stuk voor stuk deelaspecten van het bredere thema van veiliger en betrouwbaarder e-mail adresseren, zoals authenticatie, integriteit, onweerlegbaarheid en vertrouwelijkheid. Inmiddels ontstaan er ook initiatieven die meerdere van deze bouwstenen samennemen om de bedreigingen van misleidende e-mail tegen te gaan[14]. DomainKeys Identified Mail (DKIM), een authenticatietechniek voor e-mail, wordt gezien als één van deze bouwstenen[15].

DKIM maakt het mogelijk om een e-mail zodanig te koppelen aan een (overheids-) domein/organisatie, dat de ontvanger deze op een gestandaardiseerde manier kan valideren. Een burger of bedrijf kan met behulp van DKIM nagaan of de overheidsorganisatie die de e-mail heeft verzonden (of laten verzenden) ook daadwerkelijk verantwoordelijk is voor de (inhoud van de) mail.

Het gebruik van DKIM kan helpen om misbruik van domeinnamen in e-mail adressen tegen te gaan c.q. zichtbaar te maken en kan helpen voorkomen dat berichten van de overheid in spamfilters en quarantainegebieden terecht komen.

DKIM is een standaard die:
- de overheid in staat stelt, zich als verifieerbaar betrouwbare verzender op te stellen. De ontvanger moet dan wel gebruik maken van de mogelijkheid dit vast te stellen: de standaard werkt alleen als zowel verzender als ontvanger zijn mogelijkheden benutten. De burger is daarbij als eindgebruiker afhankelijk van een implementatie en gebruik van DKIM bij zijn/haar ESP of ISP.
- een positieve uitspraak doet ten aanzien van het domein van herkomst: een verifieerbare handtekening betekent succesvolle domeinauthenticatie. Het ontbreken van een handtekening of een handtekening, die niet geverifieerd kan worden, leveren geen sluitende uitspraak op over (organisatorische) herkomst. De DKIM standaard doet ook geen uitspraak over mail die niet ondertekend is

14 DMARC.org, http://www.dmarc.org/news/press_release_20120130.html

15 "Trust in e-mail begins with authentication", MAAWG, 2008, http://www.maawg.org/sites/maawg/files/news/MAAWG_Email_Authentication_Paper_2008-07.pdf"

of mail die fout ondertekend is. Het is vervolgens aan degene die de validatie van de handtekening uitvoert (of de eindontvanger van de e-mail) om de uitkomst van deze validatie te interpreteren.
- organisaties ook de mogelijkheid biedt negatieve gevolgen van misbruik door derden van de eigen Internet domeinnaam in e-mail te beperken. Dit laatste geldt zowel voor communicatie vanuit bedrijven richting de overheid als vanuit de overheid richting bedrijven. De standaard draagt bij aan opbouw van reputatie.
- geen waarborg geeft op vertrouwelijkheid van de inhoud: DKIM geeft geen garanties over de aard van de inhoud en biedt geen additionele privacy maatregelen. De herleidbaarheid van het afzendende domein is nog steeds geen waarborg op de intenties van de afzender en de inhoud van het mailbericht zelf.
- één van de bouwstenen vormt voor betrouwbaar e-mail verkeer. Andere standaarden kunnen in aanvulling of vervangend, additionele of méér functionaliteit bieden. DKIM is wel een belangrijke basisbouwsteen, omdat het een oplossing biedt voor het authenticatieprobleem van e-mail die als afzenderidentiteit een overheidsdomein kent.
- geen belemmering vormt voor gebruik van andere bouwstenen (standaarden en voorzieningen). Gebruik van DKIM sluit gebruik van andere standaarden niet uit en is mogelijk naast en tegelijk met inzet van andere standaarden voor beveiliging van e-mail.

2.1.3 DKIM als authenticatiemiddel

DKIM biedt toegevoegde waarde en authenticatiemogelijkheden, waar die verder ontbreken bij het vaststellen van de herkomst van e-mail. DKIM zal dan ook primair worden toegepast op alle e-mail die vanuit de overheid wordt verstuurd via het publieke internet m.b.v. SMTP in Internet Message Format. Waar een vooropgezette, beveiligde verbinding (point-to-point systeemkoppeling) wordt ingezet om e-mail uit te wisselen, is er al authenticatie op transmissieniveau ingezet. Bij deze vorm van authenticatie, die ook op de systeem- en organisatiegrenzen plaatsvindt, biedt de verbinding al afdoende maatregelen om de herkomst van de e-mail vast te stellen.

2.1.4 Organisatiegrens

DKIM is bedoeld om bij de verzender ingezet te worden op de Mail Transfer Agent (MTA) op de organisatiegrens, waar de e-mail het (organisatie)domein verlaat. Vandaar dat DKIM nooit meer dan organisatorische herkomst kan duiden en geen (herkomst)binding van e-mail aan individuen of personen kan aangeven. Aan de kant van de ontvanger is DKIM eveneens bedoeld te worden ingezet op de MTA van een organisatiegrens. In geval van bedrijven is dat een bedrijfsdomeingrens, in geval van individuen kan dat de ISP zijn, die namens burgers de mailontvangst uitvoert. De validatie van de DKIM handtekening kan op deze MTA plaats vinden. Het waardeoordeel en de beslissing over de uitkomst van deze validatie kan zowel op deze ontvangende MTA plaats vinden, wanneer deze besluit te filteren of zelfs te blokkeren, als bij de eindgebruiker zelf, die als persoon de uitkomst van de validatie interpreteert.

2.1.5 *Persoonlijk versus automatisch gegenereerde e-mail*
Het onderscheid tussen een middels een door een geprogrammeerde procedure gegenereerde e-mail en een door personen opgestelde mail, is buiten beschouwing gelaten. Ook het onderscheid tussen mail die is bedoeld voor geautomatiseerde verwerking door systemen en verwerking door personen is niet meegenomen. DKIM biedt de ontvanger de mogelijkheid (zowel in persoon als via geautomatiseerde technieken) te kunnen vaststellen wie, op domein niveau, verantwoordelijk is voor het mailbericht: dit kan plaatsvinden los van de verdere inhoud van de mail.

2.2 Functioneel toepassingsgebied

De expertgroep heeft zich gebogen over het toepassingsgebied voor DKIM en heeft daarbij een aantal kenmerken en uitgangspunten vastgesteld met betrekking tot DKIM:

- DKIM biedt een oplossing voor het vaststellen van de authenticiteit en integriteit van een e-mail.
- Maatregelen om de confidentialiteit van de e-mail te garanderen zijn geen onderdeel van DKIM.
- DKIM valideert op een positieve waarde – als de handtekening niet klopt treden andere mechanismen in werking.
- DKIM doet geen uitspraak over de inhoud van de e-mail zelf.
- DKIM is een baseline maatregel met betrekking tot veiligheidsmaatregelen bij e-mail. Het moet gezien worden als een van de bouwstenen die in veiliger en betrouwbaarder e-mail voorzien.

DKIM dient toegepast te worden:

- Bij gebruik van e-mail en is werkzaam op het SMTP protocol (en geen andere protocollen).
- Voor authenticatie op het e-mail object zelf (en niet op bijvoorbeeld het transmissiekanaal; SMTP-AUTH, TLS).
- Voor het kunnen herleiden van de herkomst van de e-mail (via DNS of andere sleutelmanagement diensten/infrastructuren).
- Voor authenticatie door ontvanger op moment van ontvangst, waarbij voorkennis over de afzender niet vereist is en er geen vooropgezette trust relatie aanwezig is.
- Om de(het) organisatie(domein) verantwoordelijkheid te kunnen laten nemen voor verstuurde e-mail.

Het toepassingsgebied geeft aan welke functionaliteit DKIM de overheidsorganisatie biedt die de standaard inzet voor haar voorzieningen. Als functioneel toepassingsgebied adviseert de expertgroep:

> *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.*

DKIM moet daarbij worden ingezet:

- Waar domeinnamen van de overheid waarvoor zij elektronisch bereikbaar zijn (en dit conform de artikelen 2.14 en 2.15 Awb[16] ook

16 http://wetten.overheid.nl/BWBR0024779/geldigheidsdatum_01-02-2012#Hoofdstuk2_23_Artikel214 ; in het NUP is de afspraak gemaakt dat het Rijk,

aangeven), misbruikt kunnen worden voor ongewenste e-mail activiteiten.
- Waar overheids e-mail kans loopt om in spamfilters of quarantaine (zogenaamde 'blacklists') te blijven hangen.
- Als één van de noodzakelijke bouwstenen voor betrouwbaarder e-mail verkeer.

Toelichting op de definitie:
- *Faciliteren*: DKIM biedt de ontvanger de mogelijkheid na te gaan of een afzender verantwoordelijk is voor de e-mail.
- *Herleidbaarheid van organisatorische herkomst*: DKIM duidt organisatorische herkomst, geen herleidbaarheid tot individuen.
- *E-mail afkomstig van overheidsdomeinen*: DKIM kent primair meerwaarde voor de overheid bij e-mail die wordt uitgestuurd. Uitgangspunt is dat ontvangers overweg kunnen met DKIM. De meerwaarde voor de overheid om DKIM voor ontvangende e-mail in te zetten is marginaal.
- *Onbeveiligde, publieke internetverbinding*: DKIM wordt ingezet waar de overheid per e-mail communiceert over het publieke internet.
- *Waar verdere authenticatie ontbreekt*: DKIM biedt toegevoegde waarde en authenticatiemogelijkheden, als die verder ontbreken voor het vaststellen van de herkomst van e-mail.

Bij het vaststellen van het toepassingsgebied heeft de expertgroep de volgende aspecten in beschouwing genomen:
- Dat communicatie met de burger en/of bedrijven op verschillende manieren kan plaats vinden: via verschillende communicatiekanalen en verschillende koppelvlakken. E-mail is een van de deze communicatievormen.
- De EU dienstenrichtlijn en de daaruit voortgekomen Nederlandse Dienstenwet spreekt nadrukkelijk van een centraal communicatieloket voor consumenten en bedrijven. Implementaties van deze wet, zoals daar zijn de Antwoord voor Bedrijven BerichtenBox en de burger berichtenbox van MijnOverheid maken geen gebruik van e-mail (SMTP) maar van respectievelijk de standaard Digikoppeling voor server-to-server (of system-to-system, S2S) communicatie en van een webinterface. DKIM is daar niet van toepassing omdat via de beveiligde S2S verbinding de authenticiteit en integriteit van het bericht al gegarandeerd is. Toch verstuurt de overheid nog steeds direct e-mails (notificaties) naar burgers en bedrijven (al is het maar om melding te maken van een nieuw bericht in de Berichtbox). Een ander voorbeeld hiervan is de e-mail die wordt uitgestuurd bij wachtwoordherstel met betrekking tot DigiD. Dergelijke e-mails hebben baat bij het gebruik van DKIM.
- Het gebruik van DKIM is geen vervanging van de bestaande Digikoppeling tussen overheden of de koppelvlakken van de Digipoort richting burgers en bedrijven. DKIM is veeleer te positioneren als een aanvullende standaard, die de betrouwbaarheid en veiligheid van e-mail communicatie ondersteunt, daar waar deze communicatievorm wordt ingezet
- Het gebruik van DKIM is ook geen vervanging van het gebruik van PKI en de PKI overheidsinfrastructuur. DKIM werkt primair op organisatie

---

de gemeenten, de provincies en de waterschappen voor eind 2010 kenbaar maken op welke manier en voor welke procedures of diensten zij via de elektronische weg bereikbaar zijn en dit op hun website publiceren.

niveau, PKI (i.c.m. bijvoorbeeld S/MIME) werkt primair op het niveau van personen of functies/rollen (end-to-end). Te gebruiken bij aanvullende beveiliging naast DKIM, waarbij een sterkere/nauwkeuriger binding tussen identiteit en e-mail bericht noodzakelijk is, bijv. vanuit juridisch oogpunt.

2.3 Organisatorisch werkingsgebied

De expertgroep adviseert om het organisatorisch werkingsgebied van DKIM overeen te laten komen met het werkingsgebied, waarop het "pas toe of leg uit" principe van toepassing is, te weten:

> *"Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector[17]."*

Bovenstaande omschrijving van het werkingsgebied bevat naar de mening van de expertgroep direct of indirect alle relevante partijen op wie de standaard van toepassing is. De expertgroep zag dan ook geen reden om bovenstaand werkingsgebied verder in te perken.

17 Zoals vastgelegd in het actieplan "Nederland Open in Verbinding" [2].

3 Toetsing van standaard aan criteria

Om te bepalen of de DKIM standaard opgenomen moet worden op de lijst met open standaarden zijn deze getoetst aan een aantal criteria. Deze criteria staan beschreven in het rapport, *"Open standaarden, het proces om te komen tot een lijst met open standaarden"* [2] en staan op de website www.open-standaarden.nl. Het resultaat van de toetsing zal in dit hoofdstuk per criterium beschreven worden. Voor de volledigheid is tevens de definitie van elk criterium opgenomen (*cursief*).

3.1 Openheid

3.1.1 Goedkeuring en handhaving

De standaard is goedgekeurd en zal worden gehandhaafd door een non-profit organisatie. De lopende ontwikkeling gebeurt op basis van een open besluitvormingsprocedure die toegankelijk is voor alle belanghebbende partijen (consensus of meerderheidsbeschikking enz.).

DKIM is in beheer bij IETF. De verdere ontwikkeling en het onderhoud van DKIM wordt vormgegeven door het reguliere standaardisatieproces van IETF, zoals vastgelegd in RFC 2026[18]. Aan dit standaardisatieproces kan iedereen (incl. ieder individu) deelnemen, hetzij via meetings, hetzij via mailing lists. De IETF kent geen formeel lidmaatschap of lidmaatschapseisen. Het standaardisatieproces maakt gebruik van een besluitvormingsprocedure via het principe van "rough consensus"[19], waarbij de dominante mening van een groep, zoals door de voorzitter vastgesteld, de basis voor een beslissing vormt. Documenten, mailing lijsten en verslagen van bijeenkomsten en besluiten zijn publiekelijk beschikbaar op het internet. De IETF is een onderneming zonder winstoogmerk.

Hiermee is naar de mening van de expertgroep voldaan aan dit criterium.

3.1.2 Beschikbaarheid

De standaard is gepubliceerd en over het specificatiedocument van de standaard kan vrijelijk worden beschikt of het is te verkrijgen tegen een nominale bijdrage. Het moet voor een ieder mogelijk zijn om het te kopiëren, beschikbaar te stellen en te gebruiken om niet of tegen een nominale prijs.

Alle IETF standaarden zijn vrij en kosteloos beschikbaar op het Internet, via http://www.ietf.org/.

18 The Internet Standards Process -- Revision 3, http://tools.ietf.org/html/rfc2026

19 IETF Working Group Guidelines and Procedures, http://tools.ietf.org/html/rfc2418

3.1.3 Intellectueel eigendom

Het intellectuele eigendom – met betrekking tot mogelijk aanwezige patenten – van (delen) van de standaard is onherroepelijk ter beschikking gesteld op een "royalty-free" basis.

De Intellectual Property Rights (IPR) policy van IETF is vastgelegd in RFC 3979[20] . Daarin is bepaald dat leden van de werkgroep van een specifieke standaard, bestaande IPR moet onthullen die in de ogen van de werkgroep relevant is voor de standaard die in deze werkgroep in behandeling is. Partijen die hebben meegewerkt aan de DKIM standaard hebben verklaard dat zij *geen* IPR rechten claimen.

IPR claims worden vastgelegd in de RFC van de betreffende standaard en kunnen op de website van IETF worden nagegaan, door gebruik te maken van een IPR zoekfunctie[21]. Dit betekent echter niet dat er garanties gegeven kunnen worden over eventuele *toekomstige claims* met betrekking tot het intellectueel eigendom.

Het patent op een implementatie van DomainKeys (waar DKIM op gebaseerd is) berust bij Yahoo. Yahoo heeft echter de licentie op deze techniek vrijgegeven onder o.a. de Gnu General Public License V2.0 in een statement over IPR met betrekking tot RFC4871 en RFC6376 [22].

Voor de RFC's die in dit advies met betrekking tot DKIM worden beoordeeld geldt verder dat Yahoo geen rechten heeft uitgeoefend en er sinds de start van het standaardisatieproces verder geen IPR claims zijn voorgekomen. De expertgroep is daarom van mening dat daarmee in voldoende mate aan dit criterium wordt voldaan.

3.1.4 Hergebruik

Er zijn geen beperkingen omtrent het hergebruik van de standaard.

Er worden aan het hergebruik van de standaard zelf geen additionele eisen gesteld.

De copyright policy (auteursrechtenbeleid) van de IETF ten aanzien van IETF documenten waarin de standaard is vastgelegd, is in twee documenten verwoord, te weten RFC 5378[23] en de 'IETF Trust's Legal Provisions Relating to IETF Documents'[24]. Hierin is ondermeer vastgelegd, dat:

- Elk document van de IETF vrijelijk mag worden gekopieerd, gepubliceerd, getoond, vertaald en gedistribueerd.
- Elk document van de IETF alleen mag worden gemodificeerd en mag worden gebruikt voor afgeleide producten binnen het IETF standaardisatieproces.
- Iedereen ongewijzigde IETF documenten mag publiceren en vertalen voor elk doeleinde, ook buiten het standaardisatieproces.

---

20 Intellectual Property Rights in IETF Technology, http://www.ietf.org/rfc/rfc3979.txt

21 IPR Search, https://datatracker.ietf.org/ipr/search/

22 https://datatracker.ietf.org/ipr/1547/

23 http://www.rfc-editor.org/rfc/rfc5378.txt

24 http://trustee.ietf.org/docs/IETF-Trust-License-Policy.pdf

- Het niet is toegestaan om aanpassingen te doen aan en afgeleide producten te maken (behalve vertalingen) van IETF documenten en bijdragen buiten het standaardisatieproces. Na consultatie van de gemeenschap kunnen dergelijke rechten per geval eventueel worden toegekend.

Op basis van bovenstaande is de expertgroep van mening dat er geen beperkingen zijn omtrent het hergebruik van de standaard.

3.2 Bruikbaarheid

3.2.1 Volwassenheid

De standaard is voldoende uitgekristalliseerd.

In het standaardisatieproces van de IETF gaan specificaties door een aantal stadia van volwassenheid heen, die samen ook wel het 'standards track' worden genoemd[25]. Er zijn drie niveaus van volwassenheid voor een standaard te onderscheiden, te weten (in toenemende mate van volwassenheid):

- 'Proposed standard' : dit is een stabiele specificatie, waarin alle ontwerpkeuzen zijn uitgewerkt, die in het algemeen goed wordt begrepen, die aan significante review is blootgesteld en die algemeen door de gemeenschap als waardevol wordt gezien.
- 'Draft standard' : dit is een specificatie op basis waarvan ten minste twee onafhankelijke en inter-operabele implementaties zijn ontwikkeld, op basis van verschillende broncode en waarmee met succes voldoende praktijkervaring is opgedaan.
- 'Internet standard' : een specificatie waarmee in de praktijk ervaring is opgedaan in een significante hoeveelheid implementaties, kan tot Internet Standard worden verheven. Deze standaard kent dan een hoge graad van technische volwassenheid.

De huidige status van een RFC in het standaardisatieproces en de updates die op de RFC hebben plaatsgevonden, zijn in te zien op de website van de IETF[26]. In Tabel 1 is van elk van de RFC's, die wordt beoordeeld in het kader van dit expertadvies, de status weergegeven.

RFC	***Titel***	***Status***	***Datum***
6376	DomainKeys Identified Mail (DKIM) Signatures	Draft	Sept. 2011
5585	DomainKeys Identified Mail (DKIM) Service Overview	Informational	Juli 2009

Tabel 1 RFC status

In de tabel is te zien dat RFC6376 de status van 'draft standard' heeft. Dergelijke RFC's zijn in hoge mate stabiel en aan weinig veranderingen onderhevig.

RFC 5585: deze heeft de status 'informational', d.w.z. niet-normatief. Deze RFC voorziet dan ook niet in een specificatie op basis van consensus, maar is informatief en geeft een overzicht van DKIM in relatie tot een

25 The internet Standards Process – Revision 3, http://tools.ietf.org/html/rfc2026

26 Via http://www.rfc-editor.org/

messaging dienst in het algemeen en andere IETF message signature technologieën in het bijzonder. Deze RFC is aan wijzigingen onderhevig, maar zal op de uitgekristalliseerde functionaliteit van DKIM nauwelijks aanpassingen kennen.

De expertgroep is van mening, dat daarmee de DKIM standaard als geheel in voldoende mate is uitgekristalliseerd.

De verdere ontwikkeling en het onderhoud van de standaard zijn verzekerd.

Ja, de organisatie die de standaard beheert (IETF) bestaat sinds 1986 en heeft aangetoond dat zij een stabiele organisatie is die over een lange periode in staat is om standaarden te ontwikkelen en beheren. De DKIM standaarden worden verder ontwikkeld in de Domain Keys Identified Mail Working Group van de IETF.

Er is een methode waarmee conformiteit aan de standaard kan worden bepaald.

DKIM is een 'draft standard' van de IETF. Dat betekent dat interoperabiliteit tussen tenminste twee volledig verschillende software-implementaties van de standaard aangetoond moet zijn. Met DKIM zijn interoperabiliteitstesten uitgevoerd door een groot aantal partijen. De resultaten zijn vastgelegd in RFC5585.

Al deze partijen maken gebruik van DNS voor het publiceren van de publieke sleutel, hoewel andere oplossingen voor DKIM sleutelmanagement niet worden uitgesloten. Er is online tooling beschikbaar om te helpen bij uitvoeren en testen van DKIM installaties in DNS[27]. Verder zijn er diverse open-source pakketten[28] die controleren of een e-mail een geldige DKIM handtekening heeft en zijn er testsites waar een e-mail naar toe gestuurd kan worden ter controle van de DKIM settings[29].

Eventuele interoperabiliteitsgeschillen worden geanalyseerd binnen de IETF en kunnen eventueel leiden tot aanpassingen aan de standaard conform het IETF proces.

Er is voldoende praktijkervaring met het gebruik van de standaard.

De expertgroep geeft aan dat er vooral in het commerciële domein veel ervaring is opgedaan met DKIM. Vooral de zogenaamde webmail oplossingen (Gmail, Yahoo) bepalen daarbij de markt.

De expertgroep constateert ook, dat er in het overheidsdomein tot dusver nog nauwelijks gebruik wordt gemaakt van DKIM.

---

27 http://www.sendmail.org/dkim/tools

28 o.a. http://www.opendkim.org/, http://dkimproxy.sourceforge.net/

29 o.a. http://www.appmaildev.com/en/dkim/,
http://www.myiptest.com/staticpages/index.php/DomainKeys-DKIM-SPF-Validator-test

Er is nu en in de toekomst voldoende ondersteuning door (meerdere) marktpartijen voor de standaard.

Voorbeelden van internationale bedrijven die DKIM toepassen voor hun e-mail communicatie zijn Apple, PayPal, Cisco, Facebook, Twitter, Google (o.a. Gmail en Google Groups), Hotmail, LinkedIn, Yahoo! en eBay.

Er zijn ook de nodige productleveranciers (van ondermeer software voor Mail Transfer Agents, Mail User Agents, Email filtering engines, Mail appliances, DKIM library modules en Mail sending engines) die DKIM ondersteunen[30]. Een grote partij die DKIM wel inzet in de online mailomgeving (Live Mail), maar niet direct in de e-mail software oplossing is Microsoft; die heeft met Sender ID een andere oplossing binnen Microsoft Exchange. Aanvullende software dient de functionaliteit die DKIM biedt, toe te voegen.

In Nederland zijn gebruikers van de standaard bij het verzenden van e-mail o.m. Hyves, Marktplaats, Rabobank en Wehkamp.

Het zijn dus vooral de grote(re) organisaties die DKIM ondersteunen. Het gebruik van DKIM neemt daarbij nog steeds toe, zowel in termen van aantallen ondertekende e-mails als in aantallen organisaties/domeinen die ondertekenen.

Bij de Nederlandse providers is ondersteuning van DKIM aanwezig (bij het ontvangen van e-mail) bij o.m. Freeler, HetNet, KPN Planet, XS4ALL en Ziggo[31].

De verwachting van het toekomstig gebruik van de standaard is positief.

Een mechanisme als DKIM werkt het best bij een kritieke massa van gebruikers. Met ondersteuning door grote e-mail providers als Gmail, Yahoo en Hotmail zal het gebruik van de standaard naar mening van de expertgroep alleen maar toenemen.

Daarnaast kan toenemend gebruik van IPv6 als aanjager voor gebruik van DKIM dienen. Bij groeiend gebruik van IPv6 zullen DNS Blacklists voor filtering van e-mail namelijk niet langer toereikend zijn en wordt de reputatie van een domein bepalend voor aflevering van e-mail aan de geadresseerde. De implementatie van DKIM bij grote (web)mail providers en de stijgende populariteit van deze providers bij (met name) consumenten, maakt het belang van domeinreputatie nog groter voor onder andere overheidspartijen. DKIM, dat gerelateerd is aan de domeinnaam, draagt hiertoe bij.

3.2.2 Functionaliteit

De standaard voldoet aan de functionele eisen die aan de werking van de standaard gesteld worden binnen het voorgestelde toepassingsgebied.

30 http://testing.dkim.org/deploy/index.html

31 http://returnpath.net/internetserviceprovider/receivermap/

Binnen het voorgestelde toepassingsgebied van DKIM is functionaliteit geselecteerd die momenteel in de praktijk van de standaard volledig ondersteund en al toegepast wordt. Naar de mening van de expertgroep zijn er geen functies uit dit toepassingsgebied die de standaard niet ondersteunt.

3.2.3 Standaarden

Zijn er concurrerende standaarden? Zo ja, welke en door wie worden die gebruikt? Wat zijn de voor- en nadelen van deze standaarden ten opzichte van concurrerende standaarden?

Een aantal standaarden vertoont raakvlakken en/of overlap met DKIM. De volgende standaarden worden hieronder één voor één besproken[32]:

- Sender Policy Framework (SPF)[33]
- Sender ID[34]
- S/MIME[35]
- OpenPGP[36]
- DKIM Author Domain Signing Practices (ADSP)[37]

Daarnaast bestaat een aantal voorzieningen die overlap met het toepassingsgebied van DKIM vertonen:

- Digipoort, Digikoppeling[38]
- Antwoord voor Bedrijven, Berichtenbox
- Public Key Infrastructure (PKI) via PKIoverheid

SPF, Sender ID, S/MIME en OpenPGP worden allen onderhouden en beheerd door de IETF. Digipoort, Digikoppeling, de Berichtenbox en PKIoverheid zijn in ontwikkeling en beheer bij Logius.

Tenslotte wordt kort de relatie met de standaarden DNS en DNSSEC aangestipt.

SPF

Omschrijving

- SPF biedt de mogelijkheid te controleren of een bericht aangeleverd wordt vanaf een server die daartoe gerechtigd is. SPF maakt de authenticiteit van de domeinnaam in het afzenderadres van de ontvangen mail herleidbaar via de in DNS gepubliceerde IP-adressen van de verzendende mailserver(s). SPF biedt dus, net als DKIM, een vorm van e-mail authenticatie op organisatieniveau. Daar waar DKIM authenticatie biedt voor het bericht, biedt SPF dit voor een deel van het transmissiekanaal.

Kenmerken

- Is relatief simpel te implementeren en te onderhouden.

---

32 Inmiddels is er ook initiatieven dat meerdere van deze bouwstenen samenneemt om de bedreigingen van misleidende e-mail tegen te gaan: DMARC. Dit is een policy raamwerk dat voortborduurt op SPF en DKIM, zie ook http://www. dmarc.org

33 Sender Policy Framework (SPF), http://tools.ietf.org/html/rfc4408

34 Sender ID, http://tools.ietf.org/html/rfc4406

35 S/MIME, http://tools.ietf.org/html/rfc5751

36 OpenPGP, http://tools.ietf.org/html/rfc4880, http://tools.ietf.org/html/rfc3156

37 ADSP, http://tools.ietf.org/html/rfc5617

38 http://www.logius.nl/producten/gegevensuitwisseling/digikoppeling/

- Wordt al gebruikt door verschillende overheden (gemeentes)[39] en door commerciële mailproviders in Nederland[40].
- Is niet belast met patenten en licenties.
- Is nog geen officiële standaard bij het IETF (bevindt zich niet in het standards track), maar een experimentele standaard.
- Wordt al veelvuldig gebruikt door ISP's (ook in combinatie met DKIM) en enkele overheidspartijen (o.a. Logius).

Conclusie

- SPF kent een soortgelijk toepassingsgebied en biedt functionaliteit die aanvullend is aan DKIM.

Advies aan Forum/College

- Niet verplichten, wel aanbevelen voor gebruik i.c.m. DKIM

Sender ID

Omschrijving

- Sender ID is een authenticatieprotocol, voorgesteld door Microsoft, dat is afgeleid van SPF en die soortgelijke functionaliteit biedt als SPF.

Kenmerken

- Sender ID bevindt zich net als SPF in de experimentele status, doordat het technische incompatibiliteit kent met SPF en andere IETF RFC's41
- Microsoft bezit patenten op delen van de standaard, die weliswaar onder de Open Specification Promise zijn geplaatst42, maar deze licentie is niet compatibel met GPLv3.
- Sender ID wordt slechts op beperkte schaal gebruikt

Conclusie

- Sender ID kent een soortgelijk toepassingsgebied als DKIM, maar biedt geen extra functionaliteit ten opzichte van SPF.

Advies aan Forum/College

- Geen verdere acties.

S/MIME en OpenPGP

Omschrijving

- S/MIME en OpenPGP zijn standaarden voor het versleutelen en (elektronisch) ondertekenen van MIME data (de inhoudelijke opmaak van e-mail berichten). Beide kunnen dus zorgen voor garantie op privacy en dataveiligheid in het bericht (via encryptie) en zorgen voor integriteit van het bericht, onweerlegbaarheid van de afzender en authenticatie (door gebruik van een digitale handtekening).

Kenmerken

- Identiteit van afzender en ontvanger zijn gekoppeld in de beveiliging van S/MIME en OpenPGP.
- S/MIME en OpenPGP zijn primair van toepassing op de inhoud van een bericht waar DKIM de mogelijkheid biedt de integriteit en authenticiteit van de berichtheaders te controleren.
- De S/MIME en OpenPGP oplossingen werken in principe op persoonsniveau, waar DKIM werkt op organisatieniveau. Dit betekent dat de eindgebruiker zijn mail moet ondertekenen met een eigen certificaat. De herkomst van een e-mail object is dus te herleiden is naar een (juridische/rechts) persoon i.p.v. een organisatie.

---

39 O.a. Logius en gemeentes Apoeldoorn, Den Haag, Groningen, Hengelo

40 Return Path Certification Inbox Coverage,

http://www.returnpath.net/internetserviceprovider/receivermap/

41 http://www.iab.org/appeals/2006-02-08-mehnle-appeal.html

42 http://www.microsoft.com/presspass/press/2006/oct06/10-23OSPSenderIDPR.mspx

- Het inzetten van S/MIME en OpenPGP gaat gepaard met een infrastructuur die de binding verzorgt tussen de private key en de eigenaar. In geval van S/MIME is dat een Public Key Infrastructure (PKI), in geval van OpenPGP een zogenaamd Web of Trust. Bij DKIM wordt DNS gebruikt voor deze infrastructuur.
- Maakt gebruik van trusted keys of self-signed keys. In het eerste geval ontstaat een trusted infrastructure (bijvoorbeeld de PKIoverheid infrastructuur, zie verderop).

Conclusie

- DKIM werkt primair op organisatie niveau, OpenPGP en S/MIME werken primair op het niveau van personen of functies/rollen (end-to-end). Te gebruiken bij aanvullende beveiliging naast DKIM, waarbij een sterkere/nauwkeuriger binding tussen identiteit en e-mail bericht noodzakelijk is, bijv. vanuit juridisch oogpunt.

Advies aan Forum/College

- Geen verdere acties.

ADSP

Omschrijving

- Author Domain Signing Practices (ADSP) is een optionele uitbreiding van DKIM, waarmee een organisatie voor het maildomein kan aangeven welke beleid wordt gehanteerd ten aanzien van elektronische handtekeningen voor DKIM op berichten. Organisaties die al hun mail voorzien van een geldige DKIM handtekening kunnen middels ADSP bijvoorbeeld aan de ontvanger adviseren een bericht weg te gooien, wanneer de ontvanger geen DKIM handtekening aantreft of wanneer de ontvanger een ongeldige handtekening ontvangt.

Kenmerken

- Ontvangers van met DKIM ondertekende e-mail berichten kunnen via DNS informatie opvragen over het beleid van de zendende organisatie.
- ADSP biedt de verzender de mogelijkheid om policies te definiëren, zodat de ontvanger weet hoe te handelen bij ontbreken van een DKIM handtekening.

Conclusie

- ADSP kent geen overlap met het toepassingsgebied van DKIM, maar biedt aanvullende maatregelen. ADSP i.c.m. DKIM is bijvoorbeeld niet alleen te gebruiken om authenticatie te kunnen leveren op domeinen waar e-mail vandaan komt , maar ook om authenticatie op domeinen te verzorgen, waar geen mail vandaan komt en hoort te komen (bv mail van Belastingdienst.nl, Digid.nl die door ongeautoriseerde derden verzonden wordt kan dan zondermeer weggegooid worden).

Advies aan Forum/College

- Geen verdere acties.

Digikoppeling/Digipoort

Omschrijving

- Digikoppeling/Digipoort bestaat uit een set standaarden voor elektronisch berichtenverkeer tussen overheidsorganisaties. Een bedrijf kan ook informatie, zoals een e-factuur, aanleveren aan de overheid via Digipoort (het postkantoor). Digipoort zorgt er vervolgens voor dat de informatie o.b.v. Digikoppeling bij de juiste overheidsinstantie terechtkomt. De specificaties van Digipoort/Digikoppeling schrijven een aantal koppelvlakken en bijbehorende standaarden voor. Een van deze standaarden is SMTP,

waarbij uitwisseling van op SMTP gebaseerde (e-mail) berichten wordt beveiligd door het opzetten van een (veilig) communicatiekanaal tussen de verzendende en ontvangende partij met behulp van SMTP authenticatie (SMTP-AUTH). Hierbij wordt gebruik gemaakt van een PKIoverheid certificaat om het kanaal te beveiligen en partijen te authenticeren.

Kenmerken

- Gebruik van vooraf bepaalde trust relatie om een veilig communicatiekanaal op te zetten: waar DKIM de authenticatie op het mailbericht zelf legt, doet Digikoppeling dit op het niveau van transmissiekanaal.
- Herleidbaarheid van herkomst op organisatieniveau op basis van het transmissiekanaal en niet op basis van het e-mail object.
- Wordt toegepast als de inhoud van het bericht bedoeld is voor automatische verwerking

Conclusie

- Digipoort kent overlap met het toepassingsgebied van DKIM, doordat het ook uitwisseling van berichtverkeer op basis van SMTP biedt. Digipoort kent zijn gebruik bij structurele(re) trust relaties die vastgelegd worden voordat daadwerkelijke informatie uitwisseling plaatsvindt en authenticatie op transmissieniveau.

Advies aan Forum/College

- Geen: standaard staat al op de lijst.

Antwoord voor Bedrijven, Berichtenbox

Omschrijving

- De Berichtenbox voor bedrijven is een beveiligd e-mailsysteem waarmee men via Antwoord voor Bedrijven (AvB) digitaal berichten kunt uitwisselen met Nederlandse overheidsinstanties (de Rijksoverheid, provincies, gemeenten en waterschappen). Met de Berichtenbox voor burgers (via (Mijn)Overheid.nl) kan men op een veilige manier persoonlijke digitale post van overheidsorganisaties ontvangen.

Kenmerken

- De Algemene Wet Bestuursrecht (artikelen 2:13 tot en met 2:17) biedt de mogelijkheid om communicatie vanuit overheid via Berichtenbox of AvB te voeren, maar ook via andere communicatiemiddelen. E-mail als communicatiemiddel is dus toegestaan (en gebeurt ook al, bijvoorbeeld de melding i.v.m. DigiD).

Conclusie

- De Berichtenbox kent overlap met het toepassingsgebied van DKIM, doordat het ook ondersteuning voor berichtverkeer met burger en bedrijf biedt. Naast authenticiteit, biedt de Berichtenbox ook waarborg op vertrouwelijkheid bij privacy gevoelige inhoud. De Berichtenbox dient dus te worden ingezet bij privacy gevoelige inhoud.

Advies aan Forum/College

- Geen: de voorziening kent wettelijke verankering.

PKIoverheid

Omschrijving

- Een infrastructuur die de binding verzorgt tussen de private key en de eigenaar. PKIoverheid certificaten worden gebruikt bij het zetten van een rechtsgeldige elektronische handtekening, het beveiligen van

websites, het op afstand authenticeren van personen of services en het versleutelen van berichten.

Kenmerken

- In een PKI vindt de authenticatie gecentraliseerd plaats bij een externe dienstverlener, de Trusted Third Party. Kent de laatste tijd problemen m.b.t. vertrouwen en problemen bij Certificate Authorities (CA's: Diginotar, Comodo, etc.).
- In te zetten voor uitgifte van trusted certificaten voor andere standaarden (waaronder S/MIME) en bedoeld voor end-to-end authenticiteit.
- Leidt in de praktijk regelmatig tot misverstanden en problemen bij ontvanger doordat het certificaat niet goed wordt weergegeven, niet herleidbaar is of niet zichtbaar.
- Zou eventueel implementatie van sleutels DKIM kunnen verzorgen. Een van de uitgangspunten van DKIM is dat het niet afhankelijk is van een dergelijke (PKI) infrastructuur en bijbehorende X509v3 certificaten: DKIM maakt alleen gebruik van encryptiesleutels en niet van complete certificaten. Hoewel het gebruik van de PKIoverheid certificaten voor DKIM dus niet nodig is, staat de implementatie van DKIM met behulp van DNS wel toe dat behalve de sleutels ook complete certificaten worden opgeslagen. De binding tussen de sleutel (public key) en het verzendende e-mail domein wordt echter wel gelegd via opname van de sleutel in DNS, in plaats van via een vertrouwde (derde) partij.

Conclusie

- PKIoverheid kent overlap met het toepassingsgebied van DKIM, doordat het ook authenticiteit van e-mail berichtverkeer met burger en bedrijf ondersteunt. PKIoverheid ondersteunt daarnaast herleidbaarheid van herkomst tot op persoonsniveau, wanneer er een sterke/nauwkeurige binding tussen identiteit en e-mail bericht noodzakelijk is, bijv. vanuit juridisch oogpunt (mogelijk i.c.m. S/MIME). Daarnaast biedt het andere functionaliteit door vertrouwelijkheid te bieden op berichtniveau.

Advies aan Forum/College

- Geen verdere acties.

DNS, DNSSEC

Omschrijving

- DNS is een hiërarchische, gedistribueerde infrastructuur voor genetwerkte apparaten om domeinnamen (o.a.) te koppelen aan numerieke (internet) adressen. DNSSEC is een uitbreiding op DNS die voorziet in beveiliging van (een deel van) de informatie in DNS, door deze van een digitale handtekening te voorzien.

Kenmerken

- DNS is een schaalbare en efficiënte infrastructuur voor het opzoeken van mailservers
- DNSSEC biedt garanties voor de authenticiteit en integriteit van DNS informatie
- Nog niet alle domeinen zijn beveiligd middels DNSSEC waardoor er geen volledige trust hiërarchie is.

Conclusie

- Verificatie van de DKIM handtekening vindt plaats via het publieke deel van de publiek-private sleutel-combinatie waarmee de handtekening gezet is. Deze publieke sleutel wordt in het DNS domein geplaatst dat eigendom is van de organisatie die de DKIM handtekening in een bericht plaatst. Een beveiligingsrisico dat de

expertgroep onderkent is de beveiliging van de DNS infrastructuur, waardoor de authenticiteit en integriteit van de DKIM publieke sleutels niet gegarandeerd is. Tegelijkertijd merkt de expertgroep op, dat het compromitteren van DNS niet triviaal is. Met invoering van een veilig DNS, te weten DNSSEC, kan de betrouwbaarheid van DKIM als authenticatiemiddel toenemen.

Advies aan Forum/College

- Inmiddels heeft Forum en College de expertprocedure DNSSEC voor de lijst met open standaarden voor 'pas toe of leg uit' in gang gezet. De overwegingen m.b.t. DKIM zijn meegenomen in de besluitvorming rond de procedure voor DNSSEC.

3.3 Potentieel

3.3.1 Leveranciersonafhankelijkheid

Het opnemen van de standaard op de lijst draagt bij aan het vergroten van de leveranciersonafhankelijkheid.

De expertgroep is van mening, dat de introductie van DKIM noch een toename, noch een afname van leveranciersonafhankelijkheid met zich mee zal brengen.

Enerzijds is DKIM een open standaard die door iedereen geïmplementeerd kan worden. De meeste software op het gebied van mail afhandeling (Mail Transfer Agent) biedt die optie al aan, waarmee leveranciersonafhankelijkheid gecreëerd is. Anderzijds zijn er leveranciers die dit nog niet ondersteunen waardoor de keuze beperkt wordt.

3.3.2 Interoperabiliteit

Het opnemen van de standaard op de lijst draagt bij aan het vergroten van de interoperabiliteit.

Op dit moment levert het versturen van een e-mail met beveiligingsmiddelen voor authenticatie in de praktijk in sommige gevallen problemen op. Enkele van de standaarden die soortgelijke toepassing als DKIM beogen, zorgen er in de praktijk voor dat er bij validatie van herkomst (bv onjuist gebruik SPF records) of validatie van certificaten (bv onvermogen om certificaten te valideren bij gebruik van S/MIME), verstoringen kunnen optreden in de uitwisseling van e-mail. De expertgroep is daarom 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.

3.4 Impact

3.4.1 Bedrijfsvoering

Brengt de toepassing van de standaard risico's met zich mee op het gebied van de bedrijfsvoering?

De risico's zijn naar de mening van de expertgroep beperkt omdat DKIM relatief eenvoudig te implementeren is. Gebruik van DKIM kan mogelijk vereisen dat aanvullende maatregelen genomen dienen te worden om de status van de handtekening bij verzending vast te leggen zodat niemand aan de hand van een ontvangen DKIM handtekening valse claims kan poneren. Voorbeelden van dergelijke aanvullende maatregelen zijn archivering en correcte tijdstempels. Hierbij dient te worden opgemerkt, dat dergelijke maatregelen ook nodig zijn bij onbeveiligde mail communicatie.

Wel kan DKIM 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.

Brengt de toepassing van de standaard positieve effecten met zich mee op het gebied van de bedrijfsvoering?

Het gebruik van DKIM zorgt naar de mening van de expertgroep voor vertrouwen in de ontvangen mail bij de ontvanger (burger, bedrijf); het vergroot de reputatie van de overheid als betrouwbare communicatiepartner.

Daarnaast vergroot het de kans dat een verzonden mail daadwerkelijk aankomt bij de ontvanger en niet wordt uitgefilterd of in de spam-box belandt. Het niet invoeren van DKIM kan mogelijk resulteren in een verlaagde zekerheid dat een e-mail aankomt: met het toenemende belang dat grote e-mail providers hechten aan authenticatie op basis van (o.m.) DKIM, is het niet ondenkbaar dat e-mails zonder DKIM handtekening in de toekomst door deze providers gemarkeerd en/of gefilterd gaan worden.

De kans op response van de ontvangende partij wordt hiermee ook groter hetgeen de dienstverlening richting burger en bedrijf ten goede komt.

De expertgroep ziet in DKIM verder een relatief laagdrempelige en kosteneffectieve authenticatiemethode met betrekking tot e-mail. De expertgroep is daarnaast van mening, dat de maatschappelijke kosten voor het bestrijden van e-mail spoofing en phishing met DKIM kunnen worden verlaagd, doordat in een eerder stadium van verwerking van de e-mail aannames kunnen worden gedaan over de verzender.

3.4.2 Informatievoorziening

Brengt de toepassing van de standaard risico's met zich mee op het gebied van de informatievoorziening?

De expertgroep meent dat er geen zwaarwegende risico's zijn op het gebied van de informatievoorziening. DKIM kan er juist voor zorgen dat informatie in een e-mail beter aankomt, mits de standaard goed wordt geïmplementeerd en gebruikt. Er dient wel nagedacht te worden over hoe om te gaan met het wel of niet accepteren van mail bij afwezigheid of

incorrectheid van een DKIM handtekening. Andere mechanismen moeten dan in werking treden. Een foute implementatie en verkeerd gebruik van de standaard kan ervoor zorgen dat e-mails ten onrechte de ontvanger niet bereiken. Een verkeerd ingestelde DKIM key kan zo dus juist schade toebrengen aan de reputatie van de verzender en zorgen voor verlies aan 'informatie'.

Brengt de toepassing van de standaard positieve effecten met zich mee op het gebied van de informatievoorziening?

DKIM voegt een controlemechanisme aan uitwisseling van e-mails toe, waarmee de informatie in e-mail verkeer met grotere zekerheid kan aankomen bij de beoogde eindgebruikers. De ontvangen e-mail krijgt middels authenticatie meer betrouwbaarheid, terwijl de verzendende partij een betere reputatie krijgt als verstrekker van informatie.

3.4.3 Technologische risico's

Brengt de toepassing van de standaard technologische risico's met zich mee?

De expertgroep stelt vast, dat de investeringen en inspanningen die nodig zijn voor implementatie van DKIM te overzien zijn.

Tegelijkertijd is er wel een afhankelijkheid van de veiligheid van DNS: als DNS gecompromitteerd raakt, zijn de DKIM sleutels niet meer betrouwbaar. Een aanval op DNS kan voor het betreffende e-maildomein resulteren in een valse public key injectie waarvan spammers/hackers misbruik kunnen maken. Een dergelijke compromittering is naar de mening van de expertgroep in de praktijk geen zwaarwegend probleem, omdat dit geen eenvoudige opgave is (en deze gebeurtenis dus niet snel zal optreden) en omdat met een gecompromitteerd DNS de hele basis onder het e-mail verkeer en zelfs het hele internet wegvalt. Met invoering van een veilig DNS, te weten DNSSEC, kan de betrouwbaarheid van DKIM als authenticatiemiddel toenemen.

Verder zal breed gebruik van DKIM resulteren in een toename van het DNS verkeer, maar de expertgroep geeft aan dat om een relatief kleine toename gaat en de DNS infrastructuur voldoende robuust is om dit af te handelen.

De manier waarop e-mail clients omgaan met DKIM is een mogelijk verbeterpunt: extra mogelijkheden om DKIM handtekeningen te controleren via de cliënt en te visualiseren voor de eindgebruiker lijken gewenst.

Brengt de toepassing van de standaard positieve technologische effecten met zich mee?

Naar de mening van de expertgroep is het een voordeel van DKIM dat de standaard op een voor eindgebruikers transparante manier in de mail infrastructuur is te implementeren (op het niveau van de Mail Transfer Agents).

Verder kan DKIM volgens de expertgroep gezien worden als een infrastructuur oplossing voor e-mail beveiliging waar bovenop additionele, nieuwe maatregelen kunnen worden toegevoegd. Met DKIM wordt het mogelijk om andere technologieën te voorzien van betrouwbare informatie, bijvoorbeeld anti-spam voorzieningen.

Tenslotte kan worden opgemerkt, dat ongewenste mail relatief vroegtijdig gedetecteerd en geblokkeerd kan worden, zodat de belasting van de mail infrastructuur afneemt.

3.4.4 Beveiliging en privacy

Brengt de toepassing van de standaard risico's met zich mee op het gebied van beveiliging of privacy?

De expertgroep onderkent een risico in het gegeven dat DKIM geen zekerheid biedt wat betreft de bedoelingen van de verzender van de mail. Het kunnen herleiden van de afzender kan door de ontvanger worden vertaald in te grote mate van vertrouwen met betrekking tot de inhoud. De overheid heeft hier uiteraard zelf de verantwoording als verzendende organisatie en eigenaar van het betreffende e-mail domein om zorg te dragen voor veiligheid en betrouwbaarheid van de inhoud van de e-mail. Tegelijkertijd kan worden vastgesteld dat deze garantie bij andere standaarden evenmin aanwezig is.

DKIM biedt met betrekking tot beveiliging geen oplossing voor de confidentialiteit/vertrouwelijkheid van de e-mail waardoor de privacy eventueel geschaad kan worden. De praktijk wijst echter uit dat vooral authenticiteit en integriteit van mailwisseling belangrijk zijn en dat het ontbreken van confidentialiteit in veel gevallen geen drempel voor het gebruik van e-mail is. Een voorbeeld is het versturen van een elektronische factuur: de eis van de Belastingdienst is dat de twee laatstgenoemde aspecten gewaarborgd zijn, confidentialiteit/ vertrouwelijkheid wordt hierbij niet geëist.

Een beveiligingsrisico dat de expertgroep onderkent is de beveiliging van de DNS infrastructuur, waardoor de authenticiteit en integriteit van de DKIM publieke sleutels niet gegarandeerd is. Tegelijkertijd merkt de expertgroep op, dat het compromitteren van DNS niet triviaal is en met de in gang zijnde uitrol van een veilig DNS (DNSSEC) nog moeilijker gemaakt wordt. Met invoering van DNSSEC kan de betrouwbaarheid van DKIM als authenticatiemiddel toenemen. Inmiddels is er een expertprocedure gestart voor het al dan niet laten opnemen van DNSSEC op de ‘pas toe of leg uit’ lijst van open standaarden.

Brengt de toepassing van de standaard positieve technologische effecten met zich mee op het gebied van de beveiliging en privacy?

De expertgroep is van oordeel dat DKIM verschillende positieve effecten met zich mee kan brengen:

- Het maatschappelijk vertrouwen in de overheid als afzender van berichten zal toenemen.
- Het toepassen DKIM geeft extra beveiliging, gedreven vanuit de technologie.

- Door aanvullende standaarden in te zetten in combinatie met DKIM kunnen banken/verzekeraars/overheid etc. phishing bestrijden, door de organisatie policies met betrekking tot e-mail in het algemeen of met betrekking tot ongetekende e-mail in het bijzonder, duidelijk en eenduidig te maken.
- De reputatie van een mailverzender kan met DKIM eenvoudig worden gecontroleerd. Mailverzenders die misbruik maken van domeinnamen kunnen op deze manier makkelijk gefilterd worden.

3.4.5 Migratie

Kan er gemakkelijk naar de standaard worden gemigreerd?

De expertgroep is van mening dat er relatief eenvoudig naar de standaard kan worden gemigreerd. Implementatie van DKIM voor verzenden van e-mail vraagt aanpassing van DNS records en het toevoegen van een handtekening aan de mail headers. Deze implementatie is daarmee backwards compatible met bestaande processen voor e-mail uitwisseling en zal deze niet verstoren. Met betrekking tot bestaande software en ICT systemen voor verzending van e-mail vergt het gebruik een extra (complementaire) module die voor ondertekening kan zorgen. Daarbij geldt dat vele (de meeste) software en mail-appliances het gebruik van DKIM inmiddels ondersteunen of dat ondersteuning relatief eenvoudig kan worden toegevoegd.

Ondersteuning van DKIM als ontvanger vergt een controlestap op de DNS records van de afzender, een stap die eveneens zonder al te grote inspanning kan worden toegevoegd aan het bestaande e-mail proces en ook door de meeste software en mail-appliances wordt ondersteund. De grootste inspanning ligt naar mening van de expertgroep potentieel in het gebruik van de DKIM informatie in het verdere verwerkingsproces van de ontvangen e-mail. De ontvanger van de e-mail hoeft de DKIM handtekening echter niet te controleren. Ook zonder controle op de handtekening is de e-mail leesbaar.

Een aandachtspunt bij migratie is de keuze die gemaakt dient te worden voor domeinen die ondertekend moeten worden. Het potentieel grote aantal domeinen dat van een handtekening moet worden voorzien, kan door de omvang een omvangrijke migratielast opleveren.

4 Advies aan Forum en College

4.1 Samenvatting van de toetsingscriteria

Samengevat is het oordeel van de meerderheid van de expertgroep op de toetsingscriteria als volgt:

- *Openheid*

De standaard voldoet aan de criteria van openheid. Men kan vrij over de standaard beschikken en de IETF is een open organisatie die voor beheer en onderhoud van de standaarden zorgt. Er liggen weliswaar rechten op de voorloper van DKIM, maar de rechthebbende heeft deze vrijgegeven onder een GPL licentie.

- *Bruikbaarheid*

De standaard voldoet aan de criteria van 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. De ondersteuning van DKIM neemt ook bij de bepalende webmail leveranciers (Google, Yahoo, Windows Live Hotmail) toe. Bij de Nederlandse providers is ondersteuning van DKIM aanwezig (bij het ontvangen van e-mail) bij o.m. Freeler, HetNet, KPN Planet, XS4ALL en Ziggo

- *Potentieel*

DKIM zal bijdragen aan het verbeteren van de interoperabiliteit: er worden nu belemmeringen ervaren met alternatieve authenticatiemiddelen als PKI, die door inzet van DKIM opgelost worden. Er is geen impact op de leveranciersonafhankelijkheid.

- *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: de verzendende overheidspartij houdt hiervoor verantwoordelijkheid. Het maatschappelijk vertrouwen in de overheid als afzender van berichten zal echter toenemen. Daarnaast draagt brede adoptie van DKIM bij aan beter en effectiever benutten van de mogelijkheden DKIM. Verder kan DKIM worden beschouwd als een relatief laagdrempelige en kosteneffectieve authenticatiemethode met betrekking tot e-mail. Er dient opgemerkt te worden dat DKIM geen totaaloplossing voor e-mail beveiliging is; het moet gezien worden als één van de bouwstenen.

4.2 Advies aan Forum en College

De expertgroep adviseert het college in meerderheid om DKIM op te nemen op de lijst met open standaarden voor "pas toe of leg uit", met het

in hoofdstuk 2 vastgestelde toepassings- en werkingsgebied, met als 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.*

En als werkingsgebied:

> *"Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector[43]."*

Met de adoptie van de DKIM standaard worden problemen met misbruik van overheidsdomeinnamen voor ongewenste e-mail activiteiten teruggedrongen. Een merderheid 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.

De meerderheid van de expertgroep is verder van mening dat een goed voorbeeld goed doet volgen. Dit 'leading by example' argument wordt op zichzelf al als voldoende valide geacht om toetreding tot de lijst te rechtvaardigen. Andere partijen zullen gestimuleerd worden om ook DKIM te gaan gebruiken of om ermee door te gaan waardoor het effect van DKIM vergroot zal worden, namelijk een betrouwbaarder e-mail verkeer.

4.3 Aanbevelingen ten aanzien van de adoptie van de standaard

Concreet doet de expertgroep in meerderheid de volgende aanvullende aanbevelingen:

- Informeer als Forum Standaardisatie burgers over het veilig gebruik van e-mail ten aanzien van overheids e-mail (b.v. m.b.t. het uitvragen van DigiD gegevens).
- Wijs specifiek partijen als DigiD en MijnOverheid op het gebruik van aanvullende maatregelen als DKIM om e-mail notificaties vanuit deze organisaties beter te beveiligen.
- Wijs overheidspartijen op het nut van DKIM verificatie door de overheid zelf, om phishing en spoofing gericht tegen overheidspartijen en ambtenaren zichtbaar te maken: opname op de lijst richt zich uitsluitend op uitgaand e-mail verkeer
- Stel als Forum Standaardisatie in samenwerking met GovCERT en NCSC een handreiking op voor overheidspartijen voor veilig en betrouwbaar e-mail verkeer. Benoem daarin de relaties met de andere standaarden.
- Beveel voor domein authenticatie naast DKIM gebruik van SPF aan bij implementaties.

43 Zoals vastgelegd in het actieplan "Nederland Open in Verbinding" [1].

5 Referenties

[1] Digitale AgendaNL, Ministerie van EL&I, 2011, http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2011/05/30/aanbiedingsbrief-overheidsbrede-implementatieagenda-voor-dienstverlening-en-e-overheid-i-nup.html

[2] overheidsbrede implementatieagenda voor dienstverlening en e-overheid: i-NUP, Ministerie van EL&I, 2011, http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2011/05/30/aanbiedingsbrief-overheidsbrede-implementatieagenda-voor-dienstverlening-en-e-overheid-i-nup.html

[3] P.H. Minnecré and L. Korsten, Open Standaarden, Het proces om te komen tot een lijst met open standaarden, Verdonck, Klooster & Associates B.V., 2008.

[4] " Instellingsbesluit College en Forum Standaardisatie 2010". Zie: https://zoek.officielebekendmakingen.nl/stcrt-2010-4499.html

[5] Toetsingsprocedure en criteria, vastgesteld door College op 23 juni 2011, http://www.forumstandaardisatie.nl/fileadmin/os/images/Toetsingsprocedure_en_criteria_v1_0.pdf