Forum Standaardisatie

Expertadvies uitbreiding functioneel toepassingsgebied STARTTLS en DANE

Datum 3 augustus 2018

Colofon

Projectnaam	Expertadvies uitbreiding functioneel toepassingsgebied STARTTLS en DANE
Versienummer	1.0
Locatie	Den Haag
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag forumstandaardisatie@logius.nl
Auteurs	Arjen Brienen (Lost Lemon) Jasper Muskiet (Lost Lemon)

Inhoud

Samenvatting en Forumadvies

Advies aan het Forum

De experts geven het volgende advies:

De expertgroep adviseert het functioneel toepassingsgebied van STARTTLS in combinatie met DANE uit te breiden zoals hieronder aangegeven.

Als functioneel toepassingsgebied wordt geadviseerd:

STARTTLS en DANE moeten in combinatie worden toegepast op alle ontvangende en verzendende e-mailservers.

Als organisatorisch werkingsgebied wordt geadviseerd:

Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en alle instellingen uit de (semi-) publieke sector.

Waarom is uitbreiding van het functioneel toepassingsgebied belangrijk?

STARTTLS en DANE zijn in 2015 volledig getoetst en kwamen in 2016 op de 'pas toe of leg uit' lijst met verplichting voor inkomende e-mail. Verplichting voor uitgaande e-mail werd toen prematuur geacht vanwege de geringe marktondersteuning. Het Forum adviseerde destijds om een jaar later te onderzoeken of STARTTLS en DANE ook voor uitgaande e-mail verplicht kan worden. Daarover gaat dit expertadvies.

Het toepassen van de combinatie van STARTTLS en DANE voor inkomend e-mailverkeer zorgt dat alle partijen veilig e-mailberichten kunnen 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.

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 met 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 informatie op de facto anonieme wijze worden verzameld.

De Nederlandse overheid heeft de verantwoordelijkheid om 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 ook feitelijk communicatie tussen overheidspartijen, tussen de overheid en bedrijven, en tussen overheden en burgers.

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. In de IETF RFC 7672 standaard staat beschreven hoe dit op een 'opportunistische' manier kan worden gedaan, hierbij rekening houdend met SMTP-servers die geen ondersteuning voor DANE of TLS bieden. Als de ondersteuning wel aanwezig is, is het voor aanvallers niet meer mogelijk om berichtenverkeer 'af te luisteren' of te manipuleren. Door het gebruik van STARTTLS en DANE kan de verzende mailserver met zekerheid vaststellen dat de ontvangende partij een versleutelde verbinding wenst te gebruiken.

Hoe is het proces verlopen?

Om tot dit advies te komen zijn van 2 juli tot en met 30 juli 2018 experts van verschillende organisaties gebeld om over de uitbreiding van het functioneel toepassingsgebied te discussiëren en om STARTLS en DANE met het uitgebreide functionele toepassingsgebied te toetsen tegen de toetsingscriteria. Ook is er op donderdag 19 juli een beperkte expertbijeenkomst gehouden. Dit expertadvies vat de uitkomsten van de belronde en de bijeenkomst samen.

Vervolg

Dit advies zal ten behoeve van een publieke consultatie openbaar worden gemaakt door het Bureau Forum Standaardisatie. Eenieder kan gedurende de consultatieperiode op dit advies zijn/haar 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 Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) opstellen. Het OBDO bepaalt uiteindelijk op basis van het advies van het Forum of STARTTLS en DANE aangepast worden voor de lijst.

Hoe scoort de standaard met uitgebreid functioneel toepassingsgebied op de toetsingscriteria?

<u>Toegevoegde waarde</u>
Sinds 19 september 2016 geldt voor STARTTLS in combinatie met met DANE een 'pas toe of leg uit' verplichting voor <u>ontvangende</u> mailservers. Het is echter voor <u>verzendende</u> mailserver nog niet verplicht STARTTLS en DANE toe te passen (dit conform IETF RFC 7672). Daarom zijn er nog drie typen verbindingen mogelijk:

1. niet versleutelde verbindingen;
2. met een versleutelde verbinding, zonder certificaatverificatie conform DANE;
3. met een versleutelde verbindingen, met certificaatverificatie conform DANE.

De expertgroep concludeert dat de uitbreiding van het functioneel toepassingsgebied toegevoegde waarde heeft. De Nederlandse overheid moet de communicatie met burgers, bedrijven en overheden beschermen tegen afluisteren en manipulatie door aanvallers. De uitbreiding van het functioneel toepassingsgebied verplicht overheden om op basis van STARTTLS en DANE beveiligde communicatie op te zetten als de ontvangde partij dat ondersteunt. De experts zijn het er over eens dat dit een logische en noodzakelijke uitbreiding van het functioneel toepassingsgebied is.

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

Open standaardisatieproces
STARTTLS en DANE zijn IETF standaarden. Het standaardisatieproces van IETF is reeds positief getoetst bij opname van STARTTLS en DANE op de 'pas toe of leg uit' lijst in 2016.

Draagvlak
STARTTLS wordt breed ondersteund, maar het gebruik van STARTTLS in combinatie met DANE is op dit moment nog beperkt. Een aantal experts vindt dat de ondersteuning door de grote leveranciers nader onderzocht moet worden, en dat deze partijen vanuit een sterke belangenbehartiger bewogen moeten worden op korte termijn ondersteuning te bieden. Door gebruik van add-ons is het ondanks de beperkte ondersteuning mogelijk om gebruik te maken van DANE. Er zijn positieve signalen over toekomstige ondersteuning. Met name de ondersteuning van STARTTLS en DANE door TransIP en XS4ALL, beide grote hosting providers in Nederland, is een positief signaal.

Microsoft® en Google® hebben aangegeven STARTTLS in combinatie met DANE vooralsnog niet te zullen ondersteunen, maar te kiezen voor een alternatieve standaard: MTA-STS[1]. Deze staat echter nog in de kinderschoenen. 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.

Het advies verplicht overheden STARTTLS in combinatie met DANE te gebruiken als dat ontvanger dat ondersteunt, mocht ontvanger dit niet ondersteunen wordt teruggevallen op 'reguliere' versleuteling of geen versleuteling. Zo vormt de nog beperkte ondersteuning voor DANE geen risico voor de toepassing. Dit is in overeenstemming met de DANE specificatie van IETF, RFC 7672[2].

Opname bevordert de adoptie
De expertgroep concludeert dat de uitbreiding van het functioneel toepassingsgebied het passende middel is om de adoptie van de standaard binnen de (semi)overheid te bevorderen. Ook kan de wijziging een stimulerende werking hebben op de ondersteuning door leveranciers van DANE, voor zowel inkomend als uitgaand e-mailverkeer. Een aantal experts maakt zich wel zorgen over de marktondersteuning van DANE.

1 https://datatracker.ietf.org/doc/draft-ietf-uta-mta-sts/
2 https://tools.ietf.org/html/rfc7672

Opensource producten bieden voldoende ondersteuning, maar men heeft onvoldoende beeld bij commerciële producten. Men vindt echter dat er aangesloten kan worden bij de reeds bestaande verplichting voor ontvangende emailservers. Het betreft hier immers dezelfde producten.

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 adviesrapport "Maak Waar!"[3] en de strategie "Nederland Digitaal"[4] 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 OBDO besluit welke standaarden op deze lijst worden opgenomen. Het OBDO baseert zich hierbij op expertadviezen, openbare consultaties en adviezen van het Forum Standaardisatie.

1.2 Doelstelling expertadvies

STARTTLS en DANE zijn al in 2015 getoetst en staan sinds 2016 op de pas toe of leg uit lijst voor inkomende e-mail.

Het doel van dit advies is om, aan de hand van de criteria vast te stellen of het functioneel toepassingsgebied van STARTTLS en DANE op de pas toe of leg uit lijst moet worden uitgebreid met uitgaande e-mail servers, al dan niet onder bepaalde voorwaarden.

1.3 Doorlopen proces

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

1. De procesbegeleider heeft op 10 april 2018 de opdracht gekregen een expertadvies over STARTTLS en DANE op te stellen. Hiervoor is een groep experts benaderd die voor een belangrijk deel bestaat uit experts die in 2015 al betrokken waren bij de toetsing van STARTTLS en DANE voor de 'pas toe of leg uit' lijst.
2. De leden van de expertgroep hebben een voorbereidingsdossier gekregen dat is samengesteld met informatie uit de aanmelding. Voorafgaand aan de belronde heeft de expertgroep dit voorbereidingsdossier doorgenomen en aandachtspunten geïdentificeerd.
3. De expertgroep is van 2 tot en met 30 juli 2018 door middel van een belronde en via een beperkte expertbijeenkomst bevraagd om de bevindingen in het algemeen en de geïdentificeerde aandachtspunten in het bijzonder te bespreken. Tijdens deze consultaties zijn ook het toepassings- en werkingsgebied vastgesteld.

Dit expertadvies geeft de uitkomst van de expertgroep weer. De procesbegeleider heeft een concept van dit expertadvies aan de leden

3 https://www.rijksoverheid.nl/documenten/rapporten/2017/04/18/rapport-van-de-studiegroep-informatiesamenleving-en-overheid-maak-waar

4 https://www.rijksoverheid.nl/documenten/rapporten/2018/06/16/nederlandse-digitaliseringsstrategie

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 6 augustus 2018 tot en met 10 september 2018. 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 OBDO op. Het OBDO besluit met dit advies om de standaard wel of niet op de lijst open standaarden te plaatsen.

1.5 Samenstelling expertgroep

Het Forum Standaardisatie streeft naar een representatieve expertgroep met een evenwichtige vertegenwoordiging van (toekomstige) gebruikers (zowel publiek als privaat), leveranciers, wetenschappers en andere belanghebbenden. De expertgroep heeft een procesbegeleider die de expertgroep leidt en de verantwoordelijkheid neemt voor het expertadvies.

Arjen Brienen, technisch consultant bij Lost Lemon B.V. in samenwerking met Jasper Muskiet, consultant bij Lost Lemon B.V., heeft de procedure in opdracht van het Bureau Forum Standaardisatie begeleid.

Als experts hebben geadviseerd:
- Maarten Aertsen (NCSC)
- Iljitsch van Beijnum (Logius)
- Alwin de Bruin (dmarcian)
- Ralph Dolmans (NLnet Labs)
- John van Huijgevoort (VNG Realisatie)
- Michiel Leenaars (NLnet)
- Pieter Lexis (PowerDNS)

1.6 Toelichting STARTTLS en DANE

<u>STARTTLS</u>

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. Een met TLS versleutelde verbinding voorkomt dat een ‘passieve’ aanvaller het berichtenverkeer kan onderscheppen en lezen. Een ‘passieve’ aanvaller is een partij tussen verzender en ontvanger die het berichtenverkeer ongemerkt onderschept zonder het berichtenverkeer te manipuleren. Om STARTTLS in werking te laten treden is het noodzakelijk dat zowel de verzendende als de ontvangende mailserver STARTTLS ondersteunen.

Wanneer STARTTLS door één van de beide servers niet wordt ondersteund, wordt automatisch teruggevallen op een 'reguliere' TLS-verbinding en als dat niet mogelijk is een niet-versleutelde verbinding. Dit wordt opportunistische encryptie genoemd. Door het mechanisme van terugvallen wordt voorkomen dat STARTTLS de aflevering van berichten compromitteert. Opportunistische encryptie reduceert echter de vertrouwelijkheid en integriteit van e-mailverkeer.

Een 'actieve' aanvaller kan het gebruik van STARTTLS eenvoudig blokkeren met een zogeheten STRIPTLS- aanval. Een actieve aanvaller is een partij tussen verzender en ontvanger ('man in the middle') die het berichtenverkeer onderschept en manipuleert. Dit kan omdat het STARTTLS protocol wordt geinitieerd over een onversleutelde 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 voorkomt de actieve aanvaller mogelijk dat een versleutelde verbinding wordt opgezet en kan hij of zij de berichten onderscheppen en lezen. Recent onderzoek heeft aangetoond dat dergelijke aanvallen wereldwijd op grote schaal plaatsvinden[5].

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 de validiteit van een verbinding te bepalen. Hierdoor kan 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 als bescherming tegen actieve aanvallers. Het DANE-record kan gezien worden als een digitale vingerafdruk van de verbinding

Toepassing van STARTTLS in combinatie met DANE

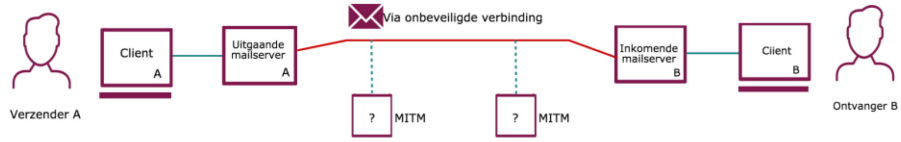
Met de toenemende digitalisering neemt ook de dreiging van digitale aanvallen toe. Zo kan via digitale (economische) spionage in een kort tijdsbestek grote hoeveelheden informatie op grotendeels anonieme en simultane wijze verzameld worden. Ook kan informatie worden gemanipuleerd. Aanvallers camoufleren hun communicatie met geïnfecteerde netwerken als regulier netwerkverkeer. Ze maken gebruik van versleuteling om de aard van hun activiteiten te verbergen. De Nederlandse overheid moet communicatie met burgers, bedrijven en overheden beschermen tegen afluisteren door aanvallers zoals cybercriminelen en statelijke actoren. Daarbij heeft de overheid een voorbeeldfunctie voor bedrijven en burgers. Door het gebruik van STARTTLS en DANE wordt voor anderen die met de overheid e-mailen de basis gelegd om dit veilig te kunnen doen.

5 http://dl.acm.org/citation.cfm?id=2815695

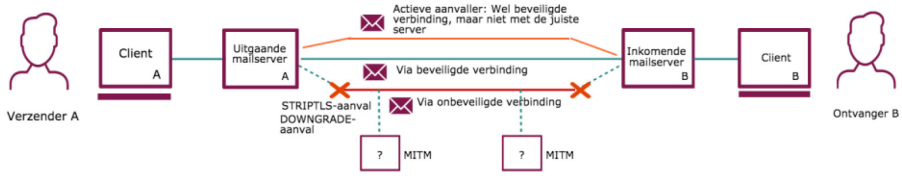
De toepassing van DANE en STARTTLS maakt het mogelijk om een beveiligde verbinding voor e-mailverkeer tot stand te brengen. Hierdoor is het voor aanvallers niet mogelijk om berichtenverkeer te onderscheppen en te lezen of manipuleren. Door het gebruik van STARTTLS en DANE kan de verzende mailserver met zekerheid vaststellen dat de ontvangende partij een versleutelde verbinding wenst te gebruiken.

Daarnaast biedt het gebruik van DANE de eigenaar van een domein de mogelijkheid om een extra verificatiemiddel, naast de certificaten van certificaat autoriteiten (CA's), in te zetten.

Wanneer zowel de verzendende als de ontvangende partij DANE toepassen wordt een verbinding pas tot stand gebracht wanneer het DNS-record van de ontvangende partij gecontroleerd is door de verzendende partij. Gebruikers van DANE en STARTTLS moeten de verbinding verbreken wanneer er geen beveiligde verbinding via STARTTLS opgezet kan worden maar deze wel aanwezig is volgens het DNS-record. Hiermee worden STRIPTLS-aanvallen door actieve aanvallers afgeweerd.



Figuur 1. E-mailverkeer zonder gebruik van TLS, STARTTLS en DANE



Figuur 2. E-mailverkeer met gebruik van TLS en STARTTLS

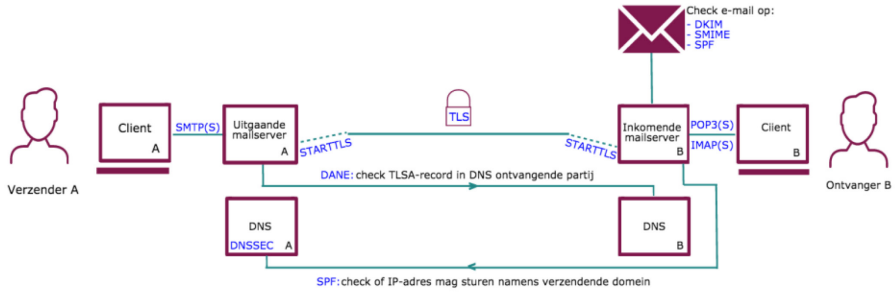
Figuur 3. E-mailverkeer met gebruik van TLS, STARTTLS en DANE

Relatie met andere standaarden

STARTTLS maakt naast DANE, gebruik van TLS. TLS is een protocol dat beveiligde transportverbindingen over het internet tot stand brengt door middel van cryptografie. Met TLS kunnen zowel verbindingen met websites als e-mail verbindingen worden beveiligd, alsmede andere verbindingen (bijvoorbeeld FTP voor bestandsoverdracht). TLS staat op de 'pas toe of leg uit' lijst van het Forum Standaardisatie.

DANE maakt direct gebruik van DNSSEC. DNSSEC beschermt het domeinnaam systeem (DNS) van het internet tegen omleiding en manipulatie. Om DANE te kunnen gebruiken is het noodzakelijk dat organisaties DNSSEC tenminste gedeeltelijk hebben geïmplementeerd. Ontvangende e-mail servers moeten een DNSSEC ondertekende zone publiceren en verzendenende e-mail servers moeten DNSSEC resolving

toepassen. Figuur 4 illustreert de relatie van STARTTLS en DANE met TLS, DANE en andere e-mail veiligheidstandaarden.



Figuur 4. Relatie STARTTLS en DANE met andere standaarden

1.7 Leeswijzer

Hoofdstuk 2 beschrijft het functioneel toepassingsgebied (situaties waarin de standaarden functioneel gebruikt moeten worden) en het organisatorisch werkingsgebied (organisaties die de standaarden moeten toepassen).

Hoofdstuk 3 beschrijft de resultaten van de toetsing van de standaarden aan de hand van de criteria voor opname op de lijst open standaarden.

2 Toepassings– en werkingsgebied

De *instructie rijksdienst inzake de aanschaf van ICT producten en ICT diensten*[6] verplicht overheidsorganisaties om relevante standaarden op de "pas toe of leg uit" 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.

Secties 2.1 en 2.2 geven het advies van de expertgroep voor het functioneel en organisatorisch toepasingsgebied van STARTTLS en DANE.

2.1 Functioneel toepassingsgebied

Als functioneel toepassingsgebied wordt voorgesteld:
STARTTLS en DANE moeten in combinatie worden toegepast op alle ontvangende en verzendende e-mailservers.

Het toepassen van de combinatie van STARTTLS en DANE voor inkomend e-mailverkeer zorgt dat alle partijen veilig e-mailberichten kunnen 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.

2.2 Organisatorisch werkingsgebied

De expertgroep adviseert om het organisatorisch werkingsgebied van de STARTTLS en DANE ongewijzigd te laten:

Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-)publieke sector.

6 http://wetten.overheid.nl/BWBR0024717/2008-11-23

3 Toetsing van standaard aan criteria

Het Forum Standaardisatie hanteert vier hoofdcriteria om te bepalen of een standaard in aanmerking komt voor opname op de lijst:
1. Heeft de standaard toegevoegde waarde?
2. Zijn de standaard en het standaardisatieproces voldoende open?
3. Heeft de standaard voldoende draagvlak?
4. Is opname op de lijst nodig om de adoptie te bevorderen?[7]

Ieder van deze hoofdcriteria heeft deelcriteria die beschreven staan in het document *"Toetsingsprocedure en criteria voor lijst met open standaarden voor indieners en experts",* te vinden op de website van het Forum Standaardisatie https://www.forumstandaardisatie.nl/content/toetsen-van-standaarden.

Dit hoofdstuk beschrijft per criterium het resultaat van de toetsing. Voor de volledigheid is tevens de beschrijving van elk criterium opgenomen.

3.1 Toegevoegde waarde

De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de risico's en nadelen.

3.1.1 Is het toepassings- en werkingsgebied van de aanmelding goed gedefinieerd?

3.1.1.1 Is het functioneel toepassingsgebied goed gedefinieerd?
Ja, zie paragraaf 2.1.

3.1.1.2 Is het organisatorisch werkingsgebied goed gedefinieerd?
Ja, zie paragraaf 2.2

3.1.1.3 Is de standaard generiek toepasbaar (en niet alleen bedoeld voor gegevensuitwisseling met één of een beperkt aantal specifieke organisaties)? (toelichtende vraag)
Ja, zie het forumadvies over STARTTLS en DANE uit 2015.[8]
De uitbreiding van het functioneel toepassingsgebied verandert niets aan de generieke toepasbaarheid.

3.1.2 Verhoudt de standaard zich goed tot andere standaarden?

3.1.2.1 Kan de standaard naast of in combinatie met reeds opgenomen standaarden worden toegepast (d.w.z. de standaard conflicteert niet met reeds opgenomen standaarden)?
Ja, zie het forumadvies over STARTTLS en DANE uit 2015.[9]
De uitbreiding van het functioneel toepassingsgebied verandert niets aan de toepasbaarheid van STARTTLS en DANE in combinatie met andere

7 Dit criterium is voornamelijk van toepassing op standaarden op de "pas toe of leg uit" lijst, niet voor aanbevolen standaarden.
8 https://www.forumstandaardisatie.nl/sites/bfs/files/FS%20160608.3E%20Forumadvies%202%20opname%20STARTTLS%20icm%20DANE.pdf
9 idem

standaarden op de 'pas toe of leg uit' lijst (in het bijzonder TLS, DNSSEC, SPF, DKIM en DMARC).

3.1.2.2 Biedt de aangemelde standaard meerwaarde boven reeds opgenomen standaarden met een overlappend functioneel toepassings- en organisatorisch werkingsgebied? (Dit kan ook om een nieuwe versie van dezelfde standaard gaan.)
Niet van toepassing, zie ook het forumadvies over STARTTLS en DANE uit 2015.[10]

3.1.2.3 Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname? (toelichtende vraag)
Ja. Microsoft®, Google®, Aol® en Yahoo® hebben aangekondigd dat ze de concurrerende standaard MTA-STS gaan gebruiken. MTA-STS maakt in eerste instantie een onbeveiligde verbinding. Voor organisaties met een kleiner mailvolume betekent dit minder beveiligingsgaranties tegen aanvallers. MTA-STS biedt vooral voordeel voor de grootste mailpartijen.

3.1.2.4 Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden? (toelichtende vraag)
Ja, zie het forumadvies over STARTTLS en DANE uit 2015.[11]

3.1.2.5 Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn? (toelichtende vraag)
Niet van toepassing, zie ook het forumadvies over STARTTLS en DANE uit 2015.[12] Uitbreiding van het functioneel toepassingsgebied introduceert geen noodzaak voor profielen of aanvullende afspraken.

3.1.3 Wegen de kwantitatieve en kwalitatieve voordelen van adoptie van de standaard, voor de (semi-)overheid als geheel en voor de maatschappij, op tegen de nadelen?

3.1.3.1 Draagt de adoptie van de standaard bij aan de oplossing van een bestaand, relevant interoperabiliteitsprobleem?
STARTTLS en DANE zijn alleen effectief in het beveiligen van e-mail verbindingen als alle mailservers (voor inkomende en uitgaande e-mail) deze implementeren. Uitbreiding van het functioneel toepassingsgebied naar verzendende e-mail servers draagt dus substantieel bij tot het beveiligen van alle overheidsmail.

3.1.3.2 Draagt de standaard bij aan het voorkomen van een vendor lock-in (leveranciersafhankelijkheid)?
Ja, een aantal leveranciers biedt ondersteuning bij de implementatie van STARTTLS en DANE. Daarnaast bestaan er open source implementaties.

3.1.3.3 Wegen de overheidsbrede en maatschappelijke baten voor de informatievoorziening en de bedrijfsvoering op tegen de kosten?
De baten van de uitbreiding van het functioneel toepassingsgebied wegen op tegen de kosten. De kosten om de standaarden technisch te

10 https://www.forumstandaardisatie.nl/sites/bfs/files/FS%20160608.3E%20Forumadvies%202%20opname%20STARTTLS%20icm%20DANE.pdf
11 Idem
12 Idem

implementeren zijn gering aangezien gebruik gemaakt kan worden van reeds benodigde (en dus bestaande) infrastructuur en eventuele bijbehorende licenties. Implementatie betreft aanvullende configuratie van mailservers. De baten betreffen aanvullende beveiliging van alle mailverkeer (inkomend en uitgaand). De experts zien hierom de baten tegen de kosten opwegen.

3.1.3.4 Zijn de kosten van implementatie acceptabel en zijn deze kosten bekend en inzichtelijk?
De kosten van de toepassing van STARTTLS en DANE voor uitgaande e-mail lijken acceptabel, aangezien bestaande infrastructuur en eventueel bijbehorende licenties gebruikt kunnen worden. Implementatie betreft met name configuratie van mailservers. Voor sommige organisaties kunnen de kosten zelfs afnemen, omdat het bij gebruik van DANE niet nodig is om door CA ondertekende certificaten te gebruiken en dus in te kopen.

3.1.3.5 Is er een (kwalitatieve) businesscase van de standaard aanwezig?
Ja, met name op het gebied van beveiliging en verminderde complexiteit van de standaard. Beveiliging van overheidsinformatie is een onderwerp met de hoogste prioriteit. Verplichting van STARTTLS en DANE voor ontvangende en verzendende mailservers is een belangrijke stap in de beveiliging van alle overheidsmail.

3.1.3.6 Is de meerwaarde van de standaard goed inzichtelijk te maken? Wat betekent de standaard voor de (bedrijfs)processen van een organisatie of keten en wat los je met de standaard op?
Ja, toepassing van STARTTLS en DANE op ontvangende en verzendende mailservers zorgt ervoor dat alle overheidsmail beveiligd wordt tegen onderschepping en manipulatie.

3.1.3.7 Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel?
Niet van toepassing, er zijn geen specifieke beveiligingsrisico's geïdentificeerd voor het uitbreiden van het functioneel toepassingsgebied.

3.1.3.8 Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel?
Niet van toepassing, er zijn geen specifieke privacyrisico's geïdentificeerd voor het uitbreiden van het functioneel toepassingsgebied.

3.1.4 Conclusie criteria 'Toegevoegde waarde'

De expertgroep concludeert dat de uitbreiding van het functioneel toepassingsgebied toegevoegde waarde heeft. De Nederlandse overheid moet de communicatie met burgers, bedrijven en overheden beschermen tegen afluisteren en manipulatie door aanvallers. De uitbreiding van het functioneel toepassingsgebied verplicht overheden om op basis van STARTTLS en DANE beveiligde communicatie op te zetten als de ontvangde partij dat ondersteunt. De experts zijn het er over eens dat dit een logische en noodzakelijke uitbreiding van het functioneel toepassingsgebied is.

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

3.2 Open standaardisatieproces

De ontwikkeling en het beheer van de standaard zijn op een open, onafhankelijke, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze ingericht.

3.2.1 Is de documentatie voor een ieder drempelvrij beschikbaar?

3.2.1.1 Is het specificatiedocument beschikbaar zonder dat er sprake is van belemmeringen (zoals hoge kosten of lidmaatschapseisen)?
Zie het forumadvies over STARTTLS en DANE uit 2015.[13]

3.2.1.2 Is de documentatie over het ontwikkel- en beheerproces (bijv. het voorlopige specificatiedocument, notulen en beschrijving van de besluitvormingsprocedure) beschikbaar zonder dat er sprake is van belemmeringen (zoals hoge kosten of lidmaatschapseisen)?
Zie het forumadvies over STARTTLS en DANE uit 2015.

3.2.2 Is het intellectuele eigendomsrecht voor eenieder beschikbaar, zodat de standaard vrij implementeerbaar en te gebruiken is?

3.2.2.1 Stelt de standaardisatieorganisatie het intellectueel eigendomsrecht op de standaard (bijvoorbeeld patenten of licenties) onherroepelijk royalty-free voor eenieder beschikbaar?
Zie het forumadvies over STARTTLS en DANE uit 2015.

3.2.2.2 Garandeert de standaardisatieorganisatie dat partijen die bijdragen aan de ontwikkeling van de standaard hun intellectueel eigendomsrecht voor (onderdelen van) de standaard onherroepelijk royalty-free voor eenieder beschikbaar stellen?
Zie het forumadvies over STARTTLS en DANE uit 2015.

3.2.3 Is de inspraak van eenieder in voldoende mate geborgd?

3.2.3.1 Is het besluitvormingsproces toegankelijk voor alle belanghebbenden (bijv. gebruikers, leveranciers, adviseurs, wetenschappers)?
Zie het forumadvies over STARTTLS en DANE uit 2015.

3.2.3.2 Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen?
Zie het forumadvies over STARTTLS en DANE uit 2015.

3.2.3.3 Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde rocedure?
Zie het forumadvies over STARTTLS en DANE uit 2015.

3.2.3.4 Organiseert de standaardisatieorganisatie regelmatig overleggen met belanghebbenden over doorontwikkeling en beheer van de standaard?
Zie het forumadvies over STARTTLS en DANE uit 2015.

3.2.3.5 Organiseert de standaardisatieorganisatie een publieke consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld?
Zie het forumadvies over STARTTLS en DANE uit 2015.

13 https://www.forumstandaardisatie.nl/sites/bfs/files/FS%20160608.3E%20Forumadvies%202%20opname%20STARTTLS%20icm%20DANE.pdf

3.2.4 Is de standaardisatieorganisatie onafhankelijk en duurzaam?

3.2.4.1 Is de ontwikkeling en het beheer van de standaard belegd bij een onafhankelijke non-profit standaardisatieorganisatie?
Zie het forumadvies over STARTTLS en DANE uit 2015.

3.2.4.2 Is de financiering van de ontwikkeling en het onderhoud van de standaard voor tenminste drie jaar gegarandeerd?
Zie het forumadvies over STARTTLS en DANE uit 2015.

3.2.5 Is het (versie) beheer van de standaard goed geregeld?

3.2.5.1 Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot (versie)beheer van de standaard? Bij voorkeur is dit beleid ook beschreven in een beheerplan (met o.a. aandacht voor migratie van gebruikers)
Zie het forumadvies over STARTTLS en DANE uit 2015.

3.2.5.2 Is de beheerdocumentatie goed vindbaar en verkrijgbaar?
Zie het forumadvies over STARTTLS en DANE uit 2015.

3.2.5.3 Is het belang van de Nederlandse overheid voldoende geborgd bij de ontwikkeling en het beheer van de standaard?
Zie het forumadvies over STARTTLS en DANE uit 2015.

3.2.5.4 Is de vertegenwoordiging van belanghebbenden bij het beheer van de standaard een goede representatie van het werkingsgebied en functioneel toepassingsgebied van de standaard?
Zie het forumadvies over STARTTLS en DANE uit 2015.

3.2.5.5 Is het standaardisatieproces van de standaardisatieorganisatie zodanig goed geregeld dat het Forum zich kan onthouden van aanvullende toetsing bij de aanmelding van een nieuwe versie van de standaard?
Zie het forumadvies over STARTTLS en DANE uit 2015.

3.2.6 Is er adoptieondersteuning voor de standaard?

3.2.6.1 Is er een toegankelijk aanspreekpunt of organisatie waar meer informatie over de standaard is te vinden en op te vragen is?
Zie het forumadvies over STARTTLS en DANE uit 2015.

3.2.6.2 Wordt er ondersteuning gegeven in de adoptie en de implementatie van de standaard?
Zie het forumadvies over STARTTLS en DANE uit 2015.

3.2.7 Conclusie criteria 'Open standaardisatieproces'
STARTTLS en DANE zijn IETF standaarden. 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 uitbreiding van het functioneel toepassingsgebied verandert niets ten aanzien van de openheid van het standaardisatieproces van IETF inzake STARTLS en DANE.

3.3 Draagvlak

Aanbieders en gebruikers moeten voldoende positieve ervaring met de standaard hebben.

3.3.1 Bestaat er voldoende marktondersteuning voor de standaard?

3.3.1.1 Bieden meerdere leveranciers ondersteuning voor de standaard?
Ja, de implementatie van STARTTLS en DANE op uitgaande e-mail servers wordt ondersteund door de mailserver-software van Postfix®, Exim® en Halo®. De ondersteuning door grote leveranciers zoals Cisco® vinden de experts echter nog mager. Voor ontvangende servers is er voldoende ondersteuning (noodzakelijk om verzending op basis van STARTTLS en DANE te kunnen doen en de functionele uitbreiding effectief te kunnen doen).

Een groot aantal (web)mailproviders ondersteunen STARTTLS, waaronder Google® (Gmail), Microsoft® (Outlook en Live), Ziggo®, KPN®, Comcast®, Yahoo®, XS4ALL® en mailbox.org. In de meeste gevallen is het enkel 'onder water' zichtbaar wanneer het opzetten van een TLS-verbinding door middel van STARTTLS mislukt en wordt terug gevallen op een niet-beveiligde verbinding. Google® en Microsoft® hebben aangegeven STARTTLS in combinatie met met DANE vooralsnog niet te zullen ondersteunen en hebben ondersteuning voor een alternatieve standaard MTA-STS aangekondigd. Ondersteuning hiervoor is nog minimaal, maar geadviseerd wordt MTA-STS in de toekomst wel te toetsen.

DANE wordt ondersteund door de mailserver-software van Postfix®, Exim® en Halo® e-mail gateway. In Nederland ondersteunen mailproviders XS4ALL® en TransIP® DANE. Zodoende kunnen overheidspartijen voor de inkomende e-mail en uitgaande e-mail gebruik maken van STARTTLS en DANE. Hoewel er voldoende ondersteuning is voor STARTTLS, is dit voor DANE nog niet het geval. Open source add-ons kunnen een oplossing bieden waar DANE nog onvoldoende ondersteund wordt.

3.3.1.2 Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen?
Er zijn meerdere websites waarop gecontroleerd kan worden of een beveiligde verbinding mogelijk is door middel van STARTTLS, en of deze op een juiste manier is geimplementeerd, waaronder www.internet.nl en www.starttls.info. Voor DANE is het op dit moment alleen mogelijk om de conformiteit van inkomende e-mails te toetsen. De planning van www.internet.nl is om einde van het jaar het ook mogelijk te maken de conformiteit te toetsen voor uitgaande mails.

3.3.1.3 Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn om de standaard te implementeren of te gebruiken?
Ja, zie het forumadvies over STARTTLS en DANE uit 2015. De uitbreiding van het functioneel toepassingsgebied introduceert geen noodzaak voor profielen of aanvullende afspraken.

3.3.1.4 Zijn er profielen of voorbeeldimplementaties van de standaard aanwezig en zijn deze vrij te gebruiken?
Ja, er zijn voorbeelden met Postfix® beschikbaar.

3.3.2 Kan de standaard rekenen op voldoende draagvlak?

3.3.2.1 Staan de belangrijkste stakeholders vanuit de overheid voor deze standaard achter de adoptie van de standaard?
Ja, voor zover benaderd in het expertonderzoek staan de experts achter de uitbreiding van het functioneel toepassingsgebied.

3.3.2.2 Staan de overheidsorganisaties die daadwerkelijk worden geraakt door een mogelijke verplichting van de standaard achter het gebruik van de standaard?
Ja, voor zover benaderd in het expertonderzoek staan de experts achter de uitbreiding van het functioneel toepassingsgebied.

3.3.2.3 Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?
Meerdere overheidsorganisaties maken gebruik van STARTTLS voor inkomende mail, waaronder eHerkenning, overheid.nl, PKI Overheid, Logius, gemeente Vught, Universiteit Twente, IBD. De combinatie van STARTTLS en DANE is nog niet geïmplementeerd binnen het organisatorisch werkingsgebied.

3.3.2.4 Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?
Niet van toepassing, aangezien er geen eerdere versies van STARTTLS en DANE zijn.

3.3.2.5 Is de aangemelde versie backwards compatible met eerdere versies van de standaard?
Niet van toepassing, zie paragraaf 3.3.2.4.

3.3.2.6 Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?
Op voordracht van een aantal grote publieke partijen, hebben SSC-ICT en de gemeente ’s-Hertogenbosch bij Cisco een feature request ingediend voor de ondersteuning van de combinatie STARTTLS en DANE op verzendende mailservers. Cisco heeft deze geïmplementeerd.

3.3.3 Conclusie criteria ‘Draagvlak’
De expertgroep concludeert dat het gebruik van STARTTLS en DANE voor uitgaande e-mail op dit moment nog beperkt is, maar dat de positieve signalen over toekomstig gebruik voldoende zijn. De ondersteuning van STARTTLS is goed, net als de ondersteuning van DANE voor inkomende e-mail. De ondersteuning van DANE voor uitgaande e-mail is beperkt, maar de experts verwachten dat dit zal toenemen.

3.4 Opname bevordert adoptie

De opname op de lijst is een geschikt middel om de adoptie van de standaard te bevorderen.

Met de lijst wil het OBDO de adoptie van open standaarden bevorderen die voldoen aan de voorgaande criteria (toegevoegde waarde, standaardisatieproces en draagvlak).

- Met de "pas toe of leg uit"-status beoogt het OBDO standaarden te verplichten als:
  a. hun huidige adoptie binnen de (semi-)overheid beperkt is;
  b. opname op de lijst bijdraagt aan de adoptie door te stimuleren (functie = stimuleren).
- Met de aanbevolen standaarden beoogt het OBDO standaarden aan te bevelen als :
  a. hun huidige adoptie binnen de (semi-)overheid reeds hoog is;
  b. opname op de lijst bijdraagt aan de adoptie door te informeren en daarmee onbedoelde afwijkende keuzes te voorkomen (functie = informeren).

3.4.1 Is "pas toe of leg uit" het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

Ja. Op dit moment is het gebruik van STARTTLS in combinatie met DANE bij de overheid nog beperkt. Deze standaarden zijn het meest effectief als alle e-mail servers ze toepassen voor zowel inkomende als uitgaande e-mail. Uitbreiding van het functioneel toepassingsgebied naar uitgaande e-mail servers zal daarom de effectiviteit van STARTTLS en DANE verhogen.

Ook kan uitbreiding van het functioneel toepassingsgebied een stimulerende werking hebben op leveranciers van DANE om de standaard ook voor uitgaand e-mailverkeer te implementeren.

3.4.2 Is de status "aanbevolen" het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

Nee. Het gecombineerde gebruik van STARTTLS en DANE is nog niet de omvang die nodig is om de standaarden als gangbaar te kunnen beschouwen.

3.4.3 Conclusie criteria 'Opname bevordert adoptie'

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.

3.5 Adoptieactiviteiten

Gebruik van de standaard is het einddoel van het Forum Standaardisatie en OBDO. Plaatsing op de lijst met open standaarden is hiervoor een goede stap, maar voor het daadwerkelijk adopteren (implementeren en gebruiken) van de standaard is vaak aanvullende actie benodigd. Aanvullend kan Forum Standaardisatie dan ook bijdragen aan adoptie van de standaard door het actief inzetten van adoptie-instrumenten of ondersteunende acties. Welke kansen zijn er om de adoptie te versnellen en welke drempels bestaan er die de adoptie van de standaard hinderen?

De expertgroep doet het OBDO de aanbeveling om bij de opname op de lijst voor 'pas toe of leg uit' de volgende oproepen ten aanzien van de adoptie van STARTTLS en DANE te doen:

- 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.
- Het Forum Standaardisatie wordt opgeroepen om over een jaar de adoptie van de concurrerende standaard MTA-STS te evalueren.
- 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.
- Organisaties die STARTTLS en DANE toepassen worden opgeroepen de standaarden te implementeren volgens de adviezen van het NCSC[14].
- 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.

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