Forum Standaardisatie

Expertadvies functioneel toepassingsgebieden internet veiligheidstandaarden

Concept ter openbare consultatie

Datum 27 juli 2017

Colofon

Projectnaam	Expertadvies functioneel toepassingsgebieden internet veiligheidstandaarden
Versienummer	1.0
Locatie	Den Haag
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag info@forumstandaardisatie.nl
Auteur(s)	Rick van Rooijen
Onafhankelijk voorzitter	Roy Tomeij

Inhoud

Samenvatting en Forumadvies

Advies aan het Forum

Als functioneel toepassingsgebied voor SPF wordt geadviseerd:

SPF moet worden toegepast op alle overheidsdomeinnamen, ook op domeinen waarvan niet wordt gemaild, én op alle mailservers waarmee de overheid e-mail ontvangt.

Als functioneel toepassingsgebied voor DKIM wordt geadviseerd:

DKIM moet worden toegepast op alle overheidsdomeinnamen waarvandaan wordt gemaild én op alle mailservers waarmee de overheid e-mail verstuurt en ontvangt.

Als functioneel toepassingsgebied voor DMARC wordt geadviseerd:

DMARC moet worden toegepast op alle overheidsdomeinnamen, ook op domeinen waarvan niet wordt gemaild, én op alle mailservers waarmee de overheid e-mail ontvangt.

Als functioneel toepassingsgebied voor HTTPS en HSTS wordt geadviseerd:

HTTPS en HSTS moeten worden toegepast op de communicatie tussen clients (zoals webbrowsers) en servers voor alle websites en webservices.

Als functioneel toepassingsgebied voor TLS wordt geadviseerd:

TLS moet worden toegepast op de uitwisseling van gegevens tussen clients en servers, inclusief machine-to-machine communicatie.

Als functioneel toepassingsgebied voor DNSSEC wordt geadviseerd:

DNSSEC moet worden toegepast op alle overheidsdomeinnamen én op DNS-resolvers die clients van overheidsorganisaties direct of indirect van DNS-antwoorden voorzien.

Waar gaat het inhoudelijk over?
SPF, DKIM, DMARC, HTTPS en HSTS, TLS en DNSSEC zijn standaarden voor de beveiliging van internetverbindingen, websites en e-mail. Het gebruik ervan levert een belangrijke bijdrage aan de betrouwbaarheid van het Nederlandse internet. De standaarden worden genoemd in de memorie van toelichting bij de Wet GDI en in het Nationaal Beraad Digitale Overheid (hierna Nationaal Beraad) van 2 februari 2016 zijn aanvullende resultaatafspraken gemaakt over de adoptie van de standaarden.

Hoe is het proces verlopen?
De internet veiligheidstandaarden zijn al opgenomen op de lijst met open standaarden waarvoor een ‘pas toe of leg uit’-verplichting geldt, met

uitzondering van DMARC. In opdracht van het Forum Standaardisatie heeft Verdonck, Klooster & Associates voorstellen gedaan voor nieuwe, duidelijkere omschrijvingen van de functioneel toepassingsgebieden van deze (en andere) standaarden. Het Forum Standaardisatie heeft besloten de voorgestelde omschrijvingen in procedure te nemen. Hierop volgend is een expertgroep samengesteld en een voorzitter aangesteld. De experts zijn bijeengekomen om de voorgestelde omschrijvingen te bespreken en verder te verduidelijken. Dit expertadvies geeft de uitkomsten van de bijeenkomst weer.

Vervolg
Het Bureau Forum Standaardisatie zal dit expertadvies openbaar maken ten behoeve van een publieke consultatie die plaatsvindt van 1 augustus 2017 tot en met 13 september 2017. Eenieder kan gedurende de consultatieperiode een reactie geven op dit expertadvies. Na afsluiting van de openbare consultatie koppelt het Bureau Forum Standaardisatie de reacties terug aan de expertgroep.

Het Forum Standaardisatie stelt met het expertadvies en de relevante inzichten uit de openbare consultatie een advies aan het Nationaal Beraad op. Het Nationaal Beraad besluit met dit advies om de omschrijvingen van de functioneel toepassingsgebieden wel of niet aan te passen op de lijst met open standaarden.

1 Doelstelling expertadvies

1.1 Achtergrond

De Nederlandse overheid streeft naar betrouwbare gegevensuitwisseling door het gebruik van open standaarden en het voorkomen van vendor lock-in. Het actieplan "Open Overheid", de Digitale Agenda 2017 en de kabinetsreactie op het Rapport Elias benadrukken dit beleid. Om dit doel te bereiken, onderstrepen het instellingsbesluit van het Forum Standaardisatie, de Generieke Digitale Infrastructuur en de verschillende architectuurkaders het gebruik van open standaarden bij het ontwerpen of inkopen van informatiesystemen.

Een van de maatregelen om de adoptie van open standaarden te bevorderen is de publicatie en het beheer van een lijst met open standaarden waarvoor een 'pas toe of leg uit'-verplichting geldt of waarvan het gebruik 'aanbevolen' is. Het Nationaal Beraad Digitale Overheid (hierna Nationaal Beraad) besluit welke standaarden op deze lijst worden opgenomen. Het Nationaal Beraad baseert zich hierbij op expertadviezen, openbare consultaties en adviezen van het Forum Standaardisatie.

1.2 Doelstelling expertadvies

Dit document is een expertadvies voor de functioneel toepassingsgebieden van de internet veiligheidstandaarden SPF, DKIM, DMARC, HTTPS en HSTS, TLS en DNSSEC gericht aan het Nationaal Beraad en Forum Standaardisatie. De omschrijvingen van de functioneel toepassingsgebieden van deze standaarden zijn verduidelijkt in opdracht van het Forum Standaardisatie.

Doel van dit document is om het Nationaal Beraad te adviseren over de functioneel toepassingsgebieden van de internet veiligheidstandaarden SPF, DKIM, DMARC, HTTPS en HSTS, TLS en DNSSEC. Met uitzondering van DMARC zijn deze standaarden al opgenomen op de lijst met open standaarden waarvoor een 'pas toe of leg uit'-verplichting geldt.

1.3 Doorlopen proces

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

1. In opdracht van het Forum Standaardisatie heeft Verdonck, Klooster & Associates een onderzoek uitgevoerd naar de omschrijvingen van de functioneel toepassingsgebieden van de verplichte (pas toe of leg uit) standaarden op de lijst met open standaarden. De resultaten van dit onderzoek zijn vastgelegd in een eindrapport, met daarin een analyse van de huidige omschrijvingen, voorstellen voor nieuwe omschrijvingen en instrumenten om omschrijvingen te verduidelijken en te uniformeren.
2. Op basis van het onderzoek heeft het Forum Standaardisatie op 14 juni 2017 besloten de voorgestelde omschrijvingen van de functioneel toepassingsgebieden van de internet veiligheidstandaarden SPF, DKIM, DMARC, HTTPS en HSTS, TLS en DNSSEC in procedure te nemen. Hierop volgend is een expertgroep samengesteld en een voorzitter aangesteld.
3. De leden van de expertgroep hebben voorafgaand aan de expertbijeenkomst het onderzoeksrapport ontvangen en zijn in de

gelegenheid gesteld om dit rapport door te nemen en aandachtspunten te identificeren.
4. De expertgroep is op 6 juli 2017 bijeengekomen om de voorgestelde omschrijvingen van de functioneel toepassingsgebieden te bespreken en verder te verduidelijken.

Dit expertadvies geeft de uitkomst van de expertgroep weer. De procesbegeleider heeft een concept van dit expertadvies aan de leden van de expertgroep gestuurd met verzoek om commentaar. Na verwerking van reacties uit de expertgroep is het rapport nogmaals toegestuurd aan de experts, afgerond en ingediend bij het Bureau Forum Standaardisatie (het secretariaat van het Forum Standaardisatie) ten behoeve van de publieke consultatieronde.

1.4 Vervolg

Het Bureau Forum Standaardisatie zal dit expertadvies openbaar maken ten behoeve van een publieke consultatie die plaatsvindt van 1 augustus 2017 tot en met 13 september 2017. Eenieder kan gedurende de consultatieperiode een reactie geven op dit expertadvies. Na afsluiting van de openbare consultatie koppelt het Bureau Forum Standaardisatie de reacties terug aan de expertgroep.

Het Forum Standaardisatie stelt met het expertadvies en de relevante inzichten uit de openbare consultatie een advies aan het Nationaal Beraad op. Het Nationaal Beraad besluit met dit advies om de omschrijvingen van de functioneel toepassingsgebieden wel of niet aan te passen op de lijst met open standaarden.

1.5 Samenstelling expertgroep

Het Forum Standaardisatie streeft in dit geval naar een representatieve expertgroep met een vertegenwoordiging van hoofdzakelijk (publieke) gebruikers. De expertgroep heeft een onafhankelijk voorzitter die de expertgroep leidt en de verantwoordelijkheid neemt voor het expertadvies.

Als onafhankelijk voorzitter is opgetreden Roy Tomeij. Rick van Rooijen heeft de procedure in opdracht van het Bureau Forum Standaardisatie begeleid.

Aan de expertbijeenkomst hebben deelgenomen:
- Gino Laan, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- Marco Davids, SIDN
- Paddy Verberne, Gemeente ‘s-Hertogenbosch
- Roland van Rijswijk-Deij, SURFnet
- Rolf Sonneveld, Sonnection
- Theo van Diepen, Logius
- Berry van Halderen, NLnet Labs
- Ralph Dolmans, NLnet Labs
- Marc van de Graaf, Ministerie van Algemene Zaken
- Juan Guillen Scholten, Logius
- John van Huijgevoort, Informatiebeveiligingsdienst voor gemeenten (IBD)
- Maarten Aertsen, Nationaal Cyber Security Centrum
- Albert Siersema, ODC-Noord
- Zarco Zwier, UWV
- Raph de Rooij, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

- Rene Bakker, Rijksdienst voor Ondernemend Nederland

Han Zuidweg en Bart Knubben van het Bureau Forum Standaardisatie en Gerben Klein Baltink van het Platform Internetstandaarden waren als toehoorder bij de expertbijeenkomst aanwezig.

1.6 Toelichting standaarden

SPF, DKIM, DMARC, HTTPS en HSTS, TLS en DNSSEC zijn standaarden voor de beveiliging van internetverbindingen, websites en e-mail. Het gebruik ervan levert een belangrijke bijdrage aan de betrouwbaarheid van het Nederlandse internet. De standaarden worden genoemd in de memorie van toelichting bij de Wet GDI en in het Nationaal Beraad van 2 februari 2016 zijn aanvullende resultaatafspraken gemaakt over de adoptie van de standaarden.

1.7 Leeswijzer

Hoofdstuk 2 beschrijft de functioneel toepassingsgebieden (situaties waarin de standaarden functioneel gebruikt moet worden).

2 Functioneel toepassingsgebieden

De *instructie rijksdienst inzake de aanschaf van ICT-producten en ICT-diensten* verplicht overheidsorganisaties om relevante standaarden op de 'pas toe of leg uit'-lijst te vragen en toe te passen bij aanbestedingstrajecten.

Afhankelijk van de aan te schaffen functionaliteit moet een overheidsorganisatie bepalen welke standaarden op de 'pas toe of leg uit'-lijst relevant zijn. Hiervoor is voor iedere standaard een *functioneel toepassingsgebied* (in welke situaties is de standaard functioneel van toepassing) en een *organisatorisch toepassingsgebied* (welke organisaties moeten de standaard gebruiken) beschreven.

De hiernavolgende paragrafen geven het advies van de expertgroep voor de functioneel toepassingsgebieden van SPF, DKIM, DMARC, HTTPS en HSTS, TLS en DNSSEC.

2.1 SPF

De expertgroep adviseert als functioneel toepassingsgebied voor SPF:

SPF moet worden toegepast op alle overheidsdomeinnamen, ook op domeinen waarvan niet wordt gemaild, én op alle mailservers waarmee de overheid e-mail ontvangt.

De expertgroep maakt de (algemene) kanttekening dat de lijst met open standaarden ook informatie moet bieden over de manier waarop SPF en de andere internet veiligheidstandaarden moeten worden toegepast (het 'hoe'). De lijst zou bijvoorbeeld duidelijk moeten maken dat de toepassing van SPF zonder beperking van de toegestane mailverzenders (zoals bij gebruik van het '+all'-mechanisme in het SPF record) weinig beveiligingswaarde heeft. Hiertoe zou ook verwezen kunnen worden naar richtlijnen van het NCSC. Deze informatie dient direct te relateren te zijn aan (delen van) het functioneel toepassingsgebied. Deze informatie hoort echter niet thuis in de omschrijving van het functioneel toepassingsgebied (het 'wanneer'). De lijst met open standaarden kent hiervoor andere velden, zoals 'Hulpmiddelen' en 'Community en Organisaties' (beide onder 'Implementatie'). Deze velden hebben bovendien als voordeel dat zij zonder voorafgaande procedure kunnen worden aangepast. Een mogelijkheid is om in toekomstige procedures met toekomstige expertgroepen expliciet bij deze velden stil te staan.

De expertgroep maakt de (algemene) kanttekening dat de lijst met open standaarden ook informatie moet bieden over het doel waarmee SPF en de andere internet veiligheidstandaarden moeten worden toegepast (het 'waarom'). Een voorbeeld van een dergelijk gebruiksdoel is het verifiëren van de identiteit van de verzender. Ook deze informatie hoort niet thuis in de omschrijving van het functioneel toepassingsgebied. De lijst met open standaarden kent hiervoor de velden 'Nut' en 'Werking' (beide onder 'Uitleg'). Ook hier geldt dat deze velden zonder voorafgaande procedure kunnen worden aangepast en dat in toekomstige procedures met toekomstige expertgroepen expliciet bij deze velden kan worden stilgestaan.

De expertgroep maakt de (algemene) kanttekening dat overheidsorganisaties onderling ook gegevens uitwisselen via besloten (overheids)netwerken. Door hun besloten karakter zijn deze netwerken veiliger dan het open internet. Als een organisatie er om deze reden voor kiest om SPF of een andere internet veiligheidstandaard met 'pas toe of leg uit'-verplichting niet toe te passen, dan dient zij dit gemotiveerd aan te geven in haar jaarverslag ('leg uit').

2.2 DKIM

De expertgroep adviseert als functioneel toepassingsgebied voor DKIM:

DKIM moet worden toegepast op alle overheidsdomeinnamen waarvandaan wordt gemaild én op alle mailservers waarmee de overheid e-mail verstuurt en ontvangt.

De expertgroep maakt geen (nieuwe) kanttekeningen bij het functioneel toepassingsgebied van DKIM.

2.3 DMARC

De expertgroep adviseert als functioneel toepassingsgebied voor DMARC:

DMARC moet worden toegepast op alle overheidsdomeinnamen, ook op domeinen waarvan niet wordt gemaild, én op alle mailservers waarmee de overheid e-mail ontvangt.

De expertgroep maakt de kanttekening dat DMARC nog niet is opgenomen op de lijst met open standaarden, omdat deze standaard formeel nog in beheer moet worden genomen door IETF. Ook is er discussie over de geschiktheid van DMARC voor brede toepassing. Met name domeinen waarop veel met e-mailverspreidingslijsten wordt gewerkt, kunnen problemen krijgen indien DMARC wordt toegepast. Het ARC-protocol (zie http://arc-spec.org) moet dit gaan oplossen. Aan de standaardisatie hiervan wordt nog hard gewerkt. Dit expertadvies betreft alleen de omschrijving van het functioneel toepassingsgebied van DMARC, niet de beantwoording van de vraag of deze standaard wel of niet moet worden opgenomen op de lijst met open standaarden.

2.4 HTTPS en HSTS

De expertgroep adviseert als functioneel toepassingsgebied voor HTTPS en HSTS:

HTTPS en HSTS moeten worden toegepast op de communicatie tussen clients (zoals webbrowsers) en servers voor alle websites en webservices.

De expertgroep maakt de kanttekening dat in deze omschrijving van het functioneel toepassingsgebied de begrippen 'clients' en 'servers' niet specifiek genoeg zijn. De expertgroep adviseert daarom om bij de omschrijving een duidelijke en (context)specifieke verklaring van deze begrippen op te nemen.

2.5 TLS

De expertgroep adviseert als functioneel toepassingsgebied voor TLS:

TLS moet worden toegepast op de uitwisseling van gegevens tussen clients en servers, inclusief machine-to-machine communicatie.

De expertgroep maakt de kanttekening dat met TLS op applicatieniveau kan worden vastgesteld of een verbinding met voldoende beveiliging is opgebouwd. Daarmee biedt TLS een signaleringsfunctie, die applicaties in staat stelt om gebruikers te waarschuwen voor onvoldoende beveiliging of om automatisch de verbinding te verbreken indien deze onvoldoende beveiligd is. Bij versleuteling op de IP laag (met bijvoorbeeld IPsec, een aanbevolen standaard) is deze signaalfunctie richting applicaties niet aanwezig. Er zijn dus alternatieven voor versleuteling met TLS, maar deze zijn niet altijd gelijkwaardig.

Voorts maakt de expertgroep de kanttekening dat er een standaard is voor DNS over TLS (die niet op de 'pas toe of leg uit' lijst staat). Deze standaard waarborgt de authenticiteit, integriteit en vertrouwelijkheid van DNS-verkeer. DNSSEC, een internet veiligheidstandaard met ‘pas toe of leg uit’-verplichting voor DNS-verkeer (zie onder), waarborgt alleen authenticiteit en integriteit. DNS over TLS is echter niet bedoeld om DNSSEC te vervangen. Dit probleem met de omschrijving van het functioneel toepassingsgebied zou ook kunnen gaan spelen bij andere, toekomstige protocolontwikkelingen. De ‘leg uit’-verplichting biedt hier uitkomst en kan aanleiding zijn om nieuwe standaarden aan te dragen voor opname op de lijst met open standaarden.

2.6 DNSSEC

De expertgroep adviseert als functioneel toepassingsgebied voor DNSSEC:

DNSSEC moet worden toegepast op alle overheidsdomeinnamen én op DNS-resolvers die clients van overheidsorganisaties direct of indirect van DNS-antwoorden voorzien.

De expertgroep maakt de kanttekening dat met deze omschrijving van het functioneel toepassingsgebied ook resolvers van derde partijen waarvan de overheid gebruik maakt DNSSEC moeten gebruiken.

De expertgroep maakt de kanttekening dat de lijst met open standaarden duidelijk moet maken dat validatie plaats moet vinden op een vertrouwd netwerk. Bij gebruik van DNSSEC op publieke resolvers, zoals die van internet serviceproviders, gaan gevalideerde antwoorden alsnog onbeveiligd over het internet voordat deze door clients worden gebruikt. Deze informatie over de toepassing van de standaard hoort niet thuis in de omschrijving van het functioneel toepassingsgebied. De lijst met open standaarden kent hiervoor andere velden.