



Uitfaseringsplan TLS1.2

TenneT front end systemen

Voorwoord

In september 2019 heeft de ALV NEDU besloten dat de Nederlandse Energiemarkt de overstap zou maken naar security standaard TLS1.3. In eerste instantie werden hier geen tijdlijnen aan gehangen, en werd uitgegaan van een infasering van TLS1.3 op basis van reguliere life cycle management van de diverse IT systemen. In maart 2022 werden er in de ALV door gebrek aan voortgang alsnog tijdlijnen afgesproken, maar ook daarna bleef de voortgang bij TenneT onvoldoende. Uiteindelijk heeft TenneT begin 2024 een taskforce opgezet om alsnog op de kortst mogelijke termijn TLS1.3 te faciliteren, en de uitfasering van de oudere security standaard TLS1.2 voor te bereiden. Alle TenneT Front End systemen ten behoeve van datastromen in de Nederlandse Energiemarkt faciliteren inmiddels TLS1.3.

Hoewel TLS1.2 formeel nog als veilig wordt gezien, **is TenneT voorstander van een snelle invoering van TLS1.3 in de Nederlandse Energiemarkt**, met inbegrip van de buitenlandse marktpartijen die in de Nederlandse markt actief zijn. Op basis van dit plan worden marktpartijen daarom verzocht om zo snel mogelijk de overstap naar TLS1.3 te maken.

De lange voorgeschiedenis is verre van optimaal. Er zijn meermaals marktafspraken gemaakt waar TenneT (en andere betrokken partijen) achteraf gezien geen akkoord op had moeten geven. Het uitzetten van TLS1.2 bij 66% market readiness zou potentieel een onacceptabel grote impact hebben op het berichtenverkeer en de processen in de energiemarkt. **Dit plan heeft als doel om zo snel mogelijk TLS1.2 uit te faseren, maar stelt het voorkomen van verstoring van processen boven de snelheid waarmee TLS1.2 uit gaat.**

TenneT zal acteren op partijen die willens en wetens de overstap naar TLS1.3 uitstellen.

Inhoudsopgave

Voorwoord	2
1. Uitgangspunten	4
1.1 Scope	4
1.2 Tijdslijnen	6
1.3 Beperkingen	7
1.4 Rapportage aan MFF	8
2. Uitfaseringsplan per systeem	8
2.1 API Gateway	8
2.2 CPS	9
2.3 CBP	10
2.4 MMC-hub	11
2.5 MyTenneT	12
2.6 OSB web services	13
2.7 TQF	14
3. Hoe om te gaan met laggard partijen	15
4. Als TLS1.2 onveilig wordt verklaard	15
Bijlage A: Overzicht marktrollen per IT systeem	16

1. Uitgangspunten

- Na een verlate start staat op alle TenneT systemen die uitwisseling van datastromen in de Nederlandse Energiemarkt faciliteren TLS1.3 dual aan met TLS1.2. Dit betekent dat marktpartijen van de veiligere TLS1.3 standaard gebruik kunnen maken, om daarmee de security risico's op die datastroom te verlagen. Dit plan richt zich op de transitie van marktpartijen naar TLS1.3 (voor zover ze dat niet al gedaan hebben), en de veilige uitfasering van TLS1.2.
- TLS1.2 wordt vanuit de officiële instanties nog als veilig verklaard. Mocht TLS1.2 onveilig verklaard worden, dan treedt een ander plan in werking, dat in hoofdstuk 4 kort wordt toegelicht.
- De communicatie naar marktpartijen over de invoering van TLS1.3 is tot nog toe door BAS verzorgd. BAS heeft echter geen volledig zicht op alle marktpartijen die via de systemen van TenneT communiceren. Daardoor heeft er nog geen of heel beperkte communicatie plaats gevonden naar Balance Responsible Parties zonder aansluitingen, Balance Service Providers en Congestion Service Providers. TenneT zal de communicatie naar de partijen met een aansluiting op haar IT systemen oppakken, en hen een redelijke termijn moeten bieden om de overstap naar TLS1.3 te maken, daarbij ook rekening houdend met de planning van Allocatie2.0.
- De impact van uitfasen van TLS1.2 verschilt sterk per systeem. Dit plan beschouwt ieder systeem daarom apart, zodat de overstap naar TLS1.3 zo snel als mogelijk wordt gedaan.
- Dit plan heeft als doel om MFF en BAS een helder beeld te scheppen van de stappen en maatregelen die TenneT neemt bij het uitfasen van TLS1.2, details over te nemen technische stappen zijn achterwege gelaten.

1.1 Scope

De scope van dit plan is beperkt tot de TenneT Front End systemen, de systemen waarmee TenneT en marktpartijen met elkaar communiceren (zo ook marktpartijen onderling). Het richt zich op een veilige uitfasering van TLS1.2 in de Nederlandse Markt. De security van TenneT interne systemen staat onder continue aandacht, maar vallen wat dat betreft buiten de onder MFF gemaakte afspraken.

De scope omvat alle partijen die actief zijn op de Nederlandse markt, inclusief de buitenlandse Balance Responsible Parties zonder aansluitingen, die ook door TenneT erkend worden. Internationale data uitwisseling zoals tussen de TSO's valt buiten deze scope, met hen zijn nog geen concrete afspraken gemaakt om TLS1.2 uit te faseren.

Overzicht van de systemen in scope

Systeem	Functie	In scope
API Gateway	De API Gateway is voor TenneT een nieuw systeem dat in de toekomst de ontsluiting van API's zal faciliteren. Op dit moment worden alleen de publicaties op tennet.eu via API's ontsloten, met inbegrip (tzt) van de A2.0 API's voor reconciliatieprijzen.	Ja
B2B Gateway	De B2B Gateway stond ten onrechte in het eerder gehanteerde overzicht en moet uit de lijst verwijderd worden. De B2B Gateway is de verzameling van systemen die TenneT gebruikt voor het berichtenverkeer, zoals de MMC-hub en de TQF.	Nee
Centraal Postbus Systeem (CPS)	Het CPS is een legacy systeem voor berichtuitwisseling, waar zowel een restant nationale berichtstromen overheen loopt (zoals Reconciliatie PRF) als internationaal verkeer (zoals TSO-TSO communicatie).	Ja
Crowd Balancing Platform (CBP)	Het CBP is het BlockChain platform dat TenneT gebruikt voor communicatie met Balance Service Providers over het product Reservevermogen (aFRR).	Ja
Edine Test Faciliteit (ETF)	De Edine Test Faciliteit is een legacy systeem dat gebruikt wordt om marktpartijen te kwalificeren voor het EDINE berichtenverkeer via het CPS. Het ETF wordt momenteel niet gebruikt, nieuwe kwalificaties voor EDINE zijn inmiddels zeer uitzonderlijk. ETF wordt niet met TLS beveiligd en valt daarmee buiten scope van dit plan.	Nee
FCR webservices	FCR webservices stonden ten onrechte in het eerder gehanteerde overzicht en moet uit de lijst verwijderd worden. De FCR berichtstroom verloopt via de MMC-hub.	Nee
GOPACS adapter	GOPACS stond ten onrechte in het eerder gehanteerde overzicht voor TenneT en moet uit de lijst verwijderd worden. GOPACS wordt gefaciliteerd door EDSN. TenneT loopt wat dat betreft mee in het uitfaseringsplan van EDSN.	Nee
Market-2-Market Communication HUB (MMC-hub)	De MMC-hub is het centrale systeem voor Wholesale berichtuitwisseling in de Nederlandse markt, variërend van near realtime balanceringsberichten tot meetberichten.	Ja
Message Handling System (MHS/tibco)	MHS stond ten onrechte in het eerder gehanteerde overzicht en moet uit de lijst verwijderd worden. Het MHS is een intern handling systeem om berichten uit het CPS op te halen, en aan TenneT backend aan te bieden. MHS draait op TLS1.3.	Nee

MyTenneT, inclusief APFAS en TQF app	MyTenneT is de self service portal van TenneT, een beveiligde website die partij specifieke informatie ontsluit. MyTenneT geeft ook toegang tot twee achterliggende portals: APFAS (veilingplatform voor balanceringsproducten) en de TQF app (gebruikers user interface op de TQF applicatie)	Ja
Oracle Service Bus (OSB)	De OSB ontsluit synchrone web services voor Noodvermogen (mFRR)	Ja
SCADA koppeling	De SCADA koppeling faciliteert een directe communicatie tussen de Energy Management Systemen van TenneT en specifieke aangesloten. De diverse soorten SCADA koppelingen maken geen gebruik van TLS voor de beveiliging en vallen daarmee buiten scope van dit plan	Nee
Test- and Qualification Facility (TQF)	De TQF is een omgeving met daarop een kopie van de MMC-hub, en systemen die marktpartijen faciliteren in het testen- en kwalificeren tegen processen in de Nederlandse Energiemarkt. Communicatie verloopt via de MMC-hub kopie.	Ja

1.2 Tijdslijnen

Dit plan zal aan de ALV van MFF van 15 mei 2024 aangeboden worden. In aanloop daar naartoe wordt dit plan op 19 april 2024 in het IISO behandeld, en op 26 april 2024 in de PF SG. TenneT start vooruitlopend op de discussies in MFF verband direct met uitvoering van dit plan, onder meer door alle marktpartijen te informeren dat van hen verwacht wordt dat ze zo spoedig mogelijk op TLS1.3 over moeten stappen.

Omdat een relevant deel van de marktpartijen nog niet over TLS1.3 is geïnformeerd, zal hen een redelijke termijn geboden moeten worden voor de transitie. Deze redelijke termijn verschilt per applicatie, afhankelijk van de impact die de transitie voor de partijen heeft. Rekening houdende met de wens van de ALV om TLS1.2 zo spoedig mogelijk uit te zetten, het feit dat TLS1.2 vanuit de instanties nog als veilig wordt bestempeld, en met oog op de planning voor Allocatie2.0, stelt TenneT twee verschillende deadlines voor:

Deadline	Rationale	Systemen
01/06/2024	- Voor MyTenneT, APFAS en de TQF app heeft de transitie naar TLS1.3 weinig impact; de meeste browsers zijn voorbereid en de website dwingt de juiste TLS zelf af. Partijen met verouderde browsers moeten echter wel gelegenheid krijgen om binnen hun security maatregelen een nieuwere browser te installeren. - Voor TQF is een snelle uitfasering van TLS1.2 wenselijk, enerzijds zodat partijen bij het testen direct van de nieuwste versie gebruik maken en anderzijds om de risico's voor de Allocatie2.0 planning te minimaliseren.	MyTenneT, inclusief APFAS en TQF app TQF

Een nog kortere deadline is niet reëel in verband met lopende transitie trajecten voor onder meer Nominations en Imbalance Settlement.

15/09/2024	Normaliter wordt marktpartijen een termijn van 6 maanden gegeven, waarbij de communicatie daarover vooraf is opgestart. Een termijn van 3 á 4 maanden zou redelijk kunnen zijn, maar dan valt de deadline zeer ongunstig t.o.v. de planning van Allocatie2.0. TenneT zal daarom vanaf medio september optreden tegen marktpartijen (in scope) die een technische uitfasering van TLS1.2 zonder verstoring van de markt verhinderen.	API Gateway CPS CBP MMC-hub OSB web services
-------------------	---	--

1.3 Beperkingen

Er zijn een aantal beperkingen waar bij de uitfasering van TLS1.2 rekening mee gehouden dient te worden:

- Zoals hierboven al staat aangegeven is een relevant deel van de marktpartijen nog niet geïnformeerd over de transitie naar TLS1.3. TenneT is er ten onrechte van uitgegaan dat die communicatie volledig via BAS zou verlopen. Alle op de TenneT front end systemen aangesloten marktpartijen zullen op korte termijn een communiqué ontvangen, en een redelijke termijn om de overstap te maken.
- Zowel richting BAS als richting TenneT hebben partijen aangegeven dat Microsoft TLS1.3 nog niet ondersteunt. Tijdens de transitie zal duidelijk moeten worden welke partijen dit precies betreft, wat de impact daarvan is en of doorzetten van uitfaseren van TLS1.2 feasible is. TenneT zal TLS1.2 alleen uitzetten als de door TenneT beoordeelde impact daarvan op de markt acceptabel is, dan wel als aan laten staan van TLS1.2 een grotere impact heeft (bijvoorbeeld als TLS1.2 formeel onveilig wordt verklaard).
- Er loopt internationaal verkeer over het CPS, zoals communicatie tussen TSO's onderling. Uitfasering van TLS1.2 staat bij die internationale communicatie nog niet ter discussie, en TenneT kan richting die partijen niet eenzijdig de overstap naar TLS1.3 afdwingen. Consequentie is dat TLS1.2 op het CPS vooralsnog technisch niet uitgezet kan worden. TenneT zal echter marktpartijen die actief zijn op de Nederlandse markt wel aan de TLS1.3 afspraak houden. Er is beperkte zichtbaarheid of een marktpartij tegen de afspraken in TLS1.2 gebruikt, maar als TenneT daar aanwijzingen toe heeft zal zij daar op acteren.
- Minstens 1 marktpartij geeft aan dat ze met het CPS niet over kán stappen. Het is onbekend welke partij in welke marktrol dit betreft, en voor welke berichtstromen die partij het CPS nog gebruikt. Tijdens de transitie zal dit duidelijk moeten worden. Het CPS wordt te zijner tijd zelf ook uitgefaseerd, maar daarentegen kan TenneT TLS1.2 op het CPS vooralsnog technisch niet uitzetten i.v.m. het TSO-TSO verkeer. De vraag is wat dit voor impact heeft op deze casus,

en of er zo nodig voldoende grond is om de bewuste partij tot snellere uitfasering van TLS1.2 te kunnen dwingen. TenneT zal hierover transparant naar MFF rapporteren.

1.4 Rapportage aan MFF

TenneT zal de status en voortgang van de TLS1.2 uitfasering transparant aan het IISO en de PF SG rapporteren, zo lang dit plan loopt. De voortgang van de transitie wordt gerapporteerd over de volgende systemen (zie hoofdstuk 2):

- CPS
- CBP
- MMC-hub
- OSB web services

2. Uitfaseringsplan per systeem

2.1 API Gateway

2.1.1 Context

- De API Gateway is voor TenneT een nieuw systeem, op dit moment worden alleen de publicaties op tennet.eu via API's ontsloten, en worden alleen nog marktpartijen op de API's toegelaten.
- Met de API Gateway voorziet TenneT in haar transparantieplichtingen, aanvullend op de publicaties op www.tennet.eu.
- Nog niet alle API Gateway gebruikende marktpartijen zijn geïnformeerd over de overstap naar TLS1.3. TenneT zal marktpartijen dan ook een redelijke termijn moeten geven om de overstap naar TLS1.3 te maken, zodat ze voldoende tijd hebben om daarop voor te bereiden.

2.1.2 Risico's

- De marktbrede risico's voor uifasieren van TLS1.2 zijn beperkt. Marktpartijen die niet tijdig zijn overgestapt missen hiermee voor hen relevante informatie, en moeten terugvallen op de publicaties op de website(s). Andere marktpartijen worden hiermee niet benadeeld.

2.1.3 Communicatie en follow up

- Gegeven de context zal TenneT geen actieve transitie opzetten, en duidelijk communiceren dat TLS1.2 onverkort op de gestelde deadline wordt uitgezet. Het is aan marktpartijen zelf om hier tijdig op te acteren.
- Gebruikers worden op de volgende momenten geïnformeerd:
 - April – Generieke mailing naar alle marktpartijen
 - Mei – Door BAS georganiseerde markt informatie sessie
 - Juni – Specifieke mailing naar gebruikers API Gateway
 - Augustus – Final call mailing naar gebruikers API Gateway

2.1.4 TLS1.2 uit

- TLS1.2 wordt op de gestelde deadline (zie paragraaf 1.2) hard uit gezet.

2.2 CPS

2.2.1 Context

- Het Centraal Postbus Systeem is een legacy systeem voor berichtuitwisseling, waar zowel een restant nationale berichtstromen overheen loopt, als internationaal verkeer, zoals TSO-TSO communicatie.
- Uitsluiting van TLS1.2 is internationaal nog geen topic, wat verhindert dat TenneT TLS1.2 op het CPS technisch uit kan zetten.
- TenneT zal marktpartijen die actief zijn op de Nederlandse markt wel naar gebruik van TLS1.3 pushen, en hen wijzen op de afspraken die gemaakt zijn onder het Afsprakenstelsel.
- Het is nog niet duidelijk in hoeverre TenneT het gebruik van TLS1.3 op het CPS door marktpartijen hard kan afdwingen, zo lang TLS1.2 formeel nog als veilig wordt beschouwd en het technisch ook aan staat. Dit wordt casus specifiek bekeken.
- De volgende marktrollen (in scope) maken nog gebruik van het CPS:
 - BRP
 - BSP
 - NB

2.2.2 Risico's

- Hoewel op dit moment niet ter sprake, brengt het technisch uitzetten van TLS1.2 significante marktbrede risico's met zich mee, voor met name balanshandhaving (berichtenverkeer met BSP's) en reconciliatie (berichtenverkeer met NB's en BRP's).
- Het feit dat TLS1.2 door het internationale verkeer technisch niet uitgezet kan worden, levert een beperkt security risico op. Als TLS1.2 onverhoopt formeel onveilig wordt verklaard is dat een handvat voor TenneT om ook internationaal de uitsluiting van TLS1.2 snel op te volgen. Het CPS is technisch voorbereid op een snelle uitsluiting van TLS1.2.

2.2.3 Communicatie en follow up

- TenneT zal partijen actief om bevestiging vragen dat ze met het CPS van TLS1.3 gebruik maken, en zo mogelijk na de gestelde deadline (zie paragraaf 1.2) de druk hierop opvoeren.
- Het IISO wordt periodiek gerapporteerd over de status en voortgang van de transitie.
- Gebruikers worden op de volgende momenten geïnformeerd:
 - April – Generieke mailing naar alle marktpartijen
 - Mei – Door BAS georganiseerde markt informatie sessie
 - Juni – Specifieke mailing naar CPS gebruikers
 - Augustus – Final call naar CPS gebruikers waarvan nog geen bevestiging is ontvangen dat ze op TLS1.3 zitten

2.2.4 TLS1.2 uit

- TLS1.2 wordt op het CPS vooralsnog niet technisch uitgezet in verband met de internationale communicatiestromen. Na de deadline zal TenneT partijen aanspreken als blijkt dat zij niet aan de afspraken onder het Afsprakenstelsel voldoen.

2.3 CBP

2.3.1 Context

- Het Crowd Balancing Platform is het BlockChain platform dat TenneT gebruikt voor communicatie met Balance Service Providers (BSP) ten behoeve van Reservevermogen (aFRR).
- Niet beschikbaarheid van het CBP brengt de balanshandhaving in gevaar door gebrek aan Reservevermogen, daardoor is een (nagenoeg) 100% transitie vereist voordat TLS1.2 uitgezet kan worden.
- Als zeker is gesteld dat de consequenties acceptabel zijn, zal TenneT TLS1.2 technisch ontmantelen.
- Balance Service Providers zijn nog niet op de hoogte gebracht van de voorgenomen uitfasering van TLS1.2.

2.3.2 Risico's

- Het technisch uitzetten van TLS1.2 brengt risico's voor balanshandhaving met zich mee, doordat er dan te weinig Reservevermogen beschikbaar kan zijn. Uitzetten wordt dan ook alleen gedaan als die risico's voldoende zijn gemanaged.

2.3.3 Communicatie en follow up

- TenneT zal monitoren of partijen nog van TLS1.2 gebruik maken, en zo nodig partijen actief benaderen om op het CBP naar TLS1.3 over te stappen.
- Het IISO wordt periodiek gerapporteerd over de status en voortgang van de transitie.
- Gebruikers worden (indien van toepassing) op de volgende momenten geïnformeerd:
 - April – Generieke mailing naar alle marktpartijen
 - Mei – Door BAS georganiseerde markt informatie sessie
 - Juni – Specifieke mailing naar CBP gebruikers
 - Augustus – Final call naar CBP gebruikers waarvan nog geen bevestiging is ontvangen dat ze op TLS1.3 zitten
 - Twee weken voor uitzetten TLS1.2: Mailing naar CBP gebruikers dat TLS1.2 uit gaat, en dat TenneT zal handhaven als blijkt dat marktpartijen hier tegen verwachting in niet op zijn voorbereid

2.3.4 TLS1.2 uit

- TLS1.2 wordt technisch uitgezet zodra de 100% uitfasering bereikt is, of na de deadline zoals gesteld in paragraaf 1.2 als het restrisico naar interpretatie van TenneT acceptabel is.

2.4 MMC-hub

2.4.1 Context

- De Market-2-Market Communication HUB is het centrale systeem voor wholesale berichtuitwisseling in de Nederlandse markt, variërend van near realtime balanceringsberichten tot meetberichten. De impact van dit systeem vereist een (nagenoeg) 100% transitie voordat TLS1.2 uitgezet kan worden.
- TenneT kan niet zien welke marktpartijen voor welke berichtstromen van welke TLS versie gebruik maken, TenneT kan alleen zien óf er nog van TLS1.2 gebruik wordt gemaakt.
- De TQF wordt gebruikt als step up om van de MMC-hub gebruik te kunnen maken. Op de TQF omgeving staat een kopie van de MMC-hub, marktpartijen dienen op de TQF omgeving aan te tonen dat zij hun TLS1.3 configuratie op orde hebben.
- De volgende marktrolleen maken gebruik van de MMC-hub:
 - BRP
 - BSP
 - MV
 - NB
- Nota bene, nieuwe partijen zoals de Leveranciers als gevolg van Allocatie 2.0 zullen direct op basis van TLS1.3 worden aangesloten.

2.4.2 Risico's

- Het technisch uitzetten van TLS1.2 brengt significante marktbrede risico's met zich mee. De MMC-hub is de centrale spil voor een groot deel van de wholesale processen. Uitzetten wordt dan ook alleen gedaan als die risico's voldoende zijn gemanaged.

2.4.3 Communicatie en follow up

- TenneT zal de transitie van marktpartijen nauwgezet monitoren en stimuleren. Partijen worden verzocht door een connectietest op de TQF omgeving aan te tonen dat zij TLS1.3 ready zijn.
- Het IISO wordt periodiek gerapporteerd over de status en voortgang van de transitie.
- Gebruikers worden op de volgende momenten geïnformeerd:
 - April – Generieke mailing naar alle marktpartijen
 - Mei – Door BAS georganiseerde markt informatie sessie
 - Begin juni – Specifieke mailing naar MMC-hub gebruikers
 - Medio augustus – Final call naar MMC-hub gebruikers waarvan nog geen bevestiging is verkregen dat ze op TLS1.3 zitten
 - Twee weken voor uitzetten TLS1.2: Mailing naar CBP gebruikers dat TLS1.2 uit gaat, en dat TenneT zal handhaven als blijkt dat marktpartijen hier tegen verwachting in niet op zijn voorbereid

2.4.4 TLS1.2 uit

- TLS1.2 wordt technisch uitgezet zodra de 100% uitfasering bereikt is, of na de deadline zoals gesteld in paragraaf 1.2 als het restrisico naar interpretatie van TenneT acceptabel is.

2.5 MyTenneT

Inclusief APFAS en TQF app

2.5.1 Context

- MyTenneT is de self service portal van TenneT, een beveiligde website die partij specifieke informatie ontsluit aan haar gebruikers. MyTenneT geeft ook toegang tot twee achterliggende portals: het veilingplatform voor balanceringsproducten APFAS en de TQF app die gebruikers een User Interface biedt op de TQF applicatie.
- Gebruikers gaan via een reguliere browser naar MyTenneT, verreweg de meeste browsers zijn TLS1.3 compatible, waarbij de aanbieder partij (TenneT) het te gebruiken securityniveau enkelzijdig kan afdwingen.
- TenneT zal desondanks gebruikers een redelijke termijn moeten bieden om eventuele verouderde, niet TLS1.3 compatible browsers te vervangen.
- De gebruikersgroep van MyTenneT is zeer breed, van partijen met bovengenoemde marktrollen tot partijen aangesloten op het TenneT net, tot Grid Service Providers die diensten leveren aan TenneT.

2.5.2 Risico's

- MyTenneT faciliteert een aantal processen met een medior risico als deze verstoord zouden raken. Hierbij moet gedacht worden aan de veiling van balanceringsproducten, de Nominations app voor BRP's en bijvoorbeeld informatie over de inzakerekening voor BRP's. De kans op verstoring door technisch uitzetten is echter beperkt door de gebruikte technologie. Het risico wordt nog verder beperkt door partijen tijdig op de uitfasering van TLS1.2 te wijzen, en een verhoogde dijkbewaking in te stellen op het moment dat TLS1.2 uit wordt gezet.

2.5.3 Communicatie en follow up

- TenneT zal geen actieve transitie opzetten, en duidelijk communiceren dat TLS1.2 onverkort op de gestelde deadline wordt uitgezet. Het is aan marktpartijen zelf om te controleren of hun browsers compatible zijn met TLS1.3.
- De communicatie over wijzigingen op MyTenneT volgt normaliter twee lijnen: 1. via een mailing aan de MyTenneT contactpersonen, 2. via een service mededeling op MyTenneT zelf.
- De communicatie vindt op de volgende momenten plaats:
 - April – Separate mailing naar MyTenneT contactpersonen
 - Mei – Door BAS georganiseerde markt informatie sessie
 - Medio mei – Herhaalde mailing naar MyTenneT contactpersonen
 - Medio mei – Service mededeling op MyTenneT

2.5.4 TLS1.2 uitzetten

- TLS1.2 wordt op de gestelde deadline (zie paragraaf 1.2) hard uit gezet. Wel overweegt TenneT bij escalatie een rollback, waarna partijen 2 weken de tijd krijgen om hun zaken op orde te brengen. Het IISO zal over die eventuele rollback worden geïnformeerd.

2.6 OSB web services

2.6.1 Context

- De Oracle Service Bus ontsluit synchrone web services voor Noodvermogen (mFRR) richting Balance Service Providers.
- Niet beschikbaarheid van de OSB web services brengt de balanshandhaving in gevaar door gebrek aan Noodvermogen, daardoor is een (nagenoeg) 100% transitie vereist voordat TLS1.2 uitgezet kan worden.
- Als zeker is gesteld dat de consequenties acceptabel zijn, zal TenneT TLS1.2 technisch uitzetten.
- Nog niet alle Balance Service Providers zijn op de hoogte gebracht van de voorgenomen uitfasering van TLS1.2.

2.6.2 Risico's

- Het technisch uitzetten van TLS 1.2 brengt risico's voor balanshandhaving met zich mee, doordat er te weinig Noodvermogen beschikbaar is. Uitzetten wordt alleen gedaan als die risico's voldoende zijn gemanaged.
- Het risico bij uitzetten van TLS1.2 wordt sterk verkleind doordat er gebruik wordt gemaakt van IsAlive services. Hierdoor kan TenneT direct zien of alle relevante BSP's nog beschikbaar zijn, en zo nodig besluiten tot een rollback als dit naar beoordeling van TenneT een onacceptabel grote impact heeft.

2.6.3 Communicatie en follow up

- TenneT zal partijen actief om bevestiging vragen dat ze met mFRR van TLS1.3 gebruik maken.
- Het IISO wordt periodiek gerapporteerd over de status en voortgang van de transitie.
- Gebruikers worden op de volgende momenten geïnformeerd:
 - April – Generieke mailing naar alle marktpartijen
 - Mei – Door BAS georganiseerde markt informatie sessie
 - Juni – Specifieke mailing naar mFRR partijen
 - Augustus – Final call naar mFRR partijen waarvan nog geen bevestiging is ontvangen dat ze op TLS1.3 zitten
 - Twee weken voor uitzetten TLS1.2: Mailing naar mFRR partijen dat TLS1.2 uit gaat, en dat TenneT zal handhaven als blijkt dat marktpartijen hier tegen verwachting in niet op zijn voorbereid

2.6.4 TLS1.2 uitzetten

- TLS1.2 wordt technisch uitgezet zodra de 100% uitfasering bereikt is, of na de deadline zoals gesteld in paragraaf 1.2 als het restrisico naar interpretatie van TenneT acceptabel is. Hierbij wordt actief gebruik gemaakt van de IsAlive service met iedere BSP.

2.7 TQF

2.7.1 Context

- De Test- and Qualification Facility biedt marktpartijen een vrije testomgeving, om voor te bereiden op deelname aan het berichtenverkeer via de MMC-hub. Voorwaarde voor deelname aan het berichtenverkeer is dat een partij zich kwalificeert (certificeert), conform NetCode artikel 13.33.
- Op de TQF omgeving staat een kopie van de MMC-hub, partijen communiceren met de TQF backend via die MMC-hub kopie. Uitfasering van TLS1.2 vindt dan ook logischerwijs eerst plaats op de TQF omgeving en daarna op de MMC-hub in Productie.
- De volgende markttrollen maken gebruik van de MMC-hub:
 - BRP
 - BSP
 - MV
 - NB
- Nota bene, nieuwe partijen zoals de Leveranciers als gevolg van Allocatie 2.0 zullen direct op basis van TLS1.3 worden aangesloten.

2.7.2 Risico's

- Het risico van technisch uitzetten van TLS1.2 op de TQF omgeving is zeer beperkt; marktpartijen kunnen niet meer testen en kwalificeren.

2.7.3 Communicatie en follow up

- De transitie van marktpartijen op de TQF maakt onderdeel uit van de MMC-hub transitie, waarbij partijen eerst op de TQF aan moeten tonen dat ze TLS1.3 ready zijn. De communicatie en rapportage loopt ook mee met de MMC-hub transitie.

2.7.4 TLS1.2 uitzetten

- TLS1.2 wordt op de gestelde deadline (zie paragraaf 1.2) hard uit gezet. Met de deadline is rekening gehouden met de lopende testen door marktpartijen, voor onder andere Nominations en Imbalance Settlement.

3. Hoe om te gaan met laggard partijen

Voor een significant deel van de marktrollen is TenneT de erkennende partij, wat inhoudt dat TenneT die erkenning in ultimo ook in kan trekken. Een dergelijke intrekking betekent echter dat het bewuste bedrijf haar business niet meer kan uitvoeren en waarschijnlijk failliet gaat. TenneT zal de erkenning dan ook niet zomaar intrekken, maar pas nadat de partij herhaaldelijk is gewezen op de gronden waarop de erkenning verleend is. In dit geval; het voldoen aan de afspraken die gemaakt zijn onder het Afsprakenstelsel.

Marktpartijen die na de gestelde deadline categorisch weigeren om aan de afspraken onder het Afsprakenstelsel te conformeren (in dit geval; de overstap naar TLS1.3) zullen door TenneT daarop worden aangesproken. Dit zal een juridisch dossier vormen, waarmee TenneT casus specifiek door gaat pakken. TenneT gaat er van uit dat deze situatie in de praktijk niet zo ver zal komen.

4. Als TLS1.2 onveilig wordt verklaard

Dit plan gaat uit van de situatie dat TLS1.2 en de onderliggende cipher suites door de officiële instanties als veilig wordt beschouwd. Als dit onverhoopt verandert, betekent dit dat de deadlines voor uitfasen van TLS1.2 opnieuw bekeken zullen worden – en afhankelijk van het dreigingsniveau sterk worden verkort. Ook wordt de risk appetite voor het verstoren van de markt als gevolg van het uitzetten van TLS1.2 dan groter. De systemen van TenneT zijn op een dergelijke situatie voorbereid, en kunnen op korte termijn technisch TLS1.2 uit zetten.

Als de veiligheid van TLS1.2 in het geding is zal TenneT pro actief optreden en de afstemming met MFFBAS op een lagere prioriteit stellen.

Bijlage A: Overzicht markttrollen per IT systeem

	Balance Responsible Party	Balance Service Provider	Aangeslotene	Congestion Service Provider	Regionaal Netbeheerder	Faciliterend Netbeheerder/ Gesloten Distributie Systeem	Meetverantwoordelijke	Overige gebruikers
API Gateway	X	X		X	X	X	X	
Centraal Postbus Systeem (CPS)	X	X			X	X		X ¹
Crowd Balancing Platform (CBP)		X						
Market-2-Market Communication HUB (MMC-hub)	X	X			X	X	X	
MyTenneT, inclusief APFAS en TQF app	X	X	X	X	X	X	X	X ²
Oracle Service Bus (OSB)		X						
Test- and Qualification Facility (TQF)	X	X			X	X	X	

¹ Er loopt internationaal verkeer over het CPS, zoals communicatie tussen TSO's onderling.

² Grid Service Providers die diensten leveren aan TenneT hebben toegang tot MyTenneT