

VRAAG & ANTWOORD

INVOERING TLS 1.3

Datum laatste update: 30 mei 2023

Versie: 1.0

1	ALGEMEEN OVER TLS	2
1.1	WAT IS TLS?	2
1.2	WAARVOOR WORDT TLS IN DE ENERGIESECTOR GEBRUIKT?	2
2	SCOPE INVOERING TLS 1.3	3
2.1	WELKE CENTRALE SYSTEMEN ZIJN IN SCOPE VAN PROJECT 'INVOERING TLS 1.3'?	3
2.1.1	Hoe weet ik welk systeem al over is?	4
2.2	Vragen met betrekking op de scope	4
2.2.1	Zijn de centrale systemen van GTS ook in scope?	4
2.2.2	Zijn de afspraken ook van toepassing op (interne) berichtenverkeer via internet, zoals bijvoorbeeld een app voor klanten?	4
2.2.3	Worden er bij EDSN bij het TLS 1.3 ready maken van de system gelijk bericht aanpassingen doorgevoerd, zoals de overgang van SOAP naar REST?	4
3	INVOERING TLS 1.3	5
3.1	WAAROM IS DE INVOERING VAN TLS 1.3 NOODZAKELIJK?	5
3.1.1	Wat is Perfect Forward Secrecy	5
3.2	IS INVOERING VAN TLS 1.3 VERPLICHT?	5
3.3	WAT IS DE PLANNING VOOR DE INVOERING VAN TLS 1.3?	5
3.3.1	Kan ik nu al over op TLS 1.3?	5
3.3.2	Moet ik wachten met invoering tot alle centrale systemen klaar zijn voor TLS 1.3?	5
3.3.3	Wanneer moet ik TLS 1.3 uiterlijk hebben ingevoerd?	6
3.3.4	Wat gebeurt er als ik niet op tijd TLS 1.3 heb ingevoerd?	6
3.3.5	Is het advies aan marktpartijen om na de overgang naar TLS 1.3 bij de communicatie met een centraal systeem gelijk TLS 1.2 deactiveren?	6
3.3.6	Is het voor 1 juli 2023 duidelijk welke endpoints bij TenneT en EDSN er gaan veranderen?	6
3.3.7	Blijft TLS 1.2 nog in een periode ondersteund door de centrale systemen?	6
3.3.8	Wat is de uiterste datum tot wanneer TLS 1.2 gebruikt kan worden?	6
4	ONDERSTEUNING INVOERING TLS 1.3	7
4.1	WELKE ONDERSTEUNING IS ER BIJ DE INVOERING VAN TLS 1.3?	7
4.1.1	Helpdesk EDSN	7
4.1.2	Helpdesk TenneT	7
4.1.3	Wie helpt met bij de invoering van TLS 1.3?	7
4.1.4	Waar vind ik meer informatie?	7
4.1.5	Q: Komt er ook een test omgeving die alleen TLS 1.3 ondersteunt, zodat zeker is dat er niet een fallback naar TLS 1.2 wordt gebruikt?	7
4.2	WAT ALS....	7
4.2.1	Wat gebeurt er als mijn softwareleverancier zijn systeem niet tijdig op orde heeft?	7
4.2.2	Worden marktpartijen actief op de hoogte gesteld of zij volgens de monitoring over zijn op TLS 1.3?	7
5	OVERIGE VRAGEN	8
5.1	WANNEER KOMT ER EEN UPDATE VAN HET DOCUMENT "230412 – INVOERING TLS 1.3 – UITVOERINGS- EN COMMUNICATIEPLAN – DEFINITIEF.PDF WAARIN OOK DE BIJLAGE 4.4.2 "CENTRALE SYSTEMEN IN BEHEER BIJ TENNET" OPGENOMEN IS?	8
5.2	ALS HET ACCEPTATIECRITERIUM 66,66% GEWOGEN MARKAANDEEL IS EN VERVOLGENS WORDT TLS 1.2 NIET MEER ONDERSTEUNT, BETEKENT DIT TOCH DAT ER MARKTVERSTORING PLAATSVINDT	8

1 Algemeen over TLS

1.1 Wat is TLS?

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.

1.2 Waarvoor wordt TLS in de energiesector gebruikt?

Binnen de energiesector wordt TLS (nu versie 1.2) gebruikt om veilig gegevens uit te wisselen tussen systemen van marktpartijen (decentrale systemen) en centrale systemen die beheerd worden door TenneT en EDSN.

Meer informatie over wat TLS is en de werking hiervan is te vinden in de presentatie van de online voorlichting 'Invoering TLS 1.3'.

Deze is te raadplegen via de SharePoint van MFFBAS: [2. Voorlichtingssessie TLS 1.3 16 mei 2023](#)

2 Scope invoering TLS 1.3

2.1 Welke Centrale systemen zijn in scope van project 'Invoering TLS 1.3'?

Iedere applicatie in het landschap van jouw organisatie die met centrale systemen communiceert als onderdeel van de marktprocessen. Daarbij kan het zijn dat ook achterliggende software, waarvan de applicatie afhankelijk is, moet worden aangepast. Voorbeelden: databasesystemen (DBMS-en), gateways, Tip: raadpleeg hiervoor de architecten en technisch beheerders van je eigen organisatie!

De Centrale Systemen die binnen de scope van de Invoering TLS 1.3 vallen zijn opgenomen in onderstaande tabel. Per systeem is aangegeven welke partij verantwoordelijk is voor het beheer van het systeem. Bij vragen kan met TenneT of EDSN contact op worden genomen.

Nr.	Systeem	Beheerd door
1	Axway API Gateway, Axway B2Bi , KONG gateway, Toestemmingsplatform, Energiedatalink Provider, CERES	EDSN
2	C-AR/Portaal (incl. sectorregister, CER, PUD, MDD, MPR, LV/RNB Register, TR, ADC, BU, GBU) (inkomend)	EDSN
3	C-AR/Portaal (incl. sectorregister, CER, PUD, MDD, MPR, LV/RNB Register, TR, ADC, BU, GBU) (uitgaand: C-AR ==> applicatie)	EDSN
4	C-ARM	EDSN
5	Data delen platform	EDSN
6	EAN-codeboek	EDSN
7	Gopacs (inkomend)	EDSN
8	Nexus (uitgaand)	EDSN
9	Portaal CTS	EDSN
10	TMR (uitgaand)	EDSN
11	CSS	EDSN
12	Gopacs (uitgaand: Gopacs ==> Applicatie)	EDSN
13	Nexus (inkomend: Applicatie ==> Nexus))	EDSN
14	TMR (inkomend: Applicatie ==> TMR)	EDSN
15	MMC Hub	TenneT
16	CPS	TenneT
17	TQF	TenneT
18	APFAS	TenneT
19	OSB voor legacy websites	TenneT
20	CPB	TenneT
21	GOPACS adapter	TenneT
22	FCR webservices	TenneT
23	B2B gateway	TenneT
24	API Gateway (KONG)	TenneT
25	MHS	TenneT

Tabel 1: Overzicht Centrale Systemen in scope incl. beheerpartij

2.1.1 Hoe weet ik welk centraal systeem al TLS 1.3 ondersteunt?

Tweewekelijks wordt op de SharePoint van mijn MFFBAS het Dashboard readiness Centrale Systemen geplaatst. Link naar de map: [1. Dashboard readiness Centrale Systemen](#)

2.2 Vragen met betrekking op de scope

2.2.1 Zijn de centrale systemen van GTS ook in scope?

Er zijn geen centrale systemen van GTS in scope. Het systeem NEXUS, dat gebruikt wordt voor de uitwisseling van allocatie- en reconciliatieberichten gas wordt beheerd door EDSN en is in scope.

2.2.2 Zijn de afspraken ook van toepassing op (interne) berichtenverkeer via internet, zoals bijvoorbeeld een app voor klanten?

Nee, dit project gaat enkel over berichtenverkeer met betrekking tot marktprocessen waarvoor MFFBAS verantwoordelijk is en plaatsvindt tussen marktpartijen en de centrale systemen die beheerd worden door EDSN en TenneT. Berichtenverkeer tussen een marktpartij en bijvoorbeeld een eigen klantenapp is daarmee niet in scope.

2.2.3 Worden er bij EDSN bij het TLS 1.3 ready maken van de system gelijk berichtaanpassingen doorgevoerd, zoals de overgang van SOAP naar REST?

Nee. Om de scope van het project af te bakenen, worden geen berichtaanpassingen doorgevoerd, want dan moeten alle marktpartijen deze nieuwe berichten implementeren en belanden we in een “traditionele” sectorrelease.

3 Invoering TLS 1.3

3.1 Waarom is de invoering van TLS 1.3 noodzakelijk?

TLS 1.3 zorgt voor snellere uitwisseling en betere beveiliging van data-uitwisselingberichten. Het Nationaal Cyber Security Center (NCSC) heeft TLS 1.2 afgeschaald van 'goed' naar 'voldoende'. Onderzoek heeft aangetoond dat de ciphers en algoritmen die TLS 1.2 gebruikt cryptografische zwakheden bevatten, die gevoelig zijn voor mogelijke aanvallen. Daarmee lopen de continuïteit en veiligheid van berichtenverkeer gevaar. De kans dat het NCSC TLS 1.2 verder afschaalt naar 'onvoldoende' is substantieel. Daarnaast wordt met TLS 1.3 een verbetering in de snelheid van berichtenverkeer bewerkstelligd, omdat het protocol tussen server en client minder stappen bevat. Tevens is de security van TLS 1.3 meer robuust, waarmee Perfect Forward Secrecy wordt afgedwongen, en heeft het verbeterde encryptie-algoritmen die geen bekende zwakheden bevatten.

3.1.1 Wat is Perfect Forward Secrecy

Perfect Forward Secrecy is een versleutelingsstijl die bekend staat om het produceren van tijdelijke privé-sleuteluitwisselingen tussen clients en servers. Voor elke individuele sessie die door een gebruiker wordt gestart, wordt een unieke sessiesleutel gegenereerd. Als een van deze sessiesleutels wordt gecompromitteerd, worden de gegevens van andere sessies niet aangetast. Daarom zijn eerdere sessies en de informatie daarin beschermd tegen toekomstige aanvallen. Deze versleutelingsstijl wordt meestal gebruikt door bel-apps, webpagina's en messaging-apps waar de privacy van gebruikers van het grootste belang is.

3.2 Is invoering van TLS 1.3 verplicht?

Ja, conform de in de ALV MFF genomen besluiten is invoering van TLS 1.3 verplicht om te kunnen blijven deelnemen aan de data uitwisseling binnen de energiesector.

Nr.	Datum	Besluit	Stuknummer	Agenda punt
1508	11 november 2020	De ALV NEDU stelt TC043 Invoering TLS 1.3 vast.	ALV NEDU 20201111-014.1	14.1
1638	9 maart 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.	ALV NEDU 20220309-014.2	14.2

Tabel 2 – Besluiten ALV NEDU / MFF

3.3 Wat is de planning voor de Invoering van TLS 1.3?

Onderdeel van de besluiten uit tabel 2 zijn de datums van overgang. Vanaf 1-7-2023 ondersteunen alle centrale systemen TLS 1.3. Hiermee start de duale fase, waarin zowel TLS 1.2 als TLS 1.3 ondersteund wordt. Vanaf 31-12-2023 wordt verwacht dat alle marktpartijen ook over zijn op TLS 1.3. Daarmee kan ter besluit aan de ALV MFF worden voorgelegd dat de ondersteuning van TLS 1.2 door TenneT en EDSN kan worden beëindigd.

3.3.1 Kan ik nu al over op TLS 1.3?

Jazeker! Een groot deel van de centrale systemen ondersteunt al TLS 1.3. Je kunt dus aan de slag om TLS 1.3 te testen bij de communicatie met deze centrale systemen. En je kunt vervolgens via TLS 1.3 gaan communiceren met deze centrale systemen.

3.3.2 Moet ik wachten met invoering tot alle centrale systemen klaar zijn voor TLS 1.3?

Nee. Het wordt aanbevolen om al te beginnen met de centrale systemen die nu al TLS 1.3 ondersteunen.

3.3.3 Wanneer moet ik TLS 1.3 uiterlijk hebben ingevoerd?

De deadline staat op 31-12-2023.

3.3.4 Wat gebeurt er als ik niet op tijd TLS 1.3 heb ingevoerd?

Zodra de 66% gewogen marktaandeel per marktrol (LBN en RNB 100%) is behaald van alle marktpartijen, zal het project dit rapporteren aan de ALV MFF. Vervolgens moet de ALV MFF besluiten wanneer de ondersteuning van TLS 1.2 beëindigd wordt. En als dat besluit genomen is en TLS 1.2 daadwerkelijk is uitgezet, kan een decentraal systeem niet langer met de centrale systemen verbinding via TLS 1.2 maken.

3.3.5 Is het advies aan marktpartijen om na de overgang naar TLS 1.3 bij de communicatie met een centraal systeem gelijk TLS 1.2 deactiveren?

Het verdient de voorkeur om TLS 1.2 gelijk te deactiveren, tenzij het betreffende systeem ook gebruikt wordt voor koppelingen met andere systemen waarvoor TLS 1.2 ingezet wordt.

3.3.6 Is het voor 1 juli 2023 duidelijk welke endpoints bij TenneT en EDSN er gaan veranderen?

Bij EDSN en TenneT is het nu niet voorzien dat endpoints wijzigen. Mocht dit desondanks toch nodig zijn, dan wordt dit gecommuniceerd via de nieuwsbrief en/of mijn MFFBAS.

3.3.7 Blijft TLS 1.2 nog in een periode ondersteund door de centrale systemen?

Ja, er is een duale periode waarin de centrale systemen zowel TLS 1.2 als TLS1.3 ondersteunen, totdat binnen de ALV MFF besloten wordt om TLS 1.2 niet meer te ondersteunen en de beheerders van de centrale systemen de mogelijkheid voor TLS 1.2 uitzetten.

3.3.8 Wat is de uiterste datum tot wanneer TLS 1.2 gebruikt kan worden?

Dat moet nog bepaald worden. De eerste prioriteit is dat bij alle berichtenverkeer met de centrale systemen TLS 1.3 gebruikt gaat worden. Hiervoor is de deadline 31-12-2023. In het najaar van 2023 gaan we kijken wat de status is van de overgang naar TLS 1.3 en een voorstel doen aan de ALV MFF wanneer TLS 1.2 niet meer ondersteund mag worden. ALV MFF neemt het uiteindelijke besluit.

4 Ondersteuning invoering TLS 1.3

4.1 Welke ondersteuning is er bij de Invoering van TLS 1.3?

4.1.1 Helpdesk EDSN

servicedesk@edsn.nl

Met in het onderwerp: TLS1.3 - <Applicatiennaam> - Probleem/vraag

4.1.2 Helpdesk TenneT

TenneT Customer Care Center: tennetccc@tennet.eu

4.1.3 Wie helpt met bij de invoering van TLS 1.3?

De beheerders van de centrale systemen, EDSN en TenneT, staan klaar om vragen te beantwoorden, de contactgegevens van beide partijen staan hierboven vermeld.

4.1.4 Waar vind ik meer informatie?

Aanvullend biedt webpagina (<https://mffbas.sharepoint.com/sites/TLS1.3>) 'Invoering TLS 1.3' meer informatie. Welke hulp biedt MFFBAS bij de invoering van TLS 1.3? Hulp wordt geboden middels delen van verkregen kennis over TLS 1.3 en de impact die mogelijk voor organisaties geldt, zoals:

- Instellingen voor het inregelen van TLS 1.3;
- Inzicht in versies van veel in de markt toegepaste standaardsoftware;
- Alternatieven.

4.1.5 Q: Komt er ook een test omgeving die alleen TLS 1.3 ondersteunt, zodat zeker is dat er niet een fallback naar TLS 1.2 wordt gebruikt?

Vanuit zowel EDSN als TenneT is dit niet voorzien. Er wordt enkel een testomgeving beschikbaar gesteld die zowel TLS 1.2 als TLS 1.3 ondersteunt, net zoals de productieomgevingen van EDSN en TenneT, die ook beide versies ondersteunen.

4.2 Wat als....

4.2.1 Wat gebeurt er als mijn softwareleverancier zijn systeem niet tijdig op orde heeft?

Dan kun je de systemen achter een proxyserver zetten, waarmee het mogelijk is om het externe verkeer via TLS 1.3 te laten lopen, terwijl intern nog niet alle systemen TLS 1.3 ready zijn. Hoe dat eruit ziet en wat je daarvoor moet doen is terug te vinden in de presentatie van de online voorlichting 'Invoering TLS 1.3'. Deze is te raadplegen via de SharePoint van MFFBAS: [2. Voorlichtingssessie TLS 1.3 16 mei 2023](#)

4.2.2 Worden marktpartijen actief op de hoogte gesteld of zij volgens de monitoring over zijn op TLS 1.3?

De overgang naar TLS 1.3 is de verantwoordelijkheid van de marktpartijen. De monitoring is primair bedoeld om inzichtelijk te krijgen over wat de status sectorbreed is m.b.t. de overgang naar TLS 1.3. Indien er twijfels zijn of de overgang naar TLS 1.3 is geslaagd dan kunnen marktpartijen terecht bij de helpdesk van EDSN of TenneT afhankelijk van de systemen waarop de vraag betrekking heeft. Zie hiervoor tabel 1.

5 Overige vragen

5.1 Wanneer komt er een update van het document “230412 – Invoering TLS 1.3 – Uitvoerings- en Communicatieplan – Definitief.pdf waarin ook de bijlage 4.4.2 “Centrale systemen in beheer bij TenneT” opgenomen is?

Deze is niet voorzien. Om welke centrale systemen het gaat is terug te vinden in de presentatie van de voorlichting en op het dashboard readiness centrale systemen. Beide zijn gepubliceerd en toegankelijk via de Sharepoint van MFFBAS.

5.2 Als het acceptatiecriterium 66,66% gewogen marktaandeel is en vervolgens wordt TLS 1.2 niet meer ondersteunt, betekent dit toch dat er marktverstoring plaatsvindt

Ja en daarom kan de ondersteuning van TLS 1.2 niet zomaar beëindigd worden. Dat besluit zal expliciet in de ALV MFF genomen moeten worden op basis van de dan beschikbare informatie en de impact van dit besluit.