



notitie

FORUM STANDAARDISATIE

Forum Standaardisatie

www.forumstandaardisatie.nl
forumstandaardisatie@logius.nl

Bureau Forum**Standaardisatie**

gehuisvest bij Logius

Postadres

Postbus 96810

2509 JE Den Haag

Bezoekadres

Wilhelmina van Pruisenweg 52

2595 AN Den Haag

Bij bezoek aan Logius is

legitimatie verplicht

Agendapunt:	3E		
Betreft:	Opname STARTTLS en DANE op de lijst met open standaarden		
Aan:	Forum Standaardisatie		
Van:	Stuurgroep Standaardisatie		
Datum:	27 mei 2016	Versie	1.0

Aanleiding en achtergrond

STARTTLS en DANE zijn (e-mail)beveiligingsstandaarden die kunnen worden gebruikt om een beveiligde verbinding tussen mailservers op te zetten. STARTTLS zorgt er voor dat een niet-versleutelde, en daarmee onbeveiligde, SMTP-verbinding geüpgrade wordt naar een versleutelde TLS-verbinding.

De toepassing van DANE zorgt er voor dat een verbinding pas tot stand wordt gebracht wanneer het DNS-record van de ontvangende mailserver is gecontroleerd door de verzendende mailserver. Hierdoor is het voor aanvallers niet mogelijk om berichtenverkeer 'af te luisteren' of te manipuleren. Gebruikers van STARTTLS en DANE moeten de verbinding verbreken wanneer er geen beveiligde verbinding via STARTTLS opgezet kan worden, maar deze wel aanwezig is volgens het DNS-records.

Geadviseerd wordt om STARTTLS en DANE in combinatie op te nemen op de lijst met open standaarden met de status 'pas toe of leg uit'.

Betrokkenen en proces

In eerste instantie is alleen DANE aangemeld voor opname op de lijst met open standaarden. Tijdens het intakegesprek is naar voren gekomen dat DANE in toenemende mate wordt toegepast met STARTTLS om een beveiligde verbinding tussen mailservers op te kunnen zetten. Daarom is besloten om STARTTLS samen met DANE in behandeling te nemen. Vervolgens heeft een expertbijeenkomst plaatsgevonden op 28 januari 2016. De conclusie van de expertgroep was om STARTTLS en DANE op te

nemen op de lijst met open standaarden, onder voorwaarde dat er binnen het organisatorisch werkingsgebied tenminste twee organisaties de standaarden succesvol hebben geïmplementeerd. Naar aanleiding hiervan is een meting op gebruik uitgevoerd, waaruit bleek dat aan deze voorwaarde is voldaan.

27 mei 2016

Tijdens de openbare consultatie van het expertadvies van 16 februari tot 16 maart 2016 is één reactie ontvangen. Wel is tijdens de openbare consultatie een nieuwe soortgelijke standaard (SMTP STS) gepubliceerd ondersteund door de grotere mail platformen (Gmail, Yahoo, Microsoft). In samenspraak met de experts en het Forum is toen besloten om hier een aanvullend onderzoek naar te doen.

Consequenties en vervolgstappen

Het gebruik van de standaarden is binnen het geadviseerde organisatorische werkingsgebied nog beperkt, met name waar het DANE betreft. Wel zijn er verschillende overheidsorganisaties die de standaarden ondersteunen zo heeft het Nationaal Cyber Security Center (NCSC) de standaarden onlangs succesvol geïmplementeerd. Ook zijn er positieve signalen bij andere overheidspartijen om de standaarden op korte termijn in gebruik te nemen. Daarnaast is het mogelijk om de implementatie van de standaarden te toetsen via Internet.nl. Verder is de opname van STARTTLS en DANE een positieve impuls voor de adoptie van DNSSEC omdat de standaarden verplicht gebruik maken van DNSSEC.

Gezien de recente ontwikkeling met betrekking tot SMTP STS is het belangrijk om zicht te houden op het gebruik van de standaarden bij de grote mailplatformen. En de ontwikkeling rondom SMTP STS goed te volgen. Verder zijn er enkele adviezen om de adoptie van de standaard te bevorderen. Deze staan in onderstaand advies.

Gevraagd besluit

Het Forum Standaardisatie wordt gevraagd om in te stemmen met onderstaande advies.

Het Forum Standaardisatie adviseert het Nationaal Beraad Digitale Overheid om:

1. STARTTLS en DANE op te nemen als 'pas toe of leg uit'-standaard op de lijst met open standaarden voor het hieronder geformuleerde toepassings- en werkingsgebied.
2. In te stemmen met de additionele adviezen ten aanzien van de adoptie van STARTTLS en DANE, zoals hieronder geformuleerd.

Ad 1 Opname van STARTTLS en DANE op de lijst met open standaarden

27 mei 2016

Geadviseerd wordt op de combinatie STARTTLS en DANE als zodanig op te nemen op de 'pas toe of leg uit'-lijst. Opname is wenselijk omdat op dit moment het gecombineerd gebruik van de standaarden voor e-mail nog beperkt is. STARTTLS als zodanig wordt wel veel gebruikt, maar alleen een gecombineerd opname is wenselijk voor veilige mailuitwisseling omdat STARTTLS gevoelig is voor 'man in the middle' aanvallen. DANE voorkomt dit omdat het zorgt voor het veilig opstarten van e-mailverbindingen en zorgt er dus voor dat de organisaties in het werkingsgebied veilig kunnen mailen.

Er zijn positieve signalen over toekomstig gebruik. Zo heeft ten tijde van het opstellen van dit Forumadvies het NCSC de standaarden succesvol geïmplementeerd op alle inkomende mailservers. En vanuit het platform Internet.nl is een meting uitgevoerd naar het gebruik van onder overheidsorganisaties. Deze meting kan gebruikt worden om toekomstige adoptie te monitoren.

Als functioneel toepassingsgebied voor STARTTLS en DANE wordt geadviseerd:

Inkomende mailservers passen STARTTLS (SMTP over STARTTLS, oftewel ESMTPS) in combinatie met DANE toe, zodat verzendende mailservers daarmee een versleutelde verbinding over een onvertrouwd netwerk (zoals internet) kunnen opzetten. Dit voorkomt dat aanvallers het mailverkeer kunnen afluisteren (passieve aanvallers) en/of kunnen manipuleren (actieve aanvallers).¹



Figuur 1. Geadviseerd functioneel toepassingsgebied

Het toepassingsgebied geldt voor alle mailverbindingen buiten de eigen (besloten) infrastructuur. Met andere woorden: de communicatie met mailservers buiten de eigen invloedssfeer. Ook betreft de toepassing voornamelijk inkomende mailservers. De implementatie van STARTTLS in combinatie met DANE is voor uitgaande mailservers ingewikkelder en vraagt meer inzet in tijd en middelen. Ook is er nog onvoldoende ervaring binnen de overheid met de implementatie van de standaarden voor uitgaande mail. Zodra er meer ervaring is opgedaan met implementatie van de standaard kan het toepassingsgebied worden uitgebreid met uitgaande mailstromen. Geadviseerd wordt om dit een jaar na opname van de standaarden te toetsen in samenspraak met de expertgroep.

Als organisatorisch werkingsgebied van STARTTLS en DANE wordt geadviseerd: *Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi)publieke sector.*

In diverse baselines zoals de Baseline Informatiebeveiliging Rijksdienst (BIR), Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en de Baseline Informatiebeveiliging waterschappen (BIWA) is opgenomen dat persoonsgegevens niet onversleuteld over onbeveiligde/onvertrouwde netwerken verzonden mogen worden. Het gebruik van geforceerde encryptie wordt zodoende ook afgedwongen door deze baselines.

27 mei 2016

Ad 2 Additionele adviezen ten aanzien van de adoptie van STARTTLS en DANE

Naar aanleiding van de expertgroep en het aanvullend onderzoek zijn er voor het Forum en het Nationaal Beraad bij opname op de lijst met open standaarden de volgende oproepen ten aanzien van de adoptie van de standaarden:

1. Het Forum Standaardisatie wordt opgeroepen om een infographic over e-mailbeveiligingsstandaarden op te stellen om zodoende de relatie met onder andere S/MIME, PGP, IMAP(S), POP3(S), x509, DMARC, SPF en DKIM beter weer te geven.
2. NCSC wordt opgeroepen om, in aanvulling op de whitepaper 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)', een factsheet uit te brengen over het implementeren van STARTTLS en DANE. Dit dient Internet.nl vervolgens ook als uitgangspunt te nemen in hun metingen.
3. Het Forum Standaardisatie wijst er bij de mailstandaarden op de lijst met gangbare standaarden die tussen mailclient en mailserver gebruikt kunnen worden (POP, IMAP, SMTP) op dat deze bij voorkeur met TLS beveiligd moeten worden.
4. KING wordt opgeroepen om beveiligingsstandaarden als STARTTLS en DANE op te nemen in de GEMMA Softwarecatalogus.
5. Forum/Nationaal Beraad een 0-meting laten uitvoeren naar gebruik van de standaarden.
6. De Shared Service Centra van het Rijk (zoals SSC-ICT / DICTU) op te roepen de standaard te implementeren en hen hierop via ICCIO of CTO-raad aan te spreken.
7. 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.
8. De ontwikkelingen rondom SMTP STS in de gaten te houden en wanneer SMTP STS een ontwikkelde standaard is de relatie tussen de standaarden opnieuw te duiden. Het advies is dan ook om deze ontwikkeling nauw te volgen en waar mogelijk te participeren in de doorontwikkeling van de standaard. De aangewezen partij hiervoor is het NCSC, conform haar Cyber Security strategie².

² <https://www.ncsc.nl/english/current-topics/national-cyber-security-strategy.html>

Toelichting

27 mei 2016

1. Waar gaat het inhoudelijk over?

Met de toenemende digitalisering is ook het beveiligingsrisico aanzienlijk toegenomen. De overheid gebruikt gevoelige informatie van zowel burgers als bedrijven. Ook maakt de overheid veel gebruik van e-mail en verstuurt en ontvangt zij e-mails van andere overheden, bedrijven en burgers mét gevoelige informatie. Dit vraagt om aandacht voor de dreiging van digitale (economische) spionage en identiteitsdiefstal. Zonder adequate beveiligingsmaatregelen kan in een kort tijdsbestek een grote hoeveelheid aan informatie op de facto anonieme wijze worden verzameld. Informatie kan worden geblokkeerd en onder bepaalde voorwaarden worden aangepast en vervalst.

De Nederlandse overheid heeft vanuit haar rol de taak en verplichting om (toevertrouwde) vertrouwelijke informatie te beschermen tegen afluisteren door aanvallers, zoals criminele partijen en statelijke actoren. Onder de te beschermen informatiestromen valt feitelijk ook communicatie tussen overheidspartijen, tussen de overheid en bedrijven en tussen overheden en burgers.

STARTTLS

E-mails worden door de mailserver van de verzendende partij verstuurd naar de mailserver van de ontvangende partij. Historisch gebeurt dit zonder enige versleuteling of beveiliging, waardoor het aanpassen of injecteren van mailverkeer relatief eenvoudig is.

De extensie STARTTLS is in veel gevallen aanwezig op beide mailservers. Zij kunnen daarmee een niet-versleutelde en daarmee onbeveiligde verbinding opwaarderen naar een met TLS versleutelde verbinding. Met een met TLS versleutelde verbinding wordt voorkomen dat een passieve aanvaller het berichtenverkeer kan 'afluisteren'. Let op: een passieve aanvaller is een aanvaller die het berichtenverkeer niet manipuleert, maar slechts ongemerkt onderschept.

Het gaat hier bijvoorbeeld om e-mails met gevoelige informatie of e-mails waarbij documenten mee zijn gestuurd. Om STARTTLS in werking te laten treden is het noodzakelijk dat zowel de verzendende als de ontvangende mailserver STARTTLS ondersteunen.

Wanneer STARTTLS door een van de servers niet wordt ondersteund of een versleutelde verbinding om een andere reden niet tot stand kan worden gebracht, wordt automatisch teruggevallen op een niet-versleutelde verbinding. Dit wordt opportunistische encryptie genoemd. Door het terugvallen op een onbeveiligde verbinding wordt voorkomen dat de leveringszekerheid kleiner zou worden bij de toepassing van STARTTLS. Dit is echter een groot nadeel voor de vertrouwelijkheid en integriteit van e-mailverkeer.

Een actieve aanvaller kan het gebruik van STARTTLS eenvoudig blokkeren, een zogeheten STRIPTLS- aanval. Een actieve aanvaller manipuleert hiermee het berichtenverkeer. Het tot stand brengen van een beveiligde TLS-verbinding met STARTTLS gebeurt immers via een niet-versleutelde verbinding. Door in het eerste stadium het aanbod van een versleutelde verbinding te blokkeren, gaat de verzendende server er vanuit dat TLS niet beschikbaar is. De verzendende server kiest er dan voor om door te gaan met de niet-versleutelde verbinding. Door deze manipulatie van het berichtenverkeer is het voor de actieve aanvaller mogelijk om

de verbinding af te luisteren en e-mails te lezen. Recent onderzoek heeft aangetoond dat dergelijke aanvallen wereldwijd op grote schaal plaatsvinden³.

27 mei 2016

DANE

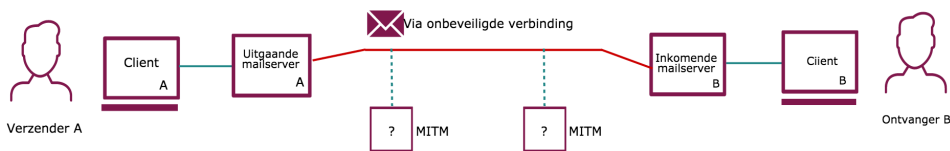
Bij het maken van een veilige verbinding naar een onbekende partij is een online controle op de authenticiteit van de verzendende partij en de eindbestemming wenselijk. Dit kan door middel van (gepubliceerde) certificaten die door certificaatautoriteiten (CA's) binnen het PKI-stelsel zijn uitgegeven of door self-signed certificates.

DANE maakt het voor de eigenaar van een domein mogelijk om via een met DNSSEC beveiligd DNS-record extra informatie bovenop de offline certificaten aan te reiken. Hierdoor kan real-time een controle worden gedaan op de authenticiteit van de server en of de server-to-server-verbinding legitiem is en niet wordt gemanipuleerd. DANE is dan ook met name belangrijk tegen actieve aanvallers.

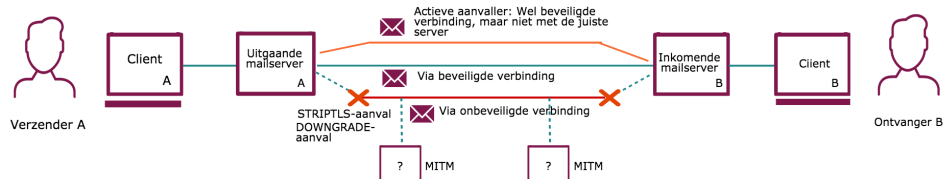
Het DANE-record kan gezien worden als een digitale vingerafdruk. Hierdoor kan het naast (of in plaats van) de certificaten van CA's worden gebruikt. DANE biedt real-time validatie per individueel certificaat, in plaats van offline per aanbieder: dit zou het gebruik van domain validated certificates op termijn overbodig kunnen maken.

Toepassing van STARTTLS in combinatie met DANE

De toepassing van STARTTLS in combinatie met DANE maakt het mogelijk om verbindingen die in principe niet als beveiligd beschouwd mogen worden (hetzij omdat er geen enkele beveiliging op zit, hetzij omdat alleen zogenaamde 'opportunistische' encryptie mogelijk is) om te zetten naar een gecontroleerde, beveiligde verbinding voor e-mailverkeer. Hierdoor is het voor aanvallers niet meer mogelijk om berichtenverkeer 'af te luisteren' of te manipuleren. Door het gebruik van STARTTLS en DANE weet de verzendende mailserver dat de e-mail daadwerkelijk via een versleutelde verbinding is verstuurd naar een mailserver van de ontvangende partij. De toepassing van STARTTLS in combinatie met DANE kan worden gezien als een 'HTTPS' voor e-mail.



Figuur 2. E-mailverkeer zonder gebruik van TLS, STARTTLS en DANE



Figuur 3. E-mailverkeer met gebruik van TLS en STARTTLS



Figuur 4. E-mailverkeer met gebruik van TLS, STARTTLS en DANE

2. Hoe is het proces verlopen?

Om tot dit forumadvies te komen hebben achtereenvolgens een intakegesprek, experttoetsing en openbare consultatie plaatsgevonden. Naar aanleiding van de intake is besloten om STARTTLS en DANE in behandeling te nemen. Aan de experttoetsing hebben (toekomstige) eindgebruikers, leveranciers, adviseurs en andere kennishebbers deelgenomen.

De conclusie uit de expertgroep was om STARTTLS en DANE op te nemen op de lijst met open standaarden met 'pas toe of leg uit'-verplichting, onder voorwaarde dat er binnen het organisatorisch werkingsgebied tenminste twee organisaties de standaarden succesvol hebben geïmplementeerd.

Het expertadvies is gepubliceerd ten behoeve van een openbare consultatie waarbij gevraagd is naar STARTTLS en DANE. Naar aanleiding hiervan is één reactie ontvangen. Deze reactie heeft geen invloed op onderliggend forumadvies. Wel is waren er ontwikkeling in de markt met betrekking tot SMTP STS die aanvullend onderzoek vergde.

3. Hoe scoort de standaard op de toetsingscriteria?

Toegevoegde waarde

De Nederlandse overheid moet vertrouwelijke informatie beschermen tegen af luisteren door aanvallers, hieronder wordt ook de communicatie tussen overheden onderling, tussen overheden en het bedrijfsleven en tussen overheden en burgers verstaan.

Technisch zijn de standaarden eenvoudig en tegen geringe kosten te implementeren met name voor de inkomende mail. Voor de uitgaande mailstromen is meer afstemming noodzakelijk. Door de implementatie van de standaarden ontstaat een relatie tussen e-mailbeheerders en DNS-beheerders. Zij moeten bijvoorbeeld afstemmen over de toevoeging en het onderhoud van DANE-records in de DNS. Hoewel deze partijen niet vanzelfsprekend een samenwerkingsrelatie hebben is afstemming tussen deze partijen noodzakelijk. De kosten voor deze afstemming kan per implementatie verschillen.

Geconcludeerd wordt dat de standaarden voldoende toegevoegde waarde hebben binnen het gekozen functioneel toepassingsgebied en organisatorisch werkingsgebied.

Open standaardisatieproces

STARTTLS en DANE worden beheerd door de Internet Engineering Task Force (IETF), een internationale standaardisatieorganisatie. Geconcludeerd wordt dat het standaardisatieproces van IETF voldoende open is: IETF kent goed gedocumenteerde en open beheerprocedures, er is geen lidmaatschap, het beheerproces en de besluitvorming hieromtrent is open en transparant.

IETF beheert naast STARTTLS en DANE ook andere standaarden op het gebied van internet en e-mail, zoals DNSSEC, TLS, IMAP, SMTP, POP3, HTTP(S), IPv6, DKIM en SPF. 27 mei 2016

Draagvlak

Het gebruik van de standaarden is binnen het geadviseerde organisatorische werkingsgebied nog beperkt. Het NCSC heeft de standaarden onlangs succesvol geïmplementeerd. Ook zijn er positieve signalen bij andere overheidspartijen om de standaarden op korte termijn in gebruik te nemen.

Opname bevordert de adoptie

Opname van de standaarden is een passend middel om een bredere adoptie van de standaard binnen de (semi)overheid te bevorderen. Het gebruik van de standaarden is nog niet in alle gevallen vanzelfsprekend.

Toelichting van eventuele risico's

Er zijn geen specifieke risico's geïdentificeerd.

4. Wat is de conclusie van de expertgroep en de consultatie?

Conclusie van de expertgroep

De expertgroep adviseert het Forum Standaardisatie en het Nationaal Beraad Digitale Overheid om STARTTLS en DANE op te nemen op de lijst met open standaarden, met 'pas toe of leg uit'-verplichting. Opname van STARTTLS en DANE is wel gebonden aan de voorwaarde dat minimaal twee partijen binnen het organisatorisch werkingsgebied de standaarden succesvol in gebruik hebben genomen. Hieraan is voldaan na meting via internet.nl.

Eventuele aanvullingen vanuit de consultatie

Tijdens de openbare consultatie van het expertadvies heeft OpenFortress positief gereageerd. OpenFortress onderschrijft het belang van de standaarden en opname op de lijst met open standaarden met de status 'pas toe of leg uit'.

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

Naar aanleiding van de expertgroep en het aanvullend onderzoek zijn er voor het Forum en het Nationaal Beraad om bij opname op de lijst met open standaarden de volgende oproepen ten aanzien van de adoptie van de standaarden te doen:

1. Het Forum Standaardisatie wordt opgeroepen om een infographic over e-mailbeveiligingsstandaarden op te stellen om zodoende de relatie met onder andere S/MIME, PGP, IMAP(S), POP3(S), x509, DMARC, SPF en DKIM beter weer te geven.
2. NCSC wordt opgeroepen om, in aanvulling op de whitepaper 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)', een factsheet uit te brengen over het implementeren van STARTTLS en DANE. Dit dient Internet.nl vervolgens ook als uitgangspunt te nemen in hun metingen.
3. Het Forum Standaardisatie wijst er bij de mailstandaarden op de lijst met gangbare standaarden die tussen mailclient en mailserver gebruikt kunnen worden (POP, IMAP, SMTP) op dat deze bij voorkeur met TLS beveiligd moeten worden.
4. KING wordt opgeroepen om beveiligingsstandaarden als STARTTLS en DANE op te nemen op de GEMMA Softwarecatalogus.
5. Aan het Forum/Nationaal Beraad 0-meting uitvoeren naar gebruik van de standaarden.

- 27 mei 2016
6. De Shared Service Centra van het Rijk (zoals SSC-ICT / DICTU) op te roepen de standaard te implementeren en hen hierop via ICCIO of CTO raad aan te spreken.
 7. 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.
 8. De ontwikkelingen rondom SMTP STS in de gaten te houden en wanneer SMTP STS een ontwikkelde standaard de relatie tussen de standaarden opnieuw te duiden. Het advies is dan ook om deze ontwikkeling nauw te volgen en waar mogelijk te participeren in de doorontwikkeling van de standaard. De aangewezen partij hiervoor is het NCSC, conform haar Cyber Security strategie⁴.

Bijlage

- [Expertadvies STARTTLS en DANE](#)
- [Overzicht reacties consultatieronde](#)

⁴ <https://www.ncsc.nl/english/current-topics/national-cyber-security-strategy.html>