Forum Standaardisatie

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

notitie

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

College Standaardisatie CS 16-09-06A

Agendapunt:	Open standaarden, lijsten		
Bijlagen:	Geen bijlage		
Aan:	College Standaardisatie		
Van:	Forum Standaardisatie		
Datum:	14 augustus 2014	**Versie**	1.0
Betreft:	Opname TLS op de lijst voor 'pas toe of leg uit'		

SAMENVATTING

Waarom is een keuze belangrijk?
Door overheden worden via internet vaak gevoelige gegevens uitgewisseld met burgers, bedrijven en andere overheden. Voor het vertrouwen in de overheid is het cruciaal dat deze gegevensuitwisseling goed is beveiligd, bijvoorbeeld door de gegevens te versleutelen. Standaarden zijn hierin belangrijk, waarbij het gaat om een samenspel van verschillende standaarden. Op de 'pas toe of leg uit'-lijst staan dan ook meerdere informatiebeveiliging standaarden. Bijvoorbeeld een standaarden ter voorkoming van 'phishing-mails' (DKIM) en frauduleuze webpagina's (DNSSEC).

De standaard TLS is ingediend voor opname op de 'pas toe of leg uit'-lijst en is complementair aan de beveiligingsstandaarden die op de lijst staan. TLS heeft tot doel om met behulp van certificaten, dit zijn een soort van digitale computer-paspoorten, netwerkverbindingen te beveiligen. Zo kan met TLS worden gecontroleerd of er een verbinding wordt opgezet met de juiste server of website. TLS versie 1.2 is de meest recente versie en geldt als een veilige, toekomstvaste upgrade van eerdere TLS-versies.

Hoe is het advies tot stand gekomen?
Door een expertgroep met vertegenwoordigers uit overheid en bedrijfsleven en input uit de openbare consultatie is aan het Forum geadviseerd de standaard op te nemen op de 'pas toe of leg uit' lijst. Vervolgens is op verzoek van het Forum nader uitgezocht wat de samenhang is van TLS ten opzichte van de andere beveiligingsstandaarden die op de lijst staan. Het expertadvies, de samenhang met andere standaarden en de consultatiereacties zijn 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. 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 versie 1.2 niet goed samenwerkt met eerdere versies van TLS (niet 'backwards compatibel'). Naast de toepassing van versie 1.2 dient een organisatie daarom ten behoeve van de interoperabiliteit ook versies 1.0 en 1.1 toe te passen. Een tweede aandachtspunt voor overheden betreft een veilige configuratie 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 worden verwijderd.

Gevraagd besluit
College Standaardisatie wordt gevraagd in te stemmen met:

1. De opname van TLS op de lijst voor 'pas toe of leg uit';
2. Het gedefinieerde functioneel toepassingsgebied en organisatorisch werkingsgebied;
3. De additionele adviezen ter bevordering van de adoptie van de standaard.

Toelichting op het gevraagde besluit
Ad 1) 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 2) 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 op het toepassingsgebied:
- 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 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-parameters-report, OWASP (https://owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet) en SSLlabs (https://www.ssllabs.com/projects/best-practices/).*

- 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 3) 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 bestaande 'best practices' voor veilige TLS-configuratie en 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.

Deze adviezen zijn met de genoemde organisaties afgestemd.

---

[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

Waar gaat het inhoudelijk over?
TLS heeft tot doel 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 kunnen bouwen en gebruik van kunnen maken. De standaard doet zijn werk bijvoorbeeld als een gebruiker "https://" in zijn browser ziet.

TLS wordt (in combinatie met andere standaarden) gebruikt in situaties waarin het nodig is om vast te stellen of men als gebruiker verbonden is met de juiste server of (overheids)website. Op deze manier kan persoonlijke of vertrouwelijke informatie worden uitgewisseld. De standaard biedt een veilige basis onder bijna alle denkbare internettoepassingen (internet browsing, mailuitwisseling, instant messaging, VoIP, etc.). TLS speelt eveneens een rol bij het uitwisselen van SAML-berichten en ook Digikoppeling bouwt voort op TLS.

Hoe is het proces verlopen?
Door een expertgroep met vertegenwoordigers uit overheid en bedrijfsleven en input uit de openbare consultatie is aan het Forum geadviseerd de standaard op te nemen op de 'pas toe of leg uit' lijst. Vervolgens is op verzoek van het Forum nader uitgezocht wat de samenhang is van TLS ten opzichte van de andere beveiligingsstandaarden die op de lijst staan. Het expertadvies, de samenhang met andere standaarden en de consultatiereacties zijn verwerkt in dit advies.

Hoe scoort de standaard op de toetsingscriteria?

<u>Open standaardisatieproces</u>
De standaard wordt beheerd door IETF. IETF 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 implementatie 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 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.

<u>Opname bevordert de adoptie</u>
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.

Versie 1.2 van 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. Voor optimale beveiliging en interoperabiliteit dienen versie 1.2, 1.1 en 1.0 gebruik te worden.

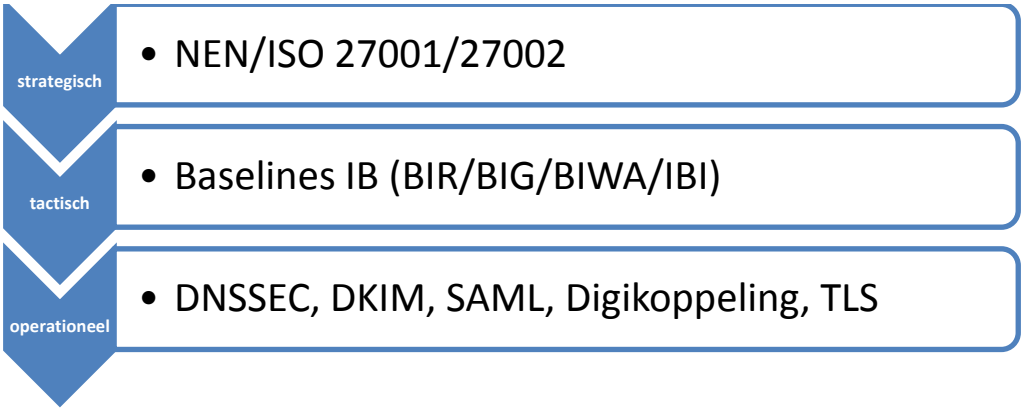
De lijst met gangbare standaarden stimuleert volgens de expertgroep de adoptie en het gebruik van de standaard onvoldoende. Gezien het belang van toekomstvaste beveiliging en aangezien niet alle organisaties uit de publieke sector automatisch ondersteuning bieden aan TLS 1.2 is de expertgroep van mening 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. Dit laatste is helemaal nodig als wederpartijen (nog) niet klaar zijn voor versie 1.2.

Samenhang tussen beveiligingsstandaarden op de 'ptolu'-lijst

Beveiligingsstandaarden op de 'pas toe of leg uit'-lijst
Standaarden zijn cruciaal voor informatiebeveiliging. Er is alleen niet één bepaalde IB-standaard die alle beveiligingsrisico's afdekt. Het gaat om een samenspel van meerdere standaarden. Op dit moment staat een vijftal standaarden die betrekking hebben op informatiebeveiliging op de 'pas toe of leg uit'-lijst, namelijk:

1. NEN-ISO27001/27002: beschrijft hoe informatiebeveiliging procesmatig in te richten. De baselines informatiebeveiliging (BIR/BIG/BIWA/IBI) zijn op deze standaarden gebaseerd;
2. DNSSEC: zorgt dat domeinnamen betrouwbaar worden vertaald naar ip-adressen;
3. DKIM: voorkomt misbruik van het afzendadres/domein en beschermt daarmee tegen phishing-mails;
4. SAML: beschrijft identiteitsattributen, uitwisselprotocollen en transport t.b.v. authenticatie;
5. Digikoppeling: zorgt voor beveiligd berichtenverkeer.

Aanvullend hierop staan er ook verschillende standaarden voor informatiebeveiliging op de gangbare lijst (AES, IPSec, SHA2, HTTPS, SSH2, X509). In schema ziet de verhouding tussen de verschillende standaarden er als volgt uit:



De NEN-ISO normen (en de daarop gebaseerde Baselines Informatiebeveiliging) geven niet aan welke concrete maatregelen een organisatie moet treffen. De technische standaarden hebben wél het karakter van concrete maatregelen. SAML helpt bijvoorbeeld bij de veilige authenticatie en autorisatie van gebruikers. De

technische standaarden geven daarmee invulling aan bepaalde aspecten, waarvan de NEN-ISO-standaarden voorschrijven dat deze moeten worden geadresseerd.

Beide typen standaarden- organisatorisch/ procesmatig enerzijds en technisch/ operationeel anderzijds- vullen elkaar aan en versterken elkaar. Een aanvaardbaar niveau van beveiliging kan pas worden bereikt als er overheidsbreed zowel organisatorische als technische als informatiebeveiligingsstandaarden worden gebruikt. Om die reden hebben Forum en College ervoor gekozen om zowel de procedurele NEN-ISO-standaarden als een (beperkt) aantal technische beveiligingsstandaarden voor te schrijven.

Relatie met de Baselines Informatiebeveiliging
De sectorale Baselines Informatiebeveiliging, die op de NEN-ISO-standaarden zijn gebaseerd, zijn eveneens organisatorische/procesmatig van aard. Deze geven voor overheden tactische invulling aan de meer abstracte, strategische normen, maar schrijven nog geen technische/operationele standaarden voor.

Nader onderzoek naar samenhang
Bij de opname van nieuwe standaarden op de 'pas toe of leg uit'-lijst wordt gekeken naar de relatie tot bestaande standaarden op de lijst. Dit kan echter onvoldoende zijn omdat hierdoor geen zicht is op welke standaarden mogelijk nog meer relevant zijn; de zogenoemde 'witte vlekken'. Bovendien is de samenhang niet altijd duidelijk voor een gebruiker van de 'pas toe of leg uit'-lijst. In het najaar start het Forum daarom met een onderzoek om de samenhang tussen beveiligingsstandaarden nog beter inzichtelijk te maken en eventuele 'witte vlekken' te identificeren .

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)