Notitie

Aan: Forum Standaardisatie

Van: Bureau Forum Standaardisatie

Datum: 11 september 2018

Versie: 1.0

Betreft: Reacties uit de openbare consultatie STARTTLS en DANE (uitbreiding functioneel toepassingsgebied)

Inleiding

Dit document bevat de reacties die tussen 6 augustus en 10 september werden ontvangen op de openbare consultatie voor de uitbreiding van het functioneel toepassingsgebied van STARTTLS en DANE op de 'pas toe of leg uit' lijst van het Forum Standaardisatie. In totaal is een zevental reacties ontvangen van de heer Christian van Bruggen, RINIS, Rechtspraak.nl, de Nederlandse Zorgautoriteit, de Sociale Verzekeringsbank (SVB), het Uitvoeringsinstituut Werkgeversverzekeringen (UWV) en de Kamer van Koophandel (KvK).

De reacties, die als e-mail binnenkwamen, zijn in zijn originele vorm zonder bewerking weergegeven in chronologische volgorde van binnenkomst. Wel zijn de contactgegevens en is voor deze consultatie niet-relevante tekst verwijderd.

Reacties uit de openbare consultatie

Reactie van de heer Christian van Bruggen

Van: Christian van Bruggen <…>
Verzonden: woensdag 15 augustus 2018 22:51
Aan: Forum standaardisatie <forumstandaardisatie@logius.nl>
Onderwerp: Opmerking publieke consultatie STARTTLS en DANE

Beste Forum Standaardisatie,

Een opmerking over de configuratie bij de standaard STARTTLS en DANE.

De standaard/oproepen gaan niet in op de vraag of het gaat om een fail-open of fail- closed configuratie. Als voorbeeld is er een mailserver waarmee verbonden wordt. Deze bied STARTTLS met een self-signed certificaat aan. Er is via DNS geen DANE record aanwezig en er zijn ook geen DNSSEC signatures meegestuurd. In het geval van fail-open zal de mail alsnog verstuurd worden, in het geval van een fail-closed niet. De standaard maakt niet duidelijk hoe te handelen.

Gezien (de STARTTLS i.c.m.) DANE zou moeten beschermen tegen een actieve aanvallen, zoals bijvoorbeeld een Man-in-the-Middle aanval, lijkt mij dat een fail-open configuratie niet voldoende zal zijn. Immers is een MitM in staat om een self-signed certificate te genereren en de DNS antwoorden aan te passen (en zo de DNSSEC signature eruit te halen). Dit leidt tot de eerder genoemde situatie (STARTTLS + self- signed certificate). Voor het daadwerkelijk nut hebben van deze maatregelen lijkt het mij dus dat de voorgestelde standaard ook een fail-closed configuratie verplicht moet stellen en verbindingen moet stoppen indien er geen DANE record aanwezig is. Een fail-closed configuratie op DANE impliceert daarmee een fail-closed configuratie op DNSSEC, immers is DNSSEC een vereiste voor DANE.

Mogelijk dat ik iets over het hoofd zie, maar het lijkt mij sowieso goed om in de standaard op te nemen: 1) of een fail-closed configuratie verplicht is en 2) welke toegevoegde waarde een fail-open configuratie nog bied (tegen de dreiging van een MitM aanval).

Het verplichten van (alleen) STARTTLS als bescherming tegen passieve aanvallen kan ik mij overigens goed in vinden.

--

Met vriendelijke groet,

Christian van Bruggen

Reactie van RINIS

Van: Rob Verweij <…>
Verzonden: maandag 20 augustus 2018 09:16
Aan: Zuidweg, J. (Han) - Forum Standaardisatie <han.zuidweg@forumstandaardisatie.nl>
Onderwerp: Re: Openbare consultatie

Dag Han,

…[niet voor deze openbare consultatie relevante tekst verwijderd]

Van onze (architect) kant de volgende reactie op de gedane adviezen:

…[niet voor deze openbare consultatie relevante tekst verwijderd]

STARTTLS en DANE: mee eens

Met vriendelijke groet,

Rob Verweij
directeur
RINIS

Reactie van Rechtspraak.nl

Van: Kremer, H.H.C. (IVO Rechtspraak) <…>
Verzonden: woensdag 5 september 2018 16:56
Aan: Forum standaardisatie <forumstandaardisatie@logius.nl>
CC: Smit, F.P.M. (IVO Rechtspraak) <…>; Vermeulen, D.M. (IVO Rechtspraak) <…>
Onderwerp: Consultatieprocedure STARTTLS en DANE

L.s.,

Hierbij de bijdrage van de Rechtspraak op de Consultatieprocedure STARTTLS en DANE

Vraag 1 Doelstelling expertadvies: nee

Vraag 2 Toepassingsgebied: ja

Vraag 3 Werkingsgebied: ja

Vraag 4 Toegevoegde waarde: ja

Vraag 5 Standaardisatieproces: ja

Vraag 6 draagvlak: deels

De 3e alinea binnen 3.3.1.1 stelt dat alle overheidspartijen gebruik kunnen maken van STARTTLS + DANE. De onderbouwing is gebaseerd op de constatering er dienstenleveranciers zijn die gateways of maildiensten bieden.

Het draagvlak lijkt niet onderzocht bij organisaties die geen (of andere) dan de genoemde mailproviders gebruiken en/of andere dan genoemde software gebruiken (waaronder Microsoft Exchange). Of dit een negatieve impact heeft om de impact is niet onderzocht.

De implicaties voor deze organisaties zijn niet duidelijk beschreven.

Vraag 7 bevordering door opname: ja

Vraag 8 Expert advies: ja

Vraag 9 Adoptie aanbevelingen: ja

Vraag 10 Inhoudelijke opmerkingen: geen

Met vriendelijke groet,

H. (Harro) Kremer
(Enterprise) Security Architect
AK&S en CIO-Office
www.rechtspraak.nl

Reactie van de Nederlandse Zorgautoriteit

Van: Pieris-van Gestel, Esther <…>
Verzonden: donderdag 6 september 2018 09:39
Aan: Forum standaardisatie <forumstandaardisatie@logius.nl>
Onderwerp: FW: Openbare consultatie TLS/DANE ihkv SMTP

Goedemorgen collega's,

Hierbij onze terugkoppeling op de openbare consultatie https://www.forumstandaardisatie.nl/thema/openbare-consultatie.

… *[Voor deze consultatie niet-relevante tekst verwijderd]*

Op verzoek van Lars hierbij mijn reactie m.b.t. DANE:

DANE (DNS-based Authentication of Named Entities) leunt zwaar op DNSSEC en staat self-signed certificaten toe. Dat is waar het op dit moment misgaat. Self-signed certificaten zijn in dit kader pas betrouwbaar als de DNS-records vertrouwd kunnen worden. Voor betrouwbare (authentieke) DNS-antwoorden is DNSSEC in het leven geroepen, maar DNSSEC is niet overal geïmplementeerd en er zijn grote partijen die het pertinent weigeren toe te passen (waaronder o.a. Amazon Route 53).

De marktleiders in mailafhandeling (w.o. Google en Microsoft) zijn daarom bezig met het ontwikkelen van een nieuwe standaard die uiteindelijk hetzelfde beoogt te bereiken als DANE for SMTP, maar waarbij DNSSEC geen voorwaarde is: Het opzetten van een vertrouwd communicatiekanaal tussen zender en ontvanger. Deze standaard heet MTA-STS (SMTP MTA Strict Transport Security).

MTA-STS en DANE for SMTP hoeven elkaar niet te bijten, ze kunnen ook parallel worden toegepast. Maar om het eenvoudig te houden wil ik voorstellen DANE geheel te laten vallen en voor betrouwbare mailverbindingen aansluiting te zoeken bij de grote partijen, dus bij de voorgestelde MTA-STS standaard. MTA-STS is nu nog een "proposed" standard, dus het is nog niet rijp om als 'aanbevolen' op te nemen in de pas-toe-of-leg-uit lijst.

Ter referentie: https://datatracker.ietf.org/doc/draft-ietf-uta-mta-sts

Groet,

Heber

Met vriendelijke groet,

Esther Pieris

Esther Pieris-van Gestel
webredacteur | Communicatie
Nederlandse Zorgautoriteit

Reactie van de Sociale Verzekeringsbank

Van: Visser, T.
Verzonden: maandag 10 september 2018 14:11
Aan: Zuidweg, J. (Han) - Forum Standaardisatie <han.zuidweg@forumstandaardisatie.nl>
CC: Oberendorff, L. (Ludwig) - Forum Standaardisatie <ludwig.oberendorff@forumstandaardisatie.nl>
Onderwerp: FW: Openbare consultatie verplichte en aanbevolen standaarden

Beste Han,

Ik begrijp dat UWV zelf een reactie zal sturen. Hierbij de ruwe reactie van SVB.

Met vriendelijke groet,

Teun Visser
.....
Ministerie van Sociale Zaken en Werkgelegenheid
Directoraat-generaal Sociale Zekerheid en Integratie
Directie Stelsel en Volksverzekeringen
Afdeling Handhaving en Gegevensuitwisseling

Van: Verheij, Fransje (Sociale Verzekeringsbank) <…>
Verzonden: dinsdag 28 augustus 2018 18:24
Aan: Visser, T. <..>
CC: …
Onderwerp: RE: Openbare consultatie verplichte en aanbevolen standaarden

Hallo Teun en Ron,

Ik heb de vraag over de consultatie uitgezet bij Geer Haas. Hieronder zijn antwoord:

Hi Fransje,

Mijn samenvatting:

…[*Niet voor deze consultatie relevante tekst verwijderd]*

TLS 1.3/STARTTLS en DANE zijn wij het mee eens (conditioneel zie feedback) – zal wij nodige coördinatie inspanning (richting leveranciers) vergen. (geraadpleegd bij SVB IT / MS ISO Reino den Hartog)

…*[Niet voor deze consultatie relevante tekst verwijderd]*

En de geconsolideerde feedback (als gekregen van onze experts) op de consultatie:

…*[Niet voor deze consultatie relevante tekst verwijderd]*

Re: STARTTLS en DANE

Vraag 1: Nee

Vraag 2: Ja, eens

Vraag 3: Ja, eens. Onder voorbehoud van de informatie in het Forum advies (STARTTLS en DANE). De link in het consultatiedocument werkt niet (“Pagina niet gevonden”).

Vraag 4: Ja, eens. Onder voorbehoud van de informatie in het Forum advies (STARTTLS en DANE). De link in het consultatiedocument werkt niet (“Pagina niet gevonden”).

Vraag 5: Ja, eens

Vraag 6: Ja, eens

Vraag 7: Ja, eens

Vraag 8: Ja, eens

Vraag 9: Nee

… *[Niet voor deze consultatie relevante tekst verwijderd]*

Reactie van het Uitvoeringsinstituut Werknemersverzekeringen

Van: Vierbergen, Kato (K.R.) <…>
Verzonden: dinsdag 11 september 2018 16:22
Aan: Forum standaardisatie <forumstandaardisatie@logius.nl>; Knubben, B.S.J. (Bart) - Forum Standaardisatie <…>
CC: Bos, Ron (R.) <…>; Franken, Leo (L.) <…>
Onderwerp: reactie UWV openbare consultatie Open Standaarden

L.S.,

In reactie op de openbare consultatie Open Standaarden en plaatsing op de PTOLU-lijst stuur ik jullie hierbij de input vanuit UWV.

Het betreft de consultatie: https://www.forumstandaardisatie.nl/thema/openbare-consultatie

… *[Niet voor deze consultatie relevante tekst verwijderd]*

Het advies om het functioneel toepassingsgebied van de standaarden STARTTLS en DANE (e-mail beveiliging) uit te breiden met uitgaande e-mail: Ja.

… *[Niet voor deze consultatie relevante tekst verwijderd]*

Als er vragen zijn, hoor ik dat graag.

Met vriendelijke groet,

Kàto Vierbergen-Schuit
Beleidadviseur Security en Privacy / Information Security Officer
UWV ICT

Reactie van de Kamer van Koophandel

[Deze reactie van de Kamer van Koophandel ontvingen wij per e-mail als bijlage in .doc formaat. Hieronder is het commentaar in de bijlage weergegeven in de oorspronkelijke tekst en gerangschikt per vraag.]

Kamer van Koophandel Advies
Datum: 10 september 2018
Auteur: Frits Maas ICT Architect Kamer van Koophandel
Onderwerp: Reacties van de Kamer van Koophandel op diverse consultaties

Uitbreiding van het functioneel toepassingsgebied van STARTTLS en DANE
Consultatiedocument STARTTLS en DANE Datum 6 augustus 2018

1. KvK: Nee

2. KvK: Als Google & Microsoft deze standaarden niet ondersteunen dan zal er voor vele overheidsdiensten een probleem zijn.

3. *[geen antwoord]*

4. KvK: Ja

5. *[geen antwoord]*

6. KvK: Nogmaals als de grote partijen als Microsoft en Gmail deze standaard niet ondersteunen zien we het draagvlak niet. Aanvullend als Microsoft de standaard niet ondersteund wordt de migratie naar een nieuwe mail platform voor de overheden een hele hoge kostenpost. Dit is anders dan wat in het expert advies verwoord is.

7. *[geen antwoord]*

8. KvK: Antwoord moet voorlopig nog NEE zijn, omdat Microsoft en Google het niet gaan ondersteunen. De migratiekosten zullen veel te hoog worden voor de overheid. Er wordt in het expert advies ook aangegeven dat bij geen enkele overheidspartij de combinatie STARTTLS met DANE is toegepast. Als er geen implementatie is bij een overheidspartij, dan kan het nog niet worden voorgedragen is mijn mening.

9. KvK: Op de PTOLU lijst voor STARTTLS/DANE moet expliciet worden aangegeven dat het toepassen van deze standaard automatisch ook betekend het toepassen van de standaarden TLS, DNSSEC, SPF, DKIM en DMARC. Geen uitzonderingen!