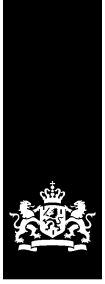


Forum Standaardisatie

Expertadvies STARTTLS en DANE

Datum 16 februari 2016

Colofon

Projectnaam	Expertadvies STARTTLS en DANE
Versienummer	1.0
Locatie	Den Haag
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag forumstandaardisatie@logius.nl
Auteur	Jasmijn Wijn
Onafhankelijk voorzitter	Marc Gill’ard

Inhoud

Forumadvies & Managementsamenvatting

Advies aan het Forum
De expertgroep adviseert het Forum Standaardisatie en het Nationaal Beraad Digitale Overheid om de combinatie STARTTLS en DANE op te nemen op de 'pas toe of leg uit'-lijst. Opname van deze standaarden is wel gebonden aan de voorwaarde dat minimaal twee organisaties binnen het organisatorisch werkingsgebied succesvol de standaarden hebben geïmplementeerd.

Aanvullend wordt geadviseerd om over twee jaar te beoordelen of de combinatie van standaarden ook verplicht zou moeten worden gesteld voor uitgaand e-mailverkeer.

Als functioneel toepassingsgebied 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]

Dit functioneel toepassingsgebied geldt voor alle mailverbindingen buiten de eigen (besloten) infrastructuur. Met andere woorden: de communicatie met mailservers buiten de eigen invloedssfeer. 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.

In diverse baselines zoals de Baseline Informatiebeveiliging Rijksdienst (BIR), Baseline Iinformatiebeveiliging 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 afgedwongen door deze baselines.

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

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 informatie op de facto anonieme wijze worden verzameld. Informatie kan worden geblokkeerd, en onder bepaalde voorwaarden worden aangepast en vervalst.

1 IETF RFC 3207 (https://tools.ietf.org/html/rfc3207), RFC 3848 (https://tools.ietf.org/html/rfc3848) en IETF RFC 7672 (https://tools.ietf.org/html/rfc7672).

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. 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 e-mailserver van de ontvangende partij. De toepassing van STARTTLS in combinatie met DANE kan worden gezien als een 'HTTPS' voor e-mail.

Hoe is het proces verlopen?
Om tot dit advies te komen is op 28 januari 2016 een groep experts bijeengekomen om over het toepassings- en werkingsgebied van STARTTLS en DANE te discussiëren en om de standaarden te toetsen tegen de toetsingscriteria. Dit expertadvies vat de uitkomsten van de discussie en toetsing samen en is als zodanig in openbare consultatie geplaatst.

Hoe scoort de standaard op de toetsingscriteria?

Toegevoegde waarde
De expertgroep concludeert dat de toegevoegde waarde van de standaarden voldoende is. De Nederlandse overheid moet informatie, zowel vertrouwelijk als niet-vertrouwelijk, beschermen tegen afluisteren 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. Door de implementatie van de standaarden ontstaat een relatie tussen e-mailbeheerders en DNS-beheerders. Hoewel deze partijen niet vanzelfsprekend een samenwerkingsrelatie hebben is afstemming tussen deze partijen noodzakelijk. De kosten voor deze afstemming kan per implementatie verschillen. Er zijn geen beveiligings- en privacyrisico's geïdentificeerd aan het implementeren en gebruiken van de standaarden.

Open standaardisatieproces
De expertgroep concludeert 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. Documentatie is kosteloos verkrijgbaar.

Draagvlak
De expertgroep concludeert dat het gebruik op dit moment 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 nog beperkt. Door gebruik van add-ons is het, ondanks de beperkte ondersteuning, wel mogelijk om gebruik te maken van DANE. Er zijn positieve signalen over toekomstige ondersteuning. Met name de uitrol van STARTTLS en DANE door TransIP, een van de grootste hostingproviders van Nederland, is een positief signaal.

Het gebruik van DANE voor inkomende e-mail neemt toe. NCSC, SSC-ICT en de gemeente 's-Hertogenbosch hebben aangegeven gebruik te willen maken van STARTTLS en DANE voor de uitgaande e-mail. SSC-ICT en de gemeente 's-Hertogenbosch hebben aangegeven op korte termijn een een feature request in te dienen bij leverancier Cisco.

Voorwaarde voor opname op de lijst is dat er minimaal twee gebruikers binnen het organisatorisch werkingsgebied gebruik maken van de combinatie STARTTLS en DANE voor inkomend e-mailverkeer.

Opname bevordert de adoptie

De expertgroep concludeert dat opname op de lijst met open standaarden het passende middel is om de adoptie van de standaard binnen de (semi)overheid te bevorderen. Ook kan opname op de lijst met open standaarden, met pas toe of leg uit-verplichting, een stimulerende werking hebben op de ondersteuning door leveranciers van DANE, voor zowel inkomend als uitgaand e-mailverkeer.

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

De expertgroep doet het Nationaal Beraad 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 Platform Internetstandaarden wordt opgeroepen om de combinatie van adoptie van STARTTLS en DANE op te nemen op de website www.internet.nl, de website om internetstandaarden mee te checken.
- 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.
- KING wordt opgeroepen om beveiligingsstandaarden als STARTTLS en DANE op te nemen op de GEMMA Softwarecatalogus.
- Het 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.

1 Doelstelling expertadvies

1.1 Achtergrond

Het gebruik van open standaarden en het voorkomen van vendor lock-in is een van de doelstellingen van de Nederlandse overheid. Dit beleid wordt herbevestigd in actieplan "Open overheid", de digitale agenda 2011-2015, de digitale agenda 2017 en de kabinetsreactie op het rapport Elias. Deze plannen onderstrepen de noodzaak van het zoveel mogelijk meenemen van open standaarden bij het ontwerpen van informatiesystemen.

Een van de maatregelen om de adoptie van standaarden te bevorderen is het beheren van een lijst met standaarden, die vallen onder het principe 'pas toe of leg uit'. Het Nationaal Beraad Digitale Overheid spreekt zich uit over de standaarden die op de lijst zullen worden opgenomen, o.a. op basis van een expertbeoordeling van de standaard. Het Nationaal Beraad wordt geadviseerd door het Forum Standaardisatie. Het Bureau Forum Standaardisatie ondersteunt beide instellingen.

1.2 Doelstelling expertadvies

Onderwerp van dit expertadvies zijn STARTTLS en DANE. DANE is aangemeld voor opname op de 'pas toe of leg uit'-lijst door Michiel Leenaars van NLnet. In het intakegesprek met de indiener 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 op aangeven van de indiener STARTTLS samen met DANE in behandeling genomen.

Doel van dit advies is om, aan de hand van de criteria vast te stellen of STARTTLS en DANE moeten worden opgenomen op de lijst met open standaarden als 'pas toe of leg uit'-standaarden, al dan niet onder bepaalde voorwaarden.

1.3 Doorlopen proces

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

- Door de procesbegeleider is een intakegesprek gevoerd met de indiener op 17 november 2015. Tijdens de intake is de standaard getoetst op uitsluitingscriteria ('criteria voor inbehandelname') en is een eerste inschatting gemaakt van de kansrijkheid van de procedure.
- Op basis van de intake is op 16 december 2015 door het Forum besloten de aanmelding in procedure te nemen. Op basis van dit besluit is een expertgroep samengesteld en een voorzitter aangesteld. Op basis van de aanmelding en de intake is een voorbereidingsdossier opgesteld voor de leden van de expertgroep.
- De expertgroep heeft voorafgaand aan de expertbijeenkomst dit voorbereidingsdossier doorgenomen en aandachtspunten geïdentificeerd.
- Tot slot is de expertgroep op 28 januari 2016 bijeengekomen om de bevindingen in het algemeen en de geïdentificeerde aandachtspunten in het bijzonder te bespreken. Tijdens deze bijeenkomst zijn ook het toepassings- en werkingsgebied vastgesteld.

De uitkomsten van de expertgroep zijn door de begeleider verwerkt in dit adviesrapport. Een eerste conceptversie is aan de leden van de expertgroep gestuurd met het verzoek om een reactie. Na verwerking van deze reacties is het rapport afgerond, nogmaals toegestuurd aan de experts en ingediend bij het Bureau Forum Standaardisatie ten behoeve van de publieke consultatieronde.

1.4 Vervolg

Dit expertadvies zal ten behoeve van een publieke consultatie openbaar worden gemaakt door het Bureau Forum Standaardisatie. Eenieder kan gedurende de consultatieperiode op dit expertadvies zijn/haar reactie geven. Het Bureau Forum Standaardisatie legt vervolgens de reacties voor aan de voorzitter en indien nodig aan de expertgroep.

De uitkomsten uit de expertbijeenkomst en de openbare consultatie liggen vervolgens voor in het Forum Standaardisatie ter besuitvorming. Het Forum zal op basis van het expertadvies en relevante inzichten uit de openbare consultatie een advies aan het Nationaal Beraad opstellen. Het Nationaal Beraad bepaalt uiteindelijk op basis van het advies van het Forum of de de standaard op de 'pas toe of leg uit'-lijst komt.

1.5 Samenstelling expertgroep

Het Forum streeft naar een zo representatief mogelijke expertgroep, met een evenwichtige vertegenwoordiging van (toekomstige) gebruikers (zowel publiek als privaat), leveranciers, wetenschappers en andere kennishebbers. Daarnaast wordt een onafhankelijke voorzitter aangesteld om de expertgroep te leiden en als verantwoordelijke op te treden voor het uiteindelijke expertadvies.

Als voorzitter is opgetreden Marc Gill’ard, directeur bij Verdonck, Klooster & Associates (VKA). Jasmijn Wijn, adviseur bij VKA, heeft de expertgroep in opdracht van het Bureau Forum Standaardisatie begeleid.

Aan de expertbijeenkomst hebben deelgenomen:
- Michiel Leenaars, NLnet (indiener)
- Paddy Verberne, gemeente ’s-Hertogenbosch
- Rolf Sonneveld, Sonnection
- Pieter Rogaar, NCSC
- Pieter Lexis, PowerDNS
- Ralph Dolmans, NLnet Labs
- Marco Davids, SIDN
- Carl Adamse, ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- Loek Kasting, ministerie van Algemene Zaken
- John van Huijgevoort, KING
- Robert van de Rijt, PKI Overheid
- René van Rijn, SSC-ICT
- Onno Hoogeveen, SSC-ICT
- Alwin de Bruin, Measuremail
- Theo van Diepen, Logius

Lancelot Schellevis van het Bureau Forum Standaardisatie was als toehoorder bij de expertbijeenkomst aanwezig. Wietse Venema, Postfix, heeft een schriftelijke bijdrage geleverd.

1.6 Toelichting STARTTLS en DANE

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 één van de beide 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 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 plaatsvinden[2].

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.

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

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.

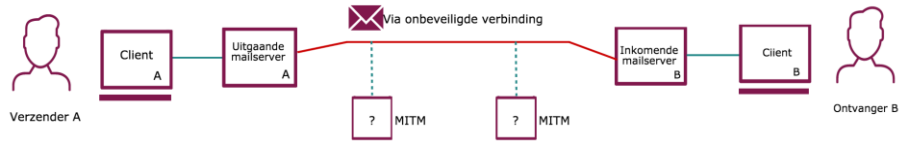
Toepassing van STARTTLS in combinatie met DANE

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. Ook kan informatie worden aangepast. Aanvallers camoufleren hun communicatie met geïnfecteerde netwerken als regulier netwerkverkeer. Ook wordt er gebruik gemaakt van versleuteling om de aard van hun activiteiten te verbergen. De Nederlandse overheid moet vertrouwelijke informatie beschermen tegen afluisteren door aanvallers, zoals cybercriminelen en statelijke actoren. Hieronder valt ook de communicatie tussen overheidspartijen, tussen de overheid en bedrijven, en tussen overheden en burgers. 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.

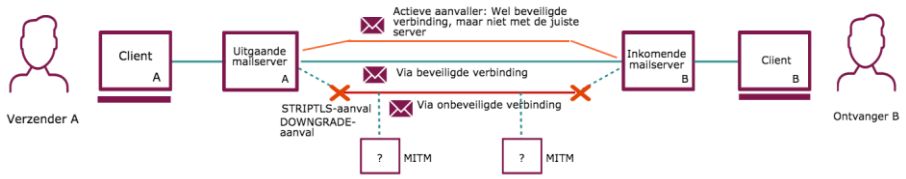
De toepassing van DANE en STARTTLS maakt het mogelijk om een beveiligde verbinding voor e-mailverkeer tot stand te brengen. Hierdoor is het voor aanvallers niet mogelijk om berichtenverkeer 'af te luisteren' of te manipuleren. Door het gebruik van STARTTLS en DANE weet de verzender dat de e-mail daadwerkelijk via een versleutelde verbinding is verstuurd naar een mailserver van de ontvangende partij, zonder dat deze onderweg is onderschept.

Daarnaast biedt het gebruik van DANE de eigenaar van een domein de mogelijkheid om een extra verificatiemiddel, naast de certificaten van 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, conform RFC 7672, 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 afgeweerd.



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

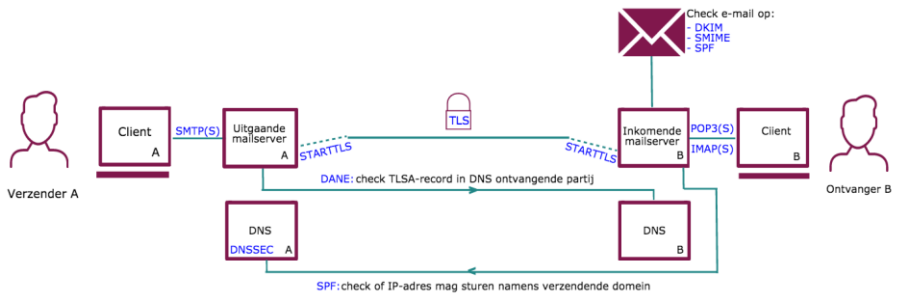


Figuur 2. E-mailverkeer met gebruik van TLS en STARTTLS

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 tot doel heeft om beveiligde verbindingen op de transportlaag over het internet te verzorgen door middel van cryptografie. TLS maakt gebruik van x509. Deze standaard is door het Forum Standaardisatie aanbevolen voor de authenticatie van onder andere servers bij het gebruik van TLS.

DANE maakt direct gebruik van DNSSEC, een standaard voor het registreren en in de Domain Name Server (DNS) publiceren van internet-domeinnamen (zogenaamde 'signing'). Om DANE te kunnen gebruiken is het noodzakelijk dat organisaties DNSSEC hebben geïmplementeerd. S/MIME (Secure Multipurpose Internet Mail Extention) is een standaard voor het coderen van e-mailberichten. Hiervoor wordt gebruik gemaakt van een digitale handtekening (handtekeningcertificaat) voor authenticatie. S/MIME zou als optionele aanvulling gebruikt kunnen worden bovenop de standaarden uit dit advies, om end-to-end beveiliging van berichten te garanderen en de identiteit van de verzendende en ontvangende mailserver te garanderen.



Figuur 4. Relatie STARTTLS en DANE met andere standaarden

1.7 Leeswijzer

In hoofdstuk 2 wordt beschreven in welke gevallen de standaard functioneel gezien gebruikt zou moet worden (functioneel toepassingsgebied) en door welke organisaties deze gebruikt zou moeten worden (organisatorisch werkingsgebied).

Om te bepalen of de standaard opgenomen moet worden op de lijst met standaarden voor 'pas toe of leg uit', is deze getoetst aan een viertal vastgestelde criteria. In hoofdstuk 3 staat het resultaat van deze toetsing.

2 Toepassings– en werkingsgebied

Van overheidsorganisaties wordt verwacht dat zij de lijst met open standaarden hanteren bij aanbestedingstrajecten volgens het 'pas toe of leg uit'-regime. Afhankelijk van de aan te schaffen functionaliteit zal bepaald moeten worden welke koppelvlakken geïmplementeerd moeten worden, en welke standaarden uit de lijst hiervoor ingezet dienen te worden. Om dit te kunnen doen heeft de expertgroep gekeken in welke gevallen de standaard functioneel gezien gebruikt zou moeten worden (functioneel toepassingsgebied), en door welke organisaties deze gebruikt zou moeten worden (organisatorisch werkingsgebied).

2.1 Functioneel toepassingsgebied

Als functioneel toepassingsgebied wordt voorgesteld:
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).[3]

Dit functioneel toepassingsgebied geldt voor alle mailverbindingen buiten de eigen (besloten) infrastructuur. Met andere woorden: de communicatie met mailservers buiten de eigen invloedssfeer. 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.

In diverse baselines zoals de Baseline Informatiebeveiliging Rijksdienst (BIR), Baseline Iinformatiebeveiliging 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 afgedwongen door deze baselines.

2.2 Organisatorisch werkingsgebied

De expertgroep adviseert om het organisatorisch werkingsgebied van de standaard overeen te laten komen met het werkingsgebied waarop het 'pas toe of leg uit'-principe van toepassing is, te weten:
Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-)publieke sector.

3 IETF RFC 3207 (https://tools.ietf.org/html/rfc3207), RFC 3848 (https://tools.ietf.org/html/rfc3848) en IETF RFC 7672 (https://tools.ietf.org/html/rfc7672).

3 Toetsing van standaard aan criteria

Om te bepalen of de standaard opgenomen moet worden op de lijst met open standaarden is deze getoetst aan een aantal criteria. Er zijn vier hoofdcriteria:

1. Toegevoegde waarde
2. Open standaardisatieproces
3. Draagvlak
4. Opname bevordert adoptie

Deze criteria staan beschreven in het rapport, *"Toetsingprocedure en criteria voor indieners en experts"* en staan op de website www.forumstandaardisatie.nl/open-standaarden. Het resultaat van de toetsing zal in dit hoofdstuk per criterium beschreven worden. Voor de volledigheid is tevens de definitie 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 voorzieningen? (toelichtende vraag)
Ja, de standaard is algemeen toepasbaar, ook binnen het werkgebied van de (semi-)overheid. De standaarden hebben betrekking op het tot stand brengen van een beveiligde verbinding tussen servers, waardoor veilige elektronische gegevensuitwisseling zoals e-mail plaats kan vinden vanuit (semi-)overheidsorganisaties richting burgers, bedrijven en andere (semi-)overheidsorganisaties.

3.1.2 Verhoudt de standaard zich goed tot andere standaarden?

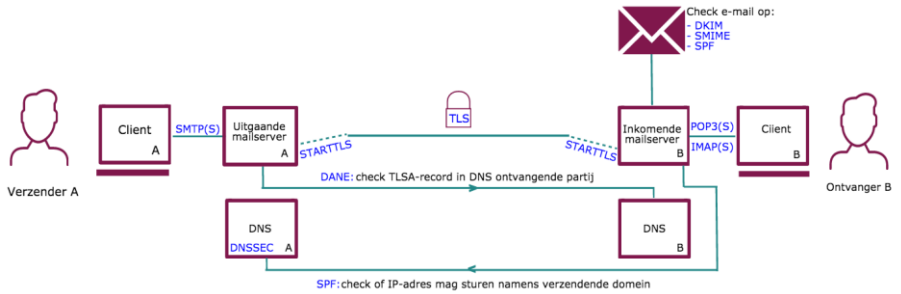
3.1.2.1 Kan de standaard naast of in combinatie met reeds opgenomen standaarden worden toegepast (d.w.z. de standaard conflicteert niet met reeds opgenomen standaarden)?
Ja. STARTTLS maakt naast DANE, gebruik van TLS. TLS is een protocol dat tot doel heeft om beveiligde verbindingen op de transportlaag over het internet te verzorgen door middel van cryptografie. DANE maakt direct gebruik van DNSSEC, een standaard voor het valideren van in de Domain Name Server (DNS) gepubliceerde records. Om DANE te kunnen gebruiken is het noodzakelijk dat organisaties DNSSEC hebben geïmplementeerd.

S/MIME (Secure Multipurpose Internet Mail Extention) is een standaard voor het coderen van e-mailberichten. Hiervoor wordt gebruik gemaakt van een digitale handtekening (handtekeningcertificaat) en het versleutelen van het bericht.

Daarnaast kennen de standaarden samenhang met e-mailstandaarden die als doel hebben misbruik van de domeinnaam middels e-mail te verminderen en/of te voorkomen: DKIM, SPF en DMARC. DKIM koppelt een e-mail aan een domeinnaam met behulp van een digitale handtekening. SPF controleert of een e-mailserver gerechtigd is om namens het opgegeven e-maildomein e-mail te verzenden.

STARTTLS en DANE zorgen er voor dat de verbindingen waarover de e-mails worden verstuurd ook beveiligd zijn. De standaarden bieden echter niet de garantie dat end-to-end niet afgeluisterd kan worden.

STARTTLS en DANE conflicteren niet met bovengenoemde standaarden.



Figuur 5. Relatie STARTTLS en DANE met andere standaarden

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, er zijn geen standaarden met een overlappend functioneel toepassingsgebied gevonden die reeds opgenomen zijn.

3.1.2.3 *Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname? (toelichtende vraag)*
Niet van toepassing, er zijn geen concurrerende standaarden gevonden.

3.1.2.4 *Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden? (toelichtende vraag)*
Ja, STARTTLS en DANE worden beheerd door de Internet Engineering Task Force (IETF). IETF is een internationale standaardisatieorganisatie voor internetstandaarden. IETF beheert onder andere ook DKIM, SPF en DNSSEC. DMARC wordt naar verwachting op korte termijn in beheer genomen door IETF.

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, zowel STARTTLS als DANE zijn eenvoudige, niet-ambigue standaarden waar geen lokale profielen voor nodig zijn. Wel is het noodzakelijk om op organisatorisch niveau af te stemmen tussen onder andere de e-mailbeheerder en de DNS-beheerder. Zie hiervoor paragraaf 3.1.3.3.

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?
Het Forum staat voor betrouwbare berichtenuitwisseling. Dit is belangrijk gezien het feit dat met de toenemende digitalisering ook de dreiging van digitale aanvallen toeneemt. Via digitale (economische) spionage kan in een kort tijdsbestek grote hoeveelheden informatie op grotendeels anonieme en simultane wijze verzameld. Ook kan informatie worden aangepast. De Nederlandse overheid moet vertrouwelijke informatie beschermen tegen afluisteren door aanvallers, zoals vijandelijke partijen en statelijke actoren. Hieronder valt ook de communicatie tussen overheidspartijen, tussen de overheid en bedrijven, en tussen overheden en burgers.

De toepassing van STARTTLS en DANE maakt het mogelijk om een beveiligde verbinding voor e-mailverkeer tot stand te brengen. Hierdoor is het voor aanvallers niet mogelijk om berichtenverkeer 'af te luisteren' of te manipuleren. Door het gebruik van STARTTLS en DANE weet de verzender dat de e-mail is verstuurd naar een mailserver van de ontvangende partij.

3.1.3.2 Draagt de standaard bij aan het voorkomen van een vendor lock-in (leveranciersafhankelijkheid)?
Ja, de standaarden zijn vrij beschikbaar. Een aantal leveranciers biedt ondersteuning bij de implementatie van STARTTLS en DANE.

3.1.3.3 Wegen de overheidsbrede en maatschappelijke baten voor de informatievoorziening en de bedrijfsvoering op tegen de kosten?
De kosten om de standaarden technisch te implementeren zijn gering. STARTTLS heeft geen onderhoud of beheer nodig, het beheer zit in TLS. Voor de implementatie van DANE is geen additionele infrastructuur nodig die tot extra beheerslast leidt. Bij een wijziging van x509-certificaten kan het nodig zijn om nieuwe informatie in de DNS te plaatsen. Dit kan geautomatiseerd worden door het gebruik van een tool als hash-slinger en Ldns-dane. Aan de validerende kant vergt het gebruik van DANE, naast het valideren van DNSSEC getekende antwoorden, eveneens geen actief beheer.

Voorafgaand aan de implementatie van STARTTLS en DANE dient op organisatorisch niveau afgestemd te worden tussen onder andere de e-mailbeheerder en de DNS-beheerder. Zij moeten bijvoorbeeld afstemmen over de toevoeging en het onderhoud van DANE-records in de DNS. Deze partijen hebben niet vanzelfsprekend een samenwerkingsrelatie. De kosten voor deze afstemming kan per implementatie verschillen. Ook andere standaarden die al op de lijst met open standaarden staan, zoals

DKIM en SPF, vergen een dergelijke samenwerkingsrelatie. Als deze standaarden al succesvol zijn ingevoerd, bestaat deze relatie al. Aanvullende kosten zijn dan niet ete verwachten.

Daarnaast zijn er ook andere kosten te benoemen, namelijk de kosten van add-ons om te kunnen werken met STARTTLS en DANE. Dit is het geval wanneer het e-mailpakket de standaarden niet *native* ondersteund.

3.1.3.4 Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel?
Niet van toepassing, er zijn geen specifieke beveiligingsrisico's geïdentificeerd.

3.1.3.5 Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel?
Niet van toepassing, er zijn geen specifieke privacyrisico's geïdentificeerd

3.1.4 Conclusie criteria 'Toegevoegde waarde'
De expertgroep concludeert dat de toegevoegde waarde van de standaarden voldoende is. De Nederlandse overheid moet vertrouwelijke informatie beschermen tegen afluisteren 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. 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. Er zijn geen beveiligings- en privacyrisico's geïdentificeerd.

3.2 Open standaardisatieproces

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

Beide standaarden zijn in beheer bij de Internet Engineering Task Force (IETF).

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 onacceptabele belemmeringen (zoals te hoge kosten en te hoge lidmaatschapseisen)?
Ja, de specificatiedocumenten zijn gratis te downloaden via de website van IETF.[4] Ook niet-gebruikers kunnen de specificaties downloaden.

3.2.1.2 Is de documentatie over het ontwikkel- en beheerproces (bijv. het voorlopige specificatiedocument, notulen en beschrijving besluitvormingsprocedure) beschikbaar zonder dat er sprake is van onacceptabele belemmeringen (zoals te hoge kosten en te hoge

4 https://www.ietf.org/rfc/rfc3207.txt
https://tools.ietf.org/html/rfc3848
https://tools.ietf.org/html/rfc7672

lidmaatschapseisen)?
Ja, de documentatie over het ontwikkel- en beheerproces is gratis en voor iedereen te downloaden via de website van IETF. De specificatiedocumenten zijn gepubliceerd op de website van IETF.

Specificaties doorlopen in het standaardisatieproces van IETF twee stadia van volwassenheid: 'proposed standard' en 'internet standard'. De voortgang van door IETF beheerde standaarden in dit proces is transparant en kosteloos te volgen via de RFC's van de standaarden. RFC 3207 en 7672 zijn proposed standards.

Overige documentatie zoals notulen van bijeenkomsten en besluiten zijn ook kosteloos beschikbaar op de website van IETF.

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 m.b.t. bijvoorbeeld eventuele patenten- onherroepelijk royalty-free voor eenieder beschikbaar?
De Intellectual Property Rights (IPR) van IETF is vastgelegd in RFC3979. Hierin staat dat leden van de werkgroep van een specifieke standaard bestaande en relevante IPR moeten bekendmaken. Voor STARTTLS en DANE zijn geen IPR geclaimd.

3.2.2.2 Garandeert de standaardisatieorganisatie dat partijen die bijdragen aan de ontwikkeling van de standaard hun intellectueel eigendomsrecht onherroepelijk royalty-free voor eenieder beschikbaar stellen?
Dat er bij inbeheername van standaarden door IETF geen IPR is geclaimd geeft geen garantie over toekomstige claims met betrekking tot het intellectueel eigendom.

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)?
Ja, verschillende werkgroepen werken aan de (door)ontwikkeling van IETF-standaarden. Samenwerking binnen deze werkgroepen vindt veelal plaats via e-mail. Belanghebbenden zoals gebruikers, leveranciers, adviseurs en wetenschappers kunnen zich via de website van IETF aanmelden voor de mailinglijsten van werkgroepen. Hier zijn geen (lidmaatschaps)kosten aan verbonden.

3.2.3.2 Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen?
Ja, het standaardisatieproces van IETF maakt gebruik van een besluitvormingsprocedure via het principe van 'rough consensus', waarbij de dominante mening van een groep, zoals door de voorzitter vastgesteld, de basis voor een beslissing vormt.

3.2.3.3 Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde procedure?
Ja, binnen de werkgroepen kunnen belanghebbenden bezwaren kenbaar maken. Buiten de werkgroepen kan bezwaar worden aangetekend bij de leden van de Internet Engineering Steering Group (IESG).

3.2.3.4 Organiseert de standaardisatieorganisatie regelmatig overleggen met

belanghebbenden over doorontwikkeling en beheer van de standaard?
Ja, belanghebbenden kunnen zich aanmelden voor werkgroepen die werken aan de doorontwikkeling van standaarden. Er wordt veelvuldig gebruik gemaakt van mailingslists waarvoor een ieder zich kan aanmelden.

3.2.3.5 *Organiseert de standaardisatieorganisatie een publieke consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld?*
Ja, IETF werkt met RFC's, het standaard publicatieformaat voor Internet Standaarden van IETF. Voordat een nieuwe RFC van een standaard wordt geaccordeerd, wordt door een werkgroep van deze standaard een zogeheten open comments proces georganiseerd waarbij belanghebbenden commentaar kunnen leveren over de (nieuwe versie van de) standaard.

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?*
Ja, IETF is een onafhankelijke organisatie zonder winstoogmerk.

3.2.4.2 *Is de financiering van de ontwikkeling en het onderhoud van de standaard voor tenminste drie jaar gegarandeerd?*
De financiering van de ontwikkeling en het onderhoud van de standaard wordt verzorgd door de leden van de werkgroep waar de standaarden onder vallen. IETF bestaat bijna 30 jaar en heeft zich in het verleden bewezen als stabiele standaardisatieorganisatie. De expertgroep is om deze reden van mening dat de continuïteit van de financiering voor IETF-standaarden hierdoor voldoende is gewaarborgd.

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

3.2.5.1 *Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot versiebeheer van de standaard? (met o.a. aandacht voor migratie van gebruikers)*
Ja, de inhoud van eerdere versies van IETF-standaarden is terug te lezen op de website van IETF. In de verschillende RFC's van een standaard is aandacht voor de implementatie van een standaard.

3.2.5.2 *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?*
Ja en nee. Het standaardisatieproces van IETF is transparant en inzichtelijk voor iedereen. Omdat de (door)ontwikkeling van standaarden in de handen ligt van een community van IETF, en er nauwelijks ervaring is met de standaarden wordt aangeraden om nieuwe versies te toetsen alvorens op de nemen op de lijst.

3.2.5.3 *Is het belang van de Nederlandse overheid voldoende geborgd bij de ontwikkeling en het beheer van de standaard?*
Voor zover bekend heeft de Nederlandse overheid geen betrokkenheid gehad bij de ontwikkeling of het beheer van de standaard. De Nederlandse overheid kan zich, indien gewenst, aanmelden voor deelname aan de werkgroepen.

3.2.6 *Conclusie criteria 'Open standaardisatieproces'*
De expertgroep concludeert 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. Documentatie is kosteloos verkrijgbaar.

3.3 Draagvlak

Aanbieders en gebruikers moeten voldoende ervaring hebben bij het ondersteunen, implementeren en gebruiken van de standaard.

3.3.1 Bestaat er voldoende marktondersteuning voor de standaard?

3.3.1.1 Bieden meerdere leveranciers ondersteuning voor de standaard?
Ja, met betrekking tot gebruik ondersteunt een groot aantal (web)mailproviders 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 is op dit moment bezig om een terugval op een niet-beveiligde verbinding inzichtelijk te maken in de interface van Gmail.

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 gebruik maken van STARTTLS en DANE. Dit geldt (nog) niet voor het verzenden van e-mail, waardoor een verplichting van het gebruik van de standaarden voor STARTTLS en DANE niet van toepassing is. Hoewel er voldoende ondersteuning is voor STARTTLS is dit voor DANE nog niet het geval. Dit kan opgelost worden door Open Source add-ons toe te voegen. Hierdoor is het mogelijk om wel gebruik te maken van DANE.

TransIP, een van de grotere hostingproviders van Nederland, is STARTTLS en DANE aan het uitrollen voor hun webhostingdomeinen (250.000+). Hierdoor kunnen de meeste overheidspartijen STARTTLS en DANE toepassen voor inkomend e-mailverkeer.

3.3.1.2 Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen?
Ja, er zijn open source tools beschikbaar voor het aanmaken van DANE-records, waaronder hash-slinger (Redhat) en Ldns-dane (NLnet Labs). Daarnaast zijn er 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 niet mogelijk om de conformiteit te toetsen. De experts adviseren om DANE als standaard toe te voegen aan www.internet.nl

3.3.1.3 Zijn er referentieprofielen van de standaard aanwezig en zijn deze referentieprofielen vrij te gebruiken?
De eerder genoemde open source tools hash-slinger en Ldns-dane genereren automatisch correcte DANE-records. Deze tools zijn vrij te gebruiken.

3.3.2 Kan de standaard rekenen op voldoende draagvlak?

3.3.2.1 Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt?
De standaarden worden in combinatie momenteel in Nederland gebruikt door onder andere Netlabs, NLnet en het Forum Standaardisatie. Meerdere overheidsorganisaties gebruik van STARTTLS voor inkomende

mail, waaronder SURFnet, 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.

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

3.3.2.3 Is de aangemelde versie backwards compatible met eerdere versies van de standaard?
Niet van toepassing, zie paragraaf 3.3.2.2.

3.3.2.4 Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?
NCSC heeft aangegeven STARTTLS en DANE op korte termijn te implementeren. SSC-ICT en de gemeente 's-Hertogenbosch, hebben bij Cisco een feature request ingediend voor de ondersteuning van de combinatie STARTTLS en DANE.

3.3.3 Conclusie criteria 'Draagvlak'
De expertgroep concludeert dat het gebruik 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 nog beperkt. Zodoende wordt geadviseerd om het toepassingsgebied vooralsnog alleen voor inkomende e-mail te laten gelden. De experts adviseren om over twee jaar de adoptie van STARTTLS en DANE voor uitgaande e-mail te toetsen. Op basis van dit onderzoek kan geadviseerd worden het verplichte toepassingsgebied breder te maken.

Door gebruik van add-ons is het, ondanks de beperkte ondersteuning, wel mogelijk om gebruik te maken van DANE. Er zijn positieve signalen over toekomstige ondersteuning. Met name de uitrol van STARTTLS en DANE door TransIP, een van de grootste hostingproviders van Nederland, is een positief signaal.

Het gebruik van DANE voor inkomende e-mail neemt toe. NCSC, SSC-ICT en de gemeente 's-Hertogenbosch hebben aangegeven gebruik te willen maken van STARTTLS en DANE voor de uitgaande e-mail. SSC-ICT en de gemeente 's-Hertogenbosch hebben aangegeven op korte termijn een een feature request in te dienen bij leverancier Cisco.

Voorwaarde voor opname op de lijst is dat er minimaal twee gebruikers binnen het organisatorisch werkingsgebied gebruik maken van de combinatie STARTTLS en DANE voor inkomend e-mailverkeer.

3.4 Opname bevordert adoptie

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

Er zijn twee lijsten: de lijst met gangbare standaarden en de lijst voor 'pas toe of leg uit'. Deze laatste lijst is bedoeld om standaarden een extra stimulans te geven wanneer:

1. Hun huidige adoptie binnen de (semi-)overheid beperkt is;
2. Opname bijdraagt aan de adoptie door te stimuleren o.b.v. het 'pas toe of leg uit' regime.

De lijst met gangbare standaarden vormt een referentie voor standaarden die veel gebruikt worden. Als standaarden voldoen aan enkele basisvoorwaarden (voor o.a. openheid), er is geen discussie over en de standaarden worden breed gebruikt, dan vindt opname op die lijst plaats.

3.4.1 Is opname op de lijst met open standaarden, met pas toe of leg uit-verplichting, het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

Ja. Gezien het feit dat het gebruik van de combinatie STARTTLS en DANE binnen de (semi)overheid nog beperkt is, kan de 'pas toe of leg uit'-verplichting de adoptie van de standaarden bevorderen. Ook kan opname op de lijst met open standaarden een stimulerende werking hebben op de ondersteuning door leveranciers van DANE, voor zowel inkomend als uitgaand e-mailverkeer.

3.4.2 Is opname op de lijst met gangbare open standaarden 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 opname op de lijst met open standaarden het passende middel is om de adoptie van de standaard binnen de (semi)overheid te bevorderen. Ook kan opname op de lijst met open standaarden, met pas toe of leg uit-verplichting, 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 en College. Plaatsing op de lijsten 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 Nationaal Beraad 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 Platform Internetstandaarden wordt opgeroepen om de combinatie van adoptie van STARTTLS en DANE op te nemen op de website www.internet.nl, de website om internetstandaarden mee te checken.
- 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.
- KING wordt opgeroepen om beveiligingsstandaarden als STARTTLS en DANE op te nemen op de GEMMA Softwarecatalogus.
- Het 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.