Forum Standaardisatie

# Expertadvies TLS 1.3

Datum 3 augustus 2018

# Colofon


| | |
|---|---|
| Projectnaam | Expertadvies TLS 1.3 |
| Versienummer | 1.0 |
| Locatie | Den Haag |
| Organisatie | Forum Standaardisatie<br>Postbus 96810<br>2509 JE Den Haag<br>forumstandaardisatie@logius.nl |
| Auteur | Arjen Brienen (Lost Lemon)<br>Jasper Muskiet (Lost Lemon)<br>Eelco Brenner (Lost Lemon) |
| Onafhankelijk voorzitter | Bas van Luxemburg (Lost Lemon) |

# Inhoud

# Samenvatting en Forumadvies

*Advies aan het Forum*

De experts geven het volgende advies:

| |
|---|
| *De expertgroep adviseert om de standaard TLS versie 1.3 op te nemen op de 'pas toe of leg uit'-lijst*. |

Als functioneel toepassingsgebied wordt geadviseerd:

| |
|---|
| *TLS moet worden toegepast op de uitwisseling van gegevens tussen clients en servers, inclusief server-server-communicatie.* |

Als organisatorisch werkingsgebied wordt geadviseerd:

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

*Waarom is opname belangrijk?*

TLS is de de facto open standaard voor beveiliging van internetverkeer. Het is daarom zeer belangrijk dat deze veilig wordt toegepast. TLS wordt gebruikt voor client-server-koppelingen en server-server-koppelingen. Via deze laatste koppelingen wordt door overheidspartijen grootschalig persoonsgebonden informatie uitgewisseld. Wanneer partijen op (te) oude versies van TLS werken, ontstaan er kwetsbare situaties voor het veilig uitwisselen van gegevens.

Door versie 1.3 van TLS als standaard op de lijst op te nemen leidt dat tot twee verbeteringen ten opzichte van versie 1.2. Door het gebruik van TLS 1.3 wordt de standaard efficiënter en worden onveilige opties geschrapt, waardoor de veiligheid toeneemt.

*Waar gaat het inhoudelijk over?*

Transport Layer Security (TLS) Protocol is een protocol-onafhankelijke beveiliging van internetverbindingen waarbij beide zijden elkaar kunnen authenticeren, waarna tussen beide zijden een encryptie-algoritme en cryptografische sleutels worden onderhandeld. Deze worden toegepast voor de rest van de sessie. Op deze manier wordt een protocolonafhankelijke beveiligde verbinding opgezet. TLS wordt gebruikt voor het beveiligen van diverse applicatieprotocollen, zoals HTTPS, SMTP, IMAP, POP3 en FTP om de uit te wisselen data te versleutelen. Het TLS-protocol bevindt zich in de sessielaag onder de genoemde applicatieprotocollen.

TLS wordt gebruikt voor client-server-koppelingen, zoals: van webbrowser naar webserver of van email-client naar email-server. Ook wordt het toegepast bij server-server-koppelingen, zoals web services (http://www.w3.org/TR/soap12/) en Digikoppeling (https://www.logius.nl/diensten/digikoppeling/). Via deze laatste

voorziening wordt door overheidspartijen grootschalig persoonsgebonden informatie uitgewisseld.

TLS is nu al opgenomen op de pas-toe-of-leg-uit-lijst met de versies 1.0, 1.1 en 1.2.

*Hoe is het proces verlopen?*

Om tot dit advies te komen is op 21 juni 2018 een groep experts bijeengekomen om over het toepassings- en organisatorisch werkingsgebied te discussiëren en om de standaard te toetsen tegen de toetsingscriteria. Dit expertadvies vat de uitkomsten van de discussie en toetsing 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 OBDO opstellen. Het OBDO bepaalt uiteindelijk op basis van het advies van het Forum of TLS 1.3 opgenomen wordt op de "pas toe of leg uit"-lijst.

*Hoe scoort de standaard op de toetsingscriteria?*

<u>Toegevoegde waarde</u>
TLS 1.3 biedt ten opzichte van eerdere versies een betere performance door TLS false start en Zero Round Trip Time (0-RTT). Deze performanceverbeteringen komen vooral bij browserverkeer tot uiting en minder bij server-server-koppeling (ebMS).

De grootste verbeteringen zijn op het vlak van beveiliging, omdat een aantal beveiligingsrisico's wordt beperkt. Dit komt doordat onveilige opties uit TLS 1.2 uitgesloten worden, SHA-1, RC4, DES, 3DES, AES-CBC en MD5, waardoor er minder kans bestaat dat het protocol op een onveilige manier geconfigureerd wordt. Ook is configuratie eenvoudiger waardoor er minder kans op verkeerde configuratie is.

<u>Open standaardisatieproces</u>
TLS 1.3 kent een open standaardisatieproces via de IETF en doordat de Simplified BSD License wordt gehanteerd is de standaard door eenieder vrij te gebruiken.

<u>Draagvlak</u>
Alhoewel versie 1.3 van TLS net beschikbaar is zal de adoptie door leveranciers snel gaan en veelal automatisch bij upgrades van software beschikbaar komen (mits deze door leveranciers wordt ondersteund).

<u>Opname bevordert de adoptie</u>
Ja, Met de verplichte aanschaf van software met ondersteuning van TLS 1.3 wordt de adoptie van de standaard bevordert.

*Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaard?*
De expertgroep doet het Forum Standaardisatie en Overheidsbreed Beleidsoverleg Digitale Overheid (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 TLS 1.3 te doen:

*Behoud oudere versies onder voorwaarde*

TLS 1.3 wordt door experts beschouwd als de meest veilige versie. Deze versie is daarom de norm. Ten behoeve van de interoperabiliteit dienen ook de versies 1.2, 1.1 en 1.0 op de lijst te blijven, met name als wederpartijen (nog) niet klaar zijn voor versie 1.3. Zoals gebruikers met oudere versies van browsers.
De expertgroep adviseert dat als voorwaarde voor behoud van de oudere versies geldt dat deze door het NCSC niet als onvelig worden aangemerkt. Als het NCSC een negatief advies over een versie afgeeft, adviseert de expertgroep om deze per direct van de "pas toe of leg uit"-lijst te halen.

*"TLS 1.3 dient in de IETF standards track minimaal gepubliceerd te zijn als "Proposed Standard"*

TLS versie 1.3 heeft op het moment van schrijven de status "Proposed standard" maar de tekst van de specificatie is nog in eindredactie. Dat betekent dat de laatste versie van de specificatie (28) nog een "internet draft" is waarin kleine wijzigingen in de beschrijvende tekst mogelijk zijn.
De expertgroep adviseert om opname op de "pas toe leg uit"-lijst door te zetten onder voorwaarde dat de IETF-editors de standaard niet terugleggen bij de auteurs van de standaard. Als dit gebeurt kan de standaard inhoudelijk wijzigen en dient nieuwe toetsing plaats te vinden. De kans dat dit gebeurt acht de expertgroep zeer klein. De expertgroep deelt het gevoel dat we aan de vroege kant zijn met aanmelding voor opname op de lijst, maar dat de opname de adoptie bespoedigt. Van andere wereldwijd gebruikte standaarden is bekend dat deze zeer lang de status "Proposed standard" kunnen houden en al breed worden toegepast.

# 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!"[1] en de strategie "Nederland Digitaal"[2] benadrukken dit beleid. Om dit doel te bereiken, onderstrepen het instellingsbesluit van het Forum Standaardisatie, de Generieke Digitale Infrastructuur en de verschillende architectuurkaders bij het gebruik van open standaarden en 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 Overheidsbreed Beleidsoverleg Digitale Overheid (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

Dit document is een expertadvies voor TLS 1.3 gericht aan het OBDO en Forum Standaardisatie. TLS 1.3 is aangemeld voor opname op de lijst met open standaarden door Michiel Leenaars van de stichting NLnet.

Doel van dit document is om het OBDO te adviseren of TLS 1.3 in aanmerking komt voor opname op de lijst met open standaarden als "pas toe of leg uit"-standaard, al dan niet onder voorwaarden.

## 1.3 Doorlopen proces

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

1. De procesbegeleider heeft op donderdag 17 mei 2018 een intakegesprek gevoerd met de indiener. Tijdens de intake is de standaard getoetst op criteria voor inbehandelname en is een eerste inschatting gemaakt van de kansrijkheid van de procedure.
2. Op basis van de intake heeft het Forum Standaardisatie op woensdag 13 juni 2018 besloten de aanmelding in procedure te nemen. Hierop volgend is een expertgroep samengesteld en een voorzitter aangesteld.
3. De leden van de expertgroep hebben een voorbereidingsdossier gekregen dat is samengesteld met informatie uit de aanmelding en het intake onderzoek. Voorafgaand aan de expertbijeenkomst heeft de expertgroep dit voorbereidingsdossier doorgenomen en aandachtspunten geïdentificeerd.
4. De expertgroep is op donderdag 21 juni 2018 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.

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

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

Dit expertadvies geeft de uitkomst van de expertgroep weer. De procesbegeleider heeft een concept van dit expertadvies aan de leden 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 Stadaardisatie zal dit expertadvies openbaar maken ten behoeve van een publieke consultatie die plaatsvindt van 6 augustus 2018 tot 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 onafhankelijk voorzitter die de expertgroep leidt en de verantwoordelijkheid neemt voor het expertadvies.

Als onafhankelijk voorzitter is opgetreden Bas van Luxemburg, partner bij Lost Lemon B.V.

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

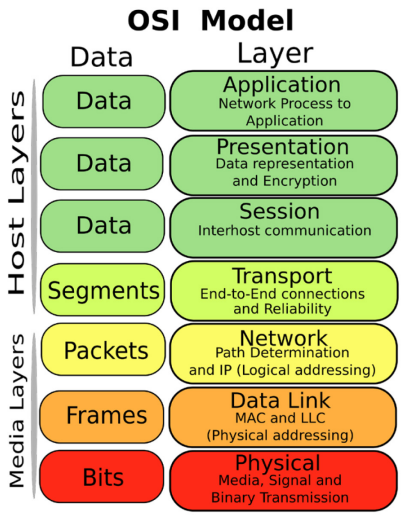
Aan de expertbijeenkomst hebben deelgenomen:
- Maarten Aertsen (NCSC)
- Iljitsch van Beijnum (Logius)
- Alwin de Bruin (DMarcian)
- John van Huijgevoort (VNG-Realisatie)
- Martijn Keizer (Enable-U)
- Pieter Lexis (PowerDNS)
- Peter Smeenk (Justitiële informatiedienst)
- Rolf Sonneveld (Sonnection)
- Tony van der Togt (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)
- Paddy Verberne (Gemeente 's-Hertogenbosch)
- Zarco Zwier (UWV)

Han Zuidweg van het Bureau Forum Standaardisatie was als toehoorder bij de expertbijeenkomst aanwezig.

## 1.6 Toelichting TLS 1.3

Transport Layer Security (TLS) Protocol is een protocol-onafhankelijke beveiliging van internetverbindingen waarbij beide zijden elkaar kunnen authenticeren, waarna tussen beide zijden een encryptie-algoritme en

cryptografische sleutels worden  onderhandeld. Deze worden toegepast voor de rest van de sessie. Op deze manier wordt een protocolonafhankelijke beveiligde verbinding opgezet. TLS wordt gebruikt voor het beveiligen van diverse applicatieprotocollen, zoals HTTPS, SMTP, POP3, IMAP en FTP om de uit te wisselen data te versleutelen. Het TLS-protocol bevindt zich in de sessielaag onder de genoemde applicatieprotocollen. Zie hiervoor bijgevoegde afbeelding.




TLS is de de facto open standaard voor beveiliging van internetverkeer. Het is daarom zeer belangrijk deze veilig wordt toegepast.

TLS wordt gebruikt voor client-server-koppelingen, zoals: van webbrowser naar webserver of van email-client naar email-server. Ook wordt het toegepast bij server-server-koppelingen, zoals web services (http://www.w3.org/TR/soap12/) en Digikoppeling (https://www.logius.nl/diensten/digikoppeling/). Via deze laatste voorziening wordt door overheidspartijen grootschalig persoonsgebonden informatie uitgewisseld.

TLS is nu al opgenomen op de pas-toe-of-leg-uit-lijst met de versies 1.0, 1.1 en 1.2.

Versie 1.3 van TLS kent twee type verbeteringen ten opzichte van versie 1.2:

- TLS 1.3 is efficiënter en leidt daarom tot snellere implementaties door de volgende verbeteringen: TLS false start en Zero Round Trip Time (0-RTT). TLS false start voorziet in eerdere start van de sessie van eerdere versies van TLS. 0-RTT slaat onderhandeling over encryptie-algoritme en cryptografische sleutels over bij terugkerende verbindingen.
- TLS 1.3 laat een aantal onveilige opties uit TLS 1.2 weg, zoals: SHA-1, RC4, DES, 3DES, AES-CBC en MD5. Hierdoor bestaat er minder kans dat het protocol op een onveilige manier geconfigureerd wordt en dus de beveiliging verzwakt wordt. TLS 1.3 kent hierdoor minder kwetsbaarheden dan de huidige meest gebruikte versie TLS 1.2.

Versie 1.2 wordt door 88%[3] van de browsers gebruikt. Daarnaast heeft Microsoft® aangekondigd per 31 oktober 2018 support voor versies 1.0 en versies 1.1 te stoppen voor haar office producten.

*Relatie met andere standaarden*

*3 zie https://blog.cloudflare.com/why-tls-1-3-isnt-in-browsers-yet/*

TLS wordt door veel standaarden gebruikt als om over een beveiligde verbinding te communiceren. Deze standaarden zullen dan ook TLS 1.3 moeten kunnen toepassen. Voorbeelden zijn:

**https** is een uitbreiding op het http protocol met als doel de veilige uitwisseling van gegevens tussen een (web)server en client.

De e-mail protocollen **POP3, IMAP en SMTP** die allen door middel van TLS beveiligd kunnen worden.

**FTP** voor het uitwisselen van (grote) bestanden dat ook door TLS beveiligd kan worden.

**STARTTLS** in combinatie met **DANE** gaan het afluisteren of manipuleren van mailverkeer tegen. STARTTLS maakt het mogelijk om transportverbindingen tussen e-mailservers op basis van certificaten met TLS te beveiligen.  Met de complementaire standaard DANE kunnen e-mailservers het gebruik van TLS bovendien afdwingen.

**Digikoppeling** bestaat uit een set standaarden voor elektronisch berichtenverkeer tussen overheidsorganisaties voor server-server-koppeling.

Deze relaties hebben verder geen gevolgen voor de toetsing van TLS 1.3.

## 1.7 Leeswijzer

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

Hoofdstuk 3 beschrijft de resultaten van de toetsing van de standaard 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*[4] 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 oranisaties moeten de standaard gebruiken) beschreven.

Secties 2.1 en 2.2 geven het advies van de expertgroep voor het functioneel en organisatorisch toepasingsgebied van TLS 1.3.

## 2.1 Functioneel toepassingsgebied

De expertgroep adviseert als functioneel toepassingsgebied voor TLS 1.3:

*TLS moet worden toegepast op de uitwisseling van gegevens tussen clients en servers, inclusief server-server-communicatie*.

## 2.2 Organisatorisch werkingsgebied

De expertgroep adviseert om het organisatorisch werkingsgebied van de standaard overeen te laten komen met het werkingsgebied waarop de "pas toe of leg uit" verplichting van toepassing is, te weten:

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

*4 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?[5]

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, de standaard is de de facto open standaard voor beveliging van internetverkeer. TLS wordt gebruikt voor client-server-koppelingen, zoals: van webbrowser naar webserver of van email-client naar email-server. Ook wordt het toegepast bij server-server-koppelingen, zoals webservices en ebMS. Via deze laatste koppelingen wordt door overheidspartijen grootschalig persoonsgebonden informatie uitgewisseld.

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 paragraaf 1.6.

*5 Dit criterium is voornamelijk van toepassing op standaarden op de "pas toe of leg uit" lijst, niet voor aanbevolen 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.)*
Ja, TLS 1.3 is een verbeterde versie van TLS 1.2 (en de versies 1.1 en 1.0). De verbeteringen zijn beschreven in paragraaf 1.6.

*3.1.2.3 Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname? (toelichtende vraag)*
Er zijn geen concurrerende of samenhangende standaarden geïdentificeerd die in aanmerking komen voor opname op de lijst. De expertgroep acht de meerwaarde van versie 1.3 ten opzicht van versie 1.2 evident.

*3.1.2.4 Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden? (toelichtende vraag)*
Ja, TLS is een internationale standaard.

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 Zijn de kosten van implementatie acceptabel en zijn deze kosten bekend en inzichtelijk?*
Er is ervaring opgedaan met de implemenatie van eerdere versies van TLS. De kosten zijn inzichtelijk en acceptabel. De kosten voor de aanschaf van de standaard zijn laag. Er is nog beperkte ervaring met de implementatie van versie 1.3, en de bestaande ervaring zit veelal in de opensource hoek. De meeste grote libraries zetten de standaard aan als deze is uitontwikkeld en deze komt dan automatisch beschikbaar voor applicaties. De aanschafkosten zijn nihil, de kosten van de implementatie zitten vooral in de configuratie.

*3.1.3.2 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. Hackers ontwikkelen zich steeds verder en ontdekken kwetsbaarheden bij het gebruik van eerdere versies van TLS.

*3.1.3.3 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?*
TLS is de de facto open standaard voor beveiliging van internetverkeer. Door versie 1.3 van TLS als standaard op de lijst op te nemen leidt dat tot twee verbeteringen ten opzichte van versie 1.2. Door het gebruik van TLS 1.3 wordt de standaard efficiënter en worden onveilige opties geschrapt, waardoor de veiligheid toeneemt. Daarnaast heeft versie 1.3 een beter performance dan versie 1.2

*3.1.3.4 Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel?*
Ja, er zijn geen specifieke beveiligingsrisico's geïdentificeerd. TLS versie 1.3 kent nog weinig implementaties. Om die reden kan het verstandig zijn om nog even te wachten met de adoptie van de standaard tot eventuele bugs die zich na implementatie openbaren, zijn opgelost. Gezien de

ontwikkeling van voorgaande versies van de standaard beschouwt de expertgroep dit als een dusdanig klein risico dat dit adoptie niet in de weg staat.
De expertgroep erkent de taak van het NCSC om de overheid te adviseren over het gebruik van specifieke onderdelen (cipher suites) van de standaard. De expertgroep adviseert om de richtlijnen van de NCSC hierin te volgen.

*3.1.3.5* *Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel?*
Ja, er zijn geen specifieke privacyrisico's geïdentificeerd.

3.1.4 Conclusie criteria 'Toegevoegde waarde'
De expertgroep concludeert dat versie 1.3 van TLS een duidelijke toegevoegde waarde heeft, met name op het gebied van beveiliging en in mindere mate op het gebied van performance. Zie ook 'Samenvatting en Forumadvies' .

## 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)?*
Ja, het specificatiedocument is kosteloos verkrijgbaar via website van IETF (https://datatracker.ietf.org/doc/draft-ietf-tls-tls13/). De specificatie van TLS 1.3 valt onder de Simplified BSD License, waarmee het vrij te gebruiken mits de copyright tekst wordt meegegeven bij hergebruik.

*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)?*
Ja, TLS wordt beheerd door IETF. IETF kent goed gedocumenteerde en open beheerprocedures. Er is geen lidmaatschap. Het beheerproces en de besluitvorming hieromtrent zijn open en transparant.

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?*
Het gebruik van de specificatie wordt aan een ieder onherroepelijk en royalty-free ter beschikking gesteld, mits copyright notice van de gehanteerde licentie (Simplified BSD License) wordt meegeleverd.

*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?*
Ja, zie 3.2.2.1

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, het beheerproces en de besluitvorming omtrent TLS 1.3 is open en transparant. Via de TLS Working Group[6] worden regelmatig met belanghebbenden overleggen gehouden over de doorontwikkeling en het beheer van TLS.

*3.2.3.2 Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen?*
Ja, IETF kent open en transparante processen waar organisaties bij kunnen aansluiten indien zij dat willen.

*3.2.3.3 Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde procedure?*
Ja, de IETF kent de mogelijkheid bezwaar aan te tekenen als standaarden in concept zijn gepubliceerd.

*3.2.3.4 Organiseert de standaardisatieorganisatie regelmatig overleggen met belanghebbenden over doorontwikkeling en beheer van de standaard?*
Ja, via de TLS Working Group worden regelmatig met belanghebbenden overleggen gehouden over de doorontwikkeling en het beheer van TLS.

*3.2.3.5 Organiseert de standaardisatieorganisatie een publieke consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld?*
Ja.

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, bij IETF.

*3.2.4.2 Is de financiering van de ontwikkeling en het onderhoud van de standaard voor tenminste drie jaar gegarandeerd?*
Ja, die is gegarandeerd door de beheerorganisatie IETF. Formeel biedt het IETF geen harde garanties maar gezien de staat van dienst en het wereldwijde belang van de IETF heeft de expertgroep vertrouwen in het onderhoud.

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)*
Ja, deze is te vinden op de website van IETF.

*3.2.5.2 Is de beheerdocumentatie goed vindbaar en verkrijgbaar?*
Ja, deze is te vinden op de website van de IETF.

*3.2.5.3 Is het belang van de Nederlandse overheid voldoende geborgd bij de ontwikkeling en het beheer van de standaard?*

*6 https://datatracker.ietf.org/wg/tls*

Het staat Nederlandse overheidspartijen vrij om deel te nemen aan de ontwikkeling en het beheer van de standaard. Het gaat om een internationale standaard die breder wordt toegepast dan alleen overheidsorganisaties. De expertgroep heeft vertrouwen in het feit dat nederlandse belangen niet worden geschaad.

*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?*
Ja, zie lijst deelnemers bij de IETF.

*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?*
Nee, aanvullende toetsing van nieuwe versies van TLS wordt aangeraden alvorens over te gaan tot opname op de pas-toe-leg-uit-lijst. Hiertoe vindt nu toetsing door ondermeer de experts plaats.

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?*
Ja, bij IETF voor de standaard. Het NCSC doet aanbevelingen over het gebruik van TLS en geeft factsheet hierover uit[7]. Daarnaast kunnen partijen tercht bij leveranciers voor de applicaties die TLS 1.3 implementeren.

*3.2.6.2* *Wordt er ondersteuning gegeven in de adoptie en de implementatie van de standaard?*
Ja, door softwareleveranciers.

3.2.7 Conclusie criteria 'Open standaardisatieproces'
De expertgroep concludeert dat het beheerproces van het IETF voldoende open is. TLS 1.3 kent een open standaardisatieproces via de IETF en doordat de Simplified BSD License wordt gehanteerd is de standaard door eenieder vrij te gebruiken.

**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?*
Versie 1.2 van TLS is al langer in gebruik door vrijwel alle overheidsorganisaties. TLS 1.3 is pas recent gepubliceerd en wordt nog weinig toegepast. Aan de clientkant wordt TLS 1.3 bij opstellen van dit advies ondersteund door de browsers Chrome® en Firefox®. Microsoft® heeft aangekondigd versie 1.3 in Q1 van 2019 te implementeren voor hun officeproducten, vwb de serverproducten zijn er nog geen mededelingen gedaan. Daarnaast hebben de drie grootste cryptolibraries aangegeven versie 1.3 te gaan ondersteunen, waarmee ook

*7 https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html*

ondersteuning op serverniveau in de toekomst is geborgd. Na het opnemen van de standaard op de lijst, verwacht de expertgroep dat het het gebruik snel zal toenemen.

*3.3.1.2 Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen?*
Ja, door een bekende implementatie als referentie-implementatie te gebruiken (bijv. Firefox® voor webservers). De expertgroep verwacht ook dat bekende testwebsites de standaard gaan ondersteunen zoals ssllabs.com, internet.nl en Testssl.sh.

*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, het is voor de gebruiker transparant.

*3.3.1.4 Zijn er profielen of voorbeeldimplementaties van de standaard aanwezig en zijn deze vrij te gebruiken?*
Ja, zoals de nieuwste versies van Firefox® en Chrome® en de cryptolibraries.

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 aanwezig op de expertbijeenkomst. Het NCSC juicht opname van de standaard op de lijst toe. Het Nationaal Beraad en het OBDO een streefbeeldafspraak hebben gemaakt voor de adoptie van TLS en https. Dat geeft blijk van een breed draagvlak voor de standaard.

*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 aanwezig tijdens de expertbijeenkomst.

*3.3.2.3 Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?*
Nog niet. Versie 1.2 van TLS is al langer in gebruik door vrijwel alle overheidsorganisaties. TLS 1.3 is pas recent gepubliceerd en wordt nog weinig toegepast. De verwachting is dat na het opnemen van de standaard op de lijst, het gebruik snel zal toenemen.

*3.3.2.4 Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?*
Ja, TLS is al een standaard op de pas-toe-of-leg-uit-lijst. TLS 1.0, 1.1 en 1.2 zijn in gebruik binnen het organisatorische werkingsgebied.

*3.3.2.5 Is de aangemelde versie backwards compatible met eerdere versies van de standaard?*
Ja, omdat TLS versie 1.3 de mogelijkheid ondersteunt om op basis van het request automatisch te downgraden naar een oudere versie van TLS.

De versies zijn dus sec niet downwards compatible, ze worden naast elkaar gebruikt.

*3.3.2.6* *Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?*
Ja, er zijn in alle gevalen geen negatieve signalen.

3.3.3 Conclusie criteria 'Draagvlak'
De expertgroep concludeert dat het draagvlak voor het gebruik van TLS 1.3 goed is. Alhoewel versie 1.3 van TLS net beschikbaar is en nog weinig wordt toegepast zal de adoptie door leveranciers snel gaan en veelal automatisch bij upgrades van software beschikbaar komen (mits deze door leveranciers wordt ondersteund).

## 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, Het plaatsen van de standaard op de lijst met verplichte standaarden stimuleert het upgraden van TLS naar de verbeterde versie en het verminderd gebruik van de oudere, potentieel kwetsbare versies (1.0 en 1.1). Opname op de lijst zal op die manier zorgen voor betere interoperabiliteit met het groeiend aantal nieuwe toepassingen die alleen de nieuwe versie van de standaard ondersteunen.

*3.4.2* *Is de status "aanbevolen" het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?*
Nee, de status "aanbevolen" is te vrijblijvend. Beveiligd internetverkeer is dusdanig belangrijk dat deze verbeterde versie van TLS als verplicht zou moeten worden opgenomen op de lijst.

*3.4.3* *Conclusie criteria 'Opname bevordert adoptie'*
De expertgroep concludeert dat opname op de verplichte "pas toe leg uit"-lijst het passende middel is om de adoptie van TLS 1.3 binnen de (semi)overheid te bevorderen.

## 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 adviseert het OBDO om bij de opname op de lijst voor "pas toe of leg uit" de volgende oproepen ten aanzien van de adoptie van TLS 1.3 te doen:

- Aan OBDO en Forum Standaardisatie: communiceer dat TLS 1.3 verplicht is vanaf het moment van opname op de "pas toe of leg uit "-lijst;
- Aan overheden: Controleer regelmatig met behulp van beschikbare validatie-tools, zoals de SSLlabs server test, of voor beveiligde verbindingen TLS 1.3 en TLS 1.2 en eventueel aanvullend versies 1.0 en 1.1 worden toegepast en controleer ook de veilige configuratie daarvan aan de hand van beschikbare best practices. Dat geldt voor alle overheden, maar met name voor organisaties die gemeenschappelijke voorzieningen leveren zoals SSC-ICT, DPC/AZ, DICTU, ICTU en Logius;
- Aan NCSC: Ontwikkel en publiceer in samenwerking met experts van andere organisaties, zoals Logius (PKIoverheid) en beheerders van sectorale Baselines Informatiebeveiliging, een update richtlijn voor veilige TLS-configuratie en houd deze up-to-date. In deze update richtlijn zou het gebruik van versie 1.3 en de relatie tot de andere versies van TLS een belangrijke rol moeten innemen, evenals de te ondersteunen cryptografische algoritmen en het afslaan van bekende aanvallen op TLS. Verder zou het gebruik van TLS validatie-tools moeten worden aangeraden;
- Aan Logius/PKIoverheid: Breng de genoemde bestaande internationale 'best practices' voor veilige TLS-configuratie en straks de NCSC-richtlijn actief onder de aandacht bij de uitgifte van certificaten aan de gebruikers van PKIoverheid;
- Aan NCSC: Fungeer als vraagbaak op het gebied van toepassing van TLS voor de primaire doelgroep, de rijksoverheid en de vitale sectoren. Voor de secundaire doelgroep kan de vraagbaakfunctie worden vormgegeven via de schakelorganisaties van NCSC (zoals VNG-Realisatie/IBD);
- Aan NCSC: Informeer het Forum Standaardisatie en andere overheden wanneer de veiligheidsstatus van de standaard wijzigt;
- Aan alle implementatiepartijen: Configureer uw TLS implementatie conform de normen zoals NCSC deze voorschrijft.