notitie

FORUM STANDAARDISATIE 10 oktober 2018

Agendapunt 3A- Plaatsing TLS 1.3 op pas-toe-of-leg-uit lijst

Nummer:	FS 181010.3A
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	26 september 2018
Versie:	1.0
Bijlagen:	Expertadvies TLS1.3 Commentaar op de openbare consultatie TLS 1.3

1. Aanleiding en achtergrond

Transport Layer Security (TLS) is een standaard voor het opzetten van veilige verbindingen over het Internet. TLS wordt gebruikt voor de beveiliging van vele applicaties waaronder e-mail, het 'world wide web', bestandsoverdracht en web services. Een https-verbinding met een website (zichtbaar als het 'groene slotje' in de browser) maakt bijvoorbeeld gebruik van TLS.

TLS staat reeds op de 'pas toe of leg uit'-lijst, waarbij TLS 1.2 als de meest veilige versie wordt verplicht. TLS 1.2 is niet compatibel met eerdere versies van TLS. Ten behoeve van de interoperabiliteit zijn daarom ook TLS 1.1 en TLS 1.0 op de pas-toe-of-leg-uit standaarden opgenomen als terugval-versies zodat er ook nog veilige verbindingen mogelijk zijn met wederpartijen die TLS 1.2 nog niet ondersteunen.

TLS 1.3 is een recent gepubliceerde nieuwe versie van het TLS protocol die als efficiënter en veiliger wordt gezien dan TLS 1.2.

2. Betrokkenen en proces

NLnet Foundation (https://nlnet.nl/) heeft TLS 1.3 in april 2018 aangemeld voor plaatsing op de 'pas toe of leg uit'-lijst. Op basis van het intake-advies heeft het Forum Standaardisatie in juni 2018 besloten om TLS 1.3 in procedure te nemen. In de zomer van 2018 heeft een expertonderzoek plaatsgevonden waaraan experts van Logius, NCSC, DMarcian (private sector), VNG Realisatie, Enable-U (private sector), PowerDNS (private sector), Justid, Sonnection (private sector), MinBZK, Gemeente 's Hertogenbosch en UWV deelnamen. Het expertadvies (zie [1]) is van 6 augustus tot en met 10 september 2018 ter openbare consultatie aangeboden.

In de openbare consultatie zijn 8 reacties ontvangen van RINIS, Rechtspraak.nl, het Ministerie van Defensie, het Ministerie van Justitie en Veiligheid, de Sociale Verzekeringsbank (SVB), het Uitvoeringsinstituut Werknemersverzekeringen (UWV), de Kamer van Koophandel (KvK) en het Bureau Keteninformatisering Werk & Inkomen (BKWI). De binnengekomen reacties (zie [2]) worden in paragraaf 5.4 van dit document besproken.

3. Consequenties en vervolgstappen

Een meerderheid van de organisaties die reageerden op de openbare consultatie steunt de opname van TLS 1.3 op de 'pas toe of leg uit'-lijst met behoud van TLS 1.2 als 'terugval-optie'. Geen enkele organisatie twijfelt

aan meerwaarde van TLS 1.3 voor het realiseren van veilige verbindingen over het Internet. Wel plaatst een aantal organisaties vraagtekens bij de marktondersteuning en formele status van de specificatie. Deze twee zaken zijn nader onderzocht, maar geven geen aanleiding om af te wijken van het positieve expertadvies. Dit wordt nader uitgelegd in de toelichting, in paragraaf 5.4.

Op één onderdeel is het expertadvies naar aanleiding van de openbare consultatie aangepast. Het advies van de reagerende organisaties om TLS 1.1 en TLS 1.0 van de pas-toe-of-leg-uit lijst te verwijderen wordt overgenomen. Ook dit wordt in paragraaf 5.4 toegelicht.

Er zijn geen specifieke beveiligingsrisico's geïdentificeerd voor de implementatie van TLS versie 1.3.

De vervolgstappen zijn als volgt: het Forum Standaardisatie adviseert op basis van dit Forumadvies aan het Overheidsbreed Beleidsoverleg Digitale Overheid. Het Overheidsbreed Beleidsoverleg Digitale Overheid bepaalt op basis van het advies of de standaard TLS 1.3 op de 'pas toe of leg uit'-lijst wordt geplaatst en de oude standaarden 1.0 en 1.1 van de lijst worden gehaald.

4. Gevraagd besluit

Het Forum Standaardisatie wordt gevraagd om in te stemmen met onderstaand advies.

Het Forum Standaardisatie adviseert het Overheidsbreed Beleidsoverleg Digitale Overheid om:

1. *TLS 1.3 op de pas-toe-leg-uit lijst te plaatsen met behoud van TLS 1.2 als terugval-versie.*
2. *TSL 1.0 en TLS 1.1 als terugval-versies van de pas-toe-leg-uit lijst te verwijderen. Het blijft voor overheden mogelijk om deze versies omwille van de interoperabiliteit te ondersteunen, maar voor deze oudere versies geldt niet langer het stimuleringsbeleid van 'pas toe of leg uit'.*
3. *In te stemmen met de additionele adviezen ten aanzien van de toepassing van TLS 1.3 zoals geformuleerd in paragraaf 5.5.*

5. Toelichting

5.1. Over de standaard

TLS is een applicatie-onafhankelijk beveiligingsprotocol voor internetverbindingen. Het protocol zorgt ervoor dat beide zijden elkaars identiteit kunnen controleren, waarna tussen beide zijden een encryptie-algoritme en cryptografische sleutels worden uitgewisseld. Met deze sleutels wordt de verbinding vervolgens versleuteld zodat de gegevensuitwisseling niet kan worden onderschept door een derde partij.

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 sessie-laag 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 webservices (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 kan op vele manieren geconfigureerd worden, en het is daarom belangrijk dat TLS veilig wordt toegepast. Wanneer partijen met (te) oude versies van TLS werken, ontstaan er kwetsbare situaties voor het veilig uitwisselen van gegevens.

TLS 1.3 biedt twee verbeteringen ten opzichte van TLS 1.2. TLS 1.3 is efficiënter dan TLS 1.2 en veiliger omdat het een aantal onveilige configuraties verbiedt die in TLS 1.2 nog toegestaan zijn.

5.2 Hoe is het proces verlopen?

TLS 1.3 is in april 2018 aangemeld door de NLnet Foundation (https://nlnet.nl/) voor plaatsing op de 'pas toe of leg uit'-lijst. Na een kort intake-onderzoek heeft het Forum Standaardisatie in juni 2018 besloten om TLS 1.3 in procedure te nemen. In de zomer van 2018 heeft een expertonderzoek plaatsgevonden waaraan experts van Logius, NCSC, DMarcian (private sector), VNG Realisatie, Enable-U (private sector), PowerDNS (private sector), Justid, Sonnection (private sector), MinBZK, Gemeente 's Hertogenbosch en UWV deelnamen. Het expertadvies (zie [1]) is van 6 augustus tot en met 10 september 2018 ter openbare consultatie aangeboden.

In de openbare consultatie zijn 8 reacties ontvangen van RINIS, Rechtspraak.nl, het Ministerie van Defensie, het Ministerie van Justitie en Veiligheid, de Sociale Verzekeringsbank (SVB), het Uitvoeringsinstituut Werknemersverzekeringen (UWV), de Kamer van Koophandel (KvK) en het Bureau Keteninformatisering Werk & Inkomen (BKWI) (zie [2]).

Naar aanleiding van de eerste reacties uit de openbare consultatie is de expertgroep nog voor het sluiten van de openbare consultatie op 5 -12 september per mail geraadpleegd over de twee belangrijkste ingekomen bezwaren. De binnengekomen reacties zijn opgenomen in [2], en worden geanalyseerd in paragraaf 5.4 dit document.

5.3 Hoe scoort de standaard op de toetsingscriteria?

Open standaardisatieproces

TLS 1.3 wordt beheerd door de IETF (ietf.org), die een zeer open standaardisatieproces heeft. IETF hanteert de Simplified BSD License zodat de standaard door eenieder vrij te gebruiken is. Alle intellectuele eigendom achter TLS is onherroepelijk vrijgegeven.

Toegevoegde waarde

TLS 1.3 biedt ten opzichte van eerdere versies van TLS een betere efficiëntie door gebruikmaking van de zogenaamde *TLS false start* en *Zero Round Trip Time* (0-RTT) technieken. Deze efficiëntieverbeteringen komen vooral bij browserverkeer tot uiting en minder bij server-server-koppeling (ebMS).

De belangrijkste verbeteringen zijn op het vlak van beveiliging, omdat een aantal beveiligingsrisico's wordt beperkt. Dit komt doordat TLS 1.2 een aantal onveilige configuraties uitsluit, met name het gebruik van de cyphersuites SHA-1, RC4, DES, 3DES, AES-CBC en MD5. De configuratie is in TLS 1.3 ook vereenvoudigd, waardoor er minder kans bestaan op een onveilige implementatie en gebruik van de standaard.

Draagvlak

Alhoewel TLS 1.3 nog een jonge standaard is, zal de adoptie door leveranciers snel gaan en veelal automatisch bij upgrades van software beschikbaar komen. OpenSSL.org, de meest gebruikte TLS open source bibliotheek ondersteunt TLS 1.3 reeds. Deze meeste commerciële en niet-commerciële server- en browserimplementaties bouwen op deze bibliotheek.

Alle experts die betrokken waren bij het expertonderzoek en alle organisaties die reageerden op de openbare consultatie onderkennen de toegevoegde waarde van TLS 1.3. Een aantal respondenten stelt wel vragen bij de huidige marktondersteuning voor de standaard.

Opname bevordert de adoptie

De experts alsmede de meerderheid van de organisaties die reageerden op de openbare consultatie, zijn het erover eens dat plaatsing van TLS 1.3 op de pas-toe-of-leg-uit lijst het juiste middel is om de adoptie van deze standaard te stimuleren en daarmee de veiligheid van verbindingen over het Internet te verhogen.

Hierbij wordt ook rekening gehouden met het feit dat TLS 1.3 al meer marktondersteuning zal hebben tegen de tijd dat de standaard daadwerkelijk op de pas-toe-of-leg-uit lijst wordt opgenomen (op z'n vroegst eind 2018 of begin 2019, rekening houdend met de agenda van het OBDO).

5.4 Wat is de conclusie van de expertgroep en de consultatie?

Conclusie van het expertonderzoek

Het expertonderzoek leidde tot een positief advies voor plaatsing van TLS 1.3 op de pas-toe-of-leg-uit lijst (zie [1]). De experts concludeerde dat het plaatsen van TLS versie 1.3 op de 'pas toe of leg uit'-lijst leidt tot twee verbeteringen ten opzichte van versie 1.2. Door het gebruik van TLS 1.3 wordt de standaard efficiënter en neemt de veiligheid toe.

In het expertadvies gaf de expertgroep de volgende adviezen:

- *TLS 1.3 dient in de IETF standards track minimaal gepubliceerd te zijn als "Proposed Standard".*
  TLS 1.3 had ten tijde van het expertonderzoek (juni 2018) de status "Proposed standard", waarbij de tekst van de specificatie (op dat moment versie 28) nog in eindredactie was. Dat betekent dat er op dat moment nog kleine wijzigingen in de tekst mogelijk waren.
  De expertgroep adviseerde om opname op de 'pas toe of leg uit'-lijst door te zetten onder

voorwaarde dat de IETF-editors de standaard niet terug zouden leggen bij de auteurs van de standaard. Als dit gebeurt zou de standaard inhoudelijk kunnen wijzigen en zou nieuwe toetsing nodig zijn. De kans dat dit gebeurt achtte de expertgroep zeer klein. De expertgroep deelde het gevoel dat we aan de vroege kant zijn met plaatsing van TLS 1.3 op de pas-toe-of-leg-uit lijst, maar dat het belang van stimulering van het gebruik van TLS 1.3 opweegt tegen het zeer kleine bovengenoemde risico dat de standaard wordt teruggelegd bij de auteurs.

- *Behoud TLS 1.2, TLS 1.1 en TLS 1.0 op de pas-toe-of-leg-uit lijst onder voorwaarde*
  TLS 1.3 wordt door experts beschouwd als de meest veilige versie, en moet daarom opgenomen worden op de pas-toe-of-leg-uit lijst. 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 onveilig 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.

Het advies *"TLS 1.3 dient in de IETF standards track minimaal gepubliceerd te zijn als "Proposed Standard"* is inmiddels overbodig omdat IETF RFC 8446 in augustus 2018 formeel werd gepubliceerd als "Proposed Standard". Een 'proposed standard' heeft bij de IETF de status van een afgeronde, stabiele standaard. Vele bekende standaarden zoals http hebben deze status 'proposed standard'. TLS 1.3 voldoet daarmee volledig aan het criterium 'open standaardisatieproces' voor opname op de pas-toe-of-leg-uit lijst.

Van het advies "*Behoud TLS 1.2, TLS 1.1 en TLS 1.0 op de pas-toe-of-leg-uit lijst onder voorwaarde"* wordt na de openbare consultatie gedeeltelijk afgeweken. Nu wordt geadviseerd om TLS 1.2 te handhaven maar TLS 1.1 en TLS 1.0 te verwijderen als "terugval-standaard" op de pas-toe-of-leg-uit lijst. Dit wordt in de volgende paragraaf toegelicht.

Analyse van reacties uit de openbare consultatie

Vanuit de openbare consultatie komen drie bezwaarpunten naar voren om TLS 1.3 nu al op te nemen op de pas-toe-of-leg-uit lijst:

1. Er is nog onvoldoende marktondersteuning. Eén organisatie stelt daarnaast dat onderzoek ontbreekt naar ondersteuning van TLS 1.3 op alle mobiele apparaten.
2. TLS 1.3 heeft nog geen formele status in IETF (Rinis, UWV, ministerie van Defensie). Ten tijde van de openbare consultatie had TLS 1.3 nog de status 'proposed standard internet-draft'. Potentieel was het mogelijk dat vanuit het redigeren van de teksten er nog een aanpassing van de standaard konden komen.
3. Het toepassingsgebied is te breed gedefinieerd: het ministerie van Defensie stelt dat zij toepassingen hebben die sterkere encryptiemiddelen dan TLS vereisen. Het ministerie van Defensie pleitte voor aanvullende adoptieactiviteiten om de veiligheid met het toepassen van TLS 1.3 ook werkelijk te laten toenemen.

De analyse van deze bezwaarpunten leidt tot de volgende conclusies:

1. De meest gebruikte open source library openssl.org ondersteunt inmiddels TLS 1.3. De servers van de meeste commerciële leveranciers gebruiken openssl.org onder de motorkap. TLS 1.3 staat op de roadmap van de meeste leveranciers. Het (moeten) uitvragen van TLS 1.3 bij aanbestedingen zal verder druk zetten op de markt om vaart te maken met de implementatie van de standaard.
2. IETF heeft RFC 8446 (TLS 1.3) in augustus 2018 formeel gepubliceerd als 'Proposed Standard'. Hiermee vervalt het argument dat TLS 1.3 nog geen formele status zou hebben.
3. Militair operationele applicaties zijn uitgesloten van de Instructie rijk inzake de aanschaf van ICT producten en diensten (bijlage, artikel 3 lid 3)[1].

Een aantal organisaties roept op om TLS 1.0 en TLS 1.1 van de lijst te verwijderen. Rechtspraak.nl roept daarbij op om met het NCSC te komen tot een gezamenlijk visie op de mate van beveiliging van TLS 1.3.

[1] http://wetten.overheid.nl/BWBR0024717/2008-11-23

In het expertonderzoek kwam dit ook ter sprake, maar Logius pleitte voor handhaving van TLS 1.0 en TLS 1.1 om gebruikers van oude smartphones niet buiten te sluiten van basisvoorzieningen als DigID en mijn.overheid. Daarbij werd opgemerkt dat TLS 1.1 en TLS 1.0 nog niet als onvoldoende veilig zijn aangemerkt door het NCSC.

Naar aanleiding van de reacties op de openbare consultatie, na beraad van experts en op basis van voortschrijdend inzicht wordt het advies overgenomen om TLS 1.1 en TLS 1.0 als “terugvalopties” van TLS 1.2 te verwijderen van de pas-toe-of-leg-uit lijst.

Door het van de ‘pas toe of leg uit’-lijst verwijderen van TLS 1.0 en TLS 1.1 wordt het gebruik van deze versies niet meer aangemoedigd; organisaties *mogen* deze versies echter nog wel blijven gebruiken om de compatibiliteit met oudere mobiele apparaten en browsers te waarborgen.

De experts houden vast aan het advies om de TLS-versies op de pas-toe-of-leg-uit lijst in lijn te houden met de richtlijnen van het NCSC.

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

De experts doen het Forum Standaardisatie en Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) de aanbeveling om bij de opname op de ‘pas-toe-of-leg-uit’-lijst de volgende oproep ten aanzien van de adoptie van TLS 1.3 te doen:

- Aan Forum Standaardisatie: Behoud de oudere versie TLS 1.2 eveneens op de lijst onder de voorwaarde dat deze door het NCSC niet als onveilig worden aangemerkt.
- Aan overheidsorganisaties: Controleer regelmatig met behulp van beschikbare validatie-tools, zoals Internet.nl, of TLS 1.3 en TLS 1.2 worden toegepast en controleer ook de veilige configuratie daarvan aan de hand van de geactualiseerde TLS-richtlijnen van NCSC. 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: Actualiseer de richtlijnen voor veilige TLS-configuratie en neem daar ook TLS 1.3 in op;
- 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 TLS wijzigt;
- Aan Logius/PKIoverheid: Breng de gactualiseerde NCSC-richtlijn actief onder de aandacht bij de uitgifte van certificaten aan de gebruikers van PKIoverheid;
- Aan Platform Internetstandaarden: ondersteun ook TLS 1.3 in de testen van Internet.nl.

6. Referenties

[1] Expertadvies TLS 1.3:
https://www.forumstandaardisatie.nl/sites/bfs/files/20180803%20Expertadvies%20TLS%201.3.pdf

[2] Reacties uit de consultatieronde TLS 1.3:
https://www.forumstandaardisatie.nl/sites/bfs/files/Commentaar%20uit%20de%20openbare%20consultatie%20TLS%201.3.pdf