

Plan van Aanpak

Invoering TLS1.3

Datum	10-09-2019	Opsteller(s) WG TC: XXXXXX
Versie	0.9	
Status	Ter vaststelling door ALV	

Inhoudsopgave

1	Introductie.....	3
1.1	Doel	3
1.2	Aanleiding.....	3
1.3	Gerelateerde (lopende) veranderingen en issues.....	4
2	Stappenplan.....	5

1 Introductie

1.1 Doel

Het doel van dit document is het beschrijven van een Plan van Aanpak voor de voorgenomen migratie van TLS1.2 naar TLS1.3.

De doelen van het gehele traject zijn:

Plan van Aanpak Migratie naar TLS1.3 in september 2019 vastgesteld

Issue TC043 Migratie naar TLS1.3 in juni 2020 vastgesteld

Start & einde Migratie naar TLS1.3 nader te bepalen.

1.2 Aanleiding

Uit: Notitie Overgang op TLS1.3 v1.0 (ALV NEDU 20190522-012.1)

In 2016 heeft de sector voor de beveiliging van de verbindingen voor gegevensoverdracht in de ketenprocessen TLS1.2 ingevoerd. Jaarlijks worden de hierbinnen te gebruiken cipher suites geëvalueerd en zo nodig bijgesteld. Tevens worden de te gebruiken beveiligingscertificaten regelmatig geëvalueerd.

Het sectorbrede upgradeproces verloopt jaarlijks moeizaam, zoals recent met TC038. Gezien de (toenemende) beveiligingseisen en de (technische) stand van TLS1.2 zal dit proces naar verwachting steeds moeizamer gaan verlopen.

Er is een opvolger voor TLS1.2 ontwikkeld, die tekortkomingen m.b.t. tot het soepel vervangen van cipher suites en certificaten grotendeels ondervangt. TLS1.3 wordt al ingevoerd, echter ondersteunen nog niet alle communicatiepakketten (de overgang naar) TLS1.3 al. De verwachting is dat dit de komende tijd snel zal verbeteren.

Met name om de partijen de gelegenheid te bieden om hun investeringen en plannen erop af te kunnen stemmen kondigen Security Commissie en de Technische Commissie reeds nu de overgang naar TLS1.3 aan met de intentie deze in de komende (2) jaren te realiseren. Dit biedt partijen tevens de mogelijkheid hun softwareleverancier aan te sporen TLS1.3 op te nemen.

Het moment, de voorwaarden en de wijze van invoering zullen nog nader worden uitgewerkt. Om tot een verantwoorde invoering over te kunnen gaan wordt de ALV gevraagd om de Technische Commissie de opdracht te geven om een Plan van Aanpak op te stellen, waarin

duidelijk wordt welke stappen dienen te worden doorlopen ter voorbereiding van een soepele overgang naar TLS1.3 en bijhorende planning.

De ALV NEDU heeft zoals voorgesteld besloten om de Technische Commissie deze opdracht te geven.

1.3 Gerelateerde (lopende) veranderingen en issues

TC024 Overgang TLS1.2 icm certificatenwissel (2016)

TC038 Jaarlijkse Update Cipher Suites (2018-2019)

TC042 Cipher Suites 2020

2 Stappenplan

Hieronder staat eerst een overzicht van het stappenplan dat opgesteld is.

Met 'Uitvoering' wordt de partij die of het gremium dat de stap hoofdzakelijk zal uitvoeren bedoeld. *Waar een stap als uit te voeren door een Externe partij wordt aangemerkt, is indien mogelijk nauwe samenwerking met of mede-uitvoering door het NEDU-Bureau voorzien.

Met 'Opdrachtgever / Klankbordgroep' wordt de partij die of het gremium dat de uit te voeren stap zal controleren en als klankbord zal fungeren.

Na het overzicht van de stappen volgt een overzicht met per stap een toelichting van de stap.

Stappenplan:

Stap	Korte omschrijving	Deliverables	Effort	Doorlooptijd (schatting)	Uitvoering	Opdrachtgever / klankbordgroep
1	Nadere invulling Plan van Aanpak voor wat betreft budget en staffing	*Verdere detaillering Plan van Aanpak *Budgetaanvraag *Resource overzicht	S	aug-okt 2019	WG	TC NEDU
2	Verzamelen lessons learned invoering TLS1.2	**Verzamelde documenten *Aparte notitie met aandachtspunten	S	aug-okt 2019	WG	TC NEDU
3	Inventariseren aard, omvang en impact van de invoering	*Eerste versie impactanalyse en scope (known knowns, known unknowns, todo)	M	sept-okt 2019	Extern*	WG TLS1.3
4	Vaststellen scope issue	*Scope statement	XS	nov-2019	WG / TC NEDU	TC NEDU
5	Stakeholder analyse	*Stakeholder overview (instanties, partijen, contactpersonen, rol)	M	okt-nov-2019	Extern*	WG TLS1.3
6	Readiness standaard IT componenten	*Overzicht status en invoeringsstrategieën	L	okt-nov 2019	Extern*	WG TLS1.3
7	Status invoering en aanpak (indien reeds bezig met invoering) sector	*Statusoverzicht stakeholders	M	okt-dec 2019	Extern*	WG TLS1.3

8	Analyse duale fase	Besluit ALV (verwacht:) *Duale fase gewenst *Opdracht tot Proof of Concept	S	jan-20	WG	TC NEDU
9	Proof of Concept	Werkende PoC	M	feb-apr 2020	Afhankelijk van keuze waar deze PoC uit te laten voeren (verwacht: EDSN)	SR NEDU
10	Invoeringsstrategie opstellen	Concept TC Issue	M	feb-apr 2020	Extern* of WG	WG TLS1.3
11	Invoeringsstrategie valideren	Review	S	mrt-mei 2020	Marktpartijen	TC NEDU
12	Issue incl. scope, invoeringsstrategie & planning vaststellen.	Vastgesteld issue	XS	jun-2020	SPC & ALV	

*zie inleidende tekst voor kopje 'Uitvoering'.

De toelichting per stap:

Stap	Toelichting
1	Verder invullen van benodigde resources expertise en verwachte kosten in het Plan van Aanpak
2	In 2016 is TLS1.2 ingevoerd, tezamen met een wisseling van certificaten. Wat kunnen we uit deze invoering meenemen als les voor de invoering van TLS1.3?
3	Inventariseren aard, omvang en impact van de invoering van TLS1.3, met name ook betreffende de gebruikte ciphersuites, en de lessons learned van Invoering TLS1.2 en certificatenwissel
4	Beschrijven op welk deel van het berichtenverkeer de invoering gedaan zal worden.
5	Inventariseren relevante stakeholders en partijen in de NL markt die van belang zijn in de invoering van TLS1.3
6	Inventariseren status en strategie invoering bij belangrijkste leveranciers software/middleware/hardware markt
7	Bepalen baseline status quo invoering TLS1.3 bij de relevante partijen in de NL markt, EDSN en NEDU leden. Inventariseren invoeringsstrategie bij de leden van de NEDU
8	Vaststellen noodzaak en mogelijkheid voor duale fase en opdracht PoC met requirements en acceptatie criteria
9	Opzetten Proof of Concept voor inrichten verbindingen met TLS1.3 met op zelfde omgeving TLS1.2 om op terug te vallen en voor duale fase tijdens invoering. Hieruit conclusies trekken voor de invoeringsstrategie
10	Opstellen invoeringsstrategie voor NEDU/EDSN en de leden obv output uit de voorgaande punten
11	Validatie invoeringsstrategie door leden en EDSN
12	Vaststelling issue inclusief scope, invoeringsstrategie, planning. Gemaakte analyses als bijlagen Inclusief impact op proces jaarlijks vaststellen cipher suites SC/TC en evt andere sectorafspraken