Aanmelding TLS 1.3 voor de ‘pas toe of leg uit ‘-lijst

0. Persoonsgegevens indiener & relatie tot standaard

Deze gegevens worden door het Forum gebruikt om met u in contact te kunnen treden. De gegevens worden vertrouwelijk behandeld.

0.	Persoonsgegevens en relatie tot de standaard
0.1	Naam
	Michiel Leenaars
0.2	Organisatie
	NLnet
0.3	Functie:
	Directeur strategie
0.4	Telefoonnummer:
	020 8884252
0.5	E-mailadres:
	michiel@nlnet.nl
0.6	Welke relatie bestaat er tussen uw organisatie en de standaard?
	NLnet stimuleert het gebruik van moderne Internetstandaarden in Nederland.
0.7	Zijn er (andere) overheidsorganisaties die de aanmelding van deze standaard ondersteunen?
	Het NCSC ondersteunt deze aanmelding.

I. Basisinformatie aanmelding standaard

De basisinformatie van de standaard vormt de basis voor de toetsing tegen de criteria. Probeer hier zo volledig mogelijk in te zijn.

1.	**Basisinformatie standaard(en)** (In geval van een set van standaarden, meerdere malen invullen)
1.1	Volledige naam van de standaard
	Transport Layer Security (TLS) Protocol Version 1.3
1.2	Verkorte naam van de standaard
	TLS 1.3
1.3	Versie van de standaard, vaststellingsdatum en status
	Draft-ietf-tls-tls13-28, 20 maart 2018
1.4	Oudere en aanstaande versies van de standaard inclusief (verwachte) publicatiedata en ondersteuningsstatus
	[TLS1.0] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", https://www.ietf.org/rfc/rfc2246.txt, January 1999. [TLS1.1] Dierks, T. and E. Rescorla, "The Transport Layer Security(TLS) Protocol Version 1.1", https://tools.ietf.org/html/rfc4346, April 2006. [TLS1.2] Dierks, T. and E. Rescorla, "The Transport Layer Security(TLS) Protocol Version 1.2", https://tools.ietf.org/html/rfc5246, Augustus 2008
1.5	Naam en vindplaats specificatiedocument (bij voorkeur URL of bijvoegen bij aanmelding)
	https://tools.ietf.org/html/draft-ietf-tls-tls13-28
1.6	Naam van de standaardisatieorganisatie
	IETF
1.7	Kosten van deelname aan het standaardisatieproces (bijv. voor lidmaatschap)
	0
1.8	Kosten voor het verkrijgen van het specificatiedocument
	0
1.9	Andere standaarden die genoemd worden in het specificatiedocument van de standaard
	Zie https://tools.ietf.org/html/draft-ietf-tls-tls13-28#section-12
1.10	Hoe werkt de standaard? (graag op een bondige en voor een buitenstaander duidelijke manier beschrijven hoe de standaard werkt en wat deze mogelijk maakt)

	Protocol-onafhankelijke beveiliging van internetverbindingen waarbij beide zijden elkaar kunnen authenticeren en een encryptie-algorithme en cryptographische sleutels kunnen onderhandelen voor de rest van de verbinding wordt opgezet.

2.	Toepassings- en werkingsgebied van opname
2.1	Wat is het beoogde functioneel toepassingsgebied voor de standaard?
	TLS moet worden toegepast op de uitwisseling van gegevens tussen clients en servers, inclusief machine-to-machine communicatie.
2.2	Wat is het beoogde organisatorisch werkingsgebied voor de standaard? (*hoeft alleen ingevuld te worden als de standaard op de "pas toe of leg uit" –lijst is opgenomen*
	Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de publieke sector

II. Criteria voor inbehandelname

De criteria voor inbehandelname worden gebruikt tijdens de intake om te bepalen of een aanmelding correct is en binnen de scope van de lijsten valt. U kunt voor het beantwoorden van deze vraag de tekstvlakken bij de betreffende criteriavragen gebruiken.

Criteria: De aanmelding is correct en valt binnen scope van de lijsten, d.w.z. de standaard:

- Is toepasbaar voor elektronische gegevensuitwisseling tussen en met (semi-)overheidsorganisaties;
- Draagt binnen het beoogde opnamegebied substantieel bij aan de interoperabiliteit van de (semi-)overheid;
- Is niet reeds wettelijke verplicht.

1.	Valt de aangemelde standaard binnen de scope van de lijsten?
1.1	Is de standaard toepasbaar voor elektronische gegevensuitwisseling tussen (semi-)overheidsorganisaties en bedrijven, tussen (semi-)overheidsorganisaties en burgers of tussen (semi-)overheidsorganisaties onderling?
	Ja.
1.2	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. Zeker met gebruik van STARTTLS en DANE die ook op de 'pas toe of leg uit' lijst staan.
1.3	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 1.3 biedt betere beveiliging dan de voorgaande versies 1.2, 1.1 en 1.0.

III. Inhoudelijke criteria

1. Inhoudelijk criterium: Toegevoegde waarde

Criterium: De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de risico's en nadelen.

Vragen:

1.1	Verhoudt de standaard zich goed tot andere standaarden?
1.1.1	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. Voorgesteld wordt om TLS 1.3 op te nemen als voorkeursversie van TLS, maar TLS 1.2, 1.1 en 1.0 nog wel toe te staan.
1.1.2	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. Ten opzichte van TLS 1.2 biedt TLS 1.3 twee verbeteringen. TLS 1.3 is efficiënter en en leidt daarom tot snellere implementaties. Belangrijker nog is dat TLS 1.3 een aantal overbodige opties uit TLS 1.2 weglaat, waardoor er minder kans bestaat dat het protocol op een onveilige manier geconfigureerd wordt. TLS 1. 3 heeft minder kwetsbaarheden dan TLS 1.2.
1.1.3	Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname?
	TLS heeft geen concurrerende standaarden. Wel zijn er verschillende versies van TLS in gebruik. Het voorstel is dan ook om TLS 1.3 als voorkeursversie op de 'pas toe of leg uit' lijst te plaatsen, maar het gebruik van TLS 1.2, 1.1 en 1.0 ook toe te staan.
1.1.4	Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden?
	Ja. TLS 1.3 is een IETF standaard en wordt over het hele Internet wereldwijd toegepast.
1.1.5	Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn?
	Ja. TLS is een beproefd mechanisme dat applicatie-onafhankelijk is.

1.2	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?

1.2.1	Draagt de adoptie van de standaard bij aan de oplossing van een bestaand, relevant interoperabiliteitsprobleem?
	TLS is van essentieel belang bij het beveiligen van Internetverbindingen.
1.2.2	Draagt de standaard bij aan het voorkomen van een vendor lock-in (leveranciersafhankelijkheid)?
	Er zijn zowel open source implementaties als commerciële producten die TLS ondersteunen.
1.2.3	Wegen de overheidsbrede en maatschappelijke baten voor de informatievoorziening en de bedrijfsvoering op tegen de kosten?
	Ja. Beveiliging van Internetverbindingen met overheidswebsites en – diensten is van essentieel maatschappelijk belang.
1.2.4	Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel?
	Ja, eerder omgekeerd. De beveiligingsrisico's van het uitblijven van adoptie zijn onacceptabel.
1.2.5	Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel?
	Ja, eerder omgekeerd. De privacyrisico's van het uitblijven van adoptie zijn onacceptabel (zeker gezien internationale ontwikkelingen van afgelopen jaar).

2. Inhoudelijk criterium: Open standaardisatieproces

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

Vragen:

2.1	Is de documentatie voor eenieder drempelvrij beschikbaar?
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 specificatie is vrij en gratis beschikbaar.
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 lidmaatschapseisen)?
	Ja. Dit is vrij en gratis beschikbaar op de website van de IETF.

2.2	Is het intellectuele eigendomsrecht voor eenieder beschikbaar, zodat de standaard vrij implementeerbaar en te gebruiken is
2.2.1	Stelt de standaardisatieorganisatie het intellectueel eigendomsrecht op de standaard m.b.t. bijvoorbeeld eventuele patenten- onherroepelijk royalty-free voor eenieder beschikbaar?
	ja. Op de TLS specificatie zelf rust geen intellectueel eigendom.
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?
	Onbekend. De École Nationale Superieure Des Telecommunications (Frankrijk) heeft een IPR declaratie gedaan ten aanzien van TLS 1.3 (zie https://datatracker.ietf.org/ipr/2900/). Of dit intellectuele eigendom onherroepelijk is vrijgegeven, is niet bekend. Dit moet in de toetsingsprocedure worden onderzocht.

2.3	Is de inspraak van eenieder in voldoende mate geborgd?
2.3.1	Is het besluitvormingsproces toegankelijk voor alle belanghebbenden (bijv. gebruikers, leveranciers, adviseurs, wetenschappers)?
	Ja. IETF heeft een zeer open standaadisatie- en beheerproces.
2.3.2	Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen?
	Ja. Zie 2.3.1, 2.3.4 en 2.3.5.

2.3.3	Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde procedure?
	Ja. Zie 2.3.1, 2.3.4 en 2.3.5.

2.3.4	Organiseert de standaardisatieorganisatie regelmatig overleggen met belanghebbenden over doorontwikkeling en beheer van de standaard?
	Ja. Via de Working Group structuur.
2.3.5	Organiseert de standaardisatieorganisatie een publieke consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld?
	Ja. Via het Request for Comments mechanisme.

2.4	Is de standaardisatieorganisatie onafhankelijk en duurzaam?
2.4.1	Is de ontwikkeling en het beheer van de standaard belegd bij een onafhankelijke non-profit standaardisatieorganisatie?
	Ja, de IETF.
2.4.2	Is de financiering van de ontwikkeling en het onderhoud van de standaard voor tenminste drie jaar gegarandeerd?
	Ja, de IETF en de TLS Working Group zijn zeer stabiele en duurzame groepen.

2.5	Is het (versie) beheer van de standaard goed geregeld?
2.5.1	Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot versiebeheer van de standaard? (met o.a. aandacht voor migratie van gebruikers)
	Ja. Volgens het standaard versiebeheer van de IETF.
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?

	Nee. Het is aan te raden om nieuwe versies van TLS wel te toetsen alvorens over te gaan tot opname op de 'pas toe of leg uit' lijst.
2.5.3	Is het belang van de Nederlandse overheid voldoende geborgd bij de ontwikkeling en het beheer van de standaard?
	Ja. Het staat Nederlandse overheidsorganisaties overigens ook vrij om deel te nemen in de ontwikkeling en het beheer van IETF standaarden.

3. Inhoudelijk criterium: Draagvlak

Criterium: Aanbieders en gebruikers hebben voldoende positieve ervaring met de standaard.

Vragen:

3.1	Bestaat er voldoende marktondersteuning voor de standaard?
3.1.1	Bieden meerdere leveranciers ondersteuning voor de standaard?
	Ja. Er is ook tenminste een open source implementatie.
3.1.2	Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen?
	Ja. Dit kan onder andere via internet.nl wanneer deze test is geïmplementeerd.

3.2	Kan de standaard rekenen op voldoende draagvlak?
3.2.1	Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt?
	TLS 1.3 is een recent gepubliceerde standaard. Deze wordt nog niet breed gebruikt.
3.2.2	Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt?
	Ja, TLS 1.2, 1.1 en 1.0 worden door vrijwel hele overheid gebruikt op alle bestuurslagen.
3.2.3	Is de aangemelde versie backwards compatible met eerdere versies van de standaard?
	Nee. Implementaties van TLS bieden echter wel een 'onderhandelingsmechanisme' waarmee de client en server een werkbare TLS versie kunnen vinden die beide ondersteunen. In de praktijk functioneert dit al in vrijwel alle browsers en webservers.
3.2.4	Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?
	Ja. Het is de verwachting dat TLS 1.3 de norm gaat worden voor veilige Internetverbindingen.

4. Inhoudelijk criterium: Opname bevordert adoptie

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

Toelichting lijsten:

a. Met de lijsten wil het College de adoptie van open standaarden bevorderen die voldoen aan de voorgaande criteria (open standaardisatieproces, toegevoegde waarde, draagvlak);
b. Met de "pas toe of leg uit"-lijst beoogt het College dit soort standaarden verplichten als:
    1. hun huidige adoptie binnen de (semi-)overheid beperkt is;
    2. opname op de lijst bijdraagt aan de adoptie door te stimuleren o.b.v. het "PToLU"-regime. (functie=stimuleren).
c. Met de lijst met gangbare standaarden beoogt het College dit soort standaarden aan te bevelen als:
    1. hun huidige adoptie binnen de (semi-)overheid reeds hoog is;
    2. opname op de lijst bijdraagt aan de adoptie door te informeren en daarmee onbedoelde afwijkende keuzes te voorkomen. (functie=informeren)

Vragen:

4.1	Opname op de lijst bevordert de adoptie van de standaard.
4.1.1	Is de "pas toe of leg uit"-lijst het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?
	Ja. Bewustwording is het grote probleem. De 'pas toe of leg uit' lijst heeft een belangrijke rol in het kader van 'agenda setting'.
4.1.2	Is de lijst met aanbevolen open standaarden het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?
	Nee, de lijst aanbevolen standaarden is te vrijblijvend. Het is van belang dat overheidsorganisaties de laatste en meest veilige versie van TLS inzetten.