Forum Standaardisatie

Wilhelmina v Pruisenweg 104
2595 AN Den Haag
Postbus 84011
2508 AA Den Haag
www.forumstandaardisatie.nl

notitie

Opname TLS 1.2 op de lijst voor 'pas toe of leg uit'

FORUM STANDAARDISATIE FS 50-06-03B2

Agendapunt:	Open standaarden, lijsten		
Bijlagen:	Geen bijlage		
Aan:	Forum Standaardisatie		
Van:	Stuurgroep open standaarden		
Datum:	5 juni 2014	**Versie**	1.1
Betreft:	Opname TLS 1.2 op de lijst voor 'pas toe of leg uit'		

Dit een bijgewerkte notitie van het expertadvies TLS 1.2 (FS49-04-04A), dat vorige Forumvergadering is besproken. Deze notitie wijkt inhoudelijk niet af van de vorige versie. Wel zijn enkele aanvullende adviezen tekstueel aangescherpt en helderder beschreven, zoals de noodzaak om naast versie 1.2 ook TLS versie 1.0 en 1.1 te blijven ondersteunen in het belang van interoperabiliteit.

Waarom is een keuze belangrijk?
Overheden wisselen over netwerken vaak gevoelige gegevens uit met burgers, bedrijven en andere overheden. Voor het vertrouwen in de overheid is het cruciaal dat de gegevensuitwisseling goed beveiligd is. TLS is de opvolger van SSL. Het is een protocol dat tot doel heeft om met behulp van certificaten (zoals conform PKI of PKIoverheid) beveiligde netwerkverbindingen te verzorgen. TLS wordt in combinatie met andere standaarden gebruikt (bijv. voor webverkeer samen met http in de vorm van https). De standaard zorgt voor versleuteling van de gegevensverbinding (encryptie) op de transportlaag. Bovendien kan met TLS controle plaatsvinden of een verbinding wordt opgezet met de juiste server of (overheids)website (authenticatie). TLS versie 1.2 is de meest recente versie en geldt als een veilige, toekomstvaste upgrade van eerdere TLS-versies en van voorganger SSL.

Hoe is het advies tot stand gekomen?
Op 23 januari 2014 is een expertgroep met vertegenwoordigers uit overheid en het bedrijfsleven bijeengekomen. De expertgroep heeft geadviseerd de standaard op te nemen op de lijst van 'pas toe of leg uit'. Het expertadvies is tussen 12 februari en 12 maart gepubliceerd ten behoeve van een openbare consultatie, die heeft geleid tot reacties van KING, NCSC en het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Geen van de respondenten was tegen TLS versie 1.2. De reacties zijn in overleg met de betrokken partijen verwerkt in dit advies.

Zijn er risico's verbonden aan de keuze?
De adoptie van TLS leidt niet tot beveiligingsrisico's of privacyrisico's, maar beperkt deze juist. De standaard dateert van 2008. Binnen en buiten de overheid is met de standaard ondertussen voldoende ervaring opgedaan. Zo wordt de standaard goed ondersteund door vrijwel alle moderne browsers. Een aandachtspunt is dat de standaard niet 'backwards compatible' is. Toepassing van versie 1.2 is daarom de norm, maar ten behoeve van de interoperabiliteit dient een organisatie ook de versies 1.0 en 1.1 toe te passen, met name als wederpartijen nog niet klaar zijn voor TLS 1.2. Een tweede aandachtspunt voor overheden betreft het veilig configureren van TLS. Tot slot kan TLS 1.0, na de opname van TLS op de 'pas toe of leg uit'-lijst, van de lijst met gangbare standaarden verwijderd worden.

Gevraagd besluit
Het Forum Standaardisatie wordt gevraagd in te stemmen met:

e. De opname van TLS op de lijst voor 'pas toe of leg uit';
f. Het door de expertgroep gedefinieerde functioneel toepassingsgebied en organisatorisch werkingsgebied;
g. De additionele adviezen ter bevordering van de adoptie van de standaard.

Ad e) Naam van de standaard en versie

- Verkorte naam: TLS
- Volledige naam: Transport Layer Security Protocol
- Versie: 1.2 (N.B. ten behoeve van de interoperabiliteit dient een organisatie ook de versies 1.1 en 1.0 te ondersteunen, met name als wederpartijen (nog) niet klaar zijn voor versie 1.2.)
- Beheerorganisatie: Internet Engineering Task Force (IETF)
- Specificatiedocument: RFC 5246[1]

Ad f) Toepassings- en werkingsgebied

Functioneel toepassingsgebied: "Het met behulp van certificaten beveiligen van de verbinding (op de transportlaag) tussen client- en serversystemen of tussen serversystemen onderling, voor zover deze gerealiseerd wordt met internettechnologie."

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

Toelichting bij de opname:
- Bij de toepassing van TLS is het van belang om kennis te nemen van de actuele internationale 'best practices' voor veilige TLS-configuratie bijv. van ENISA, OWASP en SSLlabs. Rondom de toepassing van TLS zijn er namelijk verschillende configuratie-opties (bijv. Forward Secrecy, ciphers, HSTS) die zeer bepalend zijn voor het te bereiken beveiligingsniveau.[2]

[1] *Zie: https://datatracker.ietf.org/doc/rfc5246/*
[2] *Best practices van bijvoorbeeld ENISA (Algorithms, Key Sizes and Parameters Report)*
https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-

- TLS is cruciaal voor een veilige netwerkverbinding naar niet de enige maatregel. Het is van belang ook andere beveiligingsmaatregelen (waaronder beveiligingsstandaarden) bewust te overwegen.
- Zoals blijkt uit het functioneel toepassingsgebied, is TLS alleen vereist als beveiliging van de netwerkverbinding waarover gegevens worden uitgewisseld van belang is. Dit laatste kan volgen uit wet- en regelgeving en/of de beveiligingsvoorschriften binnen een organisatie.
- TLS 1.2 wordt door experts beschouwd als de meest veilige versie. Deze versie is daarom de norm. Deze is niet echter 'backwards compatible' Ten behoeve van de interoperabiliteit dienen daarom ook de versies 1.1 en 1.0 toegepast te worden, met name als wederpartijen (nog) niet klaar zijn voor versie 1.2.Toepassing van versie 2 en ouder van SSL ('TLS-voorloper') wordt ontraden vanwege bekende ernstige kwetsbaarheden.[3]

Ad g) Additionele adviezen ter bevordering van de adoptie van de standaard

- Aan overheden: Controleer regelmatig met behulp van beschikbare validatie-tools, zoals de SSLlabs server test[4], of voor beveiligde verbindingen TLS1.2 en eventueel aanvullend versies 1.0 en 1.1 worden toegepast en controleer ook de veilige configuratie daarvan aan de hand van beschikbare best practices.[2] Dat geldt voor alle overheden, maar met name voor organisaties die gemeenschappelijke voorzieningen leveren zoals SSC-ICT, DPC/AZ, DICTU, ICTU en Logius.
- Aan NCSC: Ontwikkel en publiceer in samenwerking met experts van andere organisaties, zoals Logius (PKIoverheid) en beheerders van sectorale Baselines Informatiebeveiliging, een richtlijn voor veilige TLS-configuratie en houd deze up-to-date. In deze richtlijn zou het gebruik van versie 1.2 en de relatie tot de andere versies van TLS een belangrijke rol moeten innemen, evenals de te ondersteunen cryptografische algoritmen en het afslaan van bekende aanvallen op TLS. Verder zou het gebruik van bepaalde TLS validatie-tools moeten worden aangeraden.
- Aan Logius/PKIoverheid: Breng de genoemde bestaande internationale 'best practices' voor veilige TLS-configuratie en straks de NCSC-richtlijn actief onder de aandacht van gebruikers van PKIoverheid.
- Aan NCSC: Fungeer als vraagbaak op het gebied van toepassing van TLS voor de primaire doelgroep, de rijksoverheid en de vitale sectoren. Voor de secundaire doelgroep kan de vraagbaakfunctie worden vormgegeven via de schakelorganisaties van NCSC (zoals KING/IBD)[5].
- Aan NCSC: Informeer het Forum Standaardisatie en andere overheden wanneer de veiligheidsstatus van de standaard wijzigt.

---

parameters-report, OWASP (https://owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet) en SSLlabs (https://www.ssllabs.com/projects/best-practices/).

[3] Zie Cybersecuritybeeld Nederland 2013, https://www.ncsc.nl/binaries/nl/actueel/nieuwsberichten/cybersecuritybeeld-nederland-kwetsbaarheid-van-ict-onverminderd-hoog/1/NCSC%2BCSBN%2B3%2B3%2Bjuli%2B2013.pdf

[4] SSLlabs server test: https://www.ssllabs.com/ssltest/.

[5] Schakelorganisaties zijn organisaties die dienen om typen organisaties aan het NCSC te verbinden die niet in de primaire doelgroepen van het NCSC vallen.

Toelichting op de experttoetsing en consultatie

Datum
5 juni 2014

Waar gaat het inhoudelijk over?
TLS is een protocol, dat tot doel heeft om beveiligde verbindingen op de transportlaag 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 SMTP en 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 encryptietechniek beveiligde communicatie tussen partijen mogelijk te maken.

TLS wordt (in combinatie met andere standaarden) 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 internettoepassingen (internet browsing, mailuitwisseling, instant messaging, VoIP, etc.)

Hoe is het proces verlopen?
Na de intake is op 23 januari 2014 een expertgroep met vertegenwoordigers uit het bedrijfsleven en de overheid bijeengekomen. De expertgroep heeft geadviseerd de standaard op te nemen op de lijst van 'pas toe of leg uit'. Het expertadvies is gepubliceerd ten behoeve van een openbare consultatie, die heeft geleid tot reacties van KING, NCSC en het ministerie van BZK. Deze reacties zijn in overleg met de betrokken partijen verwerkt in dit forumadvies.

Hoe scoort de standaard op de toetsingscriteria?

<u>Open standaardisatieproces</u>
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.

<u>Toegevoegde waarde</u>
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).

<u>Draagvlak</u>
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). Iedere moderne internetbrowser ondersteunt TLS 1.2.

Opname bevordert de adoptie
De meerderheid van de experts is van mening dat het opnemen van TLS op de lijst een middel is dat adoptie van de standaard zal bevorderen. Leveranciers zullen de standaard meenemen 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 TLS1.0, die nu op de lijst met gangbare standaarden staat. Versie 1.2 geldt als een toekomstvaste upgrade van TLS 1.0 en de voorganger daarvan: de SSL-protocollen. Van TLS 1.0 en SSL is bekend dat deze kwetsbaarheden bevatten waardoor de vertrouwelijkheid van versleutelde informatie kan worden aangetast.

De lijst met gangbare standaarden stimuleert volgens de expertgroep de adoptie en het gebruik van de standaard onvoldoende. Gezien het belang van toekomstvaste beveiliging en aangezien niet alle organisaties uit de publieke sector automatisch ondersteuning bieden aan TLS 1.2 is de expertgroep van mening dat het noodzakelijk is om TLS 1.2 op de 'pas toe of leg uit'-lijst te plaatsen. Daarbij wordt aangegeven dat ten behoeve van de interoperabiliteit een organisatie ook de versies 1.1 en 1.0 dient toe te passen, met name als wederpartijen (nog) niet klaar zijn voor versie 1.2. TLS 1.0 kan dan van de lijst met gangbare standaarden worden verwijderd.

Wat is de conclusie van de expertgroep en de consultatie?

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

Toelichting van eventuele risico's
De adoptie van TLS 1.2 leidt niet tot beveiligingsrisico's of privacyrisico's, maar beperkt deze juist. Een aandachtspunt is dat de standaard niet 'backwards compatible' is. Om die reden adviseert de expertgroep TLS 1.2 te verplichten in 'greenfield situaties', maar wordt tegelijk de mogelijkheid opengehouden een eerdere versie te gebruiken indien de omgeving waarin de standaard wordt toegepast dit vereist. Indien interoperabiliteit dit noodzakelijk maakt, kunnen eerdere versies van TLS (versie 1.1 en 1.0) worden gebruikt. Verder betekent een eventuele plaatsing van TLS 1.2 een verwijdering van TLS v1.0 van de lijst met gangbare standaarden. Een additioneel punt dat uit de openbare consultatie naar voren is gekomen is de vraag of op de 'pas toe of leg uit'-lijst operationele beveiligingsstandaarden geplaatst dienen te worden of dat dit type standaarden niet thuishoort op de lijst.

Aanvullingen vanuit de consultatie
In de consultatieronde zijn door het ministerie van Binnenlandse Zaken (OBR ICCIO) bedenkingen geplaatst bij de opname van operationele beveiligingsstandaarden op de lijst voor 'pas toe of leg uit'. De 'pas toe of leg uit'-lijst is er in hun zienswijze voor om de adoptie van open standaarden te bevorderen als er momenteel gebruik gemaakt wordt van gesloten standaarden. Dat is bij TLS 1.2 niet het geval, hier speelt voornamelijk informatiebeveiliging een rol. Informatiebeveiliging op zich is geen taak van de 'pas toe of leg uit'-lijst, hier zijn binnen de overheid andere organisaties voor verantwoordelijk. Ondanks dat TLS 1.2 inhoudelijk een goede standaard is, is er dus onvoldoende reden om het op de 'pas toe of leg uit'-lijst op te nemen. Verder is het de verantwoordelijkheid van het

(lijn)management om risico's te inventariseren en de keuze te maken welke maatregelen worden genomen.

Reactie
In het instellingsbesluit is opgenomen dat de taak van het College en Forum Standaardisatie onder andere betrekking heeft op "veilige en betrouwbare uitwisseling en (her)gebruik van gegevens". Ook staat het thema informatiebeveiliging al twee jaar in het werkplan van het Forum en geven organisaties als het NCSC aan dat de lijst wordt gezien als extra drukmiddel voor veilige gegevensuitwisseling. Operationele beveiligingsstandaarden zouden dan ook op de 'pas toe of leg uit'-lijst kunnen worden geplaatst, wat in het verleden ook vaak is voorgekomen. Het voorstel is wel om:

- Het onderwerp beveiligingsstandaarden op de agenda te plaatsen van een komende Forumvergadering (daarbij komt dan ook de vraag aan de orde: zetten we de komende jaren in op het uitbreiden van de lijst met beveiligingsstandaarden, of juist - met het oog op het adoptievermogen - op een kernachtige(r) lijst);
- Het uitvoeren van een uitgebreidere samenhanganalyse voor beveiligingsstandaarden om zodoende willekeur in het opnemen van standaarden op de lijst te voorkomen. In deze analyse komt de verhouding tussen verschillende beveiligingsstandaarden aan de orde.

KING (IBD) en NCSC hebben naar aanleiding van de consultatie hun rolverdeling bij de uitvoering van de adoptieadviezen onderling afgestemd. De uitkomsten hiervan zijn in dit advies verwerkt.

Bijlagen

- Expertadvies TLS 1.2, zie: (https://lijsten.forumstandaardisatie.nl/open-standaard/tls-12)
- Overzicht reacties consultatieronde, zie: (https://lijsten.forumstandaardisatie.nl/open-standaard/tls-12)