Forum Standaardisatie

Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 96810
2509 JE Den Haag

www.forumstandaardisatie.nl

notitie

FORUM STANDAARDISATIE 13 JUNI 2018

Agendapunt:	3B		
Betreft:	Intake-advies voor TLS 1.3		
Aan:	Forum Standaardisatie		
Van:	Stuurgroep Open Standaarden		
Datum:	30 mei 2018	**Versie**	1.0
Bijlagen:	geen		

Advies

Het Forum Standaardisatie wordt geadviseerd om de standaard Transport Layer Security 1.3 (TLS 1.3) in procedure te nemen voor opname op de 'pas toe of leg uit'-lijst. TLS staat reeds op de pas-toe-of-leg-uit-lijst opgenomen met oudere versies van TLS.

TLS 1.3 wordt veiliger geacht dan voorgaande versie 1.2 en eerdere versies. Daarnaast levert TLS 1.3 performancewinst ten opzichte van eerdere versies.

TLS 1.3 voldoet aan de basiscriteria om in procedure genomen te worden.

Korte toelichting
TLS 1.3 is ingediend door NLnet met steun van het Nationaal Cyber Security Centrum (NCSC).

TLS voldoet aan de criteria om in procedure genomen te worden als 'pas toe of leg uit'-standaard. TLS 1.3 is een vernieuwde versie na SSL, TLS 1.0, 1.1 en 1.2, de laatste drie al opgenomen als verplichte standaard op de 'pas toe of leg uit' lijst met open standaarden. TLS 1.3 wordt geacht een betere beveiliging te bieden dan de voorgaande versies van TLS.

De expertgroep zal moeten onderzoeken hoe het staat met de implementatie van TLS 1.3 en het draagvlak voor deze standaard. Aandachtspunt voor de toetsingsprocedure is de consequentie van het toevoegen van TLS 1.3 voor eerdere versies die nu op de lijst zijn opgenomen. Concreet zal de expertgroep moeten bekijken welke van de versies 1.2, 1.1 en 1.0 nog moeten worden geaccepteerd naast TLS 1.3.

Toelichting

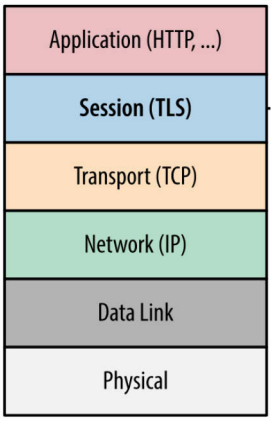
1. Aanmelding, intakegesprek en toetsingsprocedure

Op 12 april 2018 is door Michiel Leenaars (directeur strategie van NLnet) de standaard TLS 1.3 aangemeld voor opname op de lijst met open standaarden. De aanmelder heeft als doel de standaard de 'pas toe of leg uit' status te geven.

Op 17 mei 2018 heeft een intakegesprek plaatsgevonden met de indiener van TLS 1.3. In dit gesprek is de aanmelding besproken. Hierbij is gekeken of alle basisinformatie aanwezig is en of de standaard voldoet aan de criteria om in procedure genomen te worden. Daarnaast is vooruitgeblikt op de procedure.

2. Korte beschrijving standaard

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 diverse applicatieprotocollen, zoals HTTPS, SMTP, POP3, FTP om de uit te wisselen data te versleutelen. TLS is een protocol in de transportlaag die de connecties verzorgt voor de bovenstaande protocollen in de applicatielaag.



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 webservices en ebMS. Via deze laatste koppelingen 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.

Welk probleem lost de standaard op?

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 overbodige en 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% 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 officeproducten.

Indiener beschouwt deze oudere versies als potentieel kwetsbaar, waardoor beveiligingsrisico's ontstaan. Doelstelling van indiener is overheden te bewegen software, hardware en diensten te gebruiken die veilig genoeg zijn.

Wie beheert de standaard?
TLS 1.3 is een IETF-standaard die over het hele Internet wereldwijd toegepast wordt en gratis te gebruiken is. De internationale beheerorganisatie International Engineering Task Force (IETF) beheert zelf de standaard. Alle overheidsorganisaties en overige organisaties gebruiken TLS in een van de genoemde versies. Versie 1.3 is per 21 maart 2018 vrijgegeven en wordt nog niet breed ingezet.

Waarom is de standaard aangemeld voor pas toe of leg uit?
Indiener heeft in zijn schriftelijk verzoek gevraagd TLS 1.3 op de pas-toe-of-leg-uit-lijst op te nemen. In het interview bleek dat indiener ook de volgende zaken beoogt:

1. Hij wil TLS 1.3 op de pas-toe-of-leg-uit-lijst opnemen om te zorgen dat (semi)overheden bij aanschaf van nieuwe software afdwingen dat TLS versie 1.3 wordt ondersteund.
2. Hij wil TLS versie 1.2 op de pas-toe-of-leg-uit-lijst houden.
3. Hij suggereert verwijdering van TLS versie 1.0 en 1.1 van de pas-toe-of-leg-uit-lijst, en zou deze kwestie willen voorleggen aan de expertcommissie.

Het al dan niet ondersteunen van TLS 1.0 en TLS 1.1 bij nieuw aan te schaffen apparatuur en diensten hoeft geen dwingende verplichting meer te zijn, en zou tot ongewenste uitsluiting kunnen leiden. Leveranciers kunnen uiteraard deze oude versies nog wel blijven ondersteunen, maar dit wordt door het verwijderen van de pas-toe-of-leg-uit-lijst in aanbestedingen dan niet meer vereist.

Voorts wil hij bij de toepassing van TLS 1.3 bij server-server-koppeling de standaard aanbevelen en over een jaar evalueren of dit de enige toegestane protocolversie dient te worden. Het gebruik van VPN-protocollen als Wireguard zou een alternatief kunnen zijn.

Indiener heeft als doel overheden te bewegen alleen hard- en software aan te schaffen met ondersteuning van veilige versies van TLS.

3. Criteria voor inbehandelname

Om een standaard in behandeling te nemen moet de standaard vallen binnen de scope van de lijst. Hiervoor gelden drie criteria:

1. Is de standaard toepasbaar voor elektronische gegevensuitwisseling tussen (semi-)overheidsorganisaties en bedrijven, tussen (semi-)overheidsorganisaties en burgers of tussen (semi-)overheidsorganisaties onderling?

Ja. TLS 1.3 wordt toegepast bij zowel client-server (websites) als server-server (web services en eBMS) toepassingen. Via server-server koppelingen wordt door overheidspartijen grootschalig persoonsgebonden informatie uitgewisseld.

2. Is het beoogde functioneel toepassingsgebied en het organisatorisch werkingsgebied van de standaard, voldoende breed om substantieel bij te dragen aan de interoperabiliteit van de (semi-)overheid?

Ja. TLS wordt gebruikt voor het beveiligen van verbindingen met websites maar ook e-mail verbindingen. TSL heeft dus een zeer breed werkingsgebied dat niet gebonden is aan een specifieke sector.

3. Is het zinvol de standaard op te nemen, gezien het feit dat deze niet al wettelijk verplicht is voor het beoogde functioneel toepassingsgebied en organisatorisch werkingsgebied?

Ja. TLS is nog niet wettelijk verplicht.

4. Draagt de standaard bij aan de oplossing van een bestaand, relevant (interoperabiliteits)probleem en het voorkomen van leveranciersafhankelijkheid?

Ja. TLS 1.3 zorgt voor veilige verbindingen over het Internet. Hier is een grote en urgente behoefte aan. Versie 1.3 biedt daarbij betere beveiliging dan voorgaande versies 1.0, 1.1 en 1.2.

<u>Conclusie</u>
De standaard voldoet aan de criteria om in procedure genomen te worden.

4. Toetsing kansrijkheid procedure

Het Forum Standaardisatie wil voorkomen dat er standaarden in procedure worden genomen, waarvan bij voorbaat al bekend is dat deze in de expertronde of consultatieronde zullen stranden op één van de inhoudelijke criteria. Daarom heeft de procedurebegeleider de beantwoording van de criteriavragen nagelopen, waar mogelijk zelf aangevuld en vervolgens besproken met de indiener.

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

TLS wordt beheerd door IETF. Het specificatiedocument is kosteloos verkrijgbaar via website van IETF. 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.

IETF kent goed gedocumenteerde en open beheerprocedures, er is geen lidmaatschap, het beheerproces en de besluitvorming hieromtrent is open

en transparant. Via de TLS Working Group worden regelmatig met belanghebbenden overleggen gehouden over de doorontwikkeling en het beheer van TLS.

2. Toegevoegde waarde
De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de kosten, de risico's en nadelen. Voor elk van de te onderscheiden stakeholders (overheid, bedrijven en burgers) afzonderlijk zouden de baten voor de informatievoorziening en de bedrijfsvoering op moeten wegen tegen de kosten. Verder moeten de risico's aan overheidsbrede adoptie van de standaard (beveiliging, privacy) acceptabel zijn.

De interoperabiliteitswinst en andere voordelen wegen op tegen de kosten, de risico's en nadelen van de adoptie van TLS 1.3. De eerder genoemde aankondiging van Microsoft om per 31 oktober 2018 support voor versies 1.0 en versies 1.1 te stoppen voor haar officeproducten, vraagt om een aanpassing van de standaard. De oudere versies zijn potentieel kwetsbaar.

Er is nog weinig ervaring met de implementatie van TLS 1.3 omdat deze pas recent is gepubliceerd. Naar verwachting zijn de implementatiekosten van TLS 1.3 relatief laag. Wel is het nodig om versie 1.2 te behouden. TLS 1.3 is net als TLS 1.2 niet 'backwards compatible'. Ten behoeve van de interoperabiliteit dient TLS 1.2 dus ook toegepast te worden, met name als wederpartijen (nog) niet klaar zijn voor versie 1.3.

Er zijn geen beveiligings- en privacyrisico's geïdentificeerd.

3. Draagvlak
Aanbieders en gebruikers moeten voldoende ervaring hebben met de implementatie en het gebruik van de standaard.

De standaard zelf is al langer in gebruik door verreweg de meeste partijen. TLS 1.3 is pas recent gepubliceerd en wordt nog weinig toegepast. TLS 1.3 wordt bij opstellen van dit advies ondersteund door de browsers Chrome en Firefox. De verwachting is dat na het opnemen van de standaard op de lijst, het gebruik snel zal toenemen.

Het weghalen van 1.0 en 1.1 van de 'pas toe of leg uit' lijst zal naar verwachting de nodige discussie opleveren onder experts. In geval deze sessie plaatsvindt, zal hier verder over gesproken moeten worden.

4. Opname bevordert adoptie
De opname op de lijst moet een geschikt middel zijn om de adoptie van de standaard te bevorderen.

TLS 1.3 is aangemeld voor opname op de lijst met verplichte standaarden. Het plaatsen van de standaard op de lijst met verplichte standaarden stimuleert het upgraden van TLS naar de verbeterde versie en het afstoten van 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.

Conclusie
Er zijn op voorhand geen grote struikelblokken te verwachten met het adopteren van TLS 1.3. Het verwijderen van TLS 1.0 en eventueel ook TLS 1.1. zal nog tot discussie leiden.

5. Samenhang

Het Forum Standaardisatie wil weten of de aangemelde standaard samenhangt met standaarden die reeds op de lijst zijn opgenomen, of standaarden die voor toetsing in aanmerking komen. Uit de intake moet duidelijk worden of dit gevolgen heeft voor de toetsing en eventuele opname van de aangemelde standaard.

1. *Bestaat er samenhang tussen de aangemelde standaard en de verplichte ('pas-toe-of-leg-uit') standaarden die reeds op de lijst zijn opgenomen en wat betekent dit voor de toetsing en eventuele opname van de standaard?*

   TLS heeft directe samenhang met drie standaarden op de 'pas toe of leg uit' lijst:

   - **HTTPS** is een toepassing van het http protocol over TTLS verbinding met als doel de veilige uitwisseling van gegevens tussen een (web)server en client.

   - **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** maakt gebruik van TLS om het koppelvlak voor gegevensuitwisseling te beveiligen.

   Deze relatie heeft verder geen gevolgen voor de toetsing van TLS 1.3.

2. *Bestaat er samenhang tussen de aangemelde standaard en de aanbevolen standaarden die reeds op de lijst zijn opgenomen en wat betekent dit voor de toetsing en eventuele opname van de standaard?*
   TLS wordt door verschillende standaarden gebruikt om over een beveiligde verbinding te communiceren. Zo kunnen de verbindingen van FTP (bestandsuitwisseling), SMTP (e-mail), POP3 en IMAP (mailbox toegang) met TLS beveiligd worden. Deze standaarden staan op de lijst aanbevolen standaarden van het Forum Standaardisatie.

   Deze relatie heeft geen gevolgen voor de toetsing van TLS 1.3.

3. *Bestaat er samenhang tussen de aangemelde standaard en standaarden die in aanmerking komen voor opname op de lijst en wat betekent dit voor de toetsing van de standaard(en)? (Denk bijvoorbeeld ook aan een gezamenlijke toetsing met (een deel van) deze aanvullende standaarden).*

Er bestaat samenhang tussen TLS 1.3 en de aangemelde standaard S/MIME. Dit heeft echter geen gevolgen voor de toetsing van TLS 1.3.

6. Sponsorschap

De aanmelding van standaarden voor de lijst van het Forum en het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) dient ondersteund of gesponsord te worden door overheids- en/of (semi)publieke organisaties die de standaard reeds in gebruik hebben (of voornemens zijn dit te doen) en die de beoogde opname op de lijsten ondersteunen. Dit draagt bij aan het draagvlak voor de standaard, geeft zicht op de functionele usecase voor de overheid en helpt bovendien om tijdens de toetsing de juiste experts te benaderen.

1. *Welke overheden en/of (semi)publieke organisaties ondersteunen de aanmelding van de standaard?*
   De aanmelding van TLS 1.3 wordt ondersteund door het Nationaal Cyber Security Centrum (NCSC).

2. Hebben deze organisaties de standaard geïmplementeerd?
   (zie ook punt 7 voor een uitwerking)
   De NCSC heeft de standaard geïmplementeerd in een deel van haar werkprocessen.

7. Functionele use case

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. Deze zijn eerder al genoemd in dit advies (Paragraaf 2: *welk probleem lost de standaard op)*. Door het gebruik van TLS 1.3 wordt de standaard efficiënter en worden overbodige opties geschrapt, waardoor de veiligheid toeneemt.