EDSN
energiedata voor iedereen

UITFASERINGSPLAN TLS 1.2

OVERSTAP NAAR TLS 1.3 ONLY

12-02-2024
Auteurs R. Tjoelker & R. Dekker

Samenvatting

In dit plan worden de stappen beschreven die nodig zijn om **TLS 1.2 uit te faseren op 17-06-2024** voor de systemen in scope bij EDSN. Hiermee wordt de duale fase, waarin zowel communicatieprotocollen TLS 1.3 als TLS 1.2 toegestaan zijn in het berichtenverkeer, beëindigd. Vanaf dat moment is alleen TLS 1.3 berichtenverkeer toegestaan voor onderstaande systemen: dit heeft mogelijk impact op de gebruikers/ marktpartijen die van die systemen gebruik maken. Om die impact te minimaliseren wordt in dit plan aandacht besteed aan de uitfasering bij EDSN zelf, de communicatie in dit traject en de geïdentificeerde risico's.

Systemen	Gebruikers	Ontsluiting via
KONG gateway, Toestemmingsplatform, Energiedatalink Provider, CERES	RNB, MMC-Hub, LV, MV, BRP	Entry Gateway
C-AR[1]	NB, LV, MV, BRP	Direct, portaal.edsn.nl
C-ARM	RNB en GDS	Direct
CSS	MV, BRP en NB	Direct, css3.edsn.nl/css
Data delen platform	RNB, LV, MV, BRP	Entry Gateway
EAN-codeboek	Iedereen	Entry Gateway
GOPACS	CSP, BSP, NB	Entry Gateway
Nexus	RNB, LNB-G, BRP en LV	Direct
Portaal CTS	ODA, LV, RNB	Entry Gateway, p4.edsn.nl
TMR	LV, RNB	Direct

Tabel 2.0: Systemen, gebruikers en ontsluiting

Uitfasering

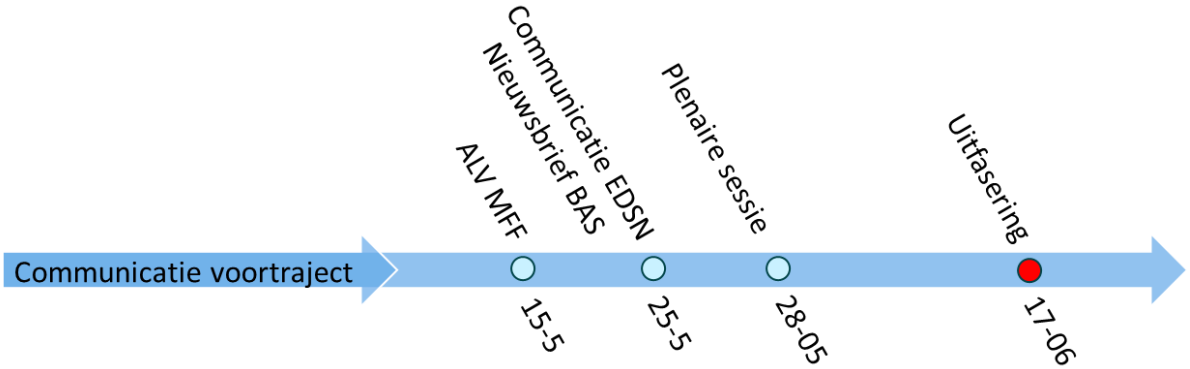
Data uitwisseling met EDSN vindt zowel plaats via de zogenaamde 'Entry Gateway', via directe verbindingen als hybride constructies. Voor alle systemen in scope wordt op 17-06-2024 changes doorgevoerd waarin TL 1.2 uitgezet wordt en enkel berichtenverkeer middels TLS 1.3 mogelijk is.

Gebruikers mogen zelf kiezen wanneer ze overgaan op enkel TLS 1.3: tot de uitfasering kunnen gebruikers nog met zowel TLS 1.2 als TLS 1.3 met de systemen communiceren.
Wanneer de partijen tijdig over zijn op TLS 1.3, wordt er geen impact verwacht. Het risico dat een partij onverhoopt TLS 1.3 toch niet ondersteunt om welke reden dan ook, is geadresseerd.

Communicatie

Om de verschillende gebruikers en marktpartijen te bereiken en de kans op impact te minimaliseren worden verschillende momenten en kanalen aangewend om de doelgroep te informeren over de uitfasering van TLS 1.2. In het schema hierop volgend wordt kort toegelicht wanneer de communicatie plaats vindt. De communicatiemiddelen en -momenten zijn bedoeld om zowel de ALV MFF-leden als de specifieke gebruikers van de systemen te bereiken.

[1] incl. sector register, CER, PUD, MDD, MPR, LV/RNB Register, TR, ADC, BU, GBU



Schema 3: Communicatie momenten uitfaseringsplannen EDSN

Risicobeheersing

De uitfasering van TLS 1.2 brengt risico's met zich mee voor de eindgebruikers van de EDSN-systemen. Deze risico's treden voornamelijk op wanneer de eindgebruikers nog niet klaar zijn om over te gaan op enkel TLS 1.3. Het mitigeren van die risico's is gericht op enerzijds het vinden van een oplossing voor de (technische)uitdagingen waar de eindgebruikers voor staan. Anderzijds, is het informeren van de eindgebruikers over de uitfaseringsplannen via verschillende kanalen een belangrijk middel om de impact van de risico's tijdens en na de uitfasering te minimaliseren. Uiteindelijk kan altijd nog gekozen worden voor een Rollback, in geval van kritieke impact, om grote verstoringen gelinkt aan de uitfasering op te lossen.

Inhoudsopgave

Uitfaseringsplan EDSN

0.1 Versiegeschiedenis

Versie	datum	wie	Afgestemd met	Markering/Wijzigingen
0.1	Maart 2024	Rukundo Tjoelker	Productowners EDSN	Concept
0.3	3 -4-2024	Rukundo Tjoelker	Werkgroep TLS 1.3	Interne review en externe review ontvangen en verwerkt
0.6	8-4-2024	Rukundo Tjoelker	Erik van Dongen, Ruud Dekker	Interne reviews ontvangen en verwerkt
0.7	11-4-2024	Rukundo Tjoelker	Bram van Straalen, Frans Willem Strabucchi, Ruud Dekker, Theo Lantink, Thijs Nijland, Michiel Hermans	Interne reviews ontvangen en verwerkt
0.8	11-4-2024	Rukundo Tjoelker	Amanda Zachariasse	Externe review ontvangen en verwerkt
0.9	12-4-2024	Rukundo Tjoelker	IISO	Ter vaststelling
0.91	22-4-2024	Rukundo Tjoelker	IISO	
0.92	26-4-2024	Rukundo Tjoelker	Portfolio Stuurgroep	
0.93	3-5-2024	Rukundo Tjoelker	Portfolio stuurgroep	
0.95	15-5-2024	Rukundo Tjoelker	ALV MFF	
1.0	15-5-2024	Rukundo Tjoelker	ALV MFF	

1 Inleiding

1.1 Aanleiding

Tijdens de MFF Algemene Leden Vergadering (ALV) van 8 maart 2023 is het 'Invoering TLS 1.3 - Uitvoerings- & Communicatieplan' vastgesteld. Momenteel is er een duale fase waarbij zowel TLS 1.2 als TLS 1.3 worden ondersteund. Deze duale fase eindigt na besluit van het ALV MFF op 15 mei en daarna wordt alleen 1.3 ondersteund. Dit plan zet de uitfasering van TLS 1.2 zorgvuldig uiteen voor de verschillende systemen[2] in scope bij Energie Data Services Nederland (EDSN).

De beoogde uitfaseringsdatum voor EDSN waarbij de systemen over gaan naar enkel TLS 1.3 is 17-06-2024.

Deze datum is gekozen om voldoende ruimte te hebben om alle betrokken partijen te bereiken. Ook is op deze datum voldoende capaciteit beschikbaar voor uitfasering en eventuele nazorg hierop.

De uitfasering van TLS 1.2 zal ertoe leiden dat het berichtenverkeer voor de EDSN-systemen in scope middels TLS 1.3 verloopt. Hiermee wordt de betrouwbaarheid en integriteit van de communicatie in data uitwisseling tussen marktpartijen en EDSN verhoogt. TLS 1.3 is namelijk sneller, veiliger, simpeler en meer flexibel op de juiste plekken om in te kunnen spelen op de toekomst. TLS 1.3 bevat tevens minder kwetsbare configuratieopties als TLS 1.2 en kan op een veiligere manier geconfigureerd worden. Hiermee wordt de kans op compromittering van de marktcommunicatie kleiner en de veiligheid van de gegevensuitwisseling groter.

Overstappen naar TLS 1.3 als enig encryptieprotocol betekent dat EDSN de voorganger, TLS 1.2, uit faseert. Voor de eindgebruikers van de betreffende systemen kan het uitzetten van TLS 1.2 verregaande consequenties hebben, indien zij op dat moment nog niet zijn overgestapt naar TLS 1.3. Om deze reden is het van belang dat de uitfasering van TLS 1.2 op een gedegen, gestructureerde en gefaseerde manier gebeurt, waarbij gerelateerde risico's voldoende gemitigeerd worden en alle betrokkenen een feilloze uitfasering ondervinden. Het uitgangspunt is uiteindelijk om alle betrokken zo goed mogelijk te begeleiden in het TLS 1.2 uitfaseringstraject.

Om inzicht te krijgen op welke partijen de TLS 1.2 uitfasering impact heeft, worden in dit document de systemen die in scope zijn geïdentificeerd samen met de daaraan gekoppelde gebruikers.

[2] In dit document spreken wij over systemen vanwege het feit dat de marktpartijen met deze systemen gegevens uitwisselen. De uitfasering is primair per gegevensstromen.

1.2 Opbouw Document

Het uitfaseringsplan zet per systeem in beheer bij EDSN uiteen in hoofdstuk 2 welke stappen genomen dienen te worden om TLS 1.2 uit te faseren. Vervolgens komt in hoofdstuk 3 de communicatie rond de uitfasering aan bod. In hoofdstuk 4 worden de risico's geïdentificeerd en de bijbehorende mitigerende maatregelen beschreven.

1.3 Scope uitfaseringsplan TLS 1.2

De EDSN-systemen en gebruikersgroepen waar TLS 1.2 voor uitgefaseerd dient te worden zijn in onderstaand tabel weergegeven. In dit uitfaseringsplan wordt de transitie van deze systemen nader uitgewerkt. Vanaf 17-06 wordt TLS 1.2 bij EDSN niet meer ondersteund en moet de transitie naar TLS 1.3 zijn afgerond.

Applicatie	Gebruikers
KONG gateway, Toestemmingsplatform, Energiedatalink Provider, CERES	RNB, MMC-Hub, LV, MV, BRP
C-AR[3]	NB, LV, MV, BRP, GDS
C-ARM	RNB
CSS	MV, BRP, RNB en GDS
Data delen platform	RNB, LV, MV, BRP
EAN-codeboek	Iedereen
GOPACS	CSP, BSP, NB
Nexus	RNB, LNB-G, BRP en LV
Portaal CTS	ODA, LV, RNB
TMR	LV, RNB

Tabel 1.2: EDSN Systemen en gebruikers in scope voor uitfasering TLS 1.2.

Buiten scope van dit document zijn de uitfaseringsplannen van de betrokken marktpartijen. Bij EDSN is namelijk niet bekend hoe de TLS configuratie bij de marktpartijen is gerealiseerd. De marktpartijen kunnen ook onafhankelijk van EDSN besluiten TLS 1.2 uit te faseren en over te stappen op enkel TLS 1.3. EDSN faciliteert zowel TLS 1.2 als 1.3 tot het uitfaseringsmoment. Indien gewenst en op aanvraag kan een marktpartij EDSN om technische en functionele ondersteuning vragen bij de overstap naar TLS 1.3.

1.4 Doelgroep en doel

Alle partijen en de consument hebben baat bij een veiligere en toekomstbestendige communicatie. Dit document is geschreven door EDSN voor de leden van de ALV MFF en alle marktpartijen waar de uitfasering van TLS 1.2 impact op heeft.

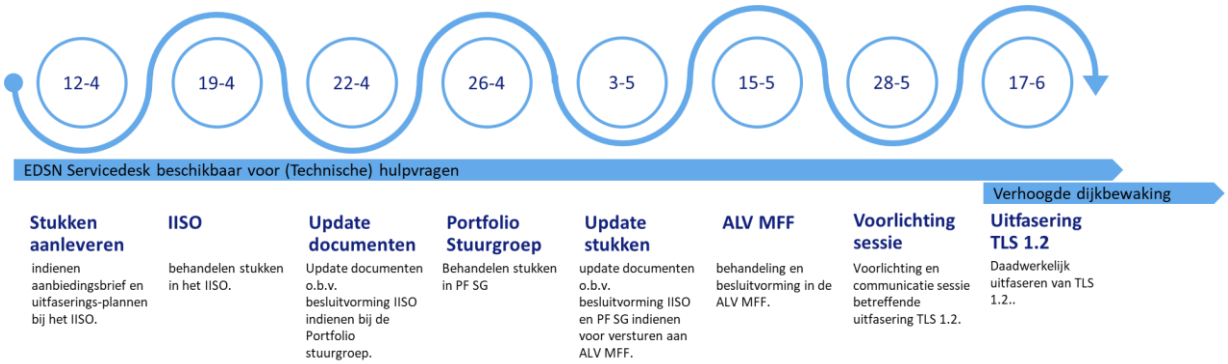
[3] incl. sector register, CER, PUD, MDD, MPR, LV/RNB Register, TR, ADC, BU, GBU

Dit document heeft tot doel de stappen te beschrijven voor het uitfaseren van TLS 1.2 voor de systemen bij EDSN. Het richt zich ook op het minimaliseren van de impact van deze uitfasering door middel van communicatie en risicovermindering, met als uiteindelijk doel de zorgen bij de marktpartijen weg te nemen.

1.5 Tijdslijnen

Om de doelgroep de kans te geven zich te verdiepen in de uitfaseringsplannen van TLS 1.2 zijn de hierop volgende tijdslijnen uitgestippeld.
In de ALV MFF van 20 maart 2024 is vastgesteld dat de uitfasering van de diverse systemen doorgang kan vinden, mits de uitfaseringsplannen worden goedgekeurd. In het schema hieronder is de tijdslijn van het uitfaseringsplan weergeven met daarin een aantal momenten waarop de plannen bijgewerkt kunnen worden. De tijdslijn is erop gericht alle betrokkenen mee te nemen in de uitfaseringsplannen.

De verhoogde dijkbewaking waarvan sprake is in onderstaande tijdslijn zal plaatsvinden vanaf het moment dat de uitfasering is doorgevoerd op 17-06-2024 tot het moment dat het aantal vragen vermindert. Ook na de verhoogde dijkbewaking is EDSN uiteraard bereikbaar voor vragen omtrent de uitfasering.



Schema 1.4: Tijdslijn uitfaseringsplan

1.6 Overgangscriteria

Wanneer het ALV MFF definitief instemt met het uitfaseringsplan van TLS 1.2 van EDSN, dan wordt de duale fase beëindigd per 17-06-2024. Wanneer TLS 1.2 uitgefaseerd is, is communicatie enkel nog mogelijk middels het TLS 1.3 protocol voor de betreffende systemen bij EDSN.
De initiële acceptatiecriteria waarop TLS 1.2 uitgefaseerd zou worden zijn reeds behaald. Dit besluit is genomen in de ALV MFF van maart 2024.

1.7 Risico’s en verhoogde dijkbewaking

Het uitfaseren van TLS 1.2 brengt risico’s met zich mee. De risico’s en bijbehorende mitigaties worden behandeld in hoofdstuk 4 en zijn er op gericht de risico’s te mitigeren voor de verschillende betrokken partijen. EDSN is en blijft beschikbaar voor (technische)vragen omtrent de uitfasering van TLS 1.2.

In het geval de uitfasering van TLS 1.2 een kritieke impact heeft op de betrokken partijen, kan geopteerd worden om de uitfasering terug te draaien en te kiezen voor een rollback. Deze optie wordt in hoofdstuk 4 verder uiteengezet.

2 Uitfaseringsstappen

De uitfaseringsdatum voor TLS 1.2 voor de door EDSN beheerde systemen is **17-06-2024.**
In de uitfaseringsstappen wordt niet specifiek ingegaan op de stappen die de marktpartijen zelf moeten nemen. Iedere marktpartij heeft een andere technische inrichting en is vrij zelf te besluiten TLS 1.2 uit te faseren tot aan 17-06-2024 aangezien EDSN tot dat moment zowel TLS 1.2 als 1.3 protocollen accepteert.

Het uitzetten van TLS 1.2 is relatief eenvoudig voor EDSN. EDSN zit reeds in een duale fase waarin zowel TLS 1.2 als TLS 1.3 worden geaccepteerd als communicatieprotocollen. Op 17-06-2024 worden de nodige changes uitgevoerd waardoor enkel TLS 1.3 nog wordt toegestaan in het berichtenverkeer voor de systemen.

Voor een groot deel van de systemen bij EDSN vindt de data uitwisseling plaats via de zogenaamde 'Entry Gateway'. Met andere woorden: de Entry Gateway is de toegangspoort die voor die specifieke systemen het TLS protocol afdwingt. Voor het andere deel gebeurt de data uitwisseling op een eigen, directe manier. Hieronder is per systeem aangegeven hoe het berichtenverkeer wordt ontsloten en waar de change wordt doorgevoerd.

Wanneer de partijen tijdig over zijn op TLS 1.3, wordt er geen impact verwacht. Het risico dat een partij onverhoopt TLS 1.3 toch niet ondersteunt om welke reden dan ook, wordt geadresseerd in de risico's.

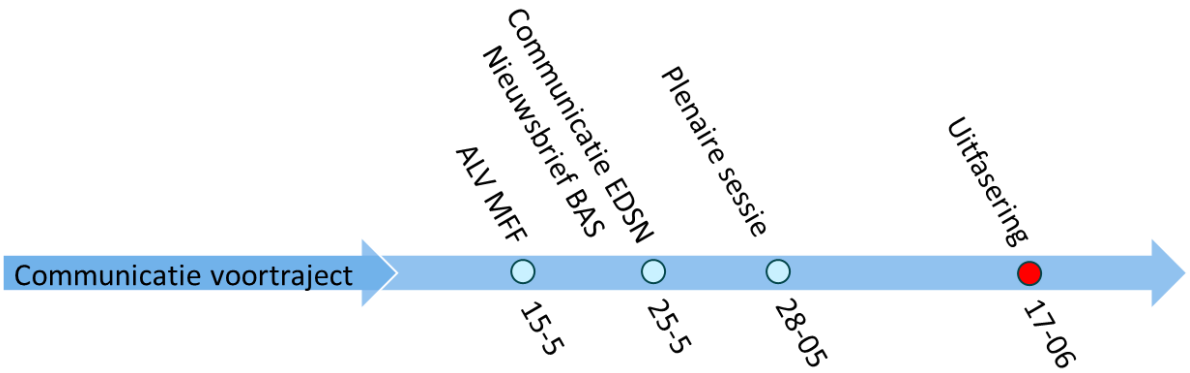
Systemen	Gebruikers	Ontsluiting via
KONG gateway, Toestemmingsplatform, Energiedatalink Provider, CERES	RNB, MMC-Hub, LV, MV, BRP	Entry Gateway
C-AR[4]	NB, LV, MV, BRP, GDS	Direct, portaal.edsn.nl
C-ARM	RNB	Direct
CSS	MV, BRP, RNB en GDS	Direct, css3.edsn.nl/css
Data delen platform	RNB, LV, MV, BRP	Entry Gateway
EAN-codeboek	Iedereen	Entry Gateway
GOPACS	CSP, BSP, NB	Entry Gateway
Nexus	RNB, LNB-G, BRP en LV	Direct
Portaal CTS	ODA, LV, RNB	Entry Gateway, p4.edsn.nl
TMR	LV, RNB	Direct

Tabel 2.0: Systemen, gebruikers en ontsluiting

[4] incl. sector register, CER, PUD, MDD, MPR, LV/RNB Register, TR, ADC, BU, GBU

3 Communicatie

In dit hoofdstuk worden de verschillende communicatiekanalen en -momenten beschreven. Per systeem zijn er ook eigen kanalen waardoor het relevant is om deze separaat te benoemen. Op deze manier worden de betrokken eindgebruikers geïnformeerd via de reguliere weg.
Gedurende het uitfaseringstraject wordt gerapporteerd aan de IISO over de voortgang van de uitfasering.
Onderstaand schema geeft per gegevensstroom weer wanneer en hoe er gecommuniceerd wordt. In de tabel eronder wordt ingezoomd op de communicatiewijze.



Schema 3: Communicatie momenten uitfaseringsplannen EDSN

Communicatie Wijze	Beschrijving
Communicatie in voortraject	Het TLS 1.2 uitfaseringstraject loopt al een geruime tijd. Hierover heeft de volgende communicatie plaatsgevonden: 1. Persoonlijke telefoongesprekken met projectteam om te checken of de partijen TLS 1.3 ready zijn en of er gerelateerde issues zijn; 2. Communicatie in aanloop naar de MFF ALV's; 3. MFF-nieuwsbrieven met de aankondigingen en details betreffende de uitfasering van TLS 1.2; 4. Het delen van de Quick Reference kaart via de MFF-site om partijen in staat te stellen zich voor te bereiden op de uitfasering van TLS 1.2; 5. Vooraankondigingen systeem specifiek over de uitfasering van TLS 1.2.
Communicatie ALV MFF 15-5	In de ALV MFF van 15 mei wordt besloten of de uitfaseringsplannen van EDSN en TenneT toereikend zijn voor de MFF-leden. Wanneer dit het geval is, kunnen de plannen doorgang vinden en kan de uitfasering plaatsvinden.
Nieuwsbrieven MFF	In aanloop naar de definitieve uitfasering van TSL 1.2 wordt deze nogmaals benoemd met daarin vermeld: 6. De plenaire sessie op 28-5 (Zie ook regel plenaire sessie); 7. De beoogde uitfaseringsdatum van 17-06-2024; 8. Een link naar de documentatie;

	9. Het verzoek contact op te nemen met de EDSN Servicedesk bij vragen.
Communicatie EDSN	Voor de verschillende systemen zijn verschillende gebruikers die op reguliere wijze worden geïnformeerd over aanpassingen en verbeteringen in het systeem. Via ditzelfde kanaal wordt er gecommuniceerd over de op hand zijnde uitfasering van TLS 1.2. Hierin zijn wederom de volgende zaken terug te vinden: 10. De plenaire sessie op 28-5 (Zie ook regel plenaire sessie); 11. De beoogde uitfaseringsdatum van 17-06-2024; 12. Een link naar de documentatie; 13. Het verzoek contact op te nemen met de EDSN Servicedesk bij (hulp)vragen.
Plenaire sessie	In een plenaire informatie sessie voor alle betrokken partijen worden de uitfaseringsplannen gedeeld en toegelicht. Ook wordt de volgende informatie nogmaals met de deelnemers gedeeld: 14. De beoogde uitfaseringsdatum van 17-06-2024; 15. Een link naar de documentatie; 16. Het verzoek contact op te nemen met de EDSN Servicedesk bij (hulp)vragen.
Vragen aan EDSN Servicedesk	Gedurende het hele uitfaseringstraject is de Servicedesk bereikbaar voor vragen. De vragen zullen in samenwerking met de achterliggende teams zelf worden beantwoord. Indien gewenst, worden er individuele sessies gepland om technische assistentie te verlenen. Voor en na de uitfasering van TLS 1.2 wordt een verhoogd aantal meldingen verwacht. In deze fases zal verhoogde dijkbewaking actief zijn tot het moment dat het aantal meldingen afneemt. Zo worden vragen en onzekerheden snel bij de betrokken partijen weggenomen.
Individuele sessies	In het geval een partij nog vragen heeft na alle bovengenoemde communicatie, is het altijd mogelijk om een hulpvraag bij de EDSN Servicedesk te plaatsen. Die vraag wordt hetzij direct beantwoord, hetzij in een persoonlijke sessie behandeld met een technisch team.
Release Notes	Rond een release is het gebruikelijk over de aanpassingen in het systeem te communiceren. Per systeem gebeurt dit via de eigen reguliere kanalen.

4 Risico's en mitigaties

De uitfasering van TLS 1.2 brengt risico's met zich mee voor de eindgebruikers van de EDSN-systemen. Deze risico's treden voornamelijk op wanneer de eindgebruikers nog niet klaar zijn om over te gaan op enkel TLS 1.3, wat de reden hiervoor ook is. In onderstaande tabel is een overzicht van de geïdentificeerde risico's weergegeven. Deze worden stuk voor stuk toegelicht en gemitigeerd in de onderliggende paragrafen. De risico's betreffende het uitfaseringsplan van TenneT komen hier niet aan bod. Als laatste mitigerende actie kan gekozen worden voor een zogenaamde rollback; deze wordt aan het einde van dit hoofdstuk besproken.

#	Risico
1	**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, of dat de keuze wordt gemaakt hierop te wachten.**
2	**Het uitfaseringsplan TLS 1.2 van EDSN is niet tijdig gereed en afgestemd om het besluitvormingsproces te volgen. Hierdoor wordt de deadline van 15 mei niet gehaald en kan TLS 1.2 nog niet worden uitgefaseerd.**
3	**Het uitfaseringsplan TLS 1.2 van EDSN wordt niet goedgekeurd door de ALV MFF. Hierdoor kan de uitfasering van TLS 1.2 geen doorgang vinden en wordt het beveiligingsrisico vergroot.**
4	**Marktpartijen worden niet bereikt met informatie over de uitfasering van TLS 1.2, waardoor zij voor een verrassing komen te staan.**
5	**Indien TLS 1.2 vanwege nieuwe gebreken door NCSC afgeschaald wordt naar 'onvoldoende', moet de overgang naar TLS 1.3 worden versneld.**
6	**Bij het uitfaseren van TLS 1.2 komen marktpartijen er toch achter dat het berichtenverkeer wordt verstoord.**
7	**Marktpartijen zijn nog niet over op TLS 1.3**
8	**Het uitfaseren van TLS 1.2 raakt (wellicht) ook gegevensstromen die niet onder het mandaat van het MFFBAS ALV besluit vallen en raakt daarmee, onterecht, marktpartijen**

- ### Risico 1: Softwareleveranciers bieden onvoldoende ondersteuning

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, of dat de keuze wordt gemaakt hierop te wachten.

Dit risico treedt op wanneer softwareleveranciers in de communicatieketen TLS 1.3 nog niet of onvoldoende ondersteunen waardoor er nog niet overgegaan kan worden naar TLS 1.3.
Om dit risico te mitigeren is het volgende mogelijk:

17. Er wordt naar een andere manier gezocht om het mankement in de niet ondersteunende software te omzeilen met een zogenaamde work-arround. Een stukje extra software of alternatieve software wordt ingezet om TLS 1.3 alsnog mogelijk te maken. EDSN heeft technische specialisten die hierin mee kunnen denken indien dit gewenst is.
18. De uitfasering van TLS 1.2 op de specifieke softwarecomponent dat TLS 1.3 niet ondersteunt, wordt uitgesteld of nog niet afgedwongen totdat TLS 1.3 wel wordt ondersteund. Wanneer EDSN op de hoogte is van dit soort situaties, kan dit, in overleg, in overweging worden genomen mits er op korte termijn zicht is op een oplossing vanuit de softwareleverancier.

- **Risico 2: Uitfaseringsplan TLS 1.2 EDSN is niet tijdig gereed en afgestemd**

Uitfaseringsplan EDSN - niet tijdig gereed en afgestemd om het besluitvormingsproces te volgen. Hierdoor wordt de deadline van 15 mei niet gehaald en kan TLS 1.2 nog niet worden uitgefaseerd.

Dit risico wordt gemitigeerd door EDSN door hier gepaste prioriteit aan te geven en voldoende resources voor beschikbaar te stellen.

- **Risico 3: Uitfaseringsplan EDSN wordt niet goedgekeurd door ALV-MFF**

Het uitfaseringsplan TLS 1.2 van EDSN wordt niet goedgekeurd door de ALV MFF. Hierdoor kan de uitfasering van TLS 1.2 geen doorgang vinden en wordt het beveiligingsrisico vergroot.

Dit is een risico die kan optreden wanneer de betrokken partijen onvoldoende vertrouwen hebben in het uitfaseringsplan. Om dit risico te mitigeren worden de betrokken partijen veelvuldig meegenomen in de communicatie en is het mogelijk voor de betrokken partijen om technische hulp te krijgen van EDSN. Het beveiligingsrisico blijft hetzelfde tot het moment er nieuwe kwetsbaarheden worden ontdekt in TLS 1.2. De communicatie momenten en mogelijkheden zijn:

19. Ieder moment voor en na de uitfasering van TLS 1.2, waarin de betrokken partijen contact kunnen opnemen met EDSN via de Servicedesk. Zo kunnen eventuele vragen op voorhand worden beantwoord;
20. In de ALV van MFF kunnen de betrokken partijen hun zorgen uiten en vragen stellen betreffende de uitfasering;
21. Een voorlichtingssessie waarin het uitfaseringsplan met details nogmaals wordt uiteengezet;
22. Systeem specifieke communicatie (indien mogelijk): toegespitst op de eindgebruikers conform de routes die normaliter ook gebruikt worden om veranderingen in het systeem aan te kondigen.

- **Risico 4: Marktpartijen worden niet bereikt en staan voor een verrassing**

Marktpartijen worden niet bereikt met informatie over de uitfasering van TLS 1.2, waardoor zij voor een verrassing komen te staan.

Dit risico treedt op wanneer een marktpartij, op wat voor een reden dan ook, de informatie betreft de uitfasering van TLS 1.2 niet heeft ontvangen.
De risico mitigatie is tweeledig:

1. Mitigatie vindt gedurende het gehele uitfaseringstraject plaats door meerdere keren te communiceren via verschillende kanalen voor en na de uitfasering zelf. De communicatie momenten en kanalen zijn:
    - MFFBAS heeft alle leden telefonisch getracht te bereiken om hen te verwittigen van de uitfasering van TLS 1.2.
    - MFFBAS verwittigd in de nieuwsbrief van de ALV MFF van 15-5 de leden over de uitfasering van TLS 1.2 op 17-06 voor EDSN-systemen;
    - In de ALV van MFF zijn de marktpartijen op de hoogte gesteld van de uitfaseringsplannen van TLS 1.2;
    - Systeem specifieke communicatie (indien mogelijk): toegespitst op eindgebruikers van een specifiek systeem conform de routes die normaliter ook gebruikt worden om veranderingen in het systeem aan te kondigen.

- Tijdens de verhoogde dijkbewaking periode is er ruimte voor nazorg en stelt EDSN-capaciteit ter beschikking om te helpen met issues.

2. Op de acceptatieomgevingen kan een marktpartij tot de feitelijke uitfasering blijven testen of zijn systemen volledig TLS 1.3 ready zijn. Hiermee zien partijen die niet bereikt zijn met de informatie dat er wel iets is veranderd in het acceptatie systeem, waarop ze actie ondernemen om te achterhalen wat er speelt.

- **Risico 5: TLS 1.2. wordt onveilig beschouwd wordt door het NCSC**

Indien TLS 1.2 vanwege nieuwe gebreken door het NCSC afgeschaald wordt naar 'onvoldoende', moet de overgang naar TLS 1.3 worden versneld.

Dit risico treedt op wanneer het NCSC (Nederlands Cyber Security Centrum) het TLS 1.2. protocol als onveilig gaat beschouwen. Dit kan gebeuren wanneer er nieuwe kwetsbaarheden of gebreken in TLS 1.2. worden ontdekt en de gebruikte encryptie sleutels onvoldoende veilig worden geacht.

De mitigatie van dit risico is het versneld uitvoeren van de uitfaseringsplannen van TLS 1.2. Hierbij gaat EDSN uit dat partijen nog niet over zijn op TLS 1.3. EDSN stelt extra capaciteit beschikbaar om hierbij te ondersteunen. De kans dat dit risico zich voordoet wordt niet heel hoog geacht.

- **Risico 6: Berichtenverkeer toch verstoord bij uitfasering TLS 1.2**

Bij het uitfaseren van TLS 1.2 komen marktpartijen er toch achter dat het berichtenverkeer wordt verstoord.

Voor de partijen die gebruik maken van de in scope zijnde systemen is het cruciaal dat ze op de datum van uitfasering TLS 1.3 ondersteunen. Zo wordt voorkomen dat het berichtenverkeer wordt verstoord. Op het moment dat de uitfasering van TLS 1.2. wordt doorgevoerd, kunnen marktpartijen er toch nog achter komen dat er issues zijn met het berichtenverkeer. Wanneer dit niet tijdig wordt opgelost kan dit impact hebben op de betrokken partijen.

De mitigatie van dit risico ligt in het tijdig communiceren en begeleiden van de partijen in de uitfasering van TLS 1.2. middels de genoemde communicatie momenten. Ook stelt EDSN technische capaciteit beschikbaar om issues van dit aard te verhelpen. Mocht het berichtenverkeer dusdanig worden verstoord, dan kan een rollback worden uitgevoerd zoals beschreven op pagina 16.

- **Risico 7: Marktpartijen praten nog niet met TLS 1.3**

Marktpartijen zijn nog niet over op TLS 1.3

Dit risico betreft marktpartijen die nog niet over zijn op TLS 1.3 op het moment van de uitfasering van TLS 1.2. Marktpartijen kunnen buitengesloten worden van het berichtenverkeer met EDSN daar waar de marktpartijen nog niet over is op TLS 1.3.
De mitigaties vanuit EDSN voor dit risico zijn:

1. Tot en na het moment van uitfaseren is het mogelijk contact op te nemen met de Servicedesk van EDSN, zij kunnen vragen beantwoorden en, indien nodig een (technische) sessie inplannen met onze experts op dit vlak.

2. Afhankelijk van het systeem dat nog niet over is op TLS 1.3, kan gekozen worden voor een tijdelijke workarround.
3. In een marktuitvraag aan de MFF-leden is gevraagd of ze TLS 1.3. ready zouden zijn per 31-3 om te toetsen of het acceptatiecriterium behaald was. In de ALV MFF in maart is vastgesteld dat de acceptatiecriteria ruimschoots behaald zijn en de uitfasering doorgang kan vinden, mits de plannen werden goedgekeurd.
4. Voor de daadwerkelijke uitfaseringsdatum worden partijen die nog niet over zijn op TLS 1.3 benaderd indien dit mogelijk is.
5. Wanneer bovenste oplossingen geen uitkomst bieden, kan een rollback (zie hieronder) naar de duale fase voor die systemen waar het speelt, een tijdelijke optie zijn.

- **Risico 8: Uitfasering TLS 1.2 levert nevenschade bij andere gegevensstromen en systemen**

Het uitfaseren van TLS 1.2 raakt (wellicht) ook gegevensstromen die niet onder het mandaat van het MFFBAS ALV besluit vallen en raakt daarmee, onterecht, marktpartijen

Dit risico houdt in dat onbedoeld andere gegevensstromen en systemen, niet vallend onder het mandaat van het ALV MFF, ook overgaan TLS 1.3-only tijdens de uitfasering van TLS 1.2.
De mitigaties vanuit EDSN zijn:

- Voor uitfasering wordt getest op acceptatie om te kijken of e gegevensstromen blijven functioneren.
- De uitfaseringsplannen zijn intern meerdere malen getoetst op risico's en onjuistheden.

- **Rollback plan**

Een rollback plan is een plan om een aanpassing in een systeem teniet te doen en het systeem terug te brengen in een vorige staat. Iedere change of aanpassing in een systeem heeft, als het goed is, een rollback mogelijkheid voor het geval de aanpassing niet het gewenste of geplande effect heeft. In het geval van de uitfasering van TLS 1.2. kunnen risico's 4.4. en 4.6 optreden. Mochten die risico's niet afdoende kunnen worden gemitigeerd, dan kan een rollback de enige overgebleven optie zijn. Of EDSN overgaat op een rollback wordt bepaald aan de hand van de impact van de verstoring.

Na het in gang zetten van het rollbackplan, zal EDSN een voorstel doen voor een nieuwe uitfaseringsdatum. Uiteraard wordt de oorzaak geanalyseerd zodat deze bij een volgende poging niet meer voorkomt.

5 Begrippen en afkortingen lijst

Afkorting	Begrip
ALV MFF	Algemene Leden Vergadering Markt Faciliterings Forum
EDSN	Energie Data Services Nederland
TLS	Transport Layer Security
NCSC	Nederlands Cyber Security Center
RBP/ Rollback plan	Een plan dat gemaakt worden om een systeem terug te zetten naar een vorige situatie waarbij de aanpassingen ongedaan worden gemaakt.
BRP	Balance Responsible Party
LV	Leverancier
NB	Netbeheerder
RNB	Regionale Netbeheerder
LNB	Landelijk Netbeheerder
MV	Meetverantwoordelijke
CSP	Congestion Service Provider (CSP)
BSP	Balance Service Providers
ODA	Overige Diensten Aanbieder

EDSN
energiedata voor iedereen

EDSN
Van Asch van Wijckstraat 55
3811 LP Amersfoort

033 422 4620
info@edsn.nl | edsn.nl