Forum Standaardisatie
www.forumstandaardisatie.nl
forumstandaardisatie@logius.nl
Bureau Forum Standaardisatie
gehuisvest bij Logius
Postadres
Postbus 96810
2509 JE Den Haag
Bezoekadres
Wilhelmina van Pruisenweg 52
2595 AN Den Haag
Bij bezoek aan Logius is legitimatie verplicht

notitie

FORUM STANDAARDISATIE

Agendapunt:	FS 160608.3D		
Betreft:	Aanvullend onderzoek SMTP STS		
Aan:	Forum Standaardisatie		
Van:	Stuurgroep Standaardisatie		
Datum:	13 mei 2016	**Versie**	1.0

Aanleiding en achtergrond
Tijdens de openbare consultatie van STARTTLS en DANE is een voorstel voor een nieuwe standaard ingediend bij de Internet Engineering Task Force (IETF), ondersteund door de grotere mailplatformen (Gmail, Yahoo, Microsoft). Het voorstel beschrijft een standaard voor de totstandkoming van versleutelde verbindingen tussen mailservers, waarbij het gebruik van DNSSEC niet noodzakelijk is. Deze (concept)standaard kan gezien worden als potentiële concurrent van DANE, en kan een grote impact hebben op de adoptie van STARTTLS en DANE. Het Forum Standaardisatie heeft zodoende de opdracht gegeven om aanvullend onderzoek te doen naar SMTP STS en de impact hiervan alvorens een besluit te nemen over de opname van de combinatie STARTTLS en DANE op de lijst met open standaarden.

Betrokkenen en proces
In dit onderzoek is gekeken naar het voorstel voor de standaard SMTP STS, zoals eind maart ingediend bij IETF. Ook is het voorstel beoordeeld tegen de toetsingscriteria voor de lijst met open standaarden. Deze notitie geeft de uitkomsten van dit onderzoek kort weer en sluit af met een advies aan het Forum Standaardisatie. Een eerste conceptversie van dit advies is aan de leden van de expertgroep STARTTLS en DANE en het Bureau Forum Standaardisatie gestuurd met het verzoek om een reactie op het advies. Na verwerking van deze reacties is het advies ingediend bij het Bureau Forum Standaardisatie.

Consequenties en vervolgstappen
Naar aanleiding van het onderzoek kan geconcludeerd worden dat SMTP STS en de combinatie STARTTLS en DANE een overlappend functioneel toepassingsgebied hebben. Het voorstel voor SMTP STS is echter nog conceptueel en het ontwerp voor de standaard is (nog) niet waterdicht. Gezien deze factoren wordt het Forum Standaardisatie geadviseerd om de ontwikkelingen omtrent SMTP STS in de gaten houden, maar de besluitvorming omtrent de opname van STARTTLS en DANE wel voort te zetten. Mede gezien het belang van de standaarden.

-

Gevraagd besluit

Datum
27 mei 2016

Het Forum Standaardisatie wordt gevraagd om:
1. kennis te nemen van de standaard SMTP STS;
2. kennis te nemen van de beoordeling van SMTP STS op de toetsingscriteria;
3. in te stemmen met het advies om de ontwikkelingen rondom SMTP STS in de gaten te houden en de besluitvorming omtrent de opname van STARTTLS en DANE voort te zetten.

Ad 1 SMTP STS
Het voorstel voor STMP STS is eind maart 2016 als Internet Draft bij de Internet Engineering Task Force (IETF) ingediend en is geldig tot 20 september 2016. Het huidige voorstel is voor een breed publiek beschikbaar voor informele beoordeling en becommentariëring. Internet Drafts hebben geen formele status, en kunnen op elk moment gewijzigd of verwijderd worden.

SMTP Strict Transport Security (SMTP STS) is een standaard voor het opzetten van versleutelde verbindingen tussen mailservers met als doel het upgraden van een onbeveiligde verbinding over een onvertrouwd netwerk naar een versleutelde verbinding over een onvertrouwd netwerk. Voor deze SMTP STS verbindingen is het niet verplicht om DNSSEC te gebruiken, maar het is wel mogelijk. STMP STS werkt voor zowel verzendende als ontvangende mailservers.

Ontvangende mailservers moeten voor elk van de e-domeinnaam een STS-beleid in een DNS-record publiceren. Het STS-record geeft dan kort gezegd aan welke acties uitgevoerd moeten worden in een bepaalde periode. In dit STS-record wordt de volgende informatie gepubliceerd:
- de vraag of e-mail van de domeinnaam alleen via TLS mag worden verzonden,
- een lijst met hostnamen van mailservers die e-mail voor het betreffende domein mogen ontvangen,
- het beleid voor het te gebruiken authenticatiemechanisme (via web PKI of DNSSEC),
- het certificaat voor het gebruikte authenticatiemechanisme (via web PKI of DANE),
- de (geldigheids)duur van dit beleid. Dit is de termijn waarbinnen mailservers het beleid moeten hanteren,
- optioneel: een e-mailadres waar verzendende mailservers geaggregeerde feedback kunnen verzenden, bijvoorbeeld over foutmeldingen.

Verzendende mailservers moeten het STS-beleid van de ontvangende mailserver controleren. Het hiervoor voorgestelde proces bij het verzenden van een e-mail is als volgt:
1. de verzendende mailserver controleert of er op de server al een beleid van de ontvangende mailserver bekend is. Als dit niet het geval is kan het beleid via de Domain Name Server (DNS) worden opgehaald,
2. de verzendende mailserver valideert de ontvangende mailserver. Als de ontvangende mailserver 'geldig' is kan de e-mail worden afgeleverd,
3. Als de ontvangende mailserver niet geldig is dient op basis van het STS-beleid een van de volgende acties uitgevoerd te worden:
   a. het versturen van een rapportage aan de ontvangende mailserver over de mislukte poging om de e-mail via een TLS-verbinding af te leveren. De e-mail wordt wel verzonden,

b. wanneer in het beleid gespecificeerd is dat e-mail alleen via een TLS-verbinding verzonden mag worden dient (via de DNS) gecontroleerd te worden of er nieuw beleid beschikbaar is. Indien dit het geval is kan het nieuwe beleid worden geauthenticeerd en het oude beleid overschreven. Vervolgens kan opnieuw worden geprobeerd de e-mail te verzenden (vanaf stap 1). Als deze nieuwe poging niet slaagt wordt de e-mail niet verzonden. De verzendende mailserver informeert de ontvangende partij per e-mail over de mislukte afleverpoging.

SMTP STS versus DANE in combinatie met STARTTLS[1]

Het doel van SMTP STS met het STS-beleid en het DANE TLSA-record is hetzelfde: het upgraden van een onbeveiligde verbinding over een onvertrouwd netwerk (opportunistische encryptie) naar een versleutelde verbinding over een onvertrouwd netwerk (verplichte encryptie). Hierdoor is het voor aanvallers niet meer mogelijk om berichtenverkeer 'af te luisteren' of te manipuleren.

Beide standaarden maken voor de authenticatie van de verzendende en de ontvangende partij gebruik van gepubliceerde certificaten die door certificaatautoriteiten (CA's) binnen het PKI-stelsel zijn uitgegeven. Aanvullend maakt DANE het mogelijk om door middel van een met DNSSEC beveiligd DNS-record extra informatie bovenop de offline certificaten uit te reiken. Dit DNS-record kan worden gezien als een digitale vingerafdruk. SMTP STS maakt naast de eerder genoemde certificaten gebruik van Trust-on-First-Use (TOFU-principe) om onderschepping te voorkomen. Dit principe houdt in dat wanneer een verzendende mailserver voor de eerste keer een verbinding op wil zetten met een nieuwe ontvangende mailserver, de verzendende mailserver wordt gevraagd om een 'sleutel' te accepteren, op te slaan en voor een bepaalde periode te gebruiken. Bij toekomstige verbindingen kan, voor de in het beleid bepaalde periode, door middel van deze sleutel de ontvangende mailserver geauthenticeerd worden. Wanneer de sleutel is veranderd wordt een waarschuwing gegeven. Nadeel van deze methode is dat de 'sleutel' voor elke unieke verbinding opgeslagen moet worden. Dit is met name voor kleinere mailproviders een intensief proces. Daarnaast kan de sleutel bij de eerste verbinding gemanipuleerd worden, waardoor het voor de verzendende mailserver lijkt alsof hij verbonden is met de juiste mailserver, maar dit in werkelijkheid niet is. Hierdoor kan de standaard een vals gevoel van veiligheid geven.

Aanvullend biedt SMTP STS een mechanisme voor fout-rapportages. Dit maakt het mogelijk om bijvoorbeeld misbruik inzichtelijk te maken. Nadeel is echter dat deze rapportageberichten via de onbeveiligde verbinding worden gestuurd, en zodoende ook gemanipuleerd kunnen worden.

Bij het gebruik van RFC 7672 (DANE over SMTP/STARTTLS) wordt afgeraden om e-mail te versturen wanneer geen beveiligde verbinding tot stand kan worden gebracht. Het voorstel voor SMTP STS doet hier geen uitspraak over.

[1] IETF RFC 7672 (https://tools.ietf.org/html/rfc7672).

	Voordelen	Nadelen
DANE over SMTP/STARTTLS	– Gestandaardiseerd. – Kan direct gebruikt worden – Geen additionele hardware nodig bij gebruik. – Directe koppeling tussen verzendende en ontvangende mailserver.	– Vereist gebruik van DNSSEC. – Nog niet door alle grote Amerikaanse mailproviders geadopteerd.
SMTP STS	– Ondersteunt door grote Amerikaanse mailproviders – Vereist geen werkende DNSSEC-implementatie. – Mechanisme voor foutrapportage.	– Standaard is nog in ontwikkeling. – Bij eerste contact kan de sleutel onderschept en/of gemanipuleerd worden. – Organisaties kunnen zelf bepalen of e-mails over een onbeveiligde verbinding mogen worden verstuurd. – Extra webserver (met PKI-certificaat) naast DNS en mailserver noodzakelijk. – Beheerlast voor kleine(re) mailproviders is groot (door policy caching).

Ad 2 Beoordeling SMTP STS op toetsingscriteria

Toegevoegde waarde
SMTP STS kent een overlappend functioneel toepassingsgebied met STARTTLS en DANE. Overigens kunnen de standaarden wel naast elkaar gebruikt worden en zijn ze technisch niet met elkaar in conflict:
Inkomende en verzendende mailservers passen SMTP STS en bijbehorend beleid toe zodat er een versleutelde verbinding over een onvertrouwd netwerk (zoals internet) opgezet kan worden. Dit voorkomt dat aanvallers het mailverkeer kunnen afluisteren (passieve aanvallers) en/of kunnen manipuleren (actieve aanvallers).

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 worden 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.

Een organisatie is in de meeste gevallen zowel verzendende partij als ontvangende partij. Dit betekent dat een organisatie als ontvangende partij een STS-beleid moet opstellen en publiceren en dat de verzendende partij dit beleid moet opvolgen. Dit betekent voor een verzendende partij dat het beleid van de ontvangende partij opgevraagd en opgeslagen moet worden. Daarbij moet de verzendende partij, afhankelijk van de (geldigheids)duur van het beleid, periodiek het beleid updaten. Dit is voor met name kleinere mailproviders een intensief proces, aangezien zij een kleinere doelgroep bedienen en daardoor niet dagelijks met alle mailservers wereldwijd communiceren.

Een nadeel van SMTP STS is dat de werking van de standaard niet volledig waterdicht is. De sleutel kan bij de eerste verbinding gemanipuleerd worden, waardoor het voor verzendende mailservers lijkt alsof hij verbonden is met dit juiste mailserver, maar dit in werkelijkheid niet is. Dit kan een vals gevoel van veiligheid geven. Daarnaast kan door het gebruik van hierboven beschreven TOFU-principe misbruik ongemerkt blijven.

In tegenstelling tot de combinatie van STARTTLS en DANE stelt SMTP STS het gebruik van DNSSEC niet verplicht. Gebruikers kunnen voor de authenticatie van mailservers kiezen om dit door middel van WebPKI (X509-standaard) of DNSSEC te doen. Het gebruik van DNSSEC heeft in Nederland met name bij de ontvangende kant nog geen grote omvang. Uit onderzoek van SIDN in 2012 is gebleken dat de implementatie van DNSSEC belemmert wordt door het gebrek aan kennis bij registrars[2], gebrek aan vraag bij eindgebruikers, gebrek aan goede ondersteuning in de software en userinterfaces en investerings- en operationele kosten[3]. Hierdoor is best de kans dat ontvangende partijen die SMTP STS willen implementeren zullen kiezen voor authenticatie door middel van WebPKI. Dit zou zodoende kunnen leiden tot een stagnatie van het gebruik van DNSSEC.

Open standaardisatieproces
De standaard SMTP STS is op dit moment enkel nog een papieren voorstel en geen werkende standaard. De standaard is zodoende ook nog niet in beheer bij een standaardisatieorganisatie. Het voorstel voor SMTP STS is eind maart als Internet Draft ingediend bij de Internet Engineering Task Force (IETF) door de grotere Amerikaanse e-mailproviders (Google, Yahoo, Microsoft e.a.) en is geldig tot 20 september 2016. Het huidige voorstel is voor een breed publiek beschikbaar voor informele beoordeling en becommentariëring. Internet Drafts hebben geen formele status, en kunnen op elk moment gewijzigd of verwijderd worden.

Tijdens eerdere toetsingsprocedures is geconcludeerd dat het standaardisatieproces van IETF voldoende open is. IETF kent goed gedocumenteerde en open beheerprocedures die gratis zijn de downloaden op de website van IETF. Er is geen lidmaatschap, het beheerproces en de besluitvorming hieromtrent is open en transparant. Belanghebbenden kunnen zich kosteloos aanmelden voor de diverse groepen die werken aan de (door)ontwikkeling van standaarden die bij IETF in beheer zijn. IETF is een internationale standaardisatieorganisatie die onder andere ook DKIM, SPF, DNSSEC, STARTTLS & DANE (RFC 7672) en TLS in beheer heeft.

[2] Een registrar is een bedrijf dat in opdracht van bedrijven, instellingen of personen een domeinnaam registreert.
[3] https://www.dnssec.nl/cases/gebrek-aan-kennis-is-belangrijkste-belemmering-voor-implementatie-dnssec.html.

Draagvlak
SMTP STS is op dit moment nog een papieren voorstel. Hierdoor hebben aanbieders en gebruikers nog geen ervaring op kunnen doen met het ondersteunen, implementeren en gebruiken van de standaard. Er zijn op dit moment geen (positieve) signalen over het gebruik van de standaard op korte termijn.

Het voorstel voor de standaard is opgesteld door medewerkers van een aantal (grote) (web)mailproviders, namelijk Google (Gmail), Microsoft (Outlook en Live) en Yahoo. Deze mailproviders bedienen wereldwijd een groot aantal gebruikers.

Opname bevordert adoptie
Dit is niet expliciet getoetst, maar er is geen wettelijke verplichting tot het gebruik van de standaard. Gezien het gegeven dat de standaard feitelijk gezien nog niet bestaat is het niet mogelijk om uitspraak te doen of opname de adoptie bevordert. Wel kan opname op de lijst de adoptie van DNSSEC belemmeren.

Ad 3 Advies
Afgaand op het voorstel voor SMTP STS en de toetsing van de standaard op de toetsingscriteria is een aantal conclusies te trekken:
- het is goed nieuws dat grote mailproviders bezig zijn met de beveiliging van e-mailverkeer,
- SMTP STS is echter vooral bedoeld voor grote (Amerikaanse) mailproviders. Voor kleine(re) mailproviders is het gebruik van de standaard een intensief, en daarmee kostbaar proces,
- het voorstel voor SMTP STS is nog niet op alle onderdelen volledig uitgewerkt of dekkend,
- het ontwerp van SMTP STS is niet waterdicht. Het is mogelijk om bij de totstandkoming van de eerste verbinding de sleutel te manipuleren, waardoor ook berichtenverkeer kan worden gemanipuleerd,
- de introductie van SMTP STS kan mogelijk het gebruik van de combinatie STARTTLS en DANE negatief beïnvloeden al conflicteren de standaarden technisch niet met elkaar,
- de introductie van SMTP STS kan een negatieve invloed hebben op de implementatie van DNSSEC.
- het is op dit moment niet duidelijk of, en wanneer, SMTP STS een officiële standaard wordt.

Gezien de huidige premature status van het voorstel van de standaard is het voor de overheid niet wenselijk om een afwachtende houding aan te nemen. STARTTLS EN DANE zijn beide ontwikkelde standaarden in beheer bij een gerenommeerde standaardisatieorganisatie en kunnen daadwerkelijk al geïmplementeerd worden. Opname van STARTTLS in combinatie met DANE maakt het mogelijk om e-mailverkeer tussen overheden, tussen overheden en bedrijven en tussen overheden en burgers via een versleutelde verbinding mogelijk te maken. Ook is opname op de lijst een stimulans voor mailproviders om DANE en DNSSEC te ondersteunen.

Het Forum Standaardisatie wordt daarnaast geadviseerd om de ontwikkelingen rondom SMTP STS in de gaten te houden. Wanneer SMTP STS een ontwikkelde standaard is dient de relatie tussen SMTP STS en STARTTLS en DANE opnieuw geduid te worden om een meer omvattend beeld te kunnen schetsen. Het advies is dan ook om deze ontwikkeling nauw te volgen en waar mogelijk te participeren in de doorontwikkeling van de standaard. De aangewezen partij hiervoor is het NCSC, conform haar Cyber Security strategie[4].

Betrokken personen bij de totstandkoming van dit advies

- Experts betrokken bij de toetsing van STARTTLS en DANE.

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