FS-20140415.04A

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

Agendapunt:	Open standaarden, lijsten		
Bijlagen:	Expertadvies TLS 1.2 en overzicht reacties consultatieronde		
Aan:	Forum Standaardisatie		
Van:	Stuurgroep Standaardisatie		
Datum:	2 april 2014	**Versie**	1.0
Betreft:	Opname TLS 1.2 op de lijst voor 'pas toe of leg uit'		

Waarom is een keuze belangrijk?
TLS versie 1.2 is een protocol, dat tot doel heeft om beveiligde verbindingen over het internet te verzorgen. TLS 1.2 is de opvolger van het SSL protocol en 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. TLS versie 1.2 geldt als een toekomstvaste upgrade van de voorganger SSL, waarvan bekend is dat deze (nu nog) in beperkte mate vatbaar is voor aanvallen en dus onvoldoende privacy en veiligheid kan bieden.

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). Deze reacties zijn in overleg met de betrokken partijen verwerkt in dit advies.

Zijn er risico's verbonden aan de keuze?
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 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 is dat BZK de vraag stelt 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. Zie voor meer informatie 'aanvulling vanuit de consultatie' verderop in het advies.

Datum
4 april 2014

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

1. De opname van TLS versie 1.2 op de lijst voor 'pas toe of leg uit'.
2. Het door de expertgroep gedefinieerde functionele toepassingsgebied en organisatorische werkingsgebied (zie ad 2).
3. De additionele adviezen ten aanzien van de adoptie van de standaard (zie ad 3).

Ad 1) Naam van de standaard en versie
Specifiek gaat het om de volgende standaard:
- Transport Layer Security (TLS) Protocol.
- Versie: 1.2.
- De standaard wordt beheerd door: Internet Engineering Task Force (IETF).

Ad 2) Toepassings- en werkingsgebied
Voorgesteld wordt om als functionele toepassingsgebied te kiezen:
"Het via certificaten beveiligen van gegevensuitwisseling tussen client- en serversystemen of tussen serversystemen onderling, voor zover deze gerealiseerd wordt met internet / IP technologie."

Als organisatorische werkingsgebied wordt voorgesteld:
"Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi)publieke sector."

Hierbij worden de volgende opmerkingen geplaatst:
- Het ondersteunen van TLS versie 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 (1.1 en 1.0). Versie 2 en ouder van het SSL protocol[1] zouden echter niet meer gebruikt moeten worden.
- De keuze voor de te gebruiken TLS versie is slechts één van de keuzes die gemaakt moeten worden bij het beveiligen van gegevensuitwisseling. Om de veiligheid verder te vergroten dient TLS in combinatie met andere internet beveiligingsstandaarden te worden ingezet.

Ad 3) Additionele adviezen ten aanzien van de adoptie van de standaard
Ten aanzien van de adoptie van de standaard worden de volgende additionele adviezen gedaan:
- Beveiligingsvoorschriften, bijvoorbeeld voor e-overheidsvoorzieningen, werkplekken en kantoorautomatisering, moeten worden nagelopen op verwijzingen naar de implementatie en het gebruik van oudere versies van

[1] *TLS is de opvolger van het SSL (Secure Socket Layer) protocol. TLS 1.0 is gebasseerd op SSL 3.0*

TLS of alternatieven voor TLS. Indien dit het geval is, dient vastgesteld te worden of het mogelijk is om dit aan te passen naar versie 1.2.
- NCSC wordt opgeroepen om een generiek advies in de vorm van een richtlijn uit te brengen over de inkoop en inzet van TLS 1.2. Dit in samenwerking met experts van andere organisaties, zoals Logius (Digikoppeling, PKIoverheid) en beheerders van sectorale Baselines Informatiebeveiliging. 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 TLS validation tools moeten worden aangeraden.
- NCSC wordt opgeroepen om voor de rijksoverheid en de vitale sectoren te fungeren als vraagbaak op het gebied van het gebruik van TLS. Dit in samenwerking met schakelorganisaties[2] van het NCSC.
- Schakelorganisaties van het NCSC (zoals de IBD) wordt gevraagd om voor hun doelgroepen te fungeren als vraagbaak op het gebied van het gebruik van TLS. Zo nodig kunnen zij vragen doorspelen aan NCSC.
- Tot slot wordt aan het NCSC gevraagd om het Forum te informeren wanneer de veiligheidsstatus van de standaard wijzigt.

Toelichting op de experttoetsing en consultatie

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 (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.

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

Hoe scoort de standaard op de toetsingscriteria?

Datum
4 april 2014

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.

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).

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). Iedere moderne internetbrowser ondersteunt 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 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. 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.

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

Ten aanzien van de adoptie van de standaard worden de volgende additionele adviezen gedaan:

- Beveiligingsvoorschriften, bijvoorbeeld voor e-overheidsvoorzieningen, werkplekken en kantoorautomatisering, moeten worden nagelopen op verwijzingen naar de implementatie en het gebruik van oudere versies van TLS of alternatieven voor TLS. Indien dit het geval is, dient vastgesteld te worden of het mogelijk is om dit aan te passen naar versie 1.2.

- NCSC wordt opgeroepen om een generiek advies in de vorm van een richtlijn uit te brengen over de inkoop en inzet van TLS 1.2. Dit in samenwerking met experts van andere organisaties, zoals Logius (Digikoppeling, PKIoverheid) en beheerders van sectorale Baselines Informatiebeveiliging. 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 TLS validation tools moeten worden aangeraden.
- NCSC wordt opgeroepen om voor de rijksoverheid en de vitale sectoren te fungeren als vraagbaak op het gebied van het gebruik van TLS. Dit in samenwerking met schakelorganisaties[3] van het NCSC.
- Schakelorganisaties van het NCSC (zoals de IBD) wordt gevraagd om voor hun doelgroepen te fungeren als vraagbaak op het gebied van het gebruik van TLS. Zo nodig kunnen zij vragen doorspelen aan NCSC.
- Tot slot wordt aan het NCSC gevraagd om het Forum te informeren wanneer de veiligheidsstatus van de standaard wijzigt.

Bijlage

- 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)

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