Forum Standaardisatie

Expertadvies TLS 1.2

Datum 12 februari 2014

Colofon

Projectnaam	Expertadvies TLS 1.2
Versienummer	1.0
Locatie	
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag forumstandaardisatie@logius.nl

Auteurs	Bart Gijsen Michael van Bekkum

Inhoud

Managementsamenvatting

Wat is de conclusie van de expertgroep en de consultatie?

De expertgroep adviseert de standaard TLS 1.2 op te nemen op de lijst van 'pas toe of leg uit' .

Als toepassingsgebied wordt geadviseerd:
"Het via certificaten beveiligen van gegevensuitwisseling tussen client- en serversystemen of tussen serversystemen onderling, voor zover deze gerealiseerd wordt met internet / IP technologie."

En als werkingsgebied:
"Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de publieke sector."

In het kort adviseert de expertgroep het volgende:
1. Zorg ervoor dat nieuw aan te schaffen ICT-systemen ondersteuning bieden voor TLS1.2 indien deze vallen binnen het toepassingsgebied (geldt voor alle overheden binnen werkingsgebied).
2. Houd rekening met terugval-opties (oudere versies) als dat omwille van interoperabiliteit noodzakelijk is (geldt voor alle overheden binnen werkingsgebied).
3. Volg bestaande internationale best practices (o.a. van SSLlabs, OWASP en NCSC) m.b.t. gebruik van TLS.
4. Ontwikkel een nederlandse versie van deze best practices (zie aanvullende adoptie maatregelen).

Hierbij plaatst de expertgroep de volgende kanttekeningen:
- Het ondersteunen van TLS 1.2 is slechts noodzakelijk indien in de bredere context van beveiligingsvoorschriften is bepaald dat het gebruik van een versleutelde gegevensuitwisseling gewenst is.
- Indien interoperabiliteit dit noodzakelijk maakt, kunnen eerdere versies van TLS worden gebruikt. Versie 2 en ouder van het SSL protocol zouden echter niet meer gebruikt moeten worden.
- De keuze voor de te gebruiken TLS versie is slechts één van de keuzes die genomen moet worden bij het beveiligen van gegevensuitwisseling. TLS zal ondersteund moeten worden in samenhang met andere (internet)standaarden om de gegevensuitwisseling met behulp van versleuteling te beveiligen.

Waar gaat het inhoudelijk over?

TLS is een protocol, dat tot doel heeft om beveiligde verbindingen over het internet te verzorgen. De standaard wordt gebruikt bovenop standaard internet transport protocollen (TCP/IP) en biedt een beveiligde basis, waar applicatie protocollen als HTTP (webverkeer) of IMAP/POP3/SMTP (mailuitwisseling) op hun beurt weer op kunnen bouwen. TLS maakt gebruik van certificaten om zekerheid te bieden over de identiteit van een of beide communicerende partijen voordat communicatie plaatsvindt. Ook wordt met behulp van (het sleutelpaar van) de certificaten op betrouwbare wijze de encryptiesleutel uitgewisseld,

die de standaard vervolgens gebruikt om met behulp van encryptie techniek beveiligde communicatie tussen partijen mogelijk te maken.

TLS wordt (in combinatie met andere standaarden) veelal gebruikt in situaties waarin het van belang is om vast te kunnen stellen of men als gebruiker verbonden is met de juiste server of (overheids)website, zodat persoonlijke of vertrouwelijke informatie kan worden uitgewisseld.

Hoe is het proces verlopen?

Op 23 januari 2014 is een expertgroep met vertegenwoordigers uit het bedrijfsleven en de overheid bijeen gekomen om de standaarden TLS 1.2 en DANE te toetsen. Vooraf zijn de aanwezige experts en enkele anderen die niet aanwezig konden zijn, in de gelegenheid gesteld input aan te leveren. Op basis van deze input en de discussie tijdens de bijeenkomst is dit adviesrapport opgesteld.

Hoe scoort de standaard op de toetsingscriteria?

Toegevoegde waarde

De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de risico's en nadelen. Technisch gezien biedt TLS 1.2 de mogelijkheid tot verbetering van de beveiliging van elektronische gegevensuitwisseling van, naar en tussen overheidsinstellingen. TLS kan worden gebruikt in combinatie met andere internetstandaarden, zoals voor webverkeer (HTTP), e-mail (POP3, IMAP, SMTP) en bestanden (FTP).

Open standaardisatieproces

De standaard wordt beheerd door IETF. Deze organisatie heeft goed gedocumenteerde en open beheerprocedures. Er is geen lidmaatschap, iedereen kan wijzigingsverzoeken indienen, het beheerproces en de besluitvorming zijn open en transparant en er zijn geen kosten verbonden aan het downloaden van de specificatie en het implementeren van de standaard.

Draagvlak

Diverse beveiligingsvoorschriften (o.a. Digikoppeling) verwijzen naar specifiek voorgeschreven versies van TLS (niet alleen versie 1.2). Belangrijke Overheidsdomeinen ondersteunen verschillende versies van TLS (bv. DigiD, MijnOverheid: TLS 1.2; Rijksoverheid: TLS 1.0). Ondersteuning voor TLS 1.2 is dus een mogelijke aanvulling op deze andere ondersteunde versies. Alle populaire desktop browsers en moderne operating systems ondersteunen TLS 1.2.

Opname bevordert de adoptie

De meerderheid van de experts is van mening dat het opnemen van TLS 1.2 op de lijst een middel is dat adoptie van de standaard zal bevorderen. Leveranciers zien de 'pas-toe-of-leg-uit'- lijst als een (milde) vorm van marktvraag en nemen de standaard daardoor mee in hun toekomstige

product roadmaps. Bij architecten en experts binnen de overheid bevordert opname het gebruik van de standaard in aanbestedingen en in de uitvoering van projecten.

De standaard biedt verbeteringen ten opzichte van de huidige versie 1.0, die nu op de lijst met gangbare standaarden staat. De standaard geldt als een toekomstvaste upgrade van deze en andere/oudere versies, waarvan bekend is dat ze (nu nog) in beperkte mate vatbaar zijn voor aanvallen en dus onvoldoende privacy en veiligheid kunnen bieden. De lijst met gangbare standaarden stimuleert echter volgens de expertgroep de hierboven genoemde marktvraag en opname in aanbestedingen onvoldoende. Verder wordt het belang van toekomstvaste beveiliging met deze lijst onvoldoende ondersteund. Aangezien niet alle organisaties uit publieke sector automatisch ondersteuning bieden aan TLS 1.2 is de expertgroep daarom van mening dat het noodzakelijk is om TLS 1.2 op de 'pas-toe-of-leg-uit'- lijst te plaatsen. TLS 1.0 kan dan van de lijst met gangbare standaarden worden verwijderd.

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

De expertgroep adviseert aanvullend de volgende maatregelen, die adoptie van de standaard TLS 1.2 kunnen bevorderen:

- Nalopen en updaten van verwijzingen naar alternatieven of oudere versies in relevante beveiligingvoorschriften (b.v. DigiKoppeling).
- Opstellen van een Nederlandse instructie en best practice handleiding (NCSC ism Logius (PKIoverheid), beheerders van sectorale baselines IB).
- Inrichten van een vraagbaak en delen van best practices ten behoeve van aanvullende ondersteuning voor de toepassing van TLS 1.2 (NCSC ism Taskforce BID, CIP of TIP).
- Monitor kwetsbaarheden in TLS en informeer (semi-)publieke sector daarover (NCSC).

1 Doelstelling expertadvies

1.1 Achtergrond

In 2007 is door het kabinet besloten tot een actieplan Nederland Open in Verbinding [1]. Het doel van dit actieplan is om de informatievoorziening toegankelijker te maken, onafhankelijkheid van ICT-leveranciers te creëren en de weg vrij te maken voor innovatie.

Eén van de maatregelen van het actieplan is het gebruik van een lijst met standaarden, die vallen onder het principe "pas toe of leg uit" (comply-or-explain) [2]. Het College Standaardisatie, dat in 2006 door het kabinet is ingesteld, spreekt zich uit over de standaarden die op de lijst zullen worden opgenomen, o.a. op basis van een expertbeoordeling van de standaard [3]. Het College Standaardisatie wordt geadviseerd door het Forum Standaardisatie. Bureau Forum Standaardisatie ondersteunt beide instellingen.

Een elftal experts is verzameld in een expertgroep, die de standaard heeft beoordeeld aan de hand van een aantal criteria. Deze criteria – vooraf vastgesteld door het College Standaardisatie [4] en uitgewerkt in de vorm van concrete vragen - worden in het hier voorliggende expertadvies genoemd en behandeld.

Onderwerp van dit expertadvies is TLS 1.2. Deze standaard is aangemeld door Michiel Leenaars, directeur strategie van NLnet, voor opname op de lijst met open standaarden voor 'pas toe of leg uit'. De opdracht aan de expertgroep was om een advies op te stellen over het wel of niet opnemen van deze standaard op de lijst, al dan niet onder bepaalde voorwaarden.

1.2 Proces

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

- Door het Bureau Forum Standaardisatie is een intakegesprek gevoerd met de indiener op 20 november 2013. Hierin is de standaard getoetst op uitsluitingscriteria ('criteria voor in behandelname') en is een eerste inschatting gemaakt van de kansrijkheid voor opname.
- Op basis van de intake is besloten tot het instellen van een expertgroep. Op basis van dit besluit is door het Bureau Forum Standaardisatie een groep samengesteld en een voorzitter aangezocht. Op basis van de aanmelding en de intake is een voorbereidingsdossier opgesteld voor leden van de expertgroep.
- De expertgroep is begonnen met het individueel scoren van TLS 1.2 aan de hand van een spreadsheet met vragen in het voorbereidingsdossier. Op basis van de verkregen antwoorden hebben voorzitter en begeleider van de expertgroep de verschillende knelpunten geïdentificeerd.
- Vervolgens is de expertgroep op 23 januari 2014 bijeengekomen om de bevindingen in het algemeen en de geïdentificeerde knelpunten in het bijzonder te bespreken. Tijdens deze bijeenkomst zijn ook het toepassings- en werkingsgebied vastgesteld.

De uitkomsten van de expertgroep zijn door de voorzitter en begeleider verwerkt in dit adviesrapport. Een eerste conceptversie is aan de leden van de expertgroep gestuurd met verzoek om reactie. Na verwerking van de reacties is het rapport afgerond, nogmaals toegestuurd aan de experts en ingediend voor de publieke consultatieronde.

1.3 Vervolg

Dit expertadvies zal ten behoeve van een publieke consultatie openbaar worden gemaakt door het Bureau Forum Standaardisatie. Eenieder kan gedurende de consultatieperiode op dit expertadvies 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 College Standaardisatie opstellen. Het College Standaardisatie bepaalt uiteindelijk op basis van het advies van het Forum of de standaard op de 'pas toe of leg uit'-lijst komt.

1.4 Samenstelling expertgroep

Voor de expertgroep zijn personen uitgenodigd die vanuit hun persoonlijke expertise of werkzaamheden bij een bepaalde organisatie direct of indirect betrokken zijn bij de standaard. Het Forum streeft naar een zo representatief mogelijke expertgroep, met een evenwichtige mix van eindgebruikers, IT-leveranciers, wetenschappers, adviseurs, en vertegenwoordigers van de standaardisatieorganisatie. Zowel technische experts als experts die inzicht hebben in de functionele impact zijn uitgenodigd. Daarnaast is een onafhankelijke voorzitter aangesteld om de expertgroep te leiden en als verantwoordelijke op te treden voor het uiteindelijke expertadvies.

Als voorzitter is opgetreden Bart Gijsen, senior consultant bij TNO op het gebied van Vitale Infrastructuren en Internet Security.

De expertgroep is in opdracht van het Forum Standaardisatie begeleid door Michael van Bekkum, adviseur standaarden en interoperabiliteit bij TNO.

Aan de expertgroep hebben deelgenomen:
- Dhr. Michiel Leenaars (Stichting NLnet)
- Dhr. Marco Davids (SIDN)
- Dhr. Frank Heijligers (MinBZK)
- Dhr. Rolf Sonneveld (Sonnection)
- Dhr. Joost van Dijk (SURFnet)
- Dhr. Rene Schut (DUO)
- Dhr. Willem Kossen (BKWI)
- Dhr. Joachim Schipper (Fox-IT)
- Dhr. Theo van Diepen (Logius)
- Dhr. Pieter Rogaar (NCSC)
- Dhr. Arno Meulenkamp (Infoblox)
- Dhr. Douglas Skirving (Logius / PKIOverheid)
- Dhr. Rob Brand (MinEZ)

Als toehoorder was aanwezig:

- Dhr. Lancelot Schellevis (Bureau Forum Standaardisatie)

1.5 Toelichting TLS 1.2

TLS is een protocol, dat tot doel heeft om beveiligde verbindingen over het internet te verzorgen. De standaard wordt gebruikt bovenop standaard internet transport protocollen (TCP/IP) en biedt een beveiligde basis, waar applicatie protocollen als HTTP (webverkeer) of IMAP (mailuitwisseling) op hun beurt weer op kunnen bouwen en gebruik van kunnen maken.

TLS maakt gebruik van certificaten om zekerheid te bieden over de identiteit van beide communicerende partijen voordat communicatie plaatsvindt. Ook wordt met behulp van (het sleutelpaar van) de certificaten op betrouwbare wijze de encryptiesleutel uitgewisseld, die de standaard vervolgens gebruikt om met behulp van encryptie techniek beveiligde communicatie tussen partijen mogelijk te maken.

TLS wordt (in combinatie met andere standaarden) veelal gebruikt in situaties waarin het van belang is om vast te kunnen stellen of men als gebruiker verbonden is met de juiste server of (overheids)website, zodat persoonlijke of vertrouwelijke informatie kan worden uitgewisseld. De standaard biedt een veilige basis onder bijna alle denkbare internet toepassingen (internet browsing, mailuitwisseling, instant messaging, VoIP, etc.)

1.6 Relatie met andere standaarden

Er bestaat een relatie met een andere standaard die voorkomt op de lijst voor ‘pas toe of leg uit’:
- *Digikoppeling*

Een eventuele plaatsing van TLS 1.2 op de lijst voor ‘pas toe of leg uit’ betekent een nadere beschouwing van het gebruik van TLS v1.0 in Digikoppeling. Dit aandachtspunt is meegenomen in dit expertadvies.

Er bestaat een relatie met een andere standaard die voorkomt op de lijst met gangbare open standaarden:
- *TLS v1.0*

Een eventuele plaatsing van TLS 1.2 op de lijst voor ‘pas toe of leg uit’ betekent een verwijdering van TLS v1.0 van de lijst. Dit aandachtspunt is meegenomen in dit expertadvies.

1.7 Leeswijzer

In hoofdstuk 2 wordt beschreven in welke gevallen de standaard functioneel gezien gebruikt zou moet worden (functioneel toepassingsgebied) en door welke organisaties deze gebruikt zou moeten worden (organisatorisch werkingsgebied).

Om te bepalen of de standaard opgenomen moet worden op de lijst met standaarden voor 'pas toe of leg uit', is deze getoetst aan een viertal door het College Standaardisatie vastgestelde criteria. In hoofdstuk 3 staat het resultaat van deze toetsing.

2 Toepassings– en werkingsgebied

Van overheidsorganisaties wordt verwacht dat zij de lijst met open standaarden hanteren bij aanbestedingstrajecten volgens het "pas toe of leg uit"-regime. Afhankelijk van de aan te schaffen functionaliteit zal bepaald moeten worden welke koppelvlakken geïmplementeerd moeten worden, en welke standaarden uit de lijst hiervoor ingezet dienen te worden. Om dit te kunnen doen heeft de expertgroep gekeken in welke gevallen de standaard functioneel gezien gebruik moeten worden (functioneel toepassingsgebied), en door welke organisaties deze gebruikt zou moeten worden (organisatorisch werkingsgebied).

2.1 Functioneel toepassingsgebied

Als functioneel toepassingsgebied wordt voorgesteld:

"Het via certificaten beveiligen van gegevensuitwisseling tussen client- en serversystemen of tussen serversystemen onderling, voor zover deze gerealiseerd wordt met internet / IP technologie."

Het plaatsen van TLS 1.2 op de 'pas-toe-of-leg-uit'-lijst sluit ondersteuning van voorgaande (of opvolgende) TLS versies niet uit. In overeenstemmig met het mandaat van de lijst, betekent plaatsing dat gebruik van versie 1.2 de voorkeur verdient en uitleg gewenst is indien hier van wordt afgeweken en alleen andere versies van TLS worden ondersteund.
De expertgroep heeft bij het functioneel toepassingsgebied dan ook een aantal overwegingen:

- De TLS standaard is een essentieel onderdeel in het bewerkstelligen van (zeer veel soorten van) beveiligde elektronische gegevensuitwisseling. In die context raakt plaatsen van TLS (versie 1.2) op de 'pas-toe-of-leg-uit'-lijst aan risico management en besluitvorming over beveiliging van de informatievoorziening van de overheid in het algemeen. De keuze voor de te gebruiken TLS versie is dan slechts één van de keuzes die genomen moet worden bij het beveiligen van gegevensuitwisseling. TLS zal ondersteund moeten worden in samenhang met andere (internet)standaarden om de gegevensuitwisseling met behulp van versleuteling te beveiligen.
- Het ondersteunen van TLS 1.2 is slechts noodzakelijk indien in de bredere context van beveiligingsvoorschriften is bepaald dat het gebruik van een versleutelde gegevensuitwisseling gewenst is.
- Een uniforme verplichting van het gebruik van (alleen deze versie van) TLS is op moment van schrijven ook niet realistisch en onwenselijk. In sommige gevallen maakt TLS of functioneel vergelijkbare technologie[1] onlosmakelijk onderdeel uit van een groter geheel (appliances[2] of operating systems van bijvoorbeeld smart phones), die gebaseerd kan zijn op een alternatief voor, of andere versie van TLS. In dat geval is ontbreken van TLS 1.2 onderdeel van

1 Versies van SSL zijn een voorbeeld van standaarden die vergelijkbaar zijn met TLS.
2 Een, meestal gesloten, 'apparaat' dat doorgaans bestaat uit afzonderlijke en discrete hardware met geïntegreerde software (firmware), die speciaal ontworpen is voor het uitvoeren van een specifieke taak.

een breder omvattende beoordeling van de oplossing als geheel, waardoor afgeweken kan worden van het toepassen van de standaard. Ook kunnen er op basis van risico analyses voor een bredere beveiliging context (b.v. DigiKoppeling) beargumenteerde keuzes gemaakt zijn voor alternatieven voor TLS 1.2.
- Indien interoperabiliteit dit noodzakelijk maakt, kunnen eerdere versies van TLS worden gebruikt. Versie 2 en ouder van het SSL protocol zouden echter niet meer gebruikt moeten worden.

2.2 Organisatorisch werkingsgebied

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

Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.

Bovenstaande omschrijving van het werkingsgebied bevat naar de mening van de expertgroep direct of indirect alle relevante partijen op wie de standaard van toepassing is. De expertgroep zag geen reden om bovenstaand werkingsgebied verder in te perken.

3 Toetsing van standaard aan criteria

Om te bepalen of de standaard opgenomen moet worden op de lijst met open standaarden is deze getoetst aan een aantal criteria. Er zijn vier hoofdcriteria:

1. Toegevoegde waarde
2. Open standaardisatieproces
3. Draagvlak
4. Opname bevordert adoptie

Deze criteria staan beschreven in het rapport, *"Toetsingprocedure en criteria voor indieners en experts"* [4] en staan op de website www.forumstandaardisatie.nl/open-standaarden. Het resultaat van de toetsing zal in dit hoofdstuk per criterium beschreven worden. Voor de volledigheid is tevens de definitie 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, dat is naar de mening van de expertgroep het geval. De standaard is generiek toepasbaar voor beveiliging van elektronische gegevensuitwisseling tussen (semi-)overheidsorganisaties en bedrijven, tussen (semi-) overheidsorganisaties en burgers of tussen (semi-) overheidsorganisaties onderling. Naar de mening van de expertgroep zijn er geen functies in het toepassingsgebied benoemd die de standaard niet ondersteunt.

3.1.1.2 Is het organisatorisch werkingsgebied goed gedefinieerd?

Ja, het in hoofdstuk 2 voorgestelde organisatorische werkingsgebied bevat naar mening van de expertgroep alle relevante partijen op wie de standaarden van toepassing kunnen worden verklaard binnen de scope van de lijst met open standaarden voor "pas toe of leg uit".

3.1.1.3 Is de standaard generiek toepasbaar en niet alleen bedoeld voor gegevensuitwisseling met één of een beperkt aantal specifieke voorzieningen? (toelichtende vraag)

De standaard is universeel toepasbaar voor vele soorten internetverkeer en is niet beperkt tot specifieke voorzieningen.

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)?

Voor de standaard is er overlap met de standaard Digikoppeling op de PToLU lijst. Digikoppeling gebruikt in haar WUS koppelvlak standaard V3.0 een eerdere versie, TLS v1.0.

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.)

TLS 1.2 biedt verbeteringen ten opzichte van TLS v1.0, die nu op de lijst met gangbare standaarden staat. De versie 1.2 van de standaard geldt als een toekomstvaste upgrade van deze en andere/oudere versies, waarvan bekend is dat ze (nu nog in beperkte mate) vatbaar zijn voor aanvallen en dus geen volledige privacy en veiligheid kunnen bieden.

3.1.2.3 Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname? (toelichtende vraag)

Naar de mening van de expertgroep is er niet direct een concurrerende standaard voorhanden.

3.1.2.4 Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden? (toelichtende vraag)

TLS 1.2 is een internationale standaard, ontwikkeld en beheerd door de internationale non-profit organisatie IETF. TLS 1.2 kan worden gezien als een basiscomponent in een internet-security-architectuur.

3.1.2.5 Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn? (toelichtende vraag)

Er zijn voor de standaard geen aanvullende afspraken nodig om interoperabiliteit te bewerkstelligen. Correcte werking van de standaard vergt door de vele configuratiemogelijkheden wel de nodige finetuning bij de installatie. Daarvoor zijn de nodige handleidingen en best practices beschikbaar, o.a. bij NCSC[3], OWASP[4] en SSL Labs[5].

3 https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html
4 https://www.owasp.org/index.php/SSL_TLS_Knowledge_Center
5 https://www.ssllabs.com/projects/best-practices/

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 Draagt de adoptie van de standaard bij aan de oplossing van een bestaand, relevant interoperabiliteitsprobleem?

TLS wordt (in combinatie met andere standaarden) veelal gebruikt in situaties waarin het van belang is om vast te kunnen stellen of men als gebruiker verbonden is met de juiste server of (overheids)website, zodat persoonlijke of vertrouwelijke informatie kan worden uitgewisseld. De standaard biedt een veilige basis onder bijna alle denkbare internet toepassingen (internet browsing, mailuitwisseling, instant messaging, VoIP, etc.). TLS kan dan ook worden gebruikt in combinatie met andere internetstandaarden, zoals voor webverkeer (HTTP), e-mail (POP3, IMAP, SMTP) en bestanden (FTP).

3.1.3.2 Draagt de standaard bij aan het voorkomen van een vendor lock-in (leveranciersafhankelijkheid)?

Voor TLS 1.2 bestaan meerdere open implementaties in software en libraries, die vrij verkrijgbaar zijn. Van vendor lock-in is bij TLS 1.2 dus geen sprake.

3.1.3.3 Wegen de overheidsbrede en maatschappelijke baten voor de informatievoorziening en de bedrijfsvoering op tegen de kosten?

Ja. TLS maakt nu al onderdeel uit van vele communicatie systemen en –voorzieningen. Nu al producten en diensten aankopen die TLS 1.2 ondersteunen, is een relatief kleine stap die ervoor zorgt ervoor dat een kostbare en overhaaste snelle overstap over enkele jaren niet nodig zal zijn

Met TLS 1.2 wordt verder een aantal kwetsbaarheden in de eerdere versies van de standaard opgelost. Met name voor TLS 1.0 geldt, dat het te verwachten is dat er binnen enkele jaren een grootschalige overstap naar TLS 1.2 noodzakelijk gaat zijn. TLS 1.0 biedt in dat scenario onvoldoende veiligheid voor de uitwisseling van gevoelige gegevens. De baten van het gebruik van TLS 1.2 ten opzichte van deze eerdere versies laten zich dan ook met name zien in de afname van de kans dat een dergelijke kwetsbaarheid wordt misbruikt door een kwaadwillende, met alle (imago)schade en kosten van dien.

De baten wegen daarmee op tegen de kosten.

3.1.3.4 Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel?

Het aanbieden van deze standaard kent in grote lijnen slechts beveiligingsvoordelen, omdat de standaard een veiligere en meer toekomstvaste variant is van de nu al gangbare versie 1.0.

Gezien de kwetsbaarheden in deze (en andere) eerdere versies van de standaard, gecombineerd met de noodzaak voor beveiligde verbindingen bij het aanbieden van online overheidsdienstverlening, lijkt het (op termijn) niet adopteren van TLS 1.2 niet acceptabel.

Bij het beveiligen van gegevensuitwisseling zal ondersteuning voor TLS daarbij in samenhang met andere beveiligingsstandaarden bekeken moeten worden.

3.1.3.5 Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel?

De online dienstverlening vanuit de overheid uit zich in de vorm van gegevensuitwisseling tussen overheid en burger enerzijds en tussen overheidsentiteiten anderzijds. Deze gegevens betreffen in veel gevallen persoonsgegevens. Het aanbieden van dergelijke dienstverlening zonder daarbij adequate beveiligingsmaatregelen aan te bieden, zoals TLS, stelt de burger aan een privacyrisico's bloot.

Voor TLS geldt dan ook juist dat de privacyrisico's van het uitblijven van adoptie niet wenselijk zijn, ondermeer gezien internationale ontwikkelingen van afgelopen jaar. Daarbij is duidelijk geworden dat op het internet op grote schaal transactionele (persoons)gegevens worden verzameld door derde partijen en is gebleken dat er partijen zijn die zich richten op het kraken of omzeilen van TLS-beveiligde verbindingen. TLS 1.2 biedt voor beide scenario's de meest toekomstvaste oplossing, wat uiteindelijk slechts winst oplevert met betrekking tot privacy.

3.1.4 Conclusie

De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de risico's en nadelen. Technisch gezien biedt TLS 1.2 de mogelijkheid tot verbetering van de beveiliging van elektronische gegevensuitwisseling van, naar en tussen overheidsinstellingen.

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 onacceptabele belemmeringen (zoals te hoge kosten en te hoge lidmaatschapseisen)?

Ja, de standaarden zijn in beheer bij IETF: ze zijn vrij en kosteloos beschikbaar op het Internet. De specificatie van TLS is beschikbaar via de

website van IETF[6]. IETF kent daarnaast geen formeel lidmaatschap of lidmaatschapseisen.

3.2.1.2 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)?

De standaard is ontwikkeld door de TLS Working Group (tls[7]). De verdere ontwikkeling en het onderhoud van TLS wordt vormgegeven door het reguliere standaardisatieproces van IETF, zoals vastgelegd in RFC 2026[8]. Documenten, mailing lijsten en verslagen van bijeenkomsten en besluiten zijn publiekelijk beschikbaar op de website van IETF (http://www.ietf.org).

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 m.b.t. bijvoorbeeld eventuele patenten- onherroepelijk royalty-free voor eenieder beschikbaar?

IPR claims worden vastgelegd in de RFC van de betreffende standaard en kunnen op de website van IETF worden nagegaan, door gebruik te maken van een IPR zoekfunctie[9]. Dit betekent echter niet dat er garanties gegeven kunnen worden over eventuele toekomstige claims met betrekking tot het intellectueel eigendom.

Voor de RFC die in dit advies met betrekking tot TLS wordt beoordeeld, geldt dat er 5 disclosures zijn op gerelateerde documenten. Van de claims (op zeer specifieke opties in het protocol) is op dit moment legitimiteit niet bevestigd.

Er worden aan het hergebruik van de standaard zelf geen additionele eisen gesteld.

De copyright policy (auteursrechtenbeleid) van de IETF ten aanzien van IETF documenten waarin de standaard is vastgelegd, is in twee documenten verwoord, te weten RFC5378[10] en de 'IETF Trust's Legal Provisions Relating to IETF Documents'[11]. Hierin is ondermeer vastgelegd, dat:

- Elk document van de IETF vrijelijk mag worden gekopieerd, gepubliceerd, getoond, vertaald en gedistribueerd.
- Elk document van de IETF alleen mag worden gemodificeerd en mag worden gebruikt voor afgeleide producten binnen het IETF standaardisatieproces.
- Iedereen ongewijzigde IETF documenten mag publiceren en vertalen voor elk doeleinde, ook buiten het standaardisatieproces.
- Het niet is toegestaan om aanpassingen te doen aan en afgeleide producten te maken (behalve vertalingen) van IETF documenten

6 http://www.rfc-editor.org/rfc/rfc5246.txt
7 http://datatracker.ietf.org/wg/tls/
8 The Internet Standards Process -- Revision 3, http://tools.ietf.org/html/rfc2026
9 IPR Search, https://datatracker.ietf.org/ipr/search/
10 http://www.rfc-editor.org/rfc/rfc5378.txt
11 http://trustee.ietf.org/docs/IETF-Trust-License-Policy.pdf

en bijdragen buiten het standaardisatieproces. Na consultatie van de gemeenschap kunnen dergelijke rechten per geval eventueel worden toegekend.

3.2.2.2 Garandeert de standaardisatieorganisatie dat partijen die bijdragen aan de ontwikkeling van de standaard hun intellectueel eigendomsrecht onherroepelijk royalty-free voor eenieder beschikbaar stellen?

De Intellectual Property Rights (IPR) policy van IETF is vastgelegd in RFC 3979[12] . Deze policy geeft geen garanties met betrekking tot IPR, maar hierin is wel vastgelegd dat leden van de werkgroep van een specifieke standaard, bestaande IPR moet onthullen, die in de ogen van de werkgroep relevant is voor de standaard die in deze werkgroep in behandeling is.

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)?

Aan het standaardisatieproces kan iedereen (incl. ieder individu) deelnemen, hetzij via meetings, hetzij via mailing lists.

3.2.3.2 Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen?

Het standaardisatieproces, zoals vastgelegd in RFC 2026[13], maakt gebruik van een besluitvormingsprocedure via het principe van "rough consensus"[14], waarbij de dominante mening van een groep, zoals door de voorzitter vastgesteld, de basis voor een beslissing vormt.

3.2.3.3 Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde procedure?

Ja, iedereen kan formeel bezwaar aantekenen tijdens verschillende stadia van het standaardisatieproces, zoals is beschreven in de IETF Working Group Guidelines and Procedures. Formele procedures voor bezwaar zijn vastgelegd in het Internet Standards Process (RFC 2026).

In deze beschrijving staat vervolgens verder uitgewerkt hoe om wordt gegaan met conflicten en beroepen. Het kan hierbij zowel gaan over een conflict binnen de werkgroep als een tekortkoming binnen het proces.

3.2.3.4 Organiseert de standaardisatieorganisatie regelmatig overleggen met belanghebbenden over doorontwikkeling en beheer van de standaard? (geen harde voorwaarde)

De IETF organiseert jaarlijks drie open bijeenkomsten, telkens op een andere locatie wereldwijd. Daarnaast wordt er veelvuldig gebruik gemaakt van mailinglists en andere informele communicatiekanalen voor o.a. (groeps)chat.

3.2.3.5 Organiseert de standaardisatieorganisatie een publieke consultatie voordat

12 Intellectual Property Rights in IETF Technology, http://www.ietf.org/rfc/rfc3979.txt
13 The Internet Standards Process -- Revision 3, http://tools.ietf.org/html/rfc2026
14 IETF Working Group Guidelines and Procedures, http://tools.ietf.org/html/rfc2418

(een nieuwe versie van) de standaard wordt vastgesteld? (geen harde voorwaarde)

Voordat een nieuwe RFC geaccordeerd wordt is er een open comments proces georganiseerd door de relevante werkgroep.

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, de De IETF Trust is een non-profit organisatie onder Amerikaans recht in de staat Virginia[15].

3.2.4.2 Is de financiering van de ontwikkeling en het onderhoud van de standaard voor tenminste drie jaar gegarandeerd?

Ja, de organisatie die de standaard beheert (IETF) bestaat sinds 1986 en heeft aangetoond dat zij een stabiele organisatie is die over een lange periode in staat is om standaarden te ontwikkelen en beheren. De continuïteit van de IETF wordt verder gegarandeerd door ISOC, de Internet Society, een wereldwijd genootschap met veel for-profit en non-profit leden[16].

3.2.5 Is het (versie) beheer van de standaard goed geregeld?

3.2.5.1 Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot versiebeheer van de standaard? (met o.a. aandacht voor migratie van gebruikers)

Ja, dat is het geval. Operationele aspecten van het standaardisatieproces zijn beschreven in http://www.ietf.org/about/process-docs.html. In RFC 2026[17] wordt in het Internet Standards Process onder andere beschreven hoe moet worden omgegaan met nieuwe versies van standaarden.

3.2.5.2 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?

Ja, dat is het geval. Het standaardisatieproces zelf van de IETF is dusdanig transparant, goed gedocumenteerd en open dat aanvullende toetsing een volgende keer op bijna alle punten onnodig is. De enige beperking geldt de IPR bepalingen die per standaard kunnen verschillen en mogelijk in specifieke gevallen afbreuk kunnen doen aan de openheid.

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

De Nederlandse overheid is zelf niet vertegenwoordigd in de werkgroep die de standaard beheert. Het generieke karakter van TLS en het brede internationale draagvlaak vermindert de noodzaak voor

15 http://iaoc.ietf.org/docs/TrustFAQ1.2.txt
16 http://www.internetsociety.org/internet/what-internet/history-internet/ietf-and-internet-society
17 The Internet Standards Process -- Revision 3, http://tools.ietf.org/html/rfc2026

de Nederlandse overheid om direct bij de ontwikkeling en het beheer van TLS betrokken te zijn.

3.2.6 Conclusie

De standaard wordt beheerd door IETF. Deze organisatie heeft naar mening van de expertgroep goed gedocumenteerde en open beheerprocedures. Er is geen lidmaatschap, iedereen kan wijzigingsverzoeken indienen, het beheerproces en de besluitvorming zijn open en transparant en zijn er geen kosten verbonden aan het downloaden van de specificatie en het implementeren van de standaard.

3.3 Draagvlak

Aanbieders en gebruikers moeten voldoende ervaring hebben bij het ondersteunen, implementeren en gebruiken van de standaard.

3.3.1 Bestaat er voldoende marktondersteuning voor de standaard?

3.3.1.1 Bieden meerdere leveranciers ondersteuning voor de standaard?

De meest recente versies van alle populaire desktop browsers en moderne operating systems ondersteunen TLS 1.2[18]. Voor verouderde verises geldt juist dat ondersteuning beperkt is. Er zijn meerdere programmeer libraries (o.a. OpenSSL, NSS, PolarSSL, JSSE) beschikbaar[19] die implementaties van TLS 1.2 verzorgen voor diverse software producten (webservers, mailservers, programmeertalen, etc.).

3.3.1.2 Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen?

Voor de standaard kan de conformiteit worden getoetst op diverse sites, waaronder SSL Labs[20] en bij Check TLS[21] (voor tests op mail servers).

3.3.2 Kan de standaard rekenen op voldoende draagvlak?

3.3.2.1 Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt?

Belangrijke Overheidsdomeinen ondersteunen TLS versie 1.2 o.a. DigiD, MijnOverheid.

Het NCSC heeft TLS opgenomen op haar lijst van mogelijkheden ter beveiliging van webapplicaties[22].

3.3.2.2 Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt?

18 http://en.wikipedia.org/wiki/Transport_Layer_Security#Web_browsers
19 http://en.wikipedia.org/wiki/Comparison_of_TLS_implementations
20 https://www.ssllabs.com/index.html
21 http://www.checktls.com/
22 https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

O.a. Digikoppeling gebruikt in haar WUS koppelvlak standaard V3.0 TLS v1.0[23]. Het overheidsdomein Rijksoverheid.nl ondersteunt TLS v1.0.

3.3.2.3 Is de aangemelde versie backwards compatible met eerdere versies van de standaard?

TLS 1.2 is backward compatible met eerdere versies van de standaard. Het TLS protocol voorziet in ingebouwde mechanismen om tijdens het opzetten van de communicatie verbinding tussen twee systemen over de versie te onderhandelen en zo voor beide systemen een bruikbare versie te selecteren[24].

3.3.2.4 Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?

De standaard wordt wereldwijd toegepast in het publieke en commerciële domein. Deze versie van de standaard wordt nu al beschouwd als de meest veilige variant en zal in belang toenemen naarmate er meer beperkingen van eerdere versies (m.n. SSl 3.0 en TLS 1.0) aan het licht komen.

3.3.3 Conclusie

De expertgroep is van mening dat het draagvlak voor de standaard voldoende groot is. Diverse beveiligingsvoorschriften (o.a. Digikoppeling) verwijzen naar specifiek voorgeschreven versies van TLS (niet alleen versie 1.2). Belangrijke Overheidsdomeinen ondersteunen verschillende versies van TLS (bv. DigiD, MijnOverheid: 1.2; Rijksoverheid: v1.0). Alle populaire desktop browsers en moderne operating systems ondersteunen TLS 1.2 en er zijn vele open programmeer libraries beschikbaar.

3.4 Opname bevordert adoptie

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

Er zijn twee lijsten: de lijst met gangbare standaarden en de lijst voor 'pas toe of leg uit'. Deze laatste lijst is bedoeld om standaarden een extra stimulans te geven wanneer:

1. Hun huidige adoptie binnen de (semi-)overheid beperkt is;
2. Opname bijdraagt aan de adoptie door te stimuleren o.b.v. het 'pas toe of leg uit' regime.

De lijst met gangbare standaarden vormt een referentie voor standaarden die veel gebruikt worden. Als standaarden voldoen aan enkele basisvoorwaarden (voor o.a. openheid), er is geen discussie over en de standaarden worden breed gebruikt, dan vindt opname op die lijst plaats.

23 http://www.logius.nl/fileadmin/logius/product/digikoppeling/Koppelvlakstandaard_WUS_Digikoppeling_3_v3.0.pdf
24 http://tools.ietf.org/html/rfc5246#page-87

Voor TLS 1.2 geldt dat een opname op de lijst voor 'pas toe of leg uit' wordt voorzien.

3.4.1 Is de "pas toe of leg uit"-lijst het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

De meerderheid van de experts is van mening dat het opnemen van TLS 1.2 op de lijst een middel is dat adoptie van de standaard zal bevorderen. Leveranciers zien de 'pas-toe-of-leg-uit'-lijst als een (milde) vorm van marktvraag en nemen de standaard daardoor mee in hun toekomstige product roadmaps. Bij architecten en experts binnen de overheid bevordert opname het gebruik van de standaard in aanbestedingen en in de uitvoering van projecten.

3.4.2 Is de lijst met gangbare open standaarden het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

De standaard biedt verbeteringen ten opzichte van de huidige versie 1.0, die nu op de lijst met gangbare standaarden staat. De standaard geldt als een toekomstvaste upgrade van deze en andere/oudere versies, waarvan bekend is dat ze (nu nog) in beperkte mate vatbaar zijn voor aanvallen en dus onvoldoende privacy en veiligheid kunnen bieden. De lijst met gangbare standaarden stimuleert echter volgens de expertgroep de hierboven genoemde marktvraag en opname in aanbestedingen onvoldoende. Verder wordt het belang van toekomstvaste beveiliging met deze lijst onvoldoende ondersteund. De expertgroep is daarom van mening dat verplaatsing van TLS v1.0 van de lijst met gangbare standaarden naar de pas-toe-of-leg-uit lijst noodzakelijk is.

4 Advies aan Forum en College

4.1 Conclusie

De expertgroep adviseert de standaard TLS 1.2 op te nemen op de lijst van 'pas toe of leg uit' .

4.2 Adoptieactiviteiten

Gebruik van de standaard het einddoel van het Forum en College. Plaatsing op de lijsten 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 aanvullend de volgende maatregelen, die adoptie van de standaard TLS 1.2 kunnen bevorderen:

- Updaten verwijzingen alternatieven: relevante beveiligingvoorschriften (b.v. DigiKoppeling) moeten worden nagelopen op verwijzingen naar specifiek gebruik van oudere versies van TLS of alternatieven. Indien dat het geval is dient vastgesteld te worden of deze verwijzingen aangepast dienen te worden.

- Opstellen van een instructie en best practice handleiding: Het is raadzaam om voor correcte werking van TLS een handleiding op te stellen, of een bestaande aan te scherpen indien deze reeds voorhanden was voor voorgaande versies van TLS. Het vermelden van best practices en aanwijzingen voor gebruik van de verschillende versies van TLS past hierin. Verder kan ondermeer worden opgenomen welke versies wel/niet te ondersteunen, welke cryptografische algoritmen wel/niet te ondersteunen en hoe specifieke bekende aanvallen af te slaan op TLS. Ook het vermelden van TLS validator tools ter ondersteuning is hierbij aan te raden. Aan NCSC de vraag om deze taak uit te voeren in afstemming met relevante gebruiksgroepen binnen de overheid (Logius, PKIoverheid, beheerders van sectorale baselines IB).

- Inrichten van een vraagbaak: Ten behoeve van aanvullende ondersteuning voor de toepassing van TLS 1.2 kunnen één of meer groepen binnen de overheid als vraagbaak en platform fungeren[25]. Dit platform deelt best-practises voor inkopers, beheerders en project-teams die met deze standaard zullen gaan werken. NCSC heeft aangegeven deze taak op zich te willen nemen, mogelijk samen met de Taskforce BID, CIP of TIP. Coördinatie voor deze ondersteuning is wenselijk als adoptieactiviteit.

25 . Organisaties kunnen hiervoor dan contact op nemen via hun gebruikelijke contactpersoon. Contacten voor overheden buiten de primaire doelgroepen (vitale sectoren en Rijksoverheid) lopen via hun schakelorganisaties (gemeenten via IBD, bijvoorbeeld).

- Monitoren beveiligingsproblemen TLS: nieuwe ontwikkelingen in beveiligingsproblematiek met TLS moeten worden gemonitord. NCSC wordt gevraagd om het Forum te informeren bij problemen die met versies van TLS kunnen ontstaan, zodat voorschriften voor gebruik van TLS zonodig kunnen worden bijgewerkt.

5 Referenties

[1] *Actieplan Nederland Open in Verbinding*, 's-Gravenhage: Ministerie van Economische Zaken, 2007.

[2] "Pas toe of leg uit" is vastgelegd in de "Instructie rijksdienst bij aanschaf ICT-diensten of ICT- producten" van 8 november 2008, en daarnaast in convenanten en afspraken met decentrale overheden. http://www.forumstandaardisatie.nl/open-standaarden/voor-overheden/pas-toe-of-leg-uit-regime/

[3] "Instellingsbesluit College en Forum Standaardisatie 2010", https://zoek.officielebekendmakingen.nl/stcrt-2010-4499.html

[4] "Toetsingprocedure en criteria voor indieners en experts", http://www.forumstandaardisatie.nl/open-standaarden/aanmelden-en-toetsing/toetsingscriteria/