

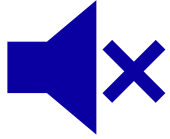
Voorlichting Invoering TLS 1.3

16 MEI 2023



Welkom bij de voorlichting Invoering TLS 1.3

– Topic 22.T08.F06



Zet je microfoon
op **mute**.



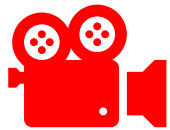
Zet je camera
uit.



Stel je vragen via **de chat**. We werken met
een moderator.



Presentatie op
mijnMFFBAS.



**Sessie wordt
opgenomen.**



Sessie is 4 weken
beschikbaar. Mail
projecten@mffbas.nl



Opname is voor
genodigden.



1. Introductie

Mirjam van der Horst



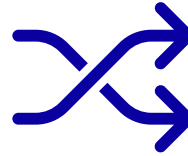
Agenda

1. Introductie (Mirjam van der Horst)
2. Wat is TLS? (John van der Stap)
3. Waarom van TLS 1.2 naar TLS 1.3? (John van der Stap)
4. Welke veranderingen brengt TLS 1.3 met zich mee?
 - a. Algemeen (John van der Stap)
 - b. Centrale systemen EDSN (Jurjan Woltman)
 - c. Centrale systemen TenneT (Jan Heerschop)
5. Organisatie & planning (Amanda Zachariasse)
6. Documentatie & communicatie (Amanda Zachariasse)

Doel van de voorlichting



Wat is TLS?



Waarom van TLS 1.2
naar TLS 1.3? Wat
verandert er?



Centrale systemen:
system readiness



Inzicht in planning
en overgangscriteria



Documentatie &
communicatie



2. Wat is TLS 1.3?

John van der Stap

Wat is TLS?

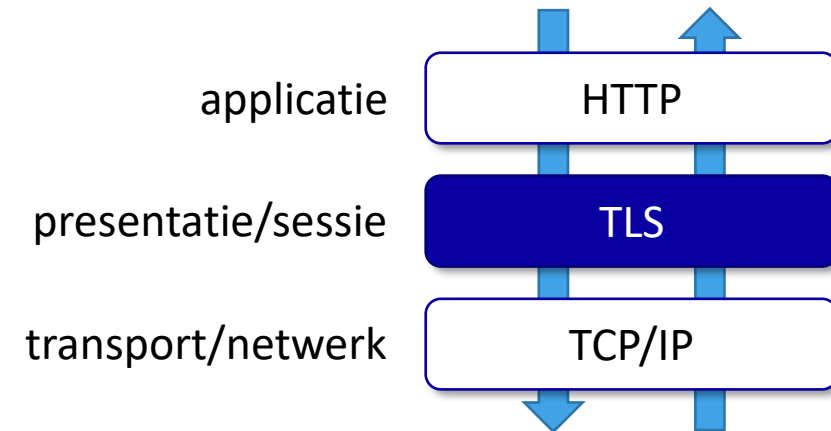
Transport Layer Security – veilige verbinding door encryptie en authenticatie

Wat is TLS?

- ✓ TLS (Transport Layer Security) is een beveiligingsprotocol voor gegevensbeveiliging
- ✓ Veilige HTTP(S)-verbinding door encryptie en authenticatie
- ✓ Zit tussen HTTP en TCP/IP

Historie

- ✓ TLS 1.2 bestaat sinds 2008, TLS 1.3 sinds 2018
- ✓ Energiesector werkt met TLS 1.2 sinds 2016





Wat is TLS?

Transport Layer Security – veilige verbinding door encryptie en authenticatie

TLS

- TLS is een protocol dat tot doel heeft om beveiligde verbindingen over het internet te verzorgen.
- TLS 1.2 bestaat sinds 2008. Het veiligheidsniveau van dit protocol loopt achteruit. Het Nationaal Cyber Security Center (NCSC) heeft de beoordeling van het protocol in januari 2021 afgewaardeerd van **goed** naar **voldoende**.
- De opvolger TLS 1.3 is beschikbaar, maar nog niet overal ingevoerd.

TLS binnen de energiesector

- Sinds 2016 wordt TLS 1.2 gebruikt voor het berichtenverkeer in de sector.
- Om te zorgen voor een veilige uitwisseling van informatie in de sector is de invoering van TLS 1.3 vastgelegd in issue TC043. Dit issue is op 11 november 2020 vastgesteld door de ALV NEDU.



3. Waarom van TLS 1.2 naar TLS 1.3?

John van der Stap

Waarom van TLS 1.2 naar TLS 1.3?

Sectorbreed waarborgen van veilige gegevensuitwisseling



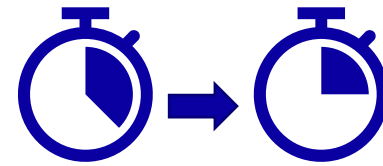
Urgentie

TLS 1.2 is 'op leeftijd', kent geen nieuwe ontwikkelingen en de kans op meer kwetsbaarheden neemt toe



Security

Betrouwbaarder en veiliger dan TLS 1.2.



Snelheid

Verbeterde handshake



Afgesproken

- ✓ Issue TC043 is vastgesteld
- ✓ 31-12-2023 alle systemen over op TLS 1.3
- ✓ Invoeringsplan is vastgesteld in ALV MFF



Waarom van TLS 1.2 naar TLS 1.3?

Sectorbreed waarborgen van veilige gegevensuitwisseling

Voordelen

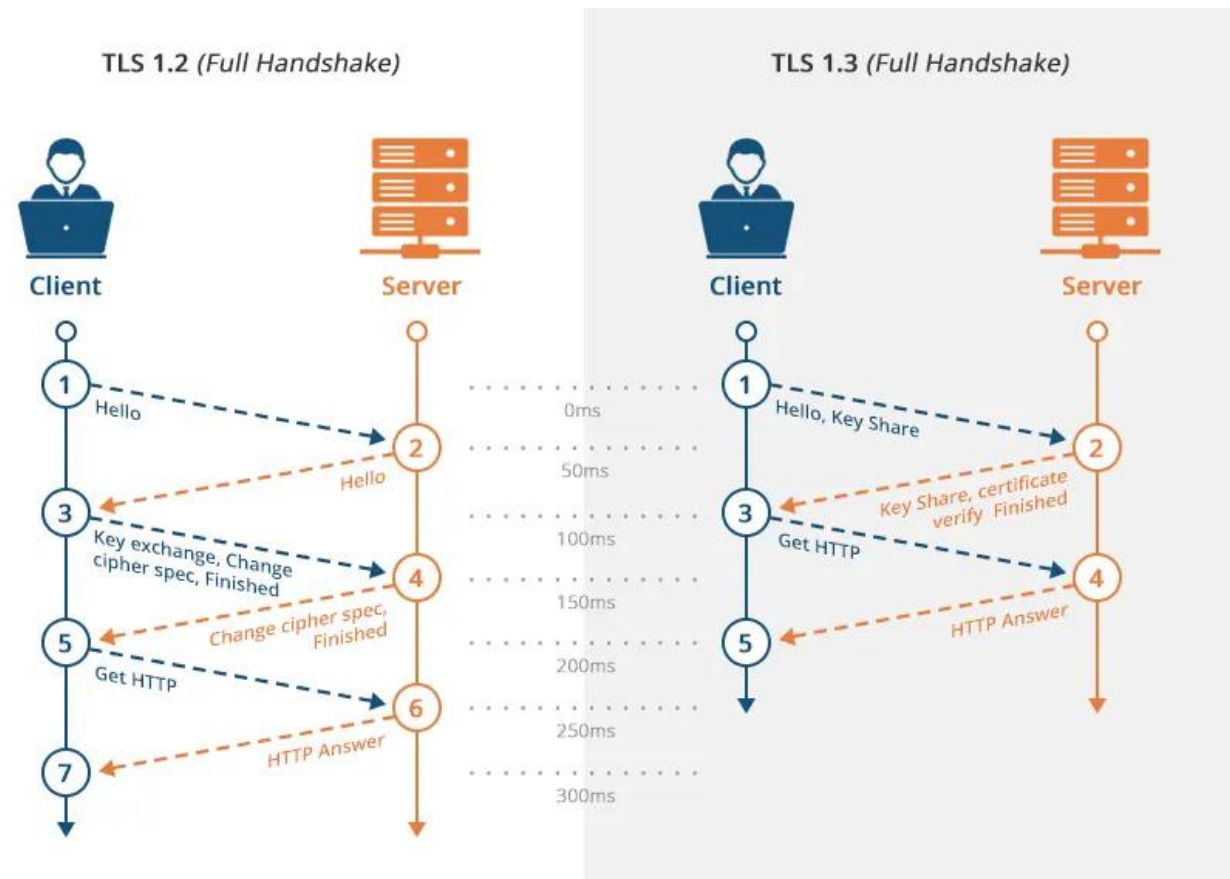
- Met TLS 1.3 wordt een verbetering in de snelheid van berichtenverkeer bewerkstelligd, omdat het protocol tussen server en client minder stappen bevat.
- De security van TLS 1.3 is meer robuust en het heeft verbeterde encryptie-algoritmen die geen bekende zwakheden bevatten.
- Kortom: TLS 1.3 zorgt voor snellere uitwisseling en betere beveiliging van berichtenverkeer.

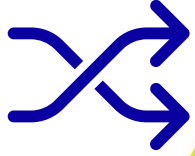
Sectorafspraken

- Om te zorgen voor een veilige uitwisseling van informatie in de sector is de invoering van TLS 1.3 vastgelegd in issue TC043. Dit issue is op 11 november 2020 vastgesteld door de ALV NEDU.
- Op 9 maart 2022 heeft de ALV NEDU besloten om TLS 1.2 voor de uitwisseling van de berichten niet langer toe te staan dan tot uiterlijk einde 2023.

Waarom van TLS 1.2 naar TLS 1.3?

TLS 1.3 is sneller dan TLS 1.2





4. Wat verandert er met TLS 1.3?

a. Algemeen

John van der Stap

Wat verandert er met TLS 1.3? - Algemeen

Impact op hoofdlijnen



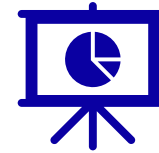
Scope

- Alle koppelingen tussen de centrale en decentrale systemen
- Overzicht van de centrale systemen zie dia's: 21-24 (EDSN) en 25-37 (TenneT)



Wijziging

- Geen certificaatwissel vereist
- Endpoints blijven in principe gelijk
- Duale periode ten minste van 1-7-2023 t/m 31-12-2023



Overgang

- Monitoring op de centrale systemen
- Let op: marktpartijen kunnen direct aan de slag met implementatie van TLS 1.3
Testen van communicatie met de centrale systemen die TLS 1.3-ready zijn



Wat verandert er met TLS 1.3? - Algemeen

Impact op hoofdlijnen

Scope

- Alle koppelingen tussen centrale en decentrale systemen zijn in scope.

Wijziging

- Voor de invoering van TLS 1.3 is geen certificaatwissel vereist.
- In principe is er geen wijziging van endpoints: huidige endpoints ondersteunen TLS 1.2 en TLS 1.3.
- De duale periode per systeem in het CMF-landschap start uiterlijk 1 juli 2023.

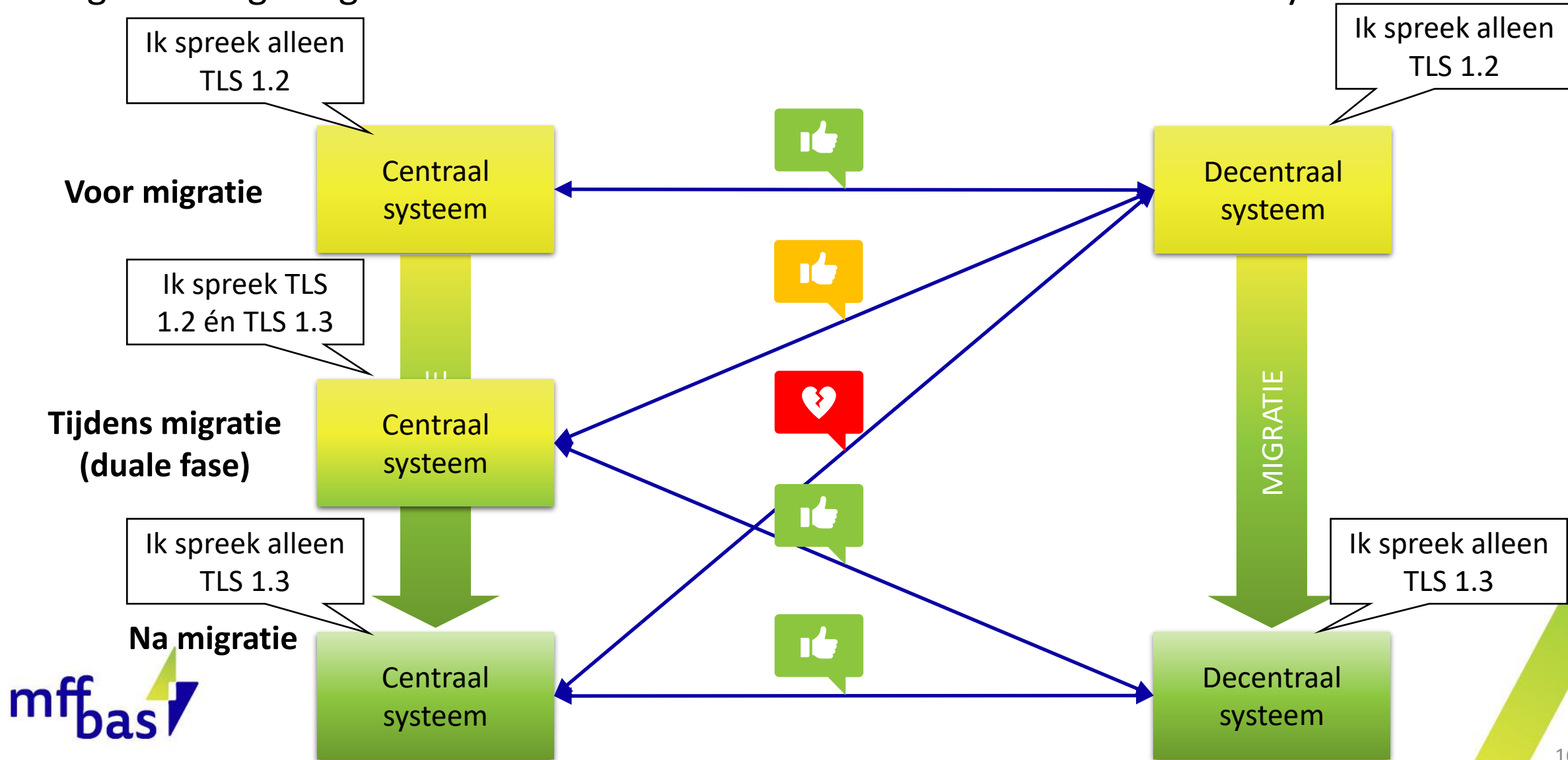
Overgang

- Marktpartijen hoeven niet te wachten tot alle centrale systemen over zijn op TLS 1.3.
- Marktpartijen dienen de overgang naar TLS 1.3 eerst te testen op de testomgevingen van de centrale systemen.
- Er is geen sprake van sectortesten. Wel zijn de standaardtestomgevingen van de systemen in het CMF-landschap beschikbaar voor testen.
- Er is een 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 eindigt uiterlijk 1 januari 2024. In afstemming met de ALV MFF kan besloten worden om de duale periode langer te laten duren.
- Na besluitvorming in de ALV MFF wordt TLS 1.2 uitgefaseerd.



Wat verandert er met TLS 1.3? - Algemeen

Migratie en gevolgen voor communicatie tussen centrale en decentrale systemen



Wat verandert er met TLS 1.3? - Algemeen

Wat als updaten naar TLS 1.3 niet wordt ondersteund of veel werk geeft?



Probleem

- Onvoldoende tijd of capaciteit
- Software niet TLS 1.3-ready



Oplossing

- Plaats een proxyserver

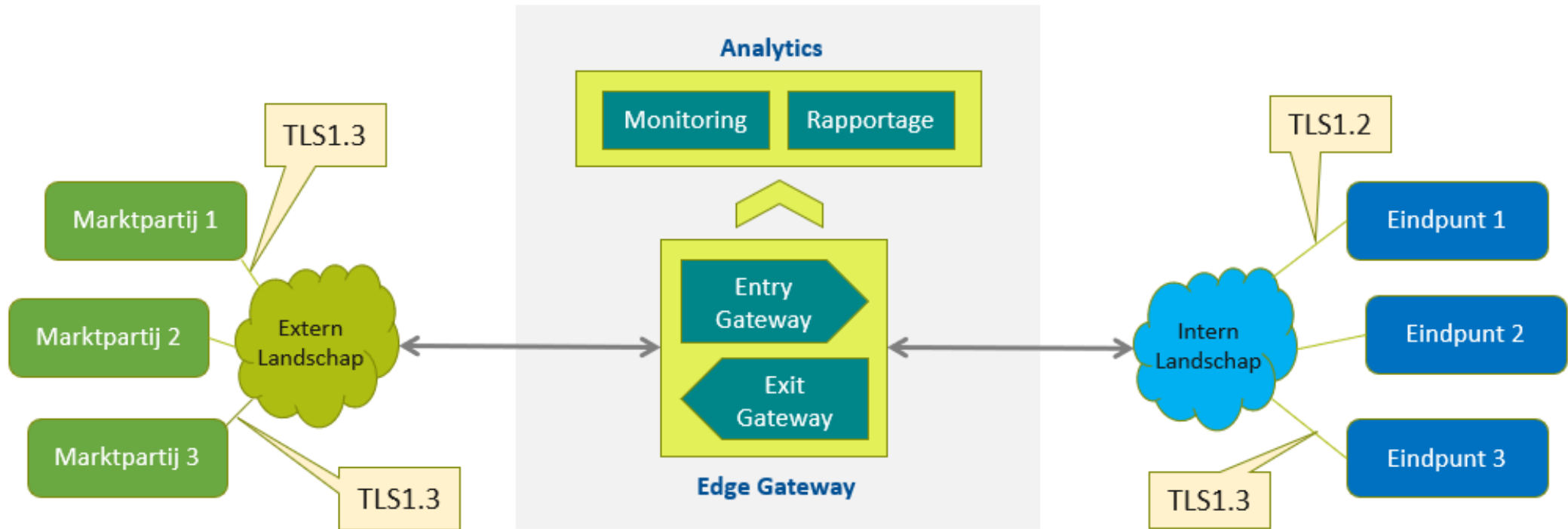


Voordelen

- Continuering data-uitwisseling
- In eigen tijd systemen upgraden naar TLS 1.3

Wat verandert er met TLS 1.3? - Algemeen

Voorbeeld inzet proxyserver (praktijkvoorbeeld EDSN)





Wat verandert er met TLS 1.3? - Algemeen

Wat als updaten naar TLS 1.3 niet wordt ondersteunt of veel werk geeft?

Probleem

Er is onvoldoende tijd of er zijn te weinig mensen om de interne systemen tijdig aan te passen.
Of een softwarefabrikant heeft zijn software nog niet aangepast om via TLS 1.3 te communiceren.

Mogelijk gevolg

in het ergste geval is er geen communicatie meer mogelijk met de centrale systemen.

Oplossing

Het plaatsen van een proxyserver tussen het decentrale systeem en het internetverkeer.
Door TLS 1.2-verkeer om te zetten naar TLS 1.3 kan de proxyserver de veiligheid van de communicatie verbeteren en ervoor zorgen dat de client en de server beide de meest recente beveiligingsprotocollen gebruiken.

Voordeel:

Je koopt tijd om interne systemen naar TLS 1.3 te upgraden.

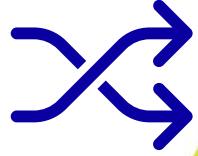


Wat verandert er met TLS 1.3? - Algemeen

Instellingen & cipher suites voor TLS 1.3 – goed en voldoende werkend voor TLS 1.3

Waardering NCSC	Sleutel-uitwisseling	Certificaat-verificatie	Bulkversleuteling en hashing	Elliptische functies	Finite-field groepen	RSA sleutellengte
Goed	• ECDHE	• ECDSA • RSA	• TLS-AES256-GCM-SHA256 • TLS-AES256-GCM-SHA384 • TLS-CHACHA20-POLY1305-SHA256	• Sep384r1 • Sep256r1 • X448 • X25519		• > 3072 bit
Voldoende	• DHE				• ffdhe4096 • ffdhe3072	• 2048 – 3071 bit
Onvoldoende			• TLS-AES128-CM-SHA256			

Voor uitgebreide beschrijving over waardering van de instellingen, zie de meest recente [richtlijnen van het NCSC](#)



4. Wat verandert er met TLS 1.3?

b. Centrale systemen EDSN

Jurjan Woltman



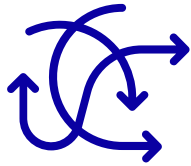
Wat verandert er met TLS 1.3? - EDSN

Systemen en subsystemen

Systeem	TLS 1.2	TLS 1.3	Toelichting
Axway API Gateway, Axway B2Bi , KONG gateway, Toestemmingsplatform, Energiedatalink Provider, CERES			
C-AR/Portaal (incl. sectorregister, CER, PUD, MDD, MPR, LV/RNB Register, TR, ADC, BU, GBU) (inkomend)			
C-AR/Portaal (incl. sectorregister, CER, PUD, MDD, MPR, LV/RNB Register, TR, ADC, BU, GBU) (uitgaand: C-AR ==> applicatie)			
C-ARM			
Data delen platform			
EAN-codeboek			
Gopacs (inkomend)			
Nexus (uitgaand)			
Portaal CTS			
TMR (uitgaand)			
CSS			Wordt 30-6-2023 geïmplementeerd
Gopacs (uitgaand: Gopacs ==> Applicatie)			Wordt 30-6-2023 geïmplementeerd
Nexus (inkomend: Applicatie ==> Nexus))			Wachtend bevestiging applicatieteam. Best-effort 30-06-2023.
TMR (inkomend: Applicatie ==> TMR)			Wachtend bevestiging applicatieteam. Best-effort 30-06-2023.

Wat verandert er met TLS 1.3? - EDSN

Verandering, testen, ondersteuning



Verandering

- EDSN behoudt zo veel mogelijk de huidige endpoints om verbinding te maken met de applicaties



Testen

- Testen kan via de reguliere weg en op eigen gelegenheid



Ondersteuning

- EDSN servicedesk (servicedesk@edsn.nl) staat voor je klaar. Zet in het onderwerp: TLS 1.3 - <Applicatiennaam> - Probleem/vraag



Wat verandert er met TLS 1.3? - EDSN

Verandering, testen, ondersteuning

Verandering

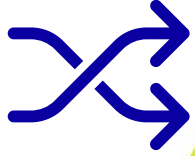
- EDSN behoudt zo veel mogelijk de huidige endpoints om verbinding te maken met de applicaties (dual).

Testen

- Testen kan op eigen gelegenheid op de test-/acceptatie-omgevingen.

Ondersteuning

- Mocht het niet lukken, dan staat de servicedesk van EDSN voor je klaar.
- Mocht het niet lukken om verbinding te maken met gebruik van TLS 1.3? Mail dan naar:
 - servicedesk@edsn.nl
 - Met in het onderwerp: TLS1.3 - <Applicatiennaam> - Probleem/vraag
 - Dan nemen we zo spoedig mogelijk contact met je op.



4. Wat verandert er met TLS 1.3?

c. Centrale systemen TenneT

Jan Heerschop



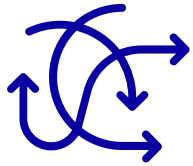
Wat verandert er met TLS 1.3? - TenneT

Systemen en subsystemen

Systeem	TLS 1.2	TLS 1.3	Toelichting
MMC Hub			Gereed, instellingen moeten nog worden gedaan
CPS		Planned	
TQF			Q2 not feasible
APFAS			Q2 not feasible, possibly done via MMC Hub
OSB voor legacy websites			Change is onderhanden en op plan
CBP			Supplier contacted
GOPACS adapter		Planned	Awaits confirmation of GOPACS team
FCR webservices			Q2 not feasible, possibly done via MMC Hub
API Gateway (KONG)		Planned	
MHS		Planned	Supplier TIBCO has not yet confirmed readiness

Wat verandert er met TLS 1.3? - TenneT

Verandering, testen, ondersteuning



Verandering

- TenneT behoudt indien mogelijk de huidige endpoints om verbinding te maken met de applicaties.



Testen

- Testen kan via de reguliere weg en op eigen gelegenheid.



Ondersteuning

- Via het TenneT Customer Care Center:
tennetccc@tennet.eu



5. Planning & organisatie

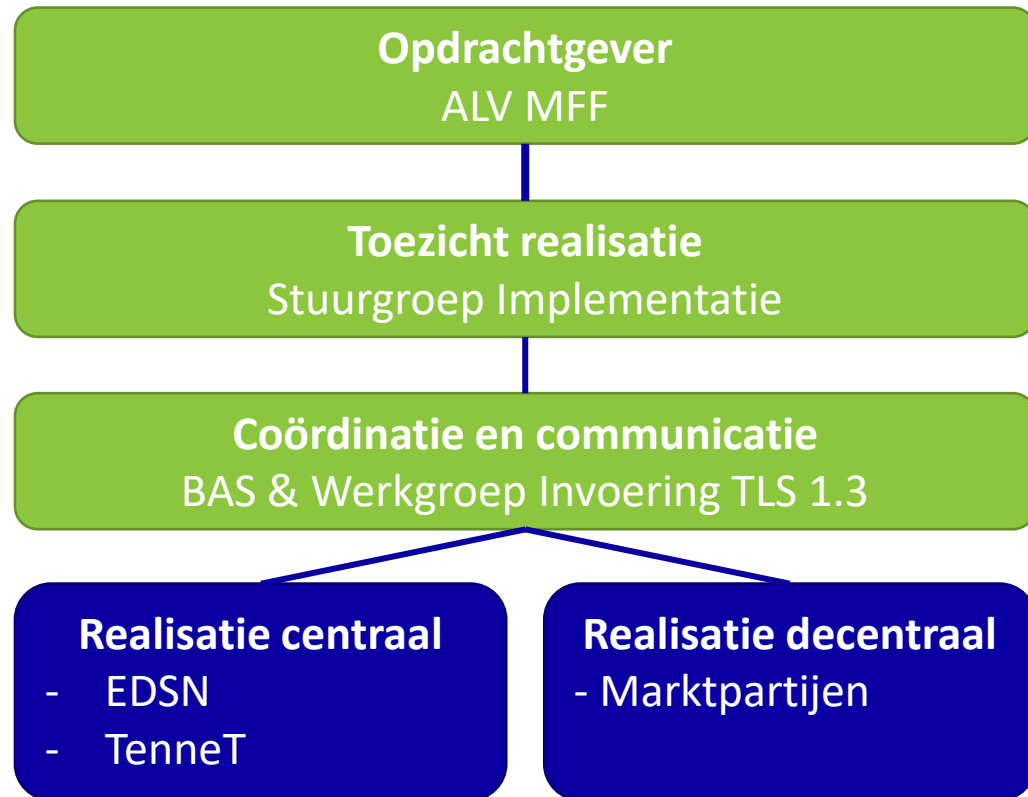
Amanda Zachariasse



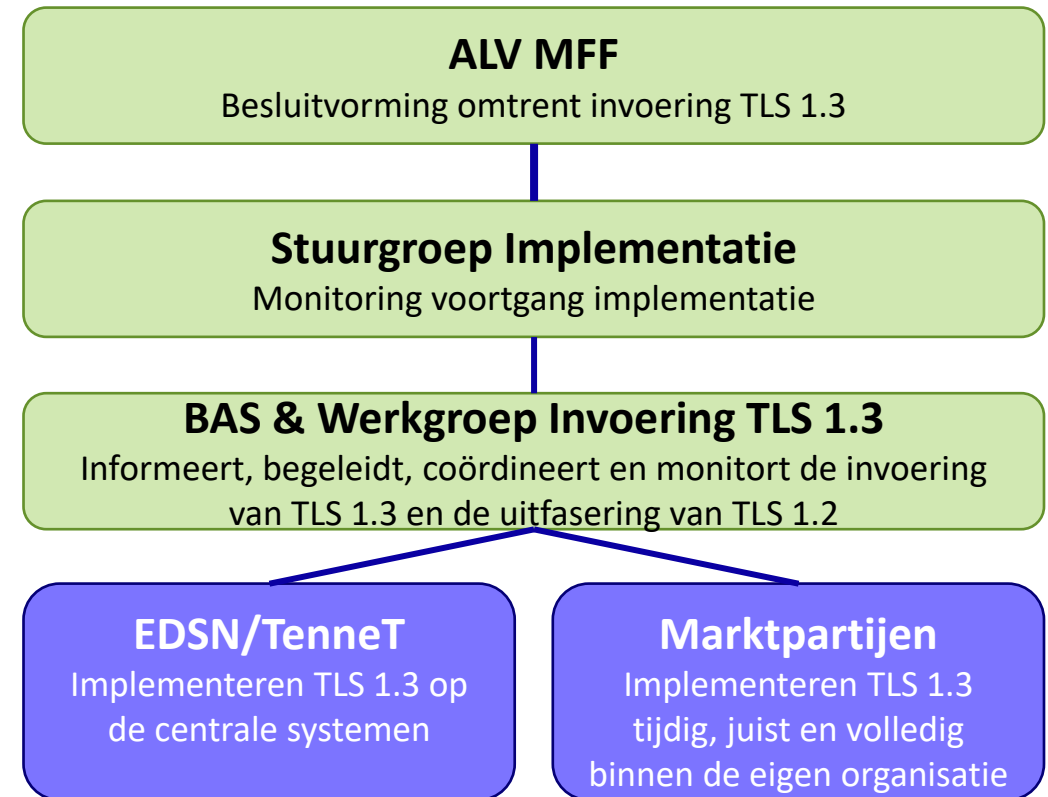
Planning & organisatie

Organisatie

Organisatiestructuur



Verantwoordelijkheden





Planning & organisatie

Organisatie

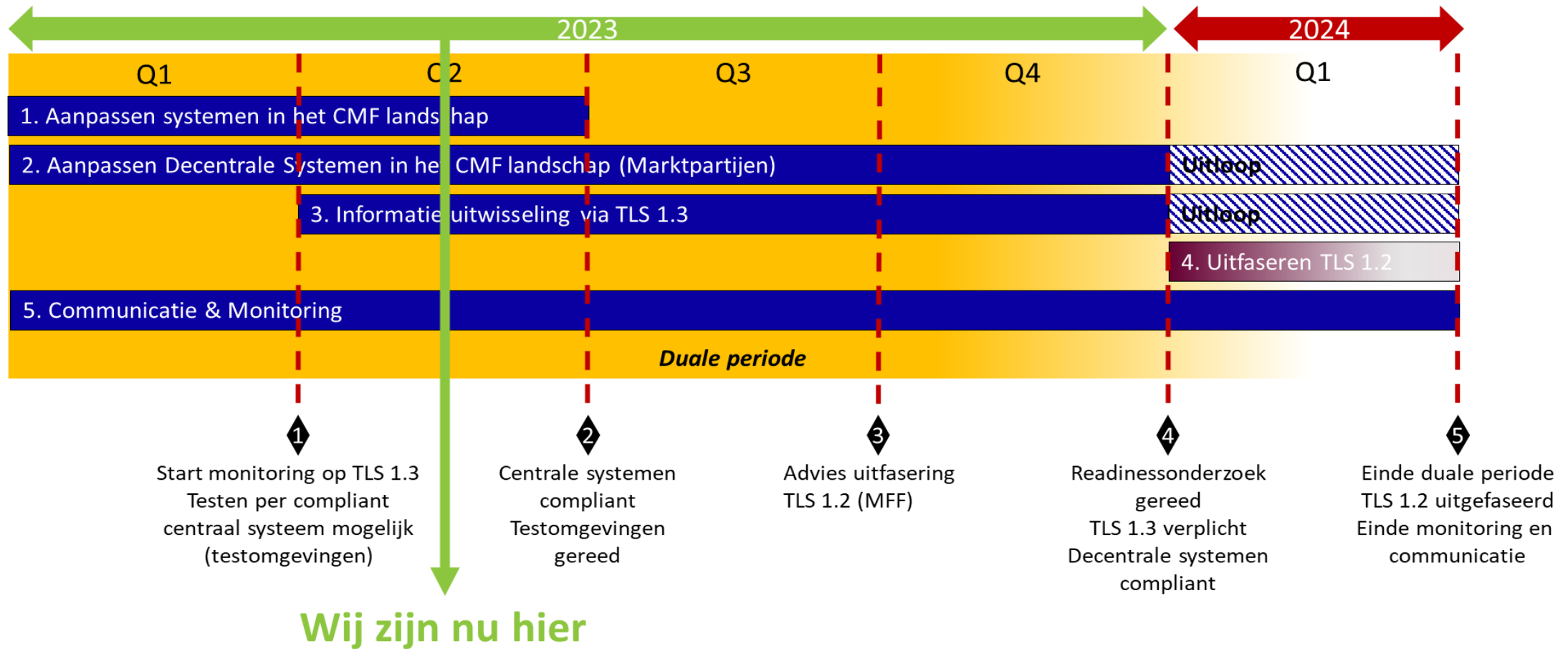
Werkgroepleden – Werkgroep Invoering TLS 1.3

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

- 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.

Planning & organisatie

Alle marktpartijen en (de)centrale systemen gaan in 2023 over op TLS 1.3



Planning & organisatie

IJkmomenten en acceptatiecriteria

Monitoring & rapportage TLS 1.3-readiness



1 juli 2023

Toetsing TLS 1.3-
readiness centrale systemen



Eind Q3

Toetsing TLS 1.3-readiness
marktpartijen (decentrale
systemen)



Acceptatiecriteria

- 100% readiness centrale systemen
- Decentrale systemen 66,66% gewogen marktaandeel marktpartijen



Planning & organisatie

Ijkmomenten en acceptatiecriteria

- 1 juli 2023 toetsen readiness centrale systemen, rapportage ALV MFF
- Eind Q3 toetsen readiness marktpartijen, rapportage ALV MFF
- 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.



6. Documentatie & communicatie

Amanda Zachariasse



Documentatie & communicatie

Alle relevante documenten zijn terug te vinden op mijnMFFBAS

 Mijn MFFBAS

SharePoint

Relevante documentatie is te raadplegen via mijnMFFBAS.

Toegang aanvragen, ook voor niet leden



Dashboard

Maandelijks update van de readiness van de centrale systemen in het dashboard, ook op mijnMFFBAS



Nieuwsbrief

Regelmatig zal een update worden gegeven via de nieuwsbrief



Monitoring

EDSN en TenneT passen monitoring toe op alle centrale systemen om de overgang van marktpartijen naar TLS 1.3 te monitoren



Documentatie & communicatie

Communicatielinks

- Het issuedocument is vastgesteld op 12 november 2020 in de ALV NEDU. De einddatum voor TLS 1.2 is vastgesteld op 9 maart 2022 in de ALV NEDU. Het uitvoerings- en communicatieplan is 8 maart 2023 vastgesteld in de ALV MFF.
- Het vastgestelde issuedocument, uitvoerings- en communicatieplan, de voorlichting, Q&A zijn te vinden op mijnMFFBAS: Release/TLS 1.3. [TLS 1.3 - Introductiepagina \(sharepoint.com\)](#)
- RFC's of andere belangrijke mededelingen worden gecommuniceerd via de nieuwsbrief. Nog geen abonnement, abonneer je op de gratis nieuwsbrief via communicatie@mffbas.nl
- Als je als marktpartij vragen hebt over dit topic, kun je deze stellen via projecten@mffbas.nl
- EDSN servicedesk (servicedesk@edsn.nl) staat voor je klaar. Zet in het onderwerp: TLS1.3 - <Applicatiennaam> - Probleem/vraag.
- Via het TenneT Customer Care Center: tennetccc@tennet.eu

Samenvatting Invoering TLS 1.3

De overgang naar TLS 1.3 kan door iedere marktpartij **vanaf nu** in gang gezet worden, op alle centrale systemen die TLS 1.3-ready zijn.



Wat is TLS?

TLS (Transport Layer Security) is een beveiligingsprotocol voor gegevensbeveiliging



Waarom TLS 1.3?

- ✓ TLS 1.2 wordt kwetsbaarder
 - ✓ Sneller, veiliger en toekomstbestendig
- ✓ Conform Issue TC043



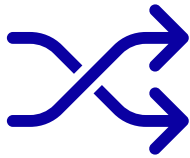
Planning

- ✓ 1-7-2023 Centrale Systemen TLS 1.3-ready
- ✓ 31-12-2023 marktpartijen TLS 1.3-ready



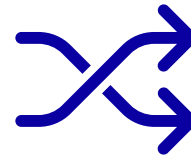
Documentatie & communicatie

- ✓ Publicaties op mijnMFFBAS
- ✓ Nieuwsbrieven



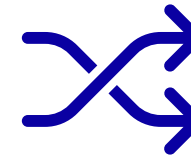
Algemeen

- Alle koppelingen tussen de centrale en decentrale systemen
- Van TLS 1.2 naar TLS 1.3 zonder certificaatwissel



EDSN

- Endpoints zo veel mogelijk gelijk
- Testen op eigen gelegenheid
- Helpdesk beschikbaar voor support



TenneT

- Endpoints zo veel mogelijk gelijk
- Testen op eigen gelegenheid
- Helpdesk beschikbaar voor support

Dank voor jullie aandacht en
succes!

