TLP: GROEN

Invoering TLS 1.3

Uitvoerings- en communicatieplan

Datum	12-04-2023
Versie	1.0
Status	Definitief
Opsteller(s)	Werkgroep TLS 1.3

Inhoudsopgave

Colofon

Versiebeheer

Versie	Status	Wijziging/Opmerking	Auteur	Datum
0.1	Concept	Interne versie	Arjan Visser, John van der Stap	12-01-23
0.2 – 0.7	Concept	Interne versies	Werkgroep Invoering TLS 1.3	02-09-23
0.8	Finale concept	Reviewversie voor de CoP Secure Architecture	Werkgroep Invoering TLS 1.3	09-02-23
0.9	Versie ter goedkeuring	Reviews verwerkt – voor aanbieding aan ALV MFF	Werkgroep Invoering TLS 1.3	22-02-23
1.0	Definitief	Goedgekeurd per 8 maart, uitgebreid met aanvullende lijst centrale systemen	Werkgroep Invoering TLS 1.3	12-04-23

Distributie

	Verstuurd (versie/datum)									
Gremium	**0.1**	**0.2**	**0.3**	**0.4**	**0.5**	**0.6**	**0.7**	**0.8**	**0.9**	**1.0**
Werkgroep	X	X	X	X	X	X	X			
CoP Secure Architecture								230210	230228	
Stuurgroep Implementatie		X	X	X	X	X	X	230210	230228	
MFF									230228	X

Werkgroepleden

Naam	Marktrol
Tony Sloos	RNB / DSO – IT Services (EDSN)
Leander Hiele	RNB / DSO – IT Services (EDSN)
Jan Heerschop	LNB / TSO E – TenneT
Jan Nienhuis	RNB / DSO – Stedin
Mirjam van der Horst	BAS / Stuurgroep Implementatie
Bram van Straalen	BAS / CoP Secure Architecture
Jacco Hogeweg	BAS
Maarten Zwart	BAS
Arjan Visser	BAS
John van der Stap	BAS

1 Inleiding

1.1 Aanleiding en achtergrond

Voor de beveiliging van de uitwisseling van informatie tussen partijen via het berichtenverkeer in de sector wordt sinds 2016 gebruikgemaakt van het protocol TLS[1], versie 1.2. TLS 1.2 bestaat sinds 2008. Dit protocol is zeker gezien vanuit de beveiligingsoptiek aan het einde van zijn levensduur (er worden ook nauwelijks meer vernieuwingen op aangebracht). De opvolger TLS 1.3 is beschikbaar, maar nog niet overal ingevoerd.

Om te zorgen voor een veilige uitwisseling van informatie in de sector is daarom de invoering van TLS 1.3 vastgelegd in issue TC043. Dit issue is op 11 november 2020 vastgesteld door de ALV NEDU. Hierin is afgesproken om de 'overgang' van TLS 1.2 naar TLS 1.3 uit te voeren middels een duaal scenario, waarbij TLS 1.2 en TLS 1.3 gedurende de duale fase naast elkaar gebruikt kunnen worden, waarna TLS 1.2 uitgezet wordt.

In TC043 is gekozen voor een aanpak waarin gestart wordt met een 'zachte' invoering van TLS 1.3 op basis van readiness per systeem in het Centrale MarktFaciliterings-landschap (hierna: CMF-landschap[2]) . De systemen in het CMF-landschap voeren op een natuurlijk moment voor dat systeem TLS 1.3 in, terwijl zij tevens de mogelijkheid blijven bieden om via TLS 1.2 met hen te communiceren. In de reguliere onderhoudscommunicatie van de beheerders van de systemen in het CMF-landschap worden marktpartijen per systeem in kennis gesteld dat TLS 1.3 ondersteund wordt. Uiterlijk 1 juli 2023 moeten alle systemen in het CMF-landschap TLS 1.3 ondersteunen.

Zodra het betreffend systeem in het CMF-landschap TLS 1.3 ondersteunt, zijn marktpartijen in de gelegenheid de beveiliging van de uitwisseling van informatie met TLS 1.3 te testen. Dit betekent dat de marktpartijen de overgang naar TLS 1.3 binnen de duale periode kunnen inplannen zodra TLS 1.3 door hun systemen ondersteund wordt.

De voormalige TC/SC-commissies hebben voorgesteld om het gebruik van TLS 1.2 uiterlijk eind 2023, op een nog nader te bepalen datum, niet meer toe te staan in de sector. Dit voorstel is door de voormalige ALV NEDU op 9 maart 2022 overgenomen[3]. Dit betekent dat de duale periode, die gestart is met de goedkeuring van issue TC043 (11 november 2020), uiterlijk eind 2023 beëindigd wordt.

Dit uitvoeringsplan geeft aan welke stappen er nodig zijn om de definitieve overgang naar TLS 1.3 goed te laten verlopen. De invoering van TLS 1.3 is release onafhankelijk.

Besluiten ALV NEDU

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

[1] ***Over 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.

[2] Onder het CMF-landschap wordt in dit document alle centrale marktfaciliterende systemen verstaan, bij zowel EDSN als TenneT

[3] Bron: NEDU Besluiten

1.2 Doelstelling

Verandertraject:
De begeleiding van het sectorbreed, gestructureerd, gecontroleerd en tijdig doorvoeren van de enabler TLS 1.3, zodat voor 1 januari 2024 het veiligheidsniveau voor berichtenuitwisseling voldoet aan de security-eisen en richtlijnen.

1.3 Stakeholders

Rol		Toelichting
☒	TSO G	Feitelijk zijn alle marktrollen stakeholders, omdat alle marktrollen gekoppeld zijn met minimaal één systeem in het CMF-landschap.
☒	TSO E	
☒	DSO	
☒	Leverancier	
☒	BRP	
☒	BSP	
☒	MV	
☒	Beheerder GDS	
☒	Datagebruiker	
☒	Andere partijen, zoals ODA's, CSP's en Aggregators	

1.4 Scope

1.4.1 Verandertraject

De scope van dit verandertraject is:

- De **market readiness** van de systemen in het CMF-landschap en marktpartijen m.b.t. de ondersteuning van TLS 1.3 te monitoren en hierover te rapporteren.
- Het **communiceren** met marktpartijen (ook via brancheorganisaties) over het doel en de aard van de aanpassingen en voortgang van het traject om hen te bewegen tijdig over te stappen op TLS 1.3.
- Het faciliteren van marktpartijen bij de invoering van TLS 1.3 door het delen van lessons learned
- Advies uitvaardigen aan de ALV MFF over de definitieve overgang naar TLS 1.3 en het uitfaseren van TLS 1.2. CMF-landschap

De systemen in het CMF-landschap zijn in scope van dit project. Per systeem is aangegeven wie de beheerder is van dit centrale systeem, welke marktrollen gebruikmaken van dit systeem en wat globaal de aard van de gegevensuitwisseling is. Hierbij zijn alle koppelingen tussen centrale en decentrale systemen in scope.

Systemen in het CMF-landschap onder beheer van EDSN
De onderstaande systemen van EDSN ondersteunen reeds TLS 1.3

Applicatie	TLS versies
Axway API Gateway, Axway B2Bi , KONG gateway, Toestemmingsplatform, Energiedatalink Provider, CERES	1.2/1.3
C-AR/Portaal (incl. sectorregister, CER, PUD, MDD, MPR, LV/RNB Register, TR, ADC, BU, GBU) (inkomend)	1.2/1.3
C-AR/Portaal (incl. sectorregister, CER, PUD, MDD, MPR, LV/RNB Register, TR, ADC, BU, GBU) (uitgaand: C-AR ==> applicatie)	1.2/1.3
C-ARM	1.2/1.3
Data delen platform	1.2/1.3
EAN-codeboek	1.2/1.3
Gopacs (inkomend)	1.2/1.3
Nexus (uitgaand)	1.2/1.3
Portaal CTS	1.2/1.3
TMR (uitgaand)	1.2/1.3

De onderstaande systemen van EDSN moeten nog aangepast worden voor de ondersteuning van TLS 1.3

Applicatie	TLS versies	Implementatieplanning
CSS	1.2	Q1 2023 onderzoek. Opdracht aan GTS gegeven
Gopacs (uitgaand: Gopacs ==> Applicatie)	1.2	Uiterlijk Q2 2023 (afwachtend op AWS)
Nexus (inkomend: Applicatie ==> Nexus))	1.2	Q1 2023 onderzoek, Q2 2023 uitvoering
TMR (inkomend: Applicatie ==> TMR)	1.2	Q1 2023 onderzoek, Q2 2023 uitvoering

Voor een overzicht van business functies die gekoppeld zijn aan de centrale systemen (EDSN) zie 4.2.1 Centrale systemen in beheer bij EDSN

Systemen in het CMF-landschap onder beheer van TenneT

Applicatie	TLS versies	Implementatieplanning
MMC Hub	1.2	Technisch klaar, wordt geconfigureerd
CPS	1.2	Uiterlijk Q2 2023 (afwachtend op AWS)
TQF	1.2	Q1 2023 onderzoek, Q2 2023 uitvoering
APFAS	1.2	Q1 2023 onderzoek, Q2 2023 uitvoering
OSB voor legacy websites	1.2	Q1 2023 onderzoek, Q2 2023 uitvoering
CPB	1.2	Q1 2023 onderzoek, Q2 2023 uitvoering
GOPACS adapter	1.2	Q1 2023 onderzoek, Q2 2023 uitvoering
FCR webservices	1.2	Q1 2023 onderzoek, Q2 2023 uitvoering
B2B gateway	1.2	Q1 2023 onderzoek, Q2 2023 uitvoering
API Gateway (KONG)	1.2	Q1 2023 onderzoek, Q2 2023 uitvoering
MHS	1.2	Q1 2023 onderzoek, Q2 2023 uitvoering

Voor een overzicht van business functies die gekoppeld zijn aan de centrale systemen (TenneT) zie 4.2.2 Centrale systemen in beheer bij TenneT

1.5 Buiten scope

Buiten scope van dit verandertraject valt het volgende:

- Doorvoeren en testen van de aanpassingen in de systemen in het CMF-landschap zoals beheerd door EDSN en TenneT. Hiervoor zijn respectievelijk de regionale netbeheerders en TenneT verantwoordelijk.
- Doorvoeren en testen van de aanpassingen in de decentrale systemen en processen van de marktpartijen die gekoppeld zijn met de systemen in het CMF-landschap van EDSN en Tennet . Hiervoor zijn de marktpartijen zelf verantwoordelijk.
- Wijziging van de methode waarmee certificaatverificatie wordt uitgevoerd. Voor de invoering van TLS 1.3 is geen certificaatwissel vereist, hetgeen de invoering minder complex en foutgevoelig maakt.
- Sectorbrede testen – zoals kopgroeptesten of een GAT – zijn niet voorzien, omdat de berichten inhoudelijk niet wijzigen.

1.6 Resultaat

Het resultaat is dat alle in scope zijnde systemen in het CMF-landschap TLS 1.3 ondersteunen per 1 juli 2023 en de marktrollen zodanig zijn geïnformeerd, gemotiveerd en gefaciliteerd dat uiterlijk per 1 januari 2024 de energiesector TLS 1.3 als beveiligingsstandaard heeft ingevoerd bij de koppelingen met de systemen in het CMF-landschap en het advies aan de ALV MFF gegeven kan worden om TLS 1.2 uit te faseren.

BAS heeft een resultaatsverplichting om marktrollen te informeren, te motiveren en te faciliteren. Voor de overige partijen zoals ODA's waarvoor de overgang wel impact heeft maar niet een marktrol is, geldt een inspanningsverplichting. Een inspanningsverplichting bestaat uit dezelfde activiteiten namelijk het informeren, motiveren en te faciliteren maar zonder dat het onderdeel is van het resultaat.

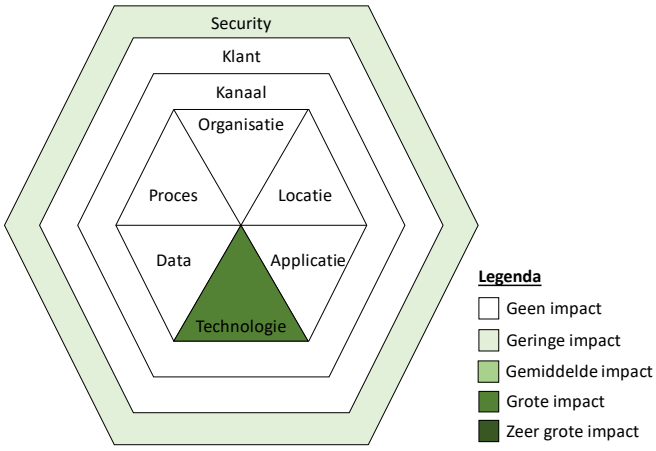
1.7 Kritische succesfactoren

Een tijdige en succesvolle overgang naar TLS 1.3 heeft alleen kans van slagen als voldaan wordt aan de volgende punten:

- **Goede en tijdige sectorbrede communicatie** over de scope en de tijdslijnen van TLS 1.3.
- **Sectorbrede** medewerking, bewustwording en urgentie.
- Prioriteit bij de regionale netbeheerders en TenneT om de door hen beheerde systemen in het CMF-landschap tijdig TLS 1.3 te laten ondersteunen en de duale periode te laten starten.
- Continue monitoring van de voortgang hoeveel partijen (per marktrol en overige partijen) via TLS 1.3 communiceren per systeem in het CMF-landschap.
- De duale periode per systeem in het CMF-landschap start uiterlijk 1 juli 2023.
- De duale periode eindigt uiterlijk 1 januari-2024. In afstemming met de ALV MFF kan besloten worden om de duale periode langer te laten duren als te veel marktpartijen problemen hebben om TLS 1.3 tijdig te ondersteunen.
- Ondersteuning van de relevante softwareleveranciers om hun software TLS 1.3 te laten ondersteunen.

1.8 Impact

De impact van overgang van TLS 1.2 naar versie 1.3 op de omgeving is aangegeven op de CC-POLDATS verandergebieden: Customer (Klant), Channel (Kanaal), Processen, Organisatie, Locatie, Data, Applicatie, Technologie en Security.



Onderdeel	Impact	Uitleg	Effort
Klant	Geen	Geen wijzigingen in klantaspect	Geen
Kanaal	Geen	Geen wijzigingen in toepassing bestaande communicatie/distributie/aanleverkanalen	Geen
Proces	Geen	Geen proceswijzigingen of nieuwe processen	Geen
Organisatie	Geen	Geen wijzigingen in rollen/besturing/governance	Geen
Locatie	Geen	Geen nieuwe locaties/ geen wijzigingen in bestaande locaties	Geen
Data	Geen	Geen aanpassingen in datastructuren/entiteiten/attributen	Geen

Onderdeel	Impact	Uitleg	Effort
Applicatie	Geen	Geen aanpassingen in (bedrijfs)toepassingen	Geen
Technologie	Groot	Invoering nieuw protocol en cypher suite, verbetering in performance als gevolg van invoering nieuw protocol	Gemiddeld
Security	Gering	Verbeterde beveiliging van webverkeer	Gering

2 Uitvoeringsplan

2.1 Werkgroep Invoering TLS 1.3

Om deze sectorbrede verandering te faciliteren wordt er een werkgroep Invoering TLS 1.3 samengesteld, met vertegenwoordigers vanuit alle marktrollen én vertegenwoordigers vanuit de beheerders van de systemen in het CMF-landschap van EDSN en TenneT. Met betrekking tot de vertegenwoordiging vanuit alle marktrollen wordt een resourceaanvraag gedaan bij de Community of Practice Secure Architecture.

Deze werkgroep zal de configuratieparameters voor de invoering van TLS 1.3, zoals vastgesteld in issue TC043, herbevestigen en formaliseren in een configuratiesheet, zodat voor alle partijen duidelijk is welke parameters gehanteerd dienen te worden.

Door EDSN en TenneT wordt momenteel in kaart gebracht welke systemen in het CMF-landschap nog geen TLS 1.3 ondersteunen en wanneer de ondersteuning van TLS 1.3 naar verwachting beschikbaar komt. Zodra deze informatie beschikbaar is zal de werkgroep dit communiceren naar de marktpartijen conform het communicatieplan.

2.2 Stappenplan op hoofdonderwerpen

Het stappenplan bestaat globaal uit vijf delen.

ONDERDEEL	OMSCHRIJVING
1. Aanpassen systemen in het CMF-landschap	De systemen in het CMF-landschap binnen de scope worden TLS 1.3 ready gemaakt.
2. Aanpassen decentrale systemen	De systemen in het CMF-landschap van alle marktpartijen worden TLS 1.3 ready gemaakt.
3. Informatie-uitwisseling via TLS 1.3	De marktpartijen testen de communicatie via TLS 1.3 met de systemen in het CMF-landschap, brengen eventueel verbeteringen aan en gaan via TLS 1.3 communiceren.
4. Einde duale fase / uitzetten TLS 1.2	De systemen in het CMF-landschap binnen de scope faseren TLS 1.2 uit.
5. Communicatie en monitoring	Communicatie richting marktpartijen en monitoring van het gebruik van TLS 1.3 tijdens de duale fase.

2.2.1 Aanpassen systemen in het CMF-landschap

Deze stap betreft het aanpassen van de systemen in het CMF-landschap om TLS 1.3 te kunnen ondersteunen. De verschillende systemen in het CMF-landschap zullen op verschillende moment TLS 1.3 ready zijn, maar uiterlijk 1 juli 2023 moeten alle systemen in het CMF-landschap aangepast zijn en moet deze stap afgerond zijn. De verantwoordelijkheid van deze stap ligt bij de beheerders van de systemen in het CMF-landschap, namelijk EDSN en TenneT.

2.2.2 Aanpassen decentrale systemen

Deze stap betreft het aanpassen van de decentrale systemen om TLS 1.3 te kunnen ondersteunen.
De verantwoordelijkheid van deze stap ligt bij de beheerders van de decentrale systemen.

BAS, EDSN en TenneT faciliteren de marktpartijen bij het overgaan naar TLS 1.3 met (niet uitputtend):

- Meer technische uitleg over TLS 1.3;

- Lijsten met versies van gangbare software waarvan bekend is vanaf welke versie TLS 1.3 wordt ondersteund;
- Checklists voor implementatie met waar mogelijk tips en tricks;
- Ondersteuning bij implementatie en testen van de connectie;
- Het delen van ervaringen van partijen die al zijn overgegaan, zodat partijen die nog bezig zijn daarvan voordeel hebben om de invoering zo soepel en snel mogelijk te laten verlopen.

2.2.3 Informatie-uitwisseling via TLS 1.3

Deze stap betreft het daadwerkelijk gebruikmaken van TLS 1.3 bij een informatie-uitwisseling tussen een decentraal systeem in het CMF-landschap en een systeem in het CMF-landschap. Hierbij geldt als randvoorwaarde dat zowel het betreffende centrale systeem als het betreffende decentrale systeem TLS 1.3 ready zijn.

2.2.4 Einde duale fase / uitzetten TLS 1.2

Deze stap betreft het moment dat de sector de communicatie met de in scope zijnde systemen in het CMF-landschap via TLS 1.2 beëindigt en alleen communicatie middels TLS 1.3 nog toegestaan is. In de systemen in het CMF-landschap zal de mogelijkheid van TLS 1.2 dan uitgezet moeten worden.
Dit moment is in lijn met het overgenomen ALV NEDU besluit 1-1-2024 als alle informatie-uitwisseling met de in scope zijnde systemen in het CMF-landschap via TLS 1.3 beveiligd is. Maar ALV MFF kan t.z.t. besluiten hiervan af te wijken door:

- Verlenging van de duale fase (indien onvoldoende marktpartijen TLS 1.3 geïmplementeerd hebben);
- Verkorting van de duale fase (indien vanuit securityperspectief TLS 1.2 eerder dan 1-1-2024 uitgefaseerd moet worden.

2.2.5 Communicatie en monitoring

Deze stap waarvoor de werkgroep primair verantwoordelijk is, vindt gedurende de gehele uitvoering plaats en behelst een aantal onderdelen:

- Monitoring van de TLS 1.3 market readiness van de systemen in het CMF-landschap;
- Monitoring van de TLS 1.3 market readiness van de marktpartijen;
- Monitoring van het daadwerkelijke gebruik van TLS 1.3 door marktpartijen. Deze monitoring zal door de beheerders van systemen in het CMF-landschap in het CMF-landschap plaatsvinden en rapporteren aan de werkgroep;
- Monitoring van de veiligheid van TLS 1.2. Deze monitoring zal door de CoP Secure Secure Architecture plaatsvinden. Als er naar aanleiding van deze monitoring aanleiding voor is, wordt TLS 1.2 versneld uitgefaseerd en wordt de duale periode versneld beëindigd;
- Communicatie naar marktpartijen en beheerders van de systemen in het CMF-landschap gedurende de gehele implementatie van TLS 1.3.

2.3 Acceptatiecriteria voor de uitfasering van TLS 1.2

Om TLS 1.2 te kunnen uitfaseren gelden de onderstaande acceptatiecriteria:

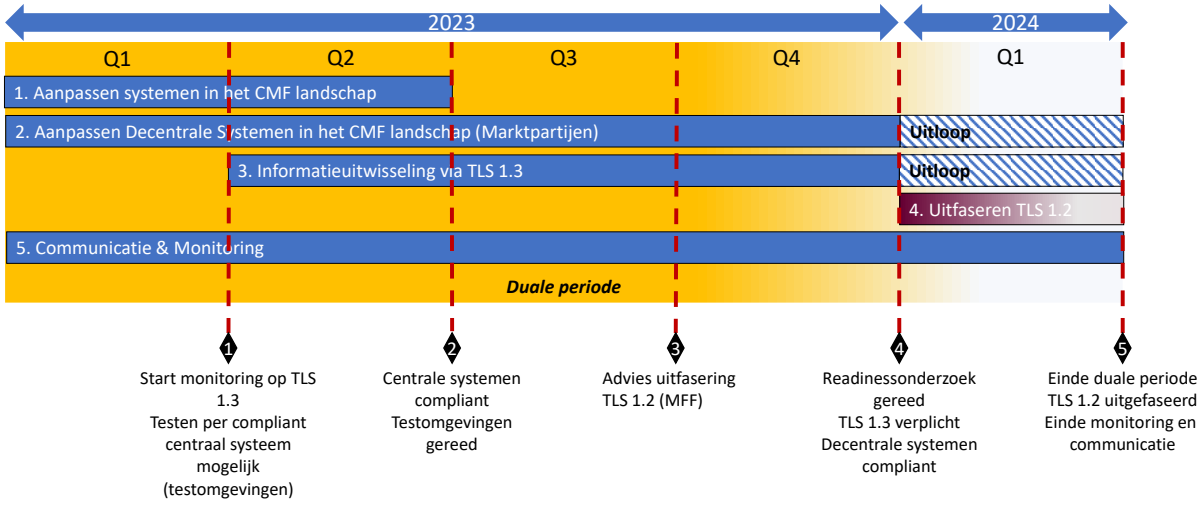
- Voor de systemen in het CMF-landschap, die binnen de scope vallen, geldt een acceptatiecriterium van 100% over op TLS 1.3.
- Voor alle koppelingen tussen decentrale systemen in het CMF landschap geldt een gewogen marktaandeel van 66% die op TLS 1.3 zitten.
- Voor ODA’s en andere marktdeelnemers kan geen gewogen marktaandeel worden afgegeven. Hiervoor geldt 51% van het absolute marktaandeel.

2.4 Planning

De belangrijkste uitgangspunten bij de planning zijn:

- Het onderliggende Uitvoeringsplan wordt op 8 maart 2023 vastgesteld door de ALV MFF;
- Marktpartijen kunnen na de TLS 1.3 market readiness van een systeem in het CMF-landschap zelf bepalen wanneer ze gebruik gaan maken van TLS 1.3 met betrekking tot de informatie-uitwisseling met het betreffende centrale systeem mits uiterlijk 31 december 2023.
- De beheerders van de systemen in het CMF-landschap EDSN en TenneT hebben TLS 1.3 conform de door de CoP Secure Architecture vastgestelde configuratiesheet geïmplementeerd en beschikbaar gesteld uiterlijk 1 juli 2023.
- Beschikbaarheid (test) faciliteiten geleverd door EDSN en TenneT. Wanneer een systeem in het CMF-landschap TLS 1.3 ready is, wordt voor dit systeem een testomgeving opengesteld. Voor de systemen in het CMF-landschap die nog worden aangepast, is uiterlijk 1 juli 2023 de testomgeving beschikbaar.
- De systemen in het CMF-landschap die TLS 1.3 ondersteunen, faciliteren ook het gebruik van TLS 1.2 tot de datum waarop TLS 1.2. uitgefaseerd wordt. Dit is de duale periode.
- TLS 1.2 wordt per 1 januari 2024 uitgefaseerd op basis van een besluit van de ALV MFF, tenzij de ALV MFF op basis van een te groot aantal marktpartijen dat nog niet over is naar TLS 1.3. besluit dat dit moment te vroeg is.
- Het daadwerkelijke gebruik van TLS 1.3 wordt tot 1 januari 2024 niet afgedwongen, tenzij het op basis van acute nieuwe inzichten met betrekking tot de veiligheid van TLS 1.2 noodzakelijk is om TLS 1.2 eerder uit te faseren.

2.5 Roadmap activiteiten en mijlpalen



2.5.1 Mijlpalen

1. Start monitoring op TLS 1.3 – Partieel duale periode (per systeem)
2. Systemen in het CMF-landschap compliant – Aanvang volledig duale periode (alle systemen)
3. Advies aan ALV MFF inzake uitfasering TLS 1.2
4. TLS 1.3 in werking – Decentrale systemen compliant – Einde duale periode
5. TLS 1.2 uitgeschakeld

2.5.2 Deliverables

Deliverable	Frequentie	Uitvoerder	Ontvanger
Rapportage monitoring	Driewekelijks	EDSN, TenneT – i.s.m. werkgroep TLS 1.3	Stuurgroep Implementatie
Samenvatting rapportage monitoring	ALV vergaderschema	EDSN, TenneT	ALV MFF
Diverse communicatie-uitingen	Zie hoofdstuk 3 Communicatieplan Communicatieplan	Werkgroep TLS 1.3	Sector breed
Rapportage readiness systemen in het CMF-landschap, per systeem	Driewekelijks	EDSN, TenneT – i.s.m. wekgroep TLS 1.3	Sector breed
Advies aan ALV MFF voor uitfasering TLS 1.2	Eenmalig, eind Q3	Werkgroep TLS 1.3	ALV MFF

2.6 Monitoring en readiness

2.6.1 Readiness systemen in het CMF-landschap

Voordat marktpartijen hun aangepaste systemen kunnen testen moeten de systemen in het CMF-landschap klaar zijn om de informatie-uitwisseling via TLS 1.3 te beveiligen.

- De systemen in het CMF-landschap worden door de beheerders, EDSN en TenneT, geüpgraded naar TLS 1.3 waarbij TLS 1.2 tijdelijk beschikbaar blijft.
- Zodra een systeem in het CMF-landschap geüpgraded is naar TLS 1.3, wordt dit aan de werkgroep gemeld.

De communicatie over de readiness van de systemen in het CMF-landschap wordt uitgevoerd door de werkgroep. Voor de uitwerking hiervan wordt verwezen naar hoofdstuk 3 Communicatieplan

- Communicatieplan verderop in dit document.

2.6.2 Readiness marktpartijen

De readiness van marktpartijen wordt op een aantal verschillende manieren bepaald:

- Mailings. De readiness van marktpartijen wordt in de eerste plaats bepaald op basis van mailings naar de marktpartijen.
- Monitoringsystemen in het CMF-landschap. De readiness van marktpartijen wordt verder gemeten op basis van monitoring op de systemen in het CMF-landschap welke marktpartij welk transportbeveiligingsprotocol gebruikt bij welke verbinding. De daadwerkelijke monitoring vindt plaats door de beheerders van de systemen in het CMF-landschap die de resultaten hiervan terugkoppelen naar de werkgroep. De readiness rapportage vanuit de monitoring door de beheerders wordt maandelijks aan de werkgroep ‘Invoering TLS 1.3’ gestuurd.

Communicatie naar sector vanuit monitoring. De communicatie over de readiness van marktpartijen wordt uitgevoerd vanuit de werkgroep. Voor de uitwerking hiervan wordt verwezen naar hoofdstuk 3 Communicatieplan

Communicatieplan verderop in dit document.

2.6.3 Readiness softwareleveranciers

Softwareleveranciers zijn bezig met het upgraden van software om TLS 1.3 te kunnen ondersteunen. Op basis van het onderzoek dat in 2020 en 2021 is uitgevoerd[4], is een niet uitputtende lijst opgesteld van in de sector meest gangbare software.
Op basis van deze lijst worden marktpartijen geïnformeerd vanaf welke versie de software TLS 1.3 ondersteunt. Deze lijst kan door marktpartijen worden gebruikt om hun eigen upgrade strategie te bepalen.
De communicatie over de readiness van softwareleveranciers wordt uitgevoerd vanuit de werkgroep. Voor de uitwerking hiervan wordt verwezen naar hoofdstuk 3 Communicatieplan

[4] Zie document 'Status TLS 1.3 door vendoren en producten versie 2021' voor de status van ondersteuning door softwareproducenten.

Communicatieplan verderop in dit document.

2.7 Realisatie

De realisatie van de implementatie van TLS 1.3 vindt plaats door:

- De beheerders van de centrale systemen m.b.t. de door hen beheerde systemen in het CMF-landschap;
- De markpartijen met betrekking tot de voor hen relevante systemen.

2.8 Testen

Er is geen sprake van sectortesten. Wel zijn de standaard testomgevingen van de systemen in het CMF-landschap beschikbaar voor testen.

2.9 Governance

BAS informeert, begeleidt, coördineert en monitort de invoering van TLS 1.3 en het uitzetten van TLS 1.2. De sectorpartijen – leden van MFF en daarbuiten – zijn verantwoordelijk voor het binnen de eigen organisatie tijdig, juist en volledig realiseren van de overgang naar TLS 1.3.

2.10 Afhankelijkheden

Afhankelijk van ondersteuning van TLS 1.3 voor software door softwareleveranciers.

2.11 Risicomanagement

R=K*I. Risico = kans op een verstorende gebeurtenis * de impact op de omgeving

Kans *Impact*	*Klein*	*Gemiddeld*	*Groot*
Groot	*Hoog Risico*	*Hoog risico*	*Hoog risico*
Gemiddeld	*Gemiddeld risico*	*Gemiddeld risico*	*Hoog risico*
Klein	*Laag Risico*	*Gemiddeld risico*	*Gemiddeld risico*

Gebeurtenis	Kans	Impact	Risico	Mitigatie
Decentrale systemen gekoppeld aan het CMF-landschap zijn 1-1-2024 niet ready	groot	groot	hoog	• Zoveel en zo breed mogelijk communiceren en kennis delen naar MFF en daarbuiten. • Escalatie naar het MFF om de marktpartijen die achterblijven tijdig te laten overstappen. • Facilitering van marktpartijen die problemen ondervinden met invoering.
Onvoldoende ondersteuning TLS 1.3 door softwareleveranciers	groot	groot	hoog	• Softwareleveranciers vragen hoe hun veranderschema van hun producten eruitziet. • Back-up plan in werking stellen: impactanalyse om welke systemen het gaat, ingegeven door de marktpartijen. • Marktpartijen werken hun eigen alternatieven uit (voorbeeld: zolang een systeem nog niet up-to-

Gebeurtenis	Kans	Impact	Risico	Mitigatie
				date is, achter een proxyserver laten plaatsen).
TLS 1.2 wordt vanwege nieuwe gebreken door NCSC afgeschaald naar 'onvoldoende'	middel	groot	hoog	• Het gebruik van TLS 1.2 levert qua beveiliging nog geen probleem op, omdat met de juiste parametersetting TLS 1.2 vooralsnog adequate beveiliging biedt. Deze parametersetting wordt afgedwongen door de systemen in het CMF-landschap. • De Community of Practice Secure Architecture monitort de veiligheid van TLS 1.2. Het risico blijft bestaan dat TLS 1.2 als onveilig wordt bevonden, waarna een 'hals-over-kop' invoering van TLS 1.3 nodig zal zijn en de duale periode versneld moet worden afgerond. Daarom is het van belang dat marktpartijen in hun betreffende communicatie-onderdelen zo snel mogelijk TLS 1.3 invoeren.
TenneT systemen in het CMF-landschap zijn niet ready op 1 juli 2023	groot	middel	hoog	• De beherende partij blijven betrekken. Indien dit niet het gewenste effect heeft, dan escalatie naar het MFF.
EDSN-systemen in het CMF-landschap zijn niet ready op 1 juli 2023	klein	middel	middel	• De beherende partij blijven betrekken. Indien dit niet het gewenste effect heeft, dan escalatie naar het MFF.

2.12 Lessons learned uit eerdere overgangstrajecten

Belangrijkste evaluatiepunten specifiek voor het project TLS 1.2[5] zijn:

Nr	Evaluatiepunt project TLS 1.2	Verwerking leerpunt in aanpak invoering TLS 1.3
1	De interne communicatie in het project moet verbeterd worden door een communicatie-escalatie op te nemen in PID, dan wel communicatieplan. Beheer communiceerde rechtstreeks met marktpartijen zonder overleg met communicatie.	• Met de beheerders van de systemen in het CMF-landschap afspreken dat BAS altijd in de cc meegenomen wordt. • Communicatie afstemmen tussen BAS, EDSN en TenneT. • Communicatie-escalatie opnemen in Communicatieplan.
2	Projectmanagementmethodiek van Technische Issues moet differentiëren van sector releases. De standaardmethodiek is onvoldoende toereikend.	• Werkgroep Invoering TLS 1.3 is samengesteld met directe vertegenwoordiging van BAS, EDSN, TenneT, de CoP Secure Architecture en de Stuurgroep Implementatie, om de samenwerking en afstemming te verbeteren en een integrale aanpak te bevorderen.
3	De kwaliteit van het issue TC024 is onvoldoende. Door vaagheid in de tekst is er op gegeven moment een keuze gemaakt voor 4 cipher suites en hun hiërarchie zonder dat te achterhalen is waarop deze keuze is gebaseerd.	• Configuratiesheet wordt vastgesteld door de CoP Secure Acrhitecture en samen met dit Uitvoeringsplan aangeboden in de ALV MFF. • In de communicatie en de monitoring wordt het compliant zijn aan de configuratie meegenomen.
4	De GAT was te vrijblijvend voor de issue dat bij niet implementeren betekent dat je geen berichtenverkeer meer hebt.	• Monitoring en rapportage over het gebruik van testomgevingen door marktpartijen. • Achterblijvende partijen najagen per email en telefoon.

[5] Bron: Project Closure Rapport TLS 1.2 v1.0

Nr	Evaluatiepunt project TLS 1.2	Verwerking leerpunt in aanpak invoering TLS 1.3
5	Marktpartijen onderschatten technische issues en wachten te lang tot implementatie live-gang.	• Escalatie naar ALV MFF bij onvoldoende voortgang • Achterblijvende partijen najagen per email en telefoon. • Lessons learned van reeds ingestapte marktpartijen delen

3 Communicatieplan

3.1 Doelstellingen en resultaat

De doelstellingen van dit Communicatieplan Invoering TLS 1.3:

- De relevante personen van de marktpartijen in de energiesector (ten minste alle MFF-leden en zo veel mogelijk niet-leden) zijn volledig, tijdig en juist geïnformeerd over de aard, de aanpassingen, de planning en voortgang van het project.
- Ze zijn tijdig op de hoogte gesteld om zelf decentrale acties te ondernemen voor een tijdige invoering van TLS 1.3.
- Het management van de marktpartijen wordt meegenomen in de noodzaak en urgentie van de invoering van TLS 1.3, zodat deze budget vrijmaken voor en prioriteit geven aan de benodigde decentrale aanpassingen en akkoord geven om over te gaan op TLS 1.3
- Er is een actieve dialoog gefaciliteerd tussen de werkgroep van BAS en de marktpartijen.

Het gewenste resultaat is dat door volledige, tijdige en juiste informatie alle marktpartijen op 31 december 2023 TLS 1.3 hebben ingevoerd en via dit protocol kunnen communiceren met de systemen in het CMF-landschap.

3.2 Scope

Voor de overgang naar TLS 1.3 moeten er centraal en decentraal wijzigingen in de softwaresystemen worden doorgevoerd. De marktpartijen worden opgeroepen de decentrale wijzigingen door te voeren en gebruik te maken van de testomgevingen. Dit communicatieplan beschrijft alle benodigde communicatie om de marktpartijen tijdig en juist te informeren, zodat zij klaar zijn voor de invoering van TLS 1.3 op 31 december 2023.

3.3 Doelgroepen

Vanuit de Werkgroep Invoering TLS 1.3 richten we ons primair op:

1. De eigenaren/business owners van decentrale systemen bij marktpartijen die MFF-lid zijn
2. De eigenaren/business owners van decentrale systemen bij alle overige marktpartijen
3. Beheerders van decentrale systemen bij marktpartijen die MFF-lid zijn
4. Beheerders van decentrale systemen bij alle overige marktpartijen

en secundair op:

5. Beheerders van de systemen in het CMF-landschap bij TenneT en EDSN
6. Brancheorganisaties
7. Stuurgroep Implementatie
8. ALV MFF

3.4 Uitgangspunten

Het slagen van het verandertraject valt of staat bij de inzet van de doelgroepen. Die moeten niet alleen weten wat ze wanneer moeten doen, maar ook overtuigd zijn van de reden waarom. Ze moeten zich betrokken voelen en de overgang naar TLS 1.3 ondersteunen. Met dit plan willen we de doelgroepen daarom goed:

- Informeren – we communiceren open, eerlijk en eenduidig
- Inspireren – we communiceren positief en enthousiast;

- Betrekken – we communiceren vanuit een wij-gevoel, informeel (jegens de primaire doelgroep) en we leggen de doelgroep keuzes voor die we inwilligen zodat het draagvlak groeit;
- Motiveren – we communiceren met overtuigende argumenten;
- Activeren – we communiceren helder.
- Faciliteren – we delen leerervaringen van marktpartijen die al overgegaan zijn (en optioneel wijzen we in tweede instantie naar extra begeleiding vanuit de helpdesk).

3.5 Aanpak en planning communicatie

De communicatieaanpak sluit aan op de onderdelen waaruit het project Invoering TLS 1.3 is opgebouwd (zie paragraaf 2.2 Stappenplan op hoofdonderwerpen.

1. Aanpassen systemen in het CMF-landschap (vanaf nu tot 1 juli 2023)
Projectdoel: de systemen in het CMF-landschap binnen de scope worden TLS 1.3-ready gemaakt.

Communicatieboodschap: marktpartijen kunnen per systeem overstappen. Ze mogen zelf bepalen wanneer, doch uiterlijk per 31 december 2023. Testen gebeurt op basis van readiness per systeem in het CMF-landschap. Sommige systemen in het CMF-landschap zijn nu al klaar om tegenaan te testen. We benadrukken de voordelen: je bent ruim op tijd compliant, je voorkomt een haastige implementatie met kans op fouten, extra veiligheid dankzij TLS 1.3 is snel geborgd en je bent de mogelijke situatie voor dat bij gebleken veiligheidsrisico's van TLS 1.2 je halsoverkop moet overschakelen.

Communicatie-inspanningen (zie ook paragraaf 3.6 Communicatiemiddelen):

- Opstellen kernboodschap voor websites van betrokken organisaties: MFFBAS, netbeheerders, EDSN en brancheorganisaties.
- Opstellen eerste versie Q&A voor website MFFBAS en mijnMFFBAS.
- Opzetten dashboard (nulmeting) plus verkeerslicht: welke systemen in het CMF-landschap zijn over, hoeveel partijen per systeem zijn over plus wanneer kun je overstappen op welk systeem, wanneer is de testomgeving gereed, hoe zit het met de readiness van software van desystemen in het CMF-landschap?
- Opvragen contactpersonen (zowel MT- als beheerdersniveau) van MFF-leden via een uitvraag met SurveyMonkey om hen te kunnen uitnodigen voor voorlichtingssessies en zo nodig aan te sporen om tijdig over te stappen.
- Verzamelen contactgegevens (zowel op MT- als beheerdersniveau)van niet-MFF leden afkomstig van netbeheerders en EDSN
- Uitnodiging voor de algemene voorlichting aan leden en niet-leden.
- Algemene voorlichtingssessie over waarom, hoe en wat van het project, inclusief een presentatie en aangevulde Q&A om na de sessie met de markt te delen.
- Nieuwsbrief MFFBAS met artikelen over onder meer: aankondiging van het project (plus kernboodschap), Q&A, updates, aankondiging en terugblik voorlichting, updates over systemen in het CMF-landschap, stand dashboard en eventueel verwijzing naar stappenplan/checklist, verwijzing naar de helpdesk, testimonials marktpartijen en interviews experts en brancheorganisaties.
- Afstemming met EDSN en netbeheerders om de invoering van TLS 1.3 ook te belichten in de nieuwsbrieven van deze organisaties

Optioneel:

- Stappenplan of checklist voor marktpartijen om over te stappen.
- Helpdesk om op maat vragen te beantwoorden van marktpartijen.
- Testimonials van marktpartijen die al succesvol zijn overgestapt.

- Interviews veiligheidsexpert/brancheorganisatie(s) over het belang om over te gaan.

2. Aanpassen decentrale systemen in het CMF-landschap (vanaf nu tot 1 januari 2024)
Projectdoel: marktpartijen maken hun systemen TLS 1.3-ready.

3. Informatie-uitwisseling via TLS 1.3 (vanaf nu tot 1 januari 2024)
Projectdoel: de marktpartijen testen de communicatie via TLS 1.3 met de systemen in het CMF-landschap, brengen eventueel verbeteringen aan en gaan via TLS 1.3 communiceren.

Communicatieboodschap: zie projectonderdeel 1.
Vanaf 1 juli 2023, wanneer alle systemen in het CMF-landschap TLS 1.3-ready zijn, benadrukken we de urgentie van de overstap. Boodschap is dat marktpartijen haast moeten maken om over te stappen. Ze hebben tot eind 2023 de tijd. Want als ze dat niet doen, dan sluiten zij zichzelf af van het berichtenverkeer met alle risico's voor hun operatie van dien. Ze kunnen nu al aan de slag, want alle systemen in het CMF-landschap zijn er inmiddels klaar voor.

Communicatie-inspanningen (zie ook paragraaf 3.6 Communicatiemiddelen):

- Q&A voor website MFFBAS en mijnMFFBAS.
- Dashboard plus verkeerslicht: welke systemen in het CMF-landschap zijn over, hoeveel partijen per systeem zijn over plus wanneer kun je overstappen op welk systeem, wanneer is de testomgeving gereed, hoe zit het met de readiness van software van desystemen in het CMF-landschap?
- Beheer contactpersonen MFF-leden.
- Beheer contactgegevens niet-leden.
- Uitnodiging voor de tweede voorlichting over het testen aan leden en niet-leden.
- Tweede voorlichtingssessie over het individueel testen tegen systemen in het CMF-landschap, inclusief een presentatie en aangevulde Q&Aom na de sessie met de markt te delen.
- Nieuwsbrief MFFBAS met artikelen over onder meer: Q&A, updates, aankondiging en terugblik tweede voorlichting, updates over systemen in het CMF-landschap, stand dashboard en eventueel verwijzing naar stappenplan/checklist, verwijzing naar de helpdesk, testimonials marktpartijen en interviews experts en brancheorganisaties.

Optioneel:

- Stappenplan of checklist voor marktpartijen om over te stappen.
- Helpdesk om op maat vragen te beantwoorden van marktpartijen en om hen te faciliteren bij problemen met de invoering van TLS 1.3.
- Testimonials van marktpartijen die al succesvol zijn overgestapt.
- Interviews veiligheidsexpert/brancheorganisatie(s) over het belang om over te gaan.

4. Einde duale fase / uitzetten TLS 1.2
Projectdoel: de systemen in het CMF-landschap binnen de scope faseren TLS 1.2 uit.

Communicatieboodschap: zie projectonderdeel 1.
Vanaf 1 oktober 2023 verhogen we nogmaals de urgentie om over te stappen naar TLS 1.3. Het uitgangspunt is dat marktpartijen hiervoor nog tijd hebben tot 1 januari 2024. Naarmate de deadline nadert, peilen we de haalbaarheid van een sectorbrede overstap en kunnen we indien nodig de uitfasering van TLS 1.2 met enkele maanden uitstellen. Inhoudelijk blijft de communicatieboodschap hetzelfde. Andersom kan het gebeuren dat we de duale fase verkorten als TLS 1.2 uit securityperspectief eerder dan 1 januari 2024 uitgefaseerd dient te worden. Dit maakt de communicatieboodschap des te urgenter.

Communicatie-inspanningen (zie ook paragraaf 3.6 Communicatiemiddelen):

- Q&A voor website MFFBAS en mijnMFFBAS.
- Dashboard plus verkeerslicht: welke systemen in het CMF-landschap zijn over, hoeveel partijen per systeem zijn over plus wanneer kun je overstappen op welk systeem, wanneer is de testomgeving gereed, hoe zit het met de readiness van software van de decentrale systemen in het CMF-landschap?
- Beheer contactpersonen MFF-leden.
- Beheer contactgegevens niet-leden.
- Nieuwsbrief MFFBAS met artikelen over onder meer: Q&A, updates, aankondiging en terugblik tweede voorlichting, updates over systemen in het CMF-landschap, stand dashboard en eventueel verwijzing naar stappenplan/checklist, verwijzing naar de helpdesk, testimonials marktpartijen en interviews experts en brancheorganisaties.
- Peilen market readiness voor Go go live onder MFF-leden via SurveyMonkey om de prognose te bepalen van het marktaandeel per marktrol dat bij de uitfasering van TLS 1.2 is overgestapt op TLS 1.3.
- Indien nodig: actief benaderen van (cruciale) achterblijvers voor een succesvolle go live via achtereenvolgens een groepsmailing, gerichte e-mail en belactie.
- Nazorg: praktische informatie (Q&A, presentaties, eventueel stappenplan of checklist) voor overstap aan (niet-cruciale) achterblijvers na een succesvolle go live op websites betrokken organisaties en mijnMFFBAS ter ondersteuning.

Optioneel:

- Stappenplan of checklist voor marktpartijen om over te stappen.
- Helpdesk om op maat vragen te beantwoorden van marktpartijen en om hen te faciliteren bij problemen met de invoering van TLS 1.3.
- Testimonials van marktpartijen die al succesvol zijn overgestapt.
- Interviews veiligheidsexpert/brancheorganisatie(s) over het belang om over te gaan.

3.6 Communicatiemiddelen

Voor TLS 1.3 zetten we communicatiemiddelen in die specifiek voor dit project bestemd zijn. Zo belasten we mensen buiten de benoemde doelgroepen niet met specifieke informatie. Bovendien vallen we deze doelgroepen niet lastig met informatie die niets met beide projecten te maken heeft. Wat we via deze middelen communiceren, is daarmee altijd urgent en relevant (need to know) en raakt niet ondergesneeuwd door nice to know-informatie. Het gaat om de volgende middelen:

Kernboodschap

- Wat: korte, motiverende standaardtekst over het waarom, hoe en wat van het project
- Doel: informeren, motiveren
- Doelgroep: 1 tot en met 8
- Wanneer: start project
- Kanaal/manier: op website MFFBAS, TenneT, EDSN en brancheverenigingen, via nieuwsbrief MFFBAS en in presentatie voorlichtingssessies

Q&A

- Wat: lijst met vooral praktische vragen en antwoorden over invoering TLS 1.3, in de loop van het project aangevuld met actuele vragen uit de markt, eventueel met link naar helpdesk
- Doel: informeren, activeren
- Doelgroep: 3 en 4
- Wanneer: vanaf start project
- Kanaal/manier: op website MFFBAS en mijnMFFBAS

Dashboard

- Wat: actuele stand van zaken over readiness van systemen in het CMF-landschap, van marktpartijen en van softwareleveranciers
- Doel: informeren, motiveren
- Doelgroep: 3 en 4
- Wanneer: vanaf start project
- Kanaal/manier: op website MFFBAS en mijnMFFBAS

Uitvragen
- Wat: enquêtes onder marktpartijen voor uitvragen contactpersonen (bij projectaanvang onder MFF-leden) en prognose go live (onder marktpartijen die in Q4 2023 nog niet over zijn gestapt)
- Doel: activeren
- Doelgroep: 1 tot en met 4
- Wanneer: bij start project en richting einde project (Q4 2023)
- Kanaal/manier: via enquêteprogramma SurveyMonkey

Uitnodiging voorlichting
- Wat: vergaderverzoek voor online voorlichtingssessies
- Doel: activeren
- Doelgroep: 1 tot en met 4
- Wanneer: bij start project (algemene voorlichting) en halverwege het project (over testen)
- Kanaal/manier: via Microsoft Outlook

Informatiebijeenkomsten en presentaties
- Wat: over doel, voortgang, planning, verwachtingen en praktische aanwijzingen rond de invoering van TLS 1.3
- Doel: informeren, betrekken, motiveren, activeren
- Doelgroep: 1 tot en met 4
- Wanneer: bij start project (algemene voorlichting) en halverwege het project (over testen)
- Kanaal/manier: via Microsoft Teams

Nieuwsbrief MFFBAS, sectie TLS 1.3
- Wat: reeks inleidingen met doorlink naar integrale artikelen op de website van MFFBAS over onder meer: aankondiging van het project (plus kernboodschap), Q&A, updates, aankondiging en terugblik voorlichting, updates over systemen in het CMF-landschap, stand dashboard
- Doel: informeren (over de algemene voortgang), inspireren (goed nieuws en goede voorbeelden communiceren), activeren (bijvoorbeeld om deel te nemen aan informatiebijeenkomsten, en decentrale acties uit te voeren)
- Doelgroep: 1 tot en met 8
- Wanneer: vanaf start project tweewekelijks
- Kanaal/manier: via specifieke projectnieuwsbrief in MFFBAS-stijl (via mailingprogramma Laposta) met links naar integrale artikelen op MFFBAS-website

Groepsmailing, e-mail, belactie
- Wat: oproep aan marktpartijen die nog niet zijn overgestapt op TLS 1.3, eerst per groep, daarna gericht op individuele marktpartijen (per e-mail en bij geen reactie per telefoon)
- Doel: activeren
- Doelgroep: 1 tot en met 4
- Wanneer: Q4 2023
- Kanaal/manier: via Microsoft Outlook en telefoon

Nazorg

- Wat: praktische informatie voor marktpartijen die na de livegang over dienen te stappen op TLS 1.3, zoals Q&A, presentaties, eventueel stappenplan of checklist
- Doel: activeren
- Doelgroep: 3 en 4
- Wanneer: na livegang
- Kanaal/manier: via mijnMFFBAS

Optioneel

Stappenplan of checklist

- Wat: een overzichtelijke uitleg hoe je voor elk systeem in het CMF-landschap overstapt op TLS 1.3
- Doel: activeren
- Doelgroep: 3 en 4
- Wanneer: vanaf start project
- Kanaal/manier: via mijnMFFBAS

Helpdesk

- Wat: een mailbox waarnaar marktpartijen praktische vragen sturen voor de overstap naar TLS 1.3 en waar medewerkers van EDSN vanaf Q4 proactief marktpartijen begeleiden bij (problemen met) de invoering van TLS 1.3
- Doel: faciliteren
- Doelgroep: 3 en 4
- Wanneer: vanaf start project
- Kanaal/manier: via mail en telefonisch

Testimonials

- Wat: artikelen waarin marktpartijen die succesvol zijn overgestapt naar TLS 1.3 aan het woord komen met als boodschap dat die overstap belangrijk is en dat die eenvoudig is te realiseren
- Doel: inspireren, motiveren
- Doelgroep: 1 tot en met 4
- Wanneer: vanaf start project
- Kanaal/manier: nieuwsbrief MFFBAS, website MFFBAS

Interviews veiligheidsexpert en brancheorganisaties

- Wat: artikelen waarin veiligheidsexpert en brancheorganisaties aan het woord komen om de noodzaak van de invoering van TLS 1.3 te benadrukken
- Doel: motiveren
- Doelgroep: 1 tot en met 4
- Wanneer: vanaf start project
- Kanaal/manier: nieuwsbrief MFFBAS, website MFFBAS

3.7 Organisatie

De Werkgroep Invoering TLS 1.3 is inhoudelijk verantwoordelijk voor de communicatie. Hiervoor stemt de Werkgroep af met TenneT en EDSN, bijvoorbeeld voor monitoring van systemen in het CMF-landschap en readiness van marktpartijen en softwareleveranciers. De communicatie wordt uitgevoerd door de communicatieadviseur BAS, die een beknopt communicatieplan opstelt (dit plan) en het bewaakt. Daarnaast verzorgt de communicatieadviseur in afstemming met de Werkgroep de communicatiemiddelen.

4 Bijlagen

4.1 Bijlage 1 – Noodzaak tot verandering

Er zijn meerdere redenen om de invoering van TLS 1.3 nu serieus ter hand te nemen en het gebruik van TLS 1.2 uit te faseren.

1. Het veiligheidsniveau van TLS 1.2 loopt achteruit. Het Nationaal Cyber Security Center (NCSC) heeft de beoordeling van het protocol afgewaardeerd van goed naar voldoende[6].
2. Bovendien heeft de sector nog slechts één cipher suite binnen TLS 1.2 voor de beveiliging waar de sector gebruik van kan maken. Als deze rekensleutels worden gekraakt heeft de sector geen veilige alternatieve cipher suite om naar uit te wijken en blokkeert dat het hele berichtenverkeer.
3. Binnen het protocol gebruikt de sector tevens beveiligingscertificaten voor de beveiliging. De huidig gebruikte certificaten (onder het PKI overheid stelsel) zijn van een verouderd type. Het is sterk aan te raden over te gaan op zogenaamde elliptische curve certificaten, die een veel hogere beveiligingsgraad bieden. Het NCSC beoordeelt alleen de op Elliptic Curves (EC) gebaseerde certificaten als goed, de overige certificaten slechts als voldoende[7]. Echter de invoering van deze EC-certificaten onder TLS 1.2 is problematisch, terwijl dit onder TLS 1.3 aanzienlijk eenvoudiger verloopt.

Daarnaast wordt met TLS 1.3 een verbetering in de snelheid van berichtenverkeer bewerkstelligd, omdat het protocol tussen server en client minder stappen bevat.
Tot slot is de security van TLS 1.3 meer robuust, waarmee Perfect Forward Secrecy[8] wordt afgedwongen, en heeft het verbeterde encryptie-algoritmen die geen bekende zwakheden bevatten.

Kortom: TLS 1.3 zorgt voor snellere uitwisseling en betere beveiliging van berichtenverkeer.

In de CoP Secure Architecture – een Community of Practice die uit deelnemers van de voormalige Technische en Security Commissies bestaat – van 25 augustus 2022 is de wenselijkheid van overgang van het transportprotocol TLS 1.2 naar TLS 1.3 besproken. Naar aanleiding hiervan is een notitie ingebracht in het ALV MFF van 28 september 2022. Hierin is de aanbeveling opgenomen om de huidige status te laten onderzoeken van de ondersteuning van TLS 1.3 door soft- en hardware leveranciers. Dit onderzoek is in opdracht van de NEDU voor het laatst uitgevoerd in juni 2021. De ondersteuning voor TLS 1.3 dient voldoende te zijn voordat dit verplicht gesteld kan worden in de sector.

Tevens is toegezegd dat een werkgroep een plan van aanpak op zal stellen, waarin zaken als aanpak, rolverdeling, risicomanagement en communicatie zijn uitgewerkt. Dit plan van aanpak zal aan de ALV MFF ter vaststelling aangeboden worden, zodat de leden actie kunnen ondernemen voor de overgang naar TLS 1.3. De rest van de marktpartijen die geen lid zijn van de MFF wordt bereikt door het nadrukkelijk naar buiten brengen van de noodzaak van de overgang. Hiervoor worden onder andere de distributielijsten gebruikt om die partijen te bereiken.

---

[6] Bron: *NCSC – ict beveiligingsrichtlijnen voor transport layer security v 2.1*

[7] Bron: Zie hetzelfde document als 3

[8] ***Over 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.

4.2 Bijlage 2 – System readiness centrale systemen

4.2.1 Centrale systemen in beheer bij EDSN

Momentopname, dd. 20-02-2023

Applicatie	Business Services	TLS versies
Axway API Gateway, Axway B2Bi , KONG gateway, Toestemmingsplatform, Energiedatalink Provider, CERES		1.2/1.3
C-AR/Portaal (incl. sectorregister, CER, PUD, MDD, MPR, LV/RNB Register, TR, ADC, BU, GBU)	Inhuizing, LV-Switch, Uithuizing, Einde Levering, PW-Switch, Wijziging Naam, Uitwisselen stamgegevens, MV-Switch, MV-beëindiging, muaties, melding meteropname, raadplegen aansluiting, Transactiedossier, Contactpersonen Contactgroep, Zoeken van aansluitingen, Toevoegen klantsleutel, Raadplegen aansluiting in pre-mutatiefase, Raadplegen aansluiting, Extract klantsleutels, Extract aansluitingen, Servicebeschrijving, Bulk PV-Switch, Distribueren stamgegevens bij GAIN, Kruisende processen, Contract Einde Register (CER), Uitwisselen meterstanden en verbruiken, Marktpartijenregister, Raadplegen leveranciers en netbeheerders, Wijzigen leveranciers en netbeheerders, Vooraankondiging einde levering, Uitwisselen individuele calorische waarden invoeders, Uitwisselen MeetCorrectieRapport, Gegevens primair deel meetinrichting, Stamgegevens meetinrichting, tarieven, Facturering en Afdracht, Uitwisseling datasets, Generieke Bestandsuitwisseling GBU	1.2/1.3
C-AR/Portaal (incl. sectorregister, CER, PUD, MDD, MPR, LV/RNB Register, TR, ADC, BU, GBU) (uitgaand: C-AR ==> applicatie)	Inhuizing, LV-Switch, Uithuizing, Einde Levering, PW-Switch, Wijziging Naam, Uitwisselen stamgegevens, MV-Switch, MV-beëindiging, mutaties, melding meteropname, raadplegen aansluiting, Transactiedossier, Contactpersonen Contactgroep, Zoeken van aanlsuitingen, Toevoegen klantsleutel, Raadplegen aansluiting in pre-mutatiefase, Raadplegen aansluiting, Extract klantsleutels, Extract aansluitingen, Servicebeschrijving, Bulk PV-Switch, Distribueren stamgegevens bij GAIN, Kruisende processen, Contract Einde Register (CER), Uitwisselen meterstanden en verbruiken, Marktpartijenregister, Raadplegen leveranciers en netbeheerders, Wijzigen leveranciers en netbeheerders, Vooraankondiging einde levering, Uitwisselen individuele calorische waarden invoeders, Uitwisselen MeetCorrectieRapport, Gegevens primair deel meetinrichting, Stamgegevens meetinrichting, tarieven, Facturering en Afdracht, Uitwisseling datasets, Generieke Bestandsuitwisseling GBU	1.2/1.3
C-ARM	Uitwisselen meetgegevens tijdseries, Uitwisselen meetgegevens volumes en meterstanden, Uitwisselen herzieningsverzoeken, Uitwisselen allocatiegegevens elektriciteit, Opvragen profielfracties elektriciteit, Aanbieden geaggregeerde volumes elektriciteit, Uitwisselen volumes voor settlement en reconciliatie elektriciteit, Uitwisselen settlementresulaten elektriciteit, Uitwisselen verzamelverrekenverzoek	1.2/1.3
CSS	Centraal Systeem Stuursignaal (CSS)	1.2
Data delen platform	Publiceren Calorische Waarden	1.2/1.3
EAN-codeboek	Raadplegen EAN Codeboek Energie	1.2
Gopacs		1.2/1.3
Gopacs (uitgaand)		1.2
Nexus	Service specification Wholesale gas Allocation and Reconciliation message exchange	1.2/1.3
Nexus (inkomend)	Service specification Wholesale gas Allocation and Reconciliation message exchange	1.2
OAD	Raadplegen aansluiting voor derden	1.2/1.3

Applicatie	Business Services	TLS versies
Portaal CTS	Raadplegen historische dagstanden slimme meter, Opvragen meterstanden slimme meter P4	1.2/1.3
SQL - PowerBI		1.2
TMR	Raadplegen TMR in pre-mutatiefase, Raadplegen TMR, Opvragen meterstanden slimme meter P4	1.2/1.3
TMR (inkomend)	Raadplegen TMR in pre-mutatiefase, Raadplegen TMR, Opvragen meterstanden slimme meter P4	1.2

4.2.2 Centrale systemen in beheer bij TenneT

< nog geen input ontvangen>

4.3 Bijlage 3 – Configuratie TLS 1.3

De onderstaande configuratie is afkomstig uit het Adviesrapport overgang naar TLS 1.3 uit 2020 en is op 15-02-2023 door de CoP Secure Architecture gereviewd.

Sleutel-uitwisseling	Certificaat-verificatie	Bulkversleuteling	Elliptische functies	Finite-field groepen	RSA Sleutellengte
ECDHE - goed DHE - voldoende	ECDSA - goed RSA - goed	TLS_AES_256_GCM_SHA383(384?) - goed TLS-AES128-GCM-SHA256 - goed TLS-AES256-GCM-SHA384 -> goed TLS-CHACHA20-POLY1305-SHA256 - goed TLS-AES128-CCM-SHA256 - onvoldoende	Sep384rl - goed Sep256rl - goed X448 - goed x25519 - goed	ffdhe4096 - voldoende ffdhe3072 - voldoende	> 3072 bit - goed 2048 – 3071 bit - voldoende

- De onderdelen aangemerkt met **onvoldoende** zijn niet langer toegestaan – indien deze onderdelen nog worden gehanteerd, moeten deze worden vervangen.
- De onderdelen aangemerkt met goed en voldoende mogen nog worden gehanteerd. Daarbij geldt als vuistregel dat de onderdelen aangemerkt met voldoende binnen vijf jaar (dus voor 31-12-2028) moeten worden vervangen door meer moderne versies.