



Update 'Uitvoerings- en communicatieplan Invoering TLS 1.3'

Inclusief advies: verlenging ondersteuning TLS 1.2

Versie 2.0

20 juni 2023

Werkgroep Invoering TLS 1.3



Goedgekeurd door ALV MFF op 5 juli 2023

Advies & Besluitvorming

Gevraagde besluiten

Situatieschets

Op 9 maart 2022 heeft de ALV NEDU het besluit genomen om TLS 1.2 uiterlijk tot 1 januari 2024 toe te staan. Hierbij is gekozen voor een gefaseerde aanpak, waarbij tot 1 juli 2023 de centrale systemen TLS 1.3 gereed worden gemaakt door TenneT en EDSN. Hiermee ontstaat dan een duale fase waarin TLS 1.2 en 1.3 naast elkaar bestaan. Gedurende de volgende (duale) fase hebben alle marktpartijen tot 1 januari 2024 de tijd om de eigen decentrale systemen TLS 1.3 geschikt te maken. Hierbij zijn er twee toetsmomenten of de einddatum van 1 januari 2024 voor TLS 1.2 haalbaar is. Toets 1: centrale systemen – juli 2023. Toets 2 decentrale systemen – november 2023.

Toetsing readiness centrale systemen en hernieuwd voorstel verlenging ondersteuning TLS 1.2

In de ALV van 8 maart 2023 is afgesproken om in de ALV van 5 juli 2023 de einddatum van de ondersteuning van TLS 1.2 te heroverwegen (actie 08-01). Uit de meest recente monitoring (19-6) is gebleken dat een heroverweging inderdaad zinvol is. Op 1 juli 2023 zijn niet alle systemen van TenneT gereed voor TLS 1.3, de systemen van EDSN zijn dit naar verwachting wel. Herzien voorstel: Splitsen van de duale fase en de einddatum tot wanneer TLS 1.2 wordt toegestaan. Waarbij de duale fase en de einddatum (1 januari 2024) voor de 14 systemen beheerd door EDSN onveranderd blijft. De duale fase en de einddatum van TLS 1.2 voor de 11 systemen beheerd door TenneT, wordt met één kwartaal verlengd tot 1 april 2024.

Gevraagd besluit Stuurgroep Implementatie

De werkgroep Invoering TLS 1.3 vraagt de Stuurgroep Implementatie akkoord te geven op het geüpdatete plan van aanpak incl. planning. Daarnaast wordt akkoord gevraagd dit document ter besluitvorming voor te leggen aan de ALV MFF op 5 juli 2023.

Gevraagd besluit ALV MFF *(onder voorbehoud van akkoord Stuurgroep Implementatie op 30 juni 2023)*

De werkgroep Invoering TLS 1.3 vraagt om het volgende besluit: “Update van het ‘Uitvoerings- en communicatieplan Invoering TLS 1.3 v1.9 vast te stellen en de einddatum tot wanneer TLS 1.2 wordt toegestaan voor systemen beheerd door EDSN blijft 1 januari 2024 en voor systemen beheerd door TenneT wordt de einddatum verlengd tot 1 april 2024”. N.B. Het NEDU-besluit (1638 - ALV NEDU 20220309-014.2) van 9 maart 2022 komt hiermee te vervallen.

Akkoord SI op 30 juni 2023

Goedgekeurd door ALV MFF op 5 juli 2023

Advies ALV MFF

Haalbaarheid NEDU-besluit einddatum TLS 1.2 op 31-12-2023.



Behaalde resultaten

Reeds genomen besluiten

De ALV NEDU en later de ALV MFF hebben de volgende besluiten genomen:

- 11-11-2020: De ALV NEDU stelt TC043 Invoering TLS 1.3 vast.
- 09-03-2022: De ALV NEDU besluit om TLS 1.2 voor de uitwisseling van de berichten niet langer toe te staan dan tot uiterlijk einde 2023.
- 08-03-2023: ALV MFF keurt het uitvoerings- en communicatieplan Invoering TLS 1.3 goed.

Resultaten

Binnen de scope van het project vallen 25 centrale systemen binnen het CMF-landschap inclusief de bijbehorende verbindingen. Op dit moment zijn de volgende resultaten behaald:

- EDSN: alle centrale systemen zijn per 01-07-2023 TLS 1.3-ready en vanaf 01-07-2023 is ook monitoring van de readiness van de marktpartijen mogelijk.
- TenneT: een deel van de centrale systemen zijn niet TLS 1.3-ready per 01-07-2023.
- Op 16 mei jl. heeft een online voorlichting plaatsgevonden met ruim 140 deelnemers.
- Alle relevante informatie is beschikbaar via SharePoint MFFBAS, waartoe alle marktpartijen toegang hebben.

Afwijkingen

- TenneT is op 01-07-2023 niet TLS 1.3-ready met alle centrale systemen. Er is commitment van TenneT dat alle systemen voor 01-10-2023 TLS 1.3 gereed zijn.

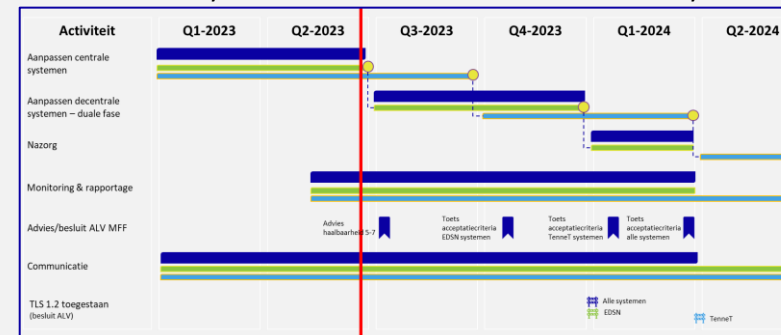


Advies haalbaarheid

Advies

In het genomen NEDU-besluit, van 09-03-2022, wordt TLS 1.2 tot uiterlijk eind 2023 toegestaan. Waarbij de centrale systemen op 1-7-2023 TLS 1.3 gereed zijn.

- De centrale systemen beheerd door EDSN zijn per 1-7-2023 TLS 1.3 gereed. Hiermee is het haalbaar dat TLS 1.2 voor de systemen van EDSN tot 1-1-2024 wordt toegestaan.
- De centrale systemen beheerd door TenneT zijn deels gereed per 1-7-2023. Op 1-10-2023 kunnen alle centrale systemen van TenneT gereed zijn.
- Om de marktpartijen, gebruikmakend van de TenneT systemen, voldoende tijd te geven (6 maanden) kan TLS 1.2 voor dit deel van de systemen tot 01-04-2024 worden toegestaan.
- Het advies blijft aan alle marktpartijen om over te gaan op TLS 1.3, zodra het centrale systeem TLS 1.3-ready is en niet te wachten tot alle centrale systemen gereed zijn.



Herziene planning op pagina 7

Introductie en verloop

De voortgang van de invoering van TLS 1.3 wordt geëvalueerd in dit document en bijgestuurd waar nodig.



Wat is TLS 1.3?

Transport Layer Security (TLS) is een cryptografisch protocol dat is ontworpen om veilige communicatie tussen webbrowsers en servers mogelijk te maken. Het wordt tegenwoordig in bijna elke app gebruikt. Veel IP-gebaseerde protocollen zoals HTTPS, SMTP, POP3 en FTP ondersteunen TLS. Dit zorgt voor veilige gegevensuitwisseling. Op dit moment wordt in de markt TLS 1.2 gebruikt.



Binnen de sector gemaakte afspraken:

- 11-11-2020: de ALV NEDU stelt TC043 Invoering TLS 1.3 vast.
- 09-03-2022: de ALV NEDU besluit om TLS 1.2 voor de uitwisseling van de berichten niet langer toe te staan dan tot uiterlijk einde 2023.
- 08-03-2023: ALV MFF keurt het uitvoerings- en communicatieplan Invoering TLS 1.3 goed.



Kernpunten uitvoerings- en communicatieplan Invoering TLS 1.3:

- 01-07-2023: centrale systemen beheert door TenneT en EDSN zijn TLS 1.3-gereed. Start officiële duale periode.
- 16-05-2023: online voorlichting Invoering TLS 1.3.
- 05-07-2023: heroverweging haalbaarheid NEDU-besluit deadline TLS 1.3 in de ALV MFF.
- Q3/Q4-2023: monitoring TLS 1.3-readiness marktpartijen (decentrale systemen), rapportage in ALV MFF begin Q4.
- 31-12-2023: rapportage TLS 1.3-readiness (de)centrale systemen, advies mogelijkheid tot uitfasen TLS 1.2 door TenneT en EDSN, besluit ALV MFF januari 2024.



Beknpte resultaten per 19-6-2023

- In totaal beheren EDSN en TenneT 25 centrale systemen en bijbehorende verbindingen. EDSN (14) en TenneT (11), zie hiervoor ook bijlage 1.
- 13 centrale systemen beschikken over TLS 1.3. Van 9 systemen wordt nog verwacht dat deze voor 1 juli 2023 gereed zijn. 3 systemen zijn zeker niet voor 1-7-2023 TLS 1.3-gereed. Voor een overzicht per beheerder zie pagina 5.
- De voorlichting Invoering TLS 1.3 heeft plaatsgevonden en marktpartijen kunnen voor alle systemen die over zijn op TLS 1.3 starten met de invoering van TLS 1.3 in de eigen organisatie.
- Monitoring en publicatie dashboard TLS 1.3-readiness komt op gang en wordt gepubliceerd op de SharePoint van mijn MFFBAS.



Doel van dit document

Rapporteren over de voortgang van de invoering van TLS 1.3 en het updaten van het Uitvoerings- en communicatieplan. Het uitbrengen van een advies over de haalbaarheid NEDU-besluit deadline TLS 1.3.

Stand van zaken invoering TLS 1.3

Toetsing t.o.v. Uitvoerings- en communicatieplan

Deliverable	Toelichting	Status	Opmerkingen
TLS 1.3 op de centrale systemen	EDSN en TenneT maken de centrale systemen voor 1-7-2023 gereed.	14 van de 25 systemen zijn TLS 1.3-ready.	Zie aantallen hieronder. Voor alle systemen die wel TLS 1.3-ready zijn kunnen de marktpartijen de overstap al maken!
Monitoringsrapportage	a. Readiness centrale systemen b. Readiness marktpartijen (decentrale systemen)	a. Beschikbaar en toegankelijk op SharePoint mijnMFFBAS b. Eerste monitoring komt beschikbaar	Voor totalen zie hieronder.
Communicatie	a. Kernboodschap b. Q&A c. Voorlichtingssessie d. Contactpersonenlijst e. Nieuwsbrief f. Helpdesk	a. Beschikbaar binnen werkgroep b. Beschikbaar op SharePoint c. Geweest op 16 mei 2023 d. Uitvraag geweest en ongoing e. Regulier via MFFBAS f. Helpdesk via TenneT en EDSN	De communicatie over de voortgang en het ondersteunen van de marktpartijen is een ongoing proces.
Advies ALV MFF voor uitfasering TLS 1.3	Gepland voor eind Q3 – begin Q4.	Nog niet van toepassing.	- Begin Q4 advies EDSN- systemen - Begin Q1 advies TenneT-systemen
Voortgangsrapportage	T.b.v. Stuurgroep Implementatie	Wordt driewekelijks opgeleverd.	

19-jun-23	Totaal	Ready	Gepland 1-7 gereed	Gepland 1-10 gereed	% ready
EDSN	14	13	1	0	93%
TenneT	11	0	8	3	0%
Totaal	25	13	9	3	52%

Readiness TLS 1.3 centrale systemen per beheerder op 19 juni 2023

Scope, deliverables & acceptatiecriteria

Voor een deel van de centrale systemen is de invoering van TLS 1.3 vertraagd. Hierdoor loopt de planning uit. Voor de scope, deliverables en acceptatiecriteria wordt beknopt de initiële aanpak weergegeven en gekeken of er wijzigingen zijn. Indien ja, wat behelst de wijziging.



Scope

Vastgesteld in Uitvoerings- en communicatieplan	Verandertraject - Ondersteunen in rapportering voortgang marktpartijen t.a.v. readiness CMF-landschap. - Communicatie aan marktpartijen over de wijziging en de voortgang. - Faciliteren van marktpartijen. - Advies uitvaardigen aan ALV MFF. Wijziging centrale systemen CMF-landschap Alle koppelingen tussen de centrale systemen van het CMF-landschap (bijlage 1) met de decentrale systemen van de marktpartijen.
---	---

(Deels) herzien

Nee – geen wijzigingen

Wijziging	N.v.t.
-----------	--------



Deliverables

Deliverable	Deadline
TLS 1.3 op de centrale systemen	1-7-2023
Monitoringsrapportage	3 wekelijks
Communicatie	Conform plan
Advies ALV MFF voor uitfasering TLS 1.2	5-7-2023/ eind Q3-2023
Voortgangsrapportage	3 wekelijks

Ja – gedeeltelijke wijziging planning

Aanpassingen op deliverables en data: TLS 1.2 op de centrale systemen - EDSN: 1-7-2023 - TenneT: 1-10-2023 Advies ALV MFF voor uitfasering TLS 1.2 - Haalbaarheid NEDU-besluit: 5-7-2023 - Readiness marktpartijen EDSN: begin Q4-23 - Readiness marktpartijen TenneT: begin Q1-24 - Definitieve overgang: Eind Q1-2024
--



Acceptatiecriteria

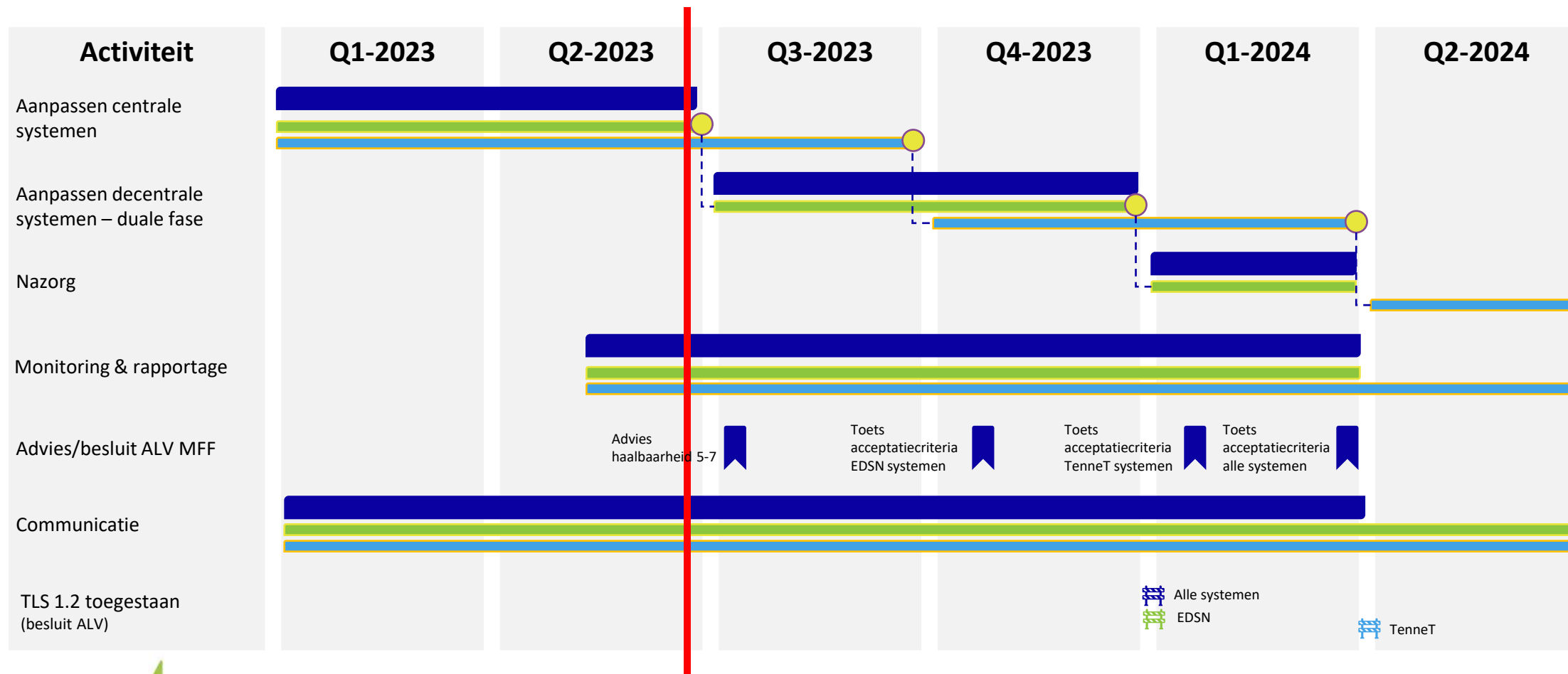
- Voor alle systemen binnen het CMF-landschap (centrale systemen) geldt een acceptatiecriterium van 100% over op TLS 1.3. - Voor alle koppelingen tussen decentrale systemen en systemen in het CMF-landschap geldt een gewogen marktaandeel van 66% over op TLS 1.3. - Voor ODA's en andere marktdeelnemers kan geen gewogen marktaandeel worden afgegeven. Hiervoor geldt een absoluut marktaandeel van 51%.
--

Ja – aanscherping criteria

- Bij het uitbrengen van het advies om TLS 1.2 uit te faseren wordt ook aangegeven welke marktprocessen geraakt worden als deze koppelingen niet meer mogelijk zijn.
--

Planning

De overgang van TLS 1.2 naar TLS 1.3 is voor de centrale systemen van TenneT vertraagd met één kwartaal, voor de centrale systemen van EDSN blijft de planning onveranderd.



Risico's

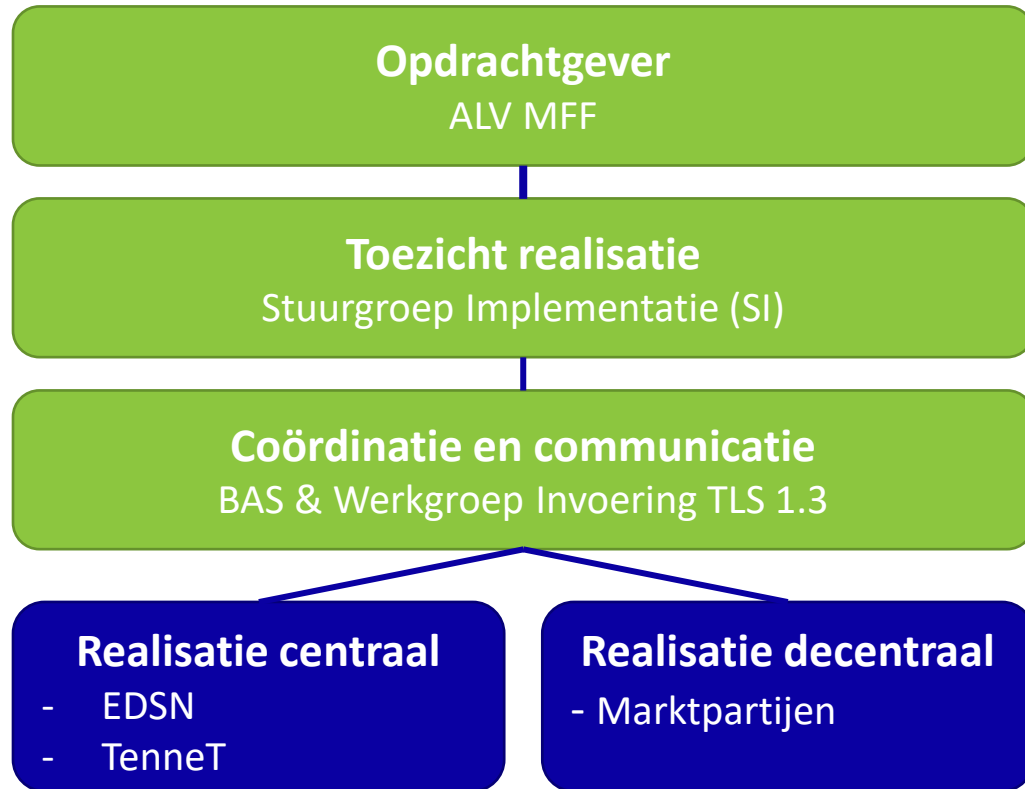
Onderstaande risico's zijn geüpdatet t.o.v. het initiële plan en afgestemd in de werkgroep Invoering TLS 1.3. Hierbij is rekening gehouden met de meest recente situatie en aangepast aanpak. Voor duiding van toegekende waarde van de kans en impact wordt verwezen naar bijlage 2.

Risico	Kans	Impact	Risico	Mitigerende maatregelen	Rest kans	Rest impact	Rest risico
Mogelijk zijn op 1 oktober 2023 niet alle centrale systemen in het CMF-landschap in beheer van TenneT ready, waardoor de marktpartijen niet over kunnen op TLS 1.3.	3	4	12	- Inzicht in systemen en voortgang per systeem. - Voortgang regulier bespreken. - Prioriteren binnen eigen organisatie. - Rapporteren aan SI en ALV MFF, om tijdige afwijking te signaleren.	3	4	12
Mogelijk zijn op 1 juli 2023 niet alle centrale systemen in het CMF-landschap in beheer van EDSN ready, waardoor de marktpartijen niet over kunnen op TLS 1.3.	1	2	2	- Inzicht in systemen en voortgang per systeem. - Voortgang regulier bespreken. - Prioriteren binnen eigen organisatie. - Rapporteren aan SI en ALV MFF, om tijdige afwijking te signaleren.	1	2	2
Mogelijk zijn de decentrale systemen (marktpartijen) gekoppeld aan het CMF-landschap beheert door TenneT niet in voldoende mate ready op 1 april 2024, waardoor de sector niet over kan op TLS 1.3.	4	4	16	- Tijdige communicatie aan alle MFF leden en marktpartijen. - Actieve monitoring en rapportage op de Centrale Systemen t.b.v. het meten van de voortgang. - Pro-actief benaderen van marktpartijen in Q4-2023 en Q1-2024. - Ondersteuning bieden aan partijen die hierom vragen.	3	4	12
Mogelijk zijn de decentrale systemen (marktpartijen) gekoppeld aan het CMF-landschap beheert door EDSN niet in voldoende mate ready op 1 januari 2024, waardoor de sector niet over kan op TLS 1.3.	4	4	16	- Tijdige communicatie aan alle MFF leden en marktpartijen. - Actieve monitoring en rapportage op de Centrale Systemen t.b.v. het meten van de voortgang. - Pro-actief benaderen van marktpartijen in Q3 en Q4. - Ondersteuning bieden aan partijen die hierom vragen.	3	4	12
Indien softwareleveranciers onvoldoende ondersteuning voor TLS 1.3 bieden, is het mogelijk dat de overgang naar TLS 1.3 voor de decentrale systemen niet mogelijk is.	5	5	25	- Inzichtelijk maken bij welke leveranciers de problemen zich voordoen. - Marktpartijen informeren over de mogelijkheid om gebruik te maken van een proxy server als alternatief.	4	2	8
Indien TLS 1.2 vanwege nieuwe gebreken door NCSC afgeschaald wordt naar 'onvoldoende', moet de overgang naar TLS 1.3 worden versneld.	3	2	6	- Monitoren besluitvorming NCSC. - Monitoring voortgang marktpartijen. - Vaststellen actieplan wanneer risico realiteit wordt.	3	1	3
Mogelijk bereikt de communicatie over TLS 1.3 niet alle marktpartijen, waardoor het mogelijk is dat niet alle marktpartijen over gaan op TLS 1.3	4	3	12	- Samenwerking met EDSN en TenneT om alle marktpartijen in beeld te krijgen en te benaderen. - Extra uitvraag contactpersonen. - Extra online voorlichting, voor partijen die in de eerste ronde nog niet in beeld waren.	2	2	4

Organisatie

De opdrachtverstrekking en uitvoering verloopt via onderstaand organogram.

Organogram – Invoering TLS 1.3



Werkgroepleden – Werkgroep Invoering TLS 1.3

Naam	Marktrol	Vertegenwoordiging in team
Amanda Zachariasse	BAS	Projectleider / Topic Manager
Leander Hiele	RNB / DSO – IT Services (EDSN)	PL readiness centrale systemen EDSN
Jan Heerschop	LNB / TSO E – TenneT	Aanspreekpunt readiness centrale systemen TenneT
Jan Nienhuis	RNB / DSO – Stedin	Aanspreekpunt security
Mirjam van der Horst	BAS / Stuurgroep Implementatie	Aanspreekpunt Stuurgroep Implementatie
Bram van Straalen	BAS / CoP Secure Architecture	Aanspreekpunt CoP Secure Architecture
Jacco Hogeweg	BAS	Aanspreekpunt communicatie
Arjan Visser	BAS	Topic Manager (back-up)

Uitvoering Invoering TLS 1.3

Monitoring, informatie & communicatie



Monitoring

Monitoring readiness centrale sytemen

- EDSN & TenneT rapporteren over eigen voortgang TLS 1.3-readiness.
- Gebundeld in dashboard.
- Dashboard wordt gepubliceerd op SharePoint (mijnMFFBAS) en is toegankelijk voor alle marktpartijen.

Monitoring voortgang decentrale systemen

- EDSN & TenneT monitoren de TLS 1.3-readiness van marktpartijen.
- Hierover wordt regelmatig geanonimiseerd gerapporteerd in absolute aantallen.
- De readiness rapportages worden gepubliceerd op: <https://mffbas.sharepoint.com/sites/TLS1.3>.
- De werkgroep Invoering TLS 1.3 bespreekt de voortgang en onderneemt acties indien nodig.
- De Stuurgroep Implementatie (SI) ontvangt een voortgangsrapportage en indien noodzakelijk escalaties.
- In Q3-2023, Q4-2023 en Q1-2024 wordt het gewogen marktaandeel bepaald en hierover naar de ALV MFF gerapporteerd.



Informatie

www.mffbas.nl

Op de website van MFFBAS (direct toegankelijk) is informatie te vinden over de invoering van TLS 1.3. Link: <https://www.mffbas.nl/themas/> Vanuit hier is ook toegang te verkrijgen tot SharePoint van MFFBAS. Iedereen kan toegang tot deze omgeving aanvragen.

SharePoint

Alle relevantie informatie over de invoering van TLS 1.3 wordt geplaatst op de SharePoint van MFFBAS (<https://mffbas.sharepoint.com/sites/TLS1.3>). Onder 'Release' is een aparte omgeving voor TLS 1.3. Hier is onder andere te vinden:

- Dashboard readiness TLS 1.3
- Presentatie online voorlichting TLS 1.3
- Vraag & antwoord
- Gewijzigde endpoints
- Engelse vertaling voorlichting en vraag en antwoord



Communicatie

Nieuwsbrief

Vanuit MFFBAS wordt regelmatig een nieuwsbrief verstuurd. De werkgroep draagt artikelen aan voor de nieuwsbrief indien er relevante informatie te melden is.

Voorlichting

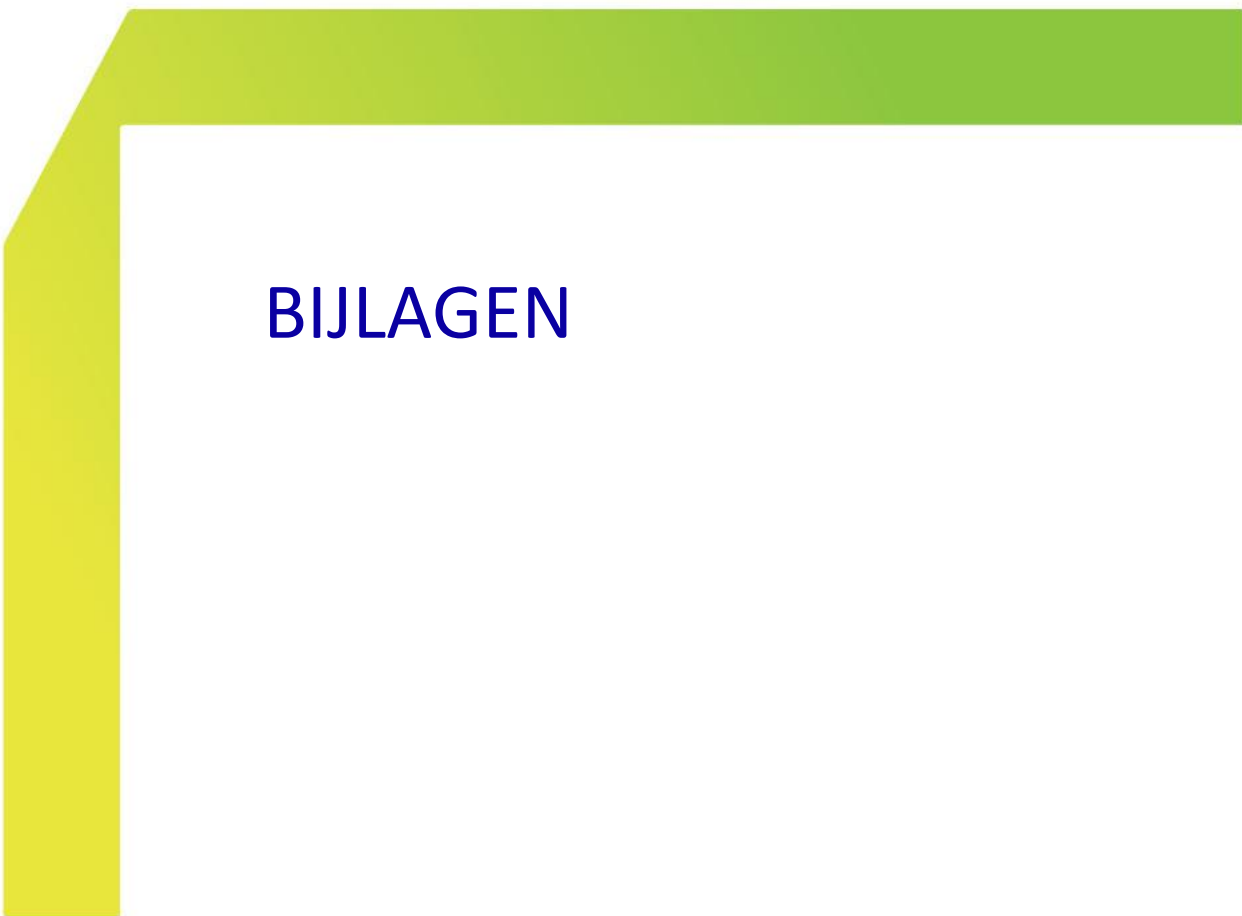
Op 16 mei is een voorlichting gehouden over de invoering van TLS 1.3. Op 4 juli wordt een extra online voorlichting georganiseerd voor de Onafhankelijk Dienstaanbieders (ODA's).

Rapportage

De voortgang van de TLS 1.3-readiness wordt gerapporteerd en beschikbaar gesteld via SharePoint (mijnMFFBAS).

Helpdesk EDSN & TenneT

EDSN en TenneT bieden de marktpartijen ondersteuning vanuit de eigen helpdesk.



BIJLAGEN

Bijlage 2 - risicomatrix

Gehanteerde maatstaven t.b.v. kwantificeren risico's

		Kans				
		Verwachte kans				
		1 <10%	2 >10% <30%	3 >30% <60%	4 >60% <90%	5 >90%
Impact Verwachte vertraging	1 0-0,5 mnd	1	2	3	4	5
	2 0,5-1 mnd	2	4	6	8	10
	3 1-2 mnd	3	6	9	12	15
	4 2-4 mnd	4	8	12	16	20
	5 >4 mnd	5	10	15	20	25

Bijlage 1 – lijst met centrale systemen in scope

Overzicht per beheerpartij

EDSN

Axway API Gateway, Axway B2Bi , KONG gateway, Toestemmingsplatform, Energiedatalink Provider, CERES
C-AR/Portaal (incl. sectorregister, CER, PUD, MDD, MPR, LV/RNB Register, TR, ADC, BU, GBU) (inkomend)
C-AR/Portaal (incl. sectorregister, CER, PUD, MDD, MPR, LV/RNB Register, TR, ADC, BU, GBU) (uitgaand: C-AR ==> applicatie)
C-ARM
Data delen platform
EAN-codeboek
Gopacs (inkomend)
Nexus (uitgaand)
Portaal CTS
TMR (uitgaand)
CSS
Gopacs (uitgaand: Gopacs ==> Applicatie)
Nexus (inkomend: Applicatie ==> Nexus))
TMR (inkomend: Applicatie ==> TMR)

TenneT

MMC Hub
CPS
TQF
APFAS
OSB voor legacy websites
CPB
GOPACS adapter
FCR webservices
B2B gateway
API Gateway (KONG)
MHS