notitie

FORUM STANDAARDISATIE 10 oktober 2018

Agendapunt 3C – Uitbreiding functioneel toepassingsgebied STARTTLS/DANE

Nummer:	FS 181010.3C
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	26 september 2018
Versie:	1.0
Bijlagen:	Expertadvies uitbreiding functioneel toepassingsgebied STARTTLS en DANE Reacties op de openbare consultatie uitbreiding functioneel toepassingsgebied STARTTLS en DANE

1. Aanleiding en achtergrond

De standaarden STARTTLS en DANE worden in combinatie gebruikt om het afluisteren en manipuleren van mailverkeer tegen te gaan. STARTTLS zorgt ervoor dat e-mailservers hun onderlinge verbindingen met TLS beveiligen. Met de complementaire standaard DANE kunnen e-mailservers het gebruik van TLS bovendien afdwingen zodat onveilige verbindingen worden geweigerd. DANE bouwt voort op de standaard DNSSEC[1] die ook op de pas-toe-of-leg-uit lijst staat.

STARTTLS en DANE zijn in 2015 getoetst en werden in 2016 op de pas-toe-of-leg-uit lijst geplaatst met verplichting voor inkomende e-mail. Verplichting voor uitgaande e-mail werd in 2016 prematuur geacht vanwege de nog weinig ontwikkelde marktondersteuning. In het Forumadvies[2] werd destijds het volgende adoptieadvies opgenomen (punt 7 op pagina 4): *"Om een jaar na opname van de standaarden te toetsen (in samenspraak met de expertgroep) hoe het verloopt met de implementatie en of de standaard ook verplicht moet worden voor de uitgaande mailstromen."*

Het toepassen van STARTTLS en DANE voor *inkomend* e-mailverkeer zorgt dat het altijd mogelijk is om veilig e-mailberichten te sturen *aan* de organisaties in het organisatorisch werkingsgebied. Uitbreiding van het functioneel toepassingsgebied naar *uitgaande* e-mail zorgt ervoor dat e-mail *van, naar en tussen* overheden altijd over versleutelde verbindingen wordt verzonden.

Toepassing van STARTTLS en DANE op inkomende en uitgaande e-mail levert een belangrijke bijdrage aan veilig e-mail verkeer. De overheid kan zo altijd op een veilige manier e-mail uitwisselen op partijen die STARTTLS en DANE ondersteunen, op het moment van schrijven zo'n 150.000 mailservers met een .nl-domein en zo'n 314.000 mailservers wereldwijd.

[1] https://www.forumstandaardisatie.nl/standaard/dnssec

[2] https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS%20160608.3E%20Forumadvies%20opname%20STARTTLS%20icm%20DANE.pdf

2. Consequentie en vervolgstappen

STARTTLS en DANE staan nu op de pas-toe-of-leg-uit lijst met een verplichting voor inkomende e-mail. Dit houdt in dat (semi)overheidsorganisaties e-mail servers moeten hebben die STARTTLS ondersteunen, en een geldig DANE record moeten hebben in het DNS.

Als STARTTLS en DANE worden verplicht voor uitgaande e-mail, dan moeten mailservers van (semi)overheidsorganisaties ook gaan controleren of de mailserver van de ontvangende partij een DANE record heeft en TLS afdwingt. Hierbij blijft het nog wel open welke policy een overheidsorganisatie wil volgen als de wederpartij geen DANE ondersteunt of als bij de DANE check een fout wordt ontdekt.

Er zijn geen specifieke risico's geïdentificeerd bij de uitbreiding van het functioneel toepassingsgebied van STARTTLS en DANE. Het gebruik van *self-signed certificates* vormt nadrukkelijk geen beveiligingsrisico omdat DANE in combinatie met de onderliggende standaard DNSSEC[3] kan zorgen voor een 'chain of trust' en daarmee veilige identificatie van een serverdomein. Wel kan een te strikte toepassing van DANE (d.w.z. 'DANE-only' oftewel 'mandatory DANE') tot gevolg hebben dat een overheidsorganisatie geen e-mail meer uitwisselt met organisaties die DANE niet of incorrect ondersteunen. Een dergelijke policy maakt echter nadrukkelijk geen deel uit van de pas-toe-of-leg-uit verplichting.

De vervolgstappen zijn als volgt: het Forum Standaardisatie adviseert op basis van dit Forumadvies aan het Overheidsbreed Beleidsoverleg Digitale Overheid. Het Overheidsbreed Beleidsoverleg Digitale Overheid bepaalt op basis van het advies of het functioneel toepassingsgebied van STARTTLS en DANE wordt uitgebreid.

3. Betrokkenen en proces

Het Forum Standaardisatie heeft op 13 juni 2018 besloten om de uitbreiding van het functioneel toepassingsgebied van STARTTLS en DANE voor uitgaande mailstromen in procedure te nemen.

In juni en juli 2018 heeft een expertonderzoek plaatsgevonden waaraan experts van Logius, NCSC, Dmarcian (private sector), NLnet Labs, VNG Realisatie, NLnet en PowerDNS (private sector) deelnamen. Het expertadvies [1] is van 6 augustus tot en met 10 september 2018 ter openbare consultatie aangeboden. In de openbare consultatie zijn in totaal zeven 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) [2].

Dit Forumadvies is gebaseerd op het expertadvies en een analyse van de reacties uit de openbare consultaties, die in paragraaf 5 verder worden toegelicht.

4. Gevraagd besluit

Het Forum Standaardisatie adviseert het Overheidsbreed Beleidsoverleg Digitale Overheid om:

1. *Het functioneel toepassingsgebied van STARTTLS en DANE uit te breiden met uitgaande email.*
2. *In te stemmen met de additionele adviezen ten aanzien van de toepassing van STARTTLS en DANE, zoals geformuleerd in paragraaf 5.5.*

5. Toelichting

5.1 Over de standaard

De overheid heeft de verantwoordelijkheid om (toevertrouwde) vertrouwelijke informatie te beschermen tegen afluisteren en manipuleren door aanvallers, zoals criminele partijen en statelijke actoren. De overheid moet daarom de informatiestromen tussen de overheid en bedrijven, tussen de overheid en burgers en tussen overheden onderling beveiligen.

[3] DANE moet in combinatie van DNSSEC gebruikt worden. DNSSEC is een standaard die het vervalsen van Internet adressen voorkomt van servers die bij een domein horen. Door gebruik van DNSSEC kan internetverkeer niet worden omgeleid naar een malafide server. DNSSEC staat op de pas-toe-of-leg-uit lijst van het Forum Standaardisatie, zie https://www.forumstandaardisatie.nl/standaard/dnssec

De overheid maakt zowel intern als extern veel gebruik van e-mail. E-mail is een oudere, zeer open technologie die kwetsbaar is voor aanvallen met het doel om berichten te vervalsen, af te luisteren of te manipuleren.

De toepassing van STARTTLS in combinatie met DANE maakt het mogelijk om de verzending van e-mail over het Internet te beveiligen tegen afluistering en manipulatie. STARTTLS zorgt ervoor dat e-mailservers hun onderlinge verbindingen met TLS[4] beveiligen. Met de complementaire standaard DANE kunnen e-mailservers het gebruik van TLS bovendien afdwingen zodat onveilige verbindingen worden geweigerd.

STARTTLS en DANE staan sinds 2016 op de pas-toe-of-leg-uit lijst met een verplichting voor inkomende e-mail servers. Dit betekent dat de mailservers van overheidsorganisaties STARTTLS moeten ondersteunen, en een DANE-record moeten hebben in het (met DNSSEC beveiligde) DNS. Bij verplichting voor uitgaande e-mail moeten mailservers ook checken of de mailserver van de ontvangende partij een valide DANE-record heeft.

5.2 Hoe is het proces verlopen?

Op 13 juni 2018 besloot het Forum Standaardisatie een procedure te starten voor uitbreiding van het functioneel toepassingsgebied van STARTTLS en DANE.

In juli 2018 heeft de procesbegeleider (Lost Lemon) een expertonderzoek geleid waarbij experts van Logius, NCSC, Dmarcian (private sector), NLnet Labs, VNG Realisatie, Nlnet en PowerDNS (private sector) werden geraadpleegd. Ook werd op 19 juli 2018 een beperkte expertbijeenkomst gehouden. De bevindingen van het expertonderzoek werden vastgelegd in het expertadvies [1].

In de periode van 6 augustus 2018 tot en met 10 september 2018 heeft het Bureau Forum Standaardisatie het expertadvies voor publieke consultatie aangeboden ter consultatie. In de openbare consultatie zijn 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) [2]. De binnengekomen reacties worden geanalyseerd in paragraaf 5.4 van dit document.

5.3 Hoe scoort de standaard op de toetsingscriteria?

Open standaardisatieproces

STARTTLS en DANE worden beheerd door de IETF (ietf.org), die een zeer open standaardisatieproces heeft. IETF hanteert de Simplified BSD License zodat de standaard door eenieder vrij te gebruiken is. Alle intellectuele eigendom achter STARTTLS en DANE is onherroepelijk vrijgegeven.

Toegevoegde waarde

De overheid moet de communicatie met burgers, bedrijven en overheden beschermen tegen afluisteren en manipulatie door aanvallers. Sinds september 2016 staat STARTTLS in combinatie met DANE op de pas-toe-of-leg-uit lijst met de verplichting voor *ontvangende* mailservers. Het is voor *verzendende* mailserver nog niet verplicht STARTTLS en DANE toe te passen waardoor er nog altijd drie typen verbindingen mogelijk zijn met e-mailservers die wel STARTTLS in combinatie met DANE ondersteunen:

1. Niet-versleutelde verbindingen: mailverkeer kan worden afgeluisterd.
2. Met een versleutelde verbinding, zonder certificaatverificatie conform DANE: het mailverkeer is normaal gesproken versleuteld maar kan door een actieve aanvaller worden onderschept en aangepast (‘*man in the middle’*).
3. Met een versleutelde verbinding, met certificaatverificatie conform DANE: veilig mailverkeer met de juiste server dat niet zomaar door een actieve aanvaller kan worden onderschept en aangepast.

Door STARTTLS en DANE toe te passen op uitgaande e-mail kunnen verbindingen van type 1 en 2 vermeden worden. De uitbreiding van het functioneel toepassingsgebied van STARTTLS en DANE met uitgaande e-mail verplicht overheden dus om altijd beveiligde communicatie op te zetten als de ontvangende partij deze standaarden ondersteunt.

Technisch zijn de standaarden relatief eenvoudig en tegen geringe kosten te implementeren. Er zijn geen beveiligings- en privacyrisico’s geïdentificeerd aan het implementeren en gebruiken van de standaarden. Het

[4] https://www.forumstandaardisatie.nl/standaard/tls

toegestaan gebruik van *self-signed*[5] certificaten wordt regelmatig genoemd als een kwetsbaarheid van DANE. Dit is onterecht omdat DANE alleen kan worden gebruikt in combinatie met DNSSEC[6], hetgeen zorgt voor een 'chain of trust' en vertrouwen in de identiteit van de server.

Er is geen risico dat het gebruik van DANE mailstromen verstoort. De verzendende e-mail server moet STARTTLS en DANE wel toepassen als de ontvangende kant de standaarden ondersteunt. Als de ontvanger geen DANE ondersteunt, dan mag in overeenstemming met de DANE specificatie[7] teruggevallen worden op een STARTTLS versleuteling zonder DANE of een verbinding zonder versleuteling. Er hoeven dus geen mailstromen 'stuk te gaan' door het gebruik van STARTTLS en DANE.

Draagvlak

STARTTLS wordt veel op zichzelf gebruikt, maar nog minder in combinatie met DANE. Sinds 2016 is de marktondersteuning van DANE op e-mailservers wel significant verbeterd. Belangrijke leveranciers en open source implementaties zoals Postfix[8], Halon[9], Cloudmark[10], Exim[11] en Mail-in-a-box[12] ondersteunen DANE al voor uitgaande e-mail. Cisco is bezig met implementatie in hun mailproduct, dat zeer veel binnen de Nederlandse overheid wordt gebruikt. Ook heeft Port 25 ondersteuning voor DANE aangekondigd in PowerMTA. Een actieve community zet druk op ondersteuning van DANE in Microsoft Office en de producten van leveranciers als Protonmail. Een aantal van de genoemde producten is inzetbaar als *mailproxy* waardoor DANE ook ondersteund kan worden in combinatie met veelgebruikte serversoftware zoals Microsoft Exchange die het zelf nog niet ondersteund.

Er zijn positieve signalen over de ontwikkeling van de marktondersteuning. Met name de ondersteuning van STARTTLS en DANE door TransIP en XS4ALL[13], beide grote hosting providers in Nederland, zegt iets over de adoptie van deze standaarden. De overheid heeft hierin ook een voorbeeldrol.

Microsoft en Google hebben aangegeven DANE vooralsnog niet te zullen ondersteunen, maar te kiezen voor een alternatieve technologie, MTA-STS[14]. Deze is echter nog in ontwikkeling en heeft in IETF nog geen status als standaard. MTA-STS geeft minder zekerheid over de geauthenticeerde transportversleuteling dan DANE, en lijkt vooral geschikt voor grotere mailproviders. Dit laatste nadeel geldt ook voor veel overheidsorganisaties (bijvoorbeeld gemeenten) die geen grootschalige e-mailinfrastructuur implementeren. Beide standaarden sluiten elkaar overigens niet uit; ze kunnen naast elkaar ingezet worden.

Een aantal experts vindt dat het Forum Standaardisatie binnen de tijdsbestek van een jaar moet bepalen welk advies of verplichting zij met betrekking tot MTA-STS wil geven of opleggen. Ook vindt een aantal experts dat de ondersteuning door de grote leveranciers (Microsoft , Google, enz.) meer aandacht verdient en dat deze partijen vanuit een sterke community bewogen moeten worden om ondersteuning te bieden.

Opname bevordert de adoptie

De experts vinden uitbreiding van het functioneel toepassingsgebied het passende middel is om de inzet van STARTTSL en DANE voor inkomende *en* uitgaande e-mail bij de (semi)overheid te bevorderen.

Ook kan de verplichting van STARTTLS voor een stimulerende werking hebben op de marktondersteuning voor DANE.

De pas-toe-of-leg-uit verplichting van STARTTLS en DANE voor inkomende *en* uitgaande e-mail versterkt ook het effect van DNSSEC op de pas-toe-of-leg-uit lijst.

---

[5] *Self-signed certificates* zijn certificaten die een partij zelf uitgeeft en waarvan de betrouwbaarheid niet kan worden gecontroleerd bij een erkende certificaatautoriteit.
[6] https://www.forumstandaardisatie.nl/standaard/dnssec
[7] https://tools.ietf.org/html/rfc7672
[8] http://www.postfix.org/TLS_README.html#client_tls_dane
[9] https://halon.io/dane
[10] https://blog.cloudmark.com/2017/03/27/dane-and-email-security/
[11] https://www.exim.org/
[12] https://github.com/mail-in-a-box/mailinabox
[13] https://mail.sys4.de/pipermail/dane-users/2018-September/000472.html
[14] https://datatracker.ietf.org/doc/draft-ietf-uta-mta-sts/

5.4 Wat is de conclusie van de expertgroep en de consultatie?

Conclusie uit het expertonderzoek

De experts concluderen dat het toepassen van de combinatie van STARTTLS en DANE voor inkomend *en* uitgaand e-mailverkeer bijdraagt tot het veilig uitwisselen van e-mail met organisaties in het organisatorisch werkingsgebied.

Uitbreiding van het functioneel toepassingsgebied naar uitgaande e-mail zorgt ervoor dat e-mail van, naar en tussen overheden altijd over versleutelde verbindingen wordt verzonden als beide partijen de standaarden ondersteunen. De expertgroep vindt dat de uitbreiding van het functioneel toepassingsgebied daarom toegevoegde waarde heeft.

Aangezien STARTTLS en DANE IETF-standaarden zijn concludeert de expertgroep dat deze een open standaardisatieproces kennen. Bovendien is het standaardisatieproces van IETF is reeds positief getoetst bij opname van STARTTLS en DANE op de 'pas toe of leg uit'-lijst in 2016.

De experts concluderen dat het marktaanbod zich voldoende heeft ontwikkeld om STARTTLS en DANE werkbaar te kunnen verplichten voor uitgaande e-mail. De vooruitzichten voor de marktontwikkeling zijn ook positief. Wat wel zorgen baart is het initiatief van grote e-mail providers (Google, Microsoft) om een alternatieve standaard te ontwikkelen, MTA-STS. Deze ontwikkeling zou nauw gevolgd moeten worden.

De expertgroep concludeert dat uitbreiding van het functioneel toepassingsgebied van STARTTLS en DANE naar uitgaande e-mail het passende middel is om de adoptie van de standaard binnen de (semi)overheid te bevorderen. Ook kan deze uitbreiding van het functioneel toepassingsgebied een stimulerende werking hebben op de ondersteuning door leveranciers van DANE, voor zowel inkomend als uitgaand e-mailverkeer.

Reacties uit de openbare consultatie

In de openbare consultatie reageerde een aantal organisaties met een steunbetuiging om het functioneel toepassingsgebied van STARTTLS en DANE met uitgaande e-mail uit te breiden.

Ook werd een aantal kritische reacties ontvangen (zie [2]):

1. Het toegestane gebruik van *self-signed certificates* is onveilig.
2. Veel (overheids)organisaties gebruiken Microsoft Exchange dat geen DANE ondersteunt.
3. DANE is afhankelijk van DNSSEC, en DNSSEC heeft wereldwijd te weinig draagvlak. Amazon gebruikt bijvoorbeeld geen DNSSEC.
4. Er is bij IETF een alternatieve standaard voor DANE in ontwikkeling, MTA-STS, die ondersteund wordt door grote marktpartijen zoals Google en Microsoft.

Analyse van deze reacties leidt tot de volgende conclusies:

1. Het idee dat het gebruik van *self-signed certificates* STARTTLS en DANE onveilig zou maken is een populaire misvatting. DANE laat inderdaad het gebruik van *self-signed certificates* toe. Een vingerafdruk (*digest*) hiervan wordt opgeslagen in het DANE record. Het DANE record is beveiligd door DNSSEC, dat van *public key infrastructure* (PKI) gebruik maakt. Hierdoor is de identiteit van de server altijd veilig te bepalen. Een aanvaller die een zogenaamde *man-in-the-middle* attack uitvoert kan zich met een *self-signed certificate* niet uitgeven voor de legitieme houder van het DANE record omdat dit een DANE en/of DNSSEC fout oplevert.
2. Om dit probleem te ondervangen kunnen mail proxies van bijv. Cisco worden ingezet. Deze oplossing is ook werkbaar voor organisaties met een kleiner budget.
   Op het moment van schrijven er lopen verzoeken bij Microsoft van Nederlandse overheidsorganisaties voor ondersteuning van STARTTLS en DANE. Het OBDO wordt geadviseerd om druk uit te oefenen op leveranciers (waaronder Microsoft) voor ondersteuning van DANE.
3. DNSSEC is een belangrijke standaard voor de beveiliging van informatie-uitwisseling over het Internet en de bestrijding van cybercriminaliteit en –spionage. Bij de Nederlandse overheid staat de adoptie van DNSSEC op 80%[15]. Ongeveer 150.000 .nl domeinen zijn beveiligd met DNSSEC; wereldwijd zijn dat er meer

[15] https://www.forumstandaardisatie.nl/thema/iv-meting-en-afspraken

dan 300.000. Ondanks weerstand vanuit sommige kringen (bijvoorbeeld Amazon) kan DNSSEC niet worden weggezet als een standaard met onvoldoende draagvlak. De verplichting van STARTTLS en DANE kan de adoptie van DNSSEC bovendien verder aanjagen.

4. MTA-STS is in ontwikkeling en is nog niet gepubliceerd als standaard. Daarentegen zijn STARTTLS en DANE gevestigde standaarden. MTA-STS geeft minder zekerheid over de geauthenticeerde transportversleuteling dan DANE, en lijkt vooral geschikt voor grotere mailproviders. Dit laatste nadeel geldt ook voor veel overheidsorganisaties (bijvoorbeeld gemeenten) die geen grootschalige e-mailinfrastructuur implementeren. Hoewel één enkele standaard te verkiezen valt boven meerdere, kan MTA-STS naast STARTTLS en DANE worden toegepast. Wel wordt geadviseerd om de stand van zaken rond MTA-STS over een jaar te evalueren.

Op basis van deze analyse wordt geen reden gezien om het expertadvies te herzien of om aanvullende adviezen te geven.

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

Naar aanleiding van het expertonderzoek wordt geadviseerd om de volgende oproepen ten aanzien van de adoptie van STARTTLS en DANE voor inkomende en uitgaande e-mail te doen:

1. Het OBDO wordt opgeroepen de ondersteuning van STARTTLS in combinatie met DANE door leveranciers nader te laten onderzoeken en als vertegenwoordiger van de Nederlandse overheid de leveranciers om betere ondersteuning te vragen.
2. Het Forum Standaardisatie wordt opgeroepen om over een jaar de stand van zaken rond de alternatieve technologie MTA-STS te evalueren.
3. Het Forum Standaardisatie wordt opgeroepen om de infographic over e-mailbeveiligingsstandaarden uit te breiden om zodoende de relatie van STARTTLS en DANE met onder andere S/MIME, PGP, IMAP(S), POP3(S), x509, DMARC, SPF en DKIM beter weer te geven.
4. Organisaties die STARTTLS en DANE toepassen worden opgeroepen de standaarden te implementeren volgens de adviezen van het NCSC[16].
5. SIDN wordt opgeroepen om DANE voor mail onderdeel te maken van de incentiveregeling op basis van de Registrar Scorecard.
6. VNG-Realisatie wordt opgeroepen om de GEMMA Softwarecatalogus aan te passen als het OBDO instemt met uitbreiding van het functioneel uitbreidingsgebied van STARTLS en DANE met uitgaande e-mail-servers. Daarmee krijgen gemeenten beter inzicht in de toepassing van deze standaarden.

De opgeroepen partijen worden gevraagd om één jaar na opname van de standaard over de voortgang op deze punten te rapporteren aan het Forum Standaardisatie.

6. Referenties

[1] Expertadvies voor uitbreiding van het functioneel toepassingsgebied van STARTTLS en DANE: https://www.forumstandaardisatie.nl/sites/bfs/files/20180803%20Expertadvies%20STARTTLS%20en%20DANE%20uitbreiding%20functioneel%20toepassingsgebied.pdf

[2] Reacties uit de Openbare Consultatie voor uitbreiding van het functioneel toepassingsgebied van STARTTLS en DANE: https://www.forumstandaardisatie.nl/sites/bfs/files/Commentaar%20uit%20de%20openbare%20consultatie%20uitbreiding%20functioneel%20toepassingsgebied%20STARTTLS%20en%20DANE.pdf

[16] https://www.ncsc.nl/actueel/factsheets/factsheet-beveilig-verbindingen-van-mailservers.html