Notitie

Aan: Forum Standaardisatie

Van: Bureau Forum Standaardisatie

Datum: 11 september 2018

Versie: 1.0

Betreft: Reacties uit de openbare consultatie TLS 1.3

Inleiding

Dit document bevat de reacties die tussen 6 augustus en 10 september werden ontvangen op de openbare consultatie voor de plaatsing van TLS 1.3 (nieuwe versie van TLS) op de 'pas toe of leg uit' lijst van het Forum Standaardisatie. In totaal is een achttal reacties ontvangen van RINIS, Rechtspraak.nl, het Ministerie van Defensie, het Ministerie van Justitie en Veiligheid, de Sociale Verzekeringsbank (SVB), het Uitvoeringsinstituut Werknemersverzekeringen (UWV), de Kamer van Koophandel (KvK) en het Bureau Keteninformatisering Werk & Inkomen (BKWI).

De reacties, die als e-mail binnenkwamen, zijn in zijn originele vorm zonder bewerking weergegeven in chronologische volgorde van binnenkomst. Wel zijn de contactgegevens en is de voor deze consultatie niet-relevante tekst verwijderd.

Reacties uit de openbare consultatie

Reactie van RINIS

Van: Rob Verweij <…>
Verzonden: maandag 20 augustus 2018 09:16
Aan: Zuidweg, J. (Han) - Forum Standaardisatie <han.zuidweg@forumstandaardisatie.nl>
Onderwerp: Re: Openbare consultatie

Dag Han,

… *[niet voor deze openbare consultatie relevante tekst verwijderd]*

Van onze (architect) kant de volgende reactie op de gedane adviezen:

Uiteraard zijn wij voor het gebruik van de nieuwste standaarden m.b.t. beveiliging en TLS 1.3 is een grote verbetering t.o.v. TLS 1.2 m.b.t. snelheid en beveiliging.

De expertgroep heeft goed haar werk gedaan en geeft alle informatie die haar beschikbaar was weer in haar rapport. Ik ben het alleen NIET eens met haar conclusie om de standaard nu al op de "pas toe en leg uit" lijst te plaatsen en aan de OBDO toe te voegen.

TLS 1.3 is als standaard net vrij gegeven, de onderliggende RFC 8446 van het IETF (Internet Engineering Task Force) is deze maand pas gepubliceerd met status "PROPOSED STANDARD" (staat ook in het expert advies). Dit betekent dat er, een heel klein, risico is dat de standaard nog kan worden aangepast. Het effect hiervan is dat er nog weinig implementaties van TLS 1.3 beschikbaar zijn, een groot deel van de browser ondersteunen het nog niet standaard en ook wat betreft server en client software is de ondersteuning beperkt en vaak in BETA.

Toevoegen aan de "pas toe of leg uit" lijst betekent dat TLS 1.3 de norm wordt en dat bij aanschaf van software ondersteuning van TLS 1.3 wordt vereist. Ik begrijp de redenering dat hierdoor de toepassing van TLS 1.3 wordt bevorderd maar gezien de status van TLS 1.3 lijkt mij het op dit moment te vroeg om dit zo op te leggen.

Dit betekent een nee voor zowel vraag 8 als 9. Met als onderbouwing dat wij voor het toepassen van TLS 1.3 zijn. Alleen dat het nog te vroeg is om deze aan beide toe te voegen, omdat er nog te weinig implementaties beschikbaar zijn. Wat zal leiden tot problemen bij aanschaf van software en implementaties voor overheidspartijen. Voorstel zou kunnen zijn om de standaard aan te kondigen en in een later stadium aan beide toe te voegen. Dit zou kunnen in de vorm van een aanbevolen standaard en een adoptie-aanbeveling zoals dit ook voor de SHACL standaard is gedaan.

Wordt het overigens geen tijd om TLS 1.0 en 1.1 van de lijst te verwijderen…

… *[niet voor deze openbare consultatie relevante tekst verwijderd]*

Met vriendelijke groet,
Rob Verweij
directeur
RINIS

Reactie van Rechtspraak.nl

Van: Kremer, H.H.C. (IVO Rechtspraak) <…>
Verzonden: woensdag 5 september 2018 16:56
Aan: Forum standaardisatie <forumstandaardisatie@logius.nl>
CC: Smit, F.P.M. (IVO Rechtspraak) <…>; Vermeulen, D.M. (IVO Rechtspraak) <…>
Onderwerp: Consultatieprocedure TLS 1.3

L.s.,

Hierbij de bijdrage van de Rechtspraak op de Consultatieprocedure TLS 1.3

Vraag 1 Doelstelling expertadvies: nee

Vraag 2 Toepassingsgebied: ja

Vraag 3 Werkingsgebied: ja

Vraag 4 Toegevoegde waarde: ja

Vraag 5 Standaardisatieproces: ja

Vraag 6 draagvlak: nee

Bij de onderbouwing in 3.3.1.1 van marktondersteuning ontbreekt onderzoek naar ondersteuning op alle mobiele apparaten. Gezien het grote gebruik van mobiele apparaten (met Android en iOS als dominante besturingssystemen) zou een negatieve ondersteuning op mobiele apparaten tot een andere conclusie m.b.t. draagvlak kunnen leiden.

Vraag 7 bevordering door opname: ja

Vraag 8 Expert advies: deels

De vraag of met het opnemen van TLS 1.3 ook de oudere 1.0 en 1.1 versies van de lijst af zouden kunnen is niet onderzocht. Om een overmaat aan versies op de lijst te beperking is een geconsolideerde beslissing over toevoegen van 1.3 en afvoeren van 1.0/1.1 gewenst. Er wordt verwezen naar het NCSC voor duiding van het beveiligingsniveau van de verschillende TLS versies; of het oordeel van het NCSC over de 1.0/1.1 versies nog actueel is lijkt niet onderzocht. Tevens ontbreekt uitspraak vanuit het NCSC over de mate van beveiliging van TLS 1.3.

Wij stellen voor om in samenwerking met het NCSC tot een gelijktijdige en gezamenlijke visie te komen op het gebruik de 1.0/1.1 en 1.3 versies van TLS.

Vraag 9 Adoptie aanbevelingen: ja

Vraag 10 Inhoudelijke opmerkingen: geen

Met vriendelijke groet,

H. (Harro) Kremer
(Enterprise) Security Architect
AK&S en CIO-Office
www.rechtspraak.nl

Reactie van het Ministerie van Defensie

[Deze reactie van het Ministerie van Defensie ontvingen wij per e-mail als nota in PDF formaat met referentie BS2018021554. Onderstaande tekst is integraal overgenomen uit deze nota.]

Deze reactie is opgesteld naar aanleiding van de openbare consultatie over TLS 1.3 door het Forum Standaardisatie. De antwoorden zijn genummerd met dezelfde nummers als de vragen in het Consultatiedocument TLS 1.3. Antwoorden op de gestelde vragen:

1. Nee.

2. Nee. Het functioneel toepassingsgebied is te ruim gedefinieerd. Met de huidige definitie ontstaat de noodzaak om al het dataverkeer met TLS te versleutelen, ongeacht de soort gegevens die worden verstuurd en ongeacht de soort verbinding waarover de gegevens worden verstuurd. Deze definitie leidt tot de volgende nadelen:

a) TLS moet worden toegepast in situaties die de uitwisseling van gegevens hindert en/of waar gebruik van TLS niet nodig is. Een voorbeeld hiervan is het synchroniseren van de tijd op alle apparatuur in een datacentrum. Het toepassen van TLS op deze gegevens (het Network Time Protocol) hindert omdat de uitwisseling van deze gegevens tijd-kritisch is. Daarnaast biedt het toepassen van TLS geen voordelen omdat deze gegevens niet vertrouwelijk zijn en de uitwisseling plaatsvindt in zones die goed beveiligd zijn (vooral in datacenters).
b) Er ontstaan te veel situaties waarvoor moet worden uitgelegd waarom TLS 1.3 niet wordt toegepast.
c) Situaties waarin transport encryptiemiddelen worden gebruikt die sterker zijn dan TLS moeten in het jaarverslag worden uitgelegd. Dit is onwenselijk omdat de situaties waarin sterkere transport encryptiemiddelen worden toegepast vaak staatsgeheime informatie zijn.

Beter is het om de situaties waarin het gebruik van TLS 1.3 nodig is expliciet te specificeren in het functioneel toepassingsgebied. Voorgesteld wordt om het volgende functioneel toepassingsgebied, inclusief referenties en toelichting, voor TLS 1.3 te hanteren:

> *TLS moet worden toegepast op de uitwisseling van gegevens tussen clients en servers, inclusief server-server-communicatie, waarvan de vertrouwelijkheid en/of integriteit[1] gewaarborgd moeten zijn wanneer die worden uitgewisseld vanaf een semi-vertrouwde zone, eventueel via een onvertrouwde zone, naar een onvertrouwde of semi-vertrouwde zone[2], tenzij een sterker, door een daartoe bevoegde partij[3] gecertificeerd transport encryptiemiddel wordt gebruikt.*

Toelichting: Inzetadvies toepassen TLS

Om te bepalen of TLS moet worden toegepast zijn een aantal stappen nodig:

- Stap 1: Moet de vertrouwelijkheid en/of de integriteit van de gegevens gewaarborgd zijn? Het antwoord volgt bijvoorbeeld uit een VIR E&E analyse.
  - Bij ja: ga naar stap 2.
  - Bij nee: Toepassing van TLS moet niet maar mag wel.
- Stap 2: Voldoet de uitwisseling van de gegevens aan één van de volgende situaties?
  a) Uitwisseling binnen één en dezelfde semi-vertrouwde zone.
  b) Uitwisseling vanaf een semi-vertrouwde zone naar een onvertrouwde zone.
  c) Uitwisseling van een semi-vertrouwde zone, eventueel via een onvertrouwde zone, naar een andere semi-vertrouwde zone.
  - Bij ja: ga naar stap 3.
  - Bij nee: Toepassing van TLS moet niet maar mag wel.
- Stap 3: Wordt een sterker transport encryptiemiddel gebruikt dat is gecertificeerd door een daartoe bevoegde partij?
  - Bij ja: Pas TLS niet toe maar het sterkere transport encryptiemiddel.
  - Bij nee: Pas TLS toe.

Toelichting: Mogelijkheid om sterkere transport encryptiemiddelen te gebruiken

[1] Zie de VIR2007 voor de definities van vertrouwelijkheid en integriteit.
[2] Zie de NORA voor de definities van onvertrouwde en semi-vertrouwde zones.
[3] Bevoegde partijen zijn afhankelijk van het domein zoals nationaal, internationaal (EU) en allianties (NAVO). De nationaal bevoegde partij is het NLNCSA; binnen de NAVO is dat de SECAM.

De ‘tenzij’ in het functioneel toepassingsgebied maakt enerzijds het gebruik van transport encryptiemiddelen die sterker zijn dan TLS mogelijk en voorkomt anderzijds dat het gebruik ervan moet worden uitgelegd. Dit uitleggen is onwenselijk omdat de situaties waarin sterkere transport encryptiemiddelen worden toegepast vaak staatsgeheime informatie zijn.

3. Ja.

4. Nee. Het nadeel van het te ruim gedefinieerde functionele toepassingsgebied weegt te zwaar om het voorstel tot opname van TLS 1.3 op de ‘pas toe of leg uit’-lijst in zijn huidige vorm te steunen. Zie het antwoord op vraag 2 voor de onderbouwing hiervan. Dit nadeel kan worden weggenomen door het functionele toepassingsgebied inclusief referenties en toelichting zoals voorgesteld in het antwoord op vraag 2 over te nemen.

Daarnaast is het voordeel van de toename in veiligheid minder groot dan wordt geschetst in het expertadvies. Als een organisatie alleen TLS 1.3 implementeert, zonder aanvullende stappen, dan neemt de veiligheid niet toe. Een kwaadwillende heeft in dat geval de mogelijkheid om over te schakelen naar een van de eerdere TLS versies 1.2, 1.1 of 1.0 waarin de onveilige opties nog wel zitten. Aanvullende adoptieactiviteiten zijn nodig om de veiligheid ook werkelijk te laten toenemen. Zie het antwoord op vraag 9 voor een opsomming van de voorgestelde extra adoptieactiviteiten.

5. Ja.

6. Defensie staat onder voorbehoud achter het gebruik van de standaard. Het voorbehoud zit in het aanpassen van het functionele toepassingsgebied conform het voorstel in het antwoord op vraag 2.

7. Ja.

8. Nee. Zie het antwoord op vraag 4 en het antwoord op vraag 2 voor de onderbouwing.

9. Ja, waarbij Defensie adviseert de volgende adoptieactiviteiten toe te voegen om de veiligheid met het toepassen van TLS 1.3 ook werkelijk te laten toenemen:

- Aan NCSC: Wijzig op zo kort mogelijke termijn de status van SHA-1, 3DES en AES-CBC in de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) naar “onvoldoende”.
- Aan Forum Standaardisatie: Start op zo kort mogelijke termijn de procedure om TLS 1.0 van de “pas toe of leg uit”-lijst af te halen.
- Aan Forum Standaardisatie: Start op zo kort mogelijke termijn de procedure om TLS 1.1 van de “pas toe of leg uit”-lijst af te halen.
- Aan NCSC: Stel een datum vast, en communiceer deze, waarop de Step Down Modus van TLS 1.3 moet worden dichtgezet. Dit voorkomt dat op basis van een verzoek automatisch wordt overgestapt naar een lagere versie van TLS.
- Aan Forum Standaardisatie: Stel een datum vast, en communiceer deze, waarop gestart wordt met de evaluatie van TLS 1.2 en wat mogelijk leidt tot het voorstel om TLS 1.2 van de “pas toe of leg uit”-lijst te halen.

10. In het expertadvies bij Samenvatting en Forumadvies in de paragraaf “Behoud oudere versies onder voorwaarde” pleiten de experts ervoor om de TLS versies 1.2, 1.1 en 1.0 op de “pas toe of leg uit”-lijst te laten staan. Vervolgens adviseert de expertgroep om bij een negatief advies over een versie door het NCSC deze versie per direct van de “pas toe of leg uit”-lijst af te halen. Defensie is er voorstander van om op zo kort mogelijke termijn stappen te zetten die de veiligheid bij het gebruik van de oudere TLS versies verbeteren. Deze punten zijn vermeld in het antwoord op vraag 9.

Daarnaast heeft het de voorkeur van Defensie om de procedure voor het van de “pas toe of leg uit”-lijst afhalen van een standaard gelijk te houden aan de procedure om een standaard op de “pas toe of leg uit”-lijst te plaatsen. Dat betekent dat een negatief advies van het NCSC er niet direct toe leidt dat een bepaalde standaard van de “pas toe of leg uit”-lijst wordt gehaald. Bij de normale procedure zijn de stappen om een oudere TLS versie van de “pas toe of leg uit”-af te halen als volgt:

1. Het NCSC meldt aan het Forum Standaardisatie (naast melding aan andere relevante partijen) het negatieve advies over het toepassen van de oudere TLS versie.
2. Het Forum Standaardisatie start de evaluatie van de betreffende standaard wat mogelijk leidt tot het voorstel om deze van de “pas toe en leg uit”-lijst te halen.
3. Het OBDO besluit of de betreffende standaard van de “pas toe en leg uit”-lijst wordt afgehaald op basis van de expertadviezen, openbare consultaties en adviezen van het Forum Standaardisatie.

Bestuursadviseur Architectuur

Ir. M.J.A. van Adrichem

Reactie van het Ministerie van Justitie en Veiligheid

Van: Groeneveld, D.A. - BD/DII/BKI <…>
Verzonden: maandag 10 september 2018 11:02
Aan: Forum standaardisatie <forumstandaardisatie@logius.nl>
Onderwerp: Reactie openbare consultatie Opname van TLS versie 1.3 op de 'pas toe of leg uit' lijst

Hallo,

Wij hebben 1 opmerking m.b.t. hoofdstuk 3.5 punt 9:

Bij TLS zouden wij het advies uit willen breiden met het verwijderen van de TLS 1.0 en 1.1 versies uit de lijst. De opeenvolgende versies zijn bedoeld om slechte eigenschappen van oudere versies te mitigeren. Door die oude versies nog steeds “verplicht” of “toe te staan” te stellen blijft de optie bestaan om terug te vallen op de oudste versie. Dat is onveilig en bevordert niet de acceptatie van 1.3. Door 1.0 en 1.1 af te schaffen bevorder je de acceptatie van 1.3. Eventueel kan het verwijderen worden aangekondigd en over een jaar geeffectueerd.

Met vriendelijke groet,

D.A. (Dick) Groeneveld
.....
Ministerie van Veiligheid en Justitie
Directie Informatisering en Inkoop
http://www.rijksoverheid.nl/ministeries/venj
Voor een veilige en rechtvaardige samenleving

Reactie van de Sociale Verzekeringsbank

Van: Visser, T.
Verzonden: maandag 10 september 2018 14:11
Aan: Zuidweg, J. (Han) - Forum Standaardisatie <han.zuidweg@forumstandaardisatie.nl>
CC: Oberendorff, L. (Ludwig) - Forum Standaardisatie <ludwig.oberendorff@forumstandaardisatie.nl>
Onderwerp: FW: Openbare consultatie verplichte en aanbevolen standaarden

Beste Han,

Ik begrijp dat UWV zelf een reactie zal sturen. Hierbij de ruwe reactie van SVB.

Met vriendelijke groet,

Teun Visser
.....
Ministerie van Sociale Zaken en Werkgelegenheid
Directoraat-generaal Sociale Zekerheid en Integratie
Directie Stelsel en Volksverzekeringen
Afdeling Handhaving en Gegevensuitwisseling

Van: Verheij, Fransje (Sociale Verzekeringsbank) <…>
Verzonden: dinsdag 28 augustus 2018 18:24
Aan: Visser, T. <..>
CC: …
Onderwerp: RE: Openbare consultatie verplichte en aanbevolen standaarden

Hallo Teun en Ron,

Ik heb de vraag over de consultatie uitgezet bij Geer Haas. Hieronder zijn antwoord:

Hi Fransje,

Mijn samenvatting:

…[*Niet voor deze consultatie relevante tekst verwijderd]*

TLS 1.3/STARTTLS en DANE zijn wij het mee eens (conditioneel zie feedback) – zal wij nodige coördinatie inspanning (richting leveranciers) vergen. (geraadpleegd bij SVB IT / MS ISO Reino den Hartog)

…*[Niet voor deze consultatie relevante tekst verwijderd]*

En de geconsolideerde feedback (als gekregen van onze experts) op de consultatie:

Re: TLS 1.3

Vraag 1: Nee

Vraag 2: Ja, eens

Vraag 3: Ja, eens

Vraag 4: Ja, eens

Vraag 5: Ja, eens

Vraag 6: Ja, eens

Vraag 7: Ja, eens

Vraag 8: Ja, eens

Vraag 9: Ja, eens

Vraag 10: Nee

… *[Niet voor deze consultatie relevante tekst verwijderd]*

Reactie van het Uitvoeringsinstituut Werknemersverzekeringen

Van: Vierbergen, Kato (K.R.) <…>
Verzonden: dinsdag 11 september 2018 16:22
Aan: Forum standaardisatie <forumstandaardisatie@logius.nl>; Knubben, B.S.J. (Bart) - Forum Standaardisatie <…>
CC: Bos, Ron (R.) <…>; Franken, Leo (L.) <…>
Onderwerp: reactie UWV openbare consultatie Open Standaarden

L.S.,

In reactie op de openbare consultatie Open Standaarden en plaatsing op de PTOLU-lijst stuur ik jullie hierbij de input vanuit UWV.

Het betreft de consultatie: https://www.forumstandaardisatie.nl/thema/openbare-consultatie

… *[Niet voor deze consultatie relevante tekst verwijderd]*

Het advies om de standaard TLS 1.3 (nieuwe versie van TLS, standaard voor de beveiliging van verbindingen over het internet) op de ‘pas toe of leg uit’ lijst te plaatsen: Nee. Te vroeg, eerst druk uitoefenen op markt t.b.v. voorzieningen.

… *[Niet voor deze consultatie relevante tekst verwijderd]*

Als er vragen zijn, hoor ik dat graag.

Met vriendelijke groet,

Kàto Vierbergen-Schuit
Beleidadviseur Security en Privacy / Information Security Officer
UWV ICT

Reactie van de Kamer van Koophandel

[Deze reactie van de Kamer van Koophandel ontvingen wij per e-mail als bijlage in .doc formaat. Hieronder is het commentaar in de bijlage weergegeven in de oorspronkelijke tekst en gerangschikt per vraag.]

Kamer van Koophandel Advies
Datum: 10 september 2018
Auteur: Frits Maas ICT Architect Kamer van Koophandel

Onderwerp: Reacties van de Kamer van Koophandel op diverse consultaties
Opname van TLS versie 1.3 op de 'pas toe of leg uit' lijst

Consultatiedocument TLS 1.3 Datum 6 augustus 2018

1. KvK: Nee

2. KvK: Ja

3. KvK: Ja

4. KvK: Ja

5. KvK: Ja

6. KvK: Ja

7. KvK: Ja

8. KvK: Ja

9. KvK: Ja

10. KvK: Met het toevoegen van TLS 1.3 op de PTOLU lijst zouden de versies TLS 1.0 en TLS 1.1 als 'deprecated' moeten worden aangemerkt met een einddatum zodat deze standaarden versneld van de PTOLU lijst worden afgevoerd. Immers deze standaarden zijn/worden steeds kwetsbaarder voor aanvallen waardoor de aanvalsvector ongewenst is voor communicatie in het publieke domein.

Reactie van het Bureau Keteninformatisering Werk & Inkomen

Van: Willem Kossen <…>
Verzonden: vrijdag 14 september 2018 09:44
Aan: Jasper Muskiet <…>; Forum standaardisatie <forumstandaardisatie@logius.nl>
CC: Arjen Brienen <…>
Onderwerp: Re: Aankondiging openbare consultatie standaarden

L.S.,

Bij deze een reactie op de lijstopname TLS 1.3 in openbare consultatie. Door afstemming in de keten zijn we daar wat laat mee. Onze inbreng is de volgende:

reactie open consultatie

Binnen BKWI heb ik mijn achterban geraadpleegd n.a.v. deze vraag en we zijn tot de volgende constateringen gekomen. We hebben ook in de SUWI keten beperkt navraag gedaan, maar ons beperkt tot impact op de systemen die wij voor de keten ontwikkelen en beheren.

- We zien de verbeteringen in TLS 1.3 t.o.v. TLS 1.2 als positief. Performance wins en risico vermindering door afslanking van de mogelijkheden spreken ons aan.
- We zijn van mening dat lijstopname, gericht op het bevorderen van de beschikbaarheid van 1.3 functionaliteit verstandig is.
- We zijn daarnaast van mening dat TLS 1.2 nog niet van de lijst moet worden verwijderd, maar dat er een expliciet implementatie-advies moet worden gegeven voor situaties waar oudere versies worden gebruikt (of geen TLS/SSL wordt toegepast)
- We zijn tevens van mening dat het wenselijk is een vervangings- of 'uitfaseringsadvies' te geven voor de onveilige oudere versies. Naar onze mening blijven partijen 'te lang hangen' op mogelijk onveilige versies.
- We zijn van mening dat een implementatie advies voor 1.3 te vroeg is aangezien daarvoor een bredere beschikbaarheid bij partijen noodzakelijk is.
- We verwachten overigens dat een deel van de beschikbaarheid middels patches en upgrades 'vanzelf' zal ontstaan, maar desondanks blijft het verstandig in aanschaf van software en appliances, alles dat een IP stack heeft, TLS 1.3 te vereisen.
- We verwachten dat - net als bij de huidige versie en voorgaande versies - een downgradeable implementatie in eerste instantie noodzakelijk is.

Wanneer we dan naar onze eigen situatie kijken, valt die uiteen in de BKWI bedrijfsvoering en de Dienstverlening aan de SUWI keten.

In onze eigen dienstverlening zullen we een natuurlijk migratie proces volgen dat gebruik maakt van upgrades zo die beschikbaar komen, maar nadat de 'kinderziektes' zijn verwijderd. we zien onszelf als early adopter, maar niet als 'vooroplopend'. We gebruiken TLS 1.2 voor onze websites, interne webapplicaties en diverse andere versleutelde verbindingen.

Voor de Suwi Keten is er veel meer afstemming nodig. Ons TLS gebruik ziet er als volgt uit:

1. Onze webapplicaties bieden nu downgradeable TLS 1.2 (en 1.1. en 1.0). We onderzoeken wanneer oudere versies kunnen worden verwijderd en zullen naar verwachting TLS 1.3 op een natuurlijk moment beschikbaar stellen, wederom in downgradeable vorm zodat partijen onafhankelijk van elkaar kunnen opschalen.
2. Onze interne services draaien allemaal op TLS 1.2. Aangezien we dit zelf kunnen doen zal dat op een natuurlijk moment gebeuren zodra alle componenten de nieuwe versie enige tijd ondersteunen (kinderziektes eruit)
3. Onze berichten uitwisselingsstandaard volgt digikoppeling. Dat betekent dat we volgen wat Digikoppeling gaat doen. De impact is hier wel stevig aangezien we met tweeweg encryptie werken en dat betekent dat alle partijen in een uitwisseling 'tegelijk' moeten migreren. Dit zal enige tijd gaan vergen, maar pas gaan gebeuren nadat we onze standaard erop hebben aangepast.
4. We gebruiken Starttls voor Suwinet Mail en ook dat is TLS 1.2 downgradeable. We hebben starttls op onze internet gerichte mailservers maar gezien de geringe beschikbaarheid van starttls in het algemeen zullen we niet op korte termijn de downgradeable kunnen uitschakelen of de ondersteuning voor oudere versies kunnen afbouwen.
5. Mochten kwetsbaarheden in TLS 1.2 gevonden worden dan (en pas dan) zullen we versneld migreren en op dat moment bepalen hoe we dat aanpakken. Het is belangrijk dat hier naar partijen duidelijke communicatie over zal zijn zo dit gebeurt.
6. we gaan volgen hoe de markt de standaard gaat adopteren en bepalen onze strategie gaandeweg.
7. we worden graag op de hoogte gehouden van ontwikkelingen

Met vriendelijke groet,

Willem Kossen
Lead en Enterprise Architect BKWI