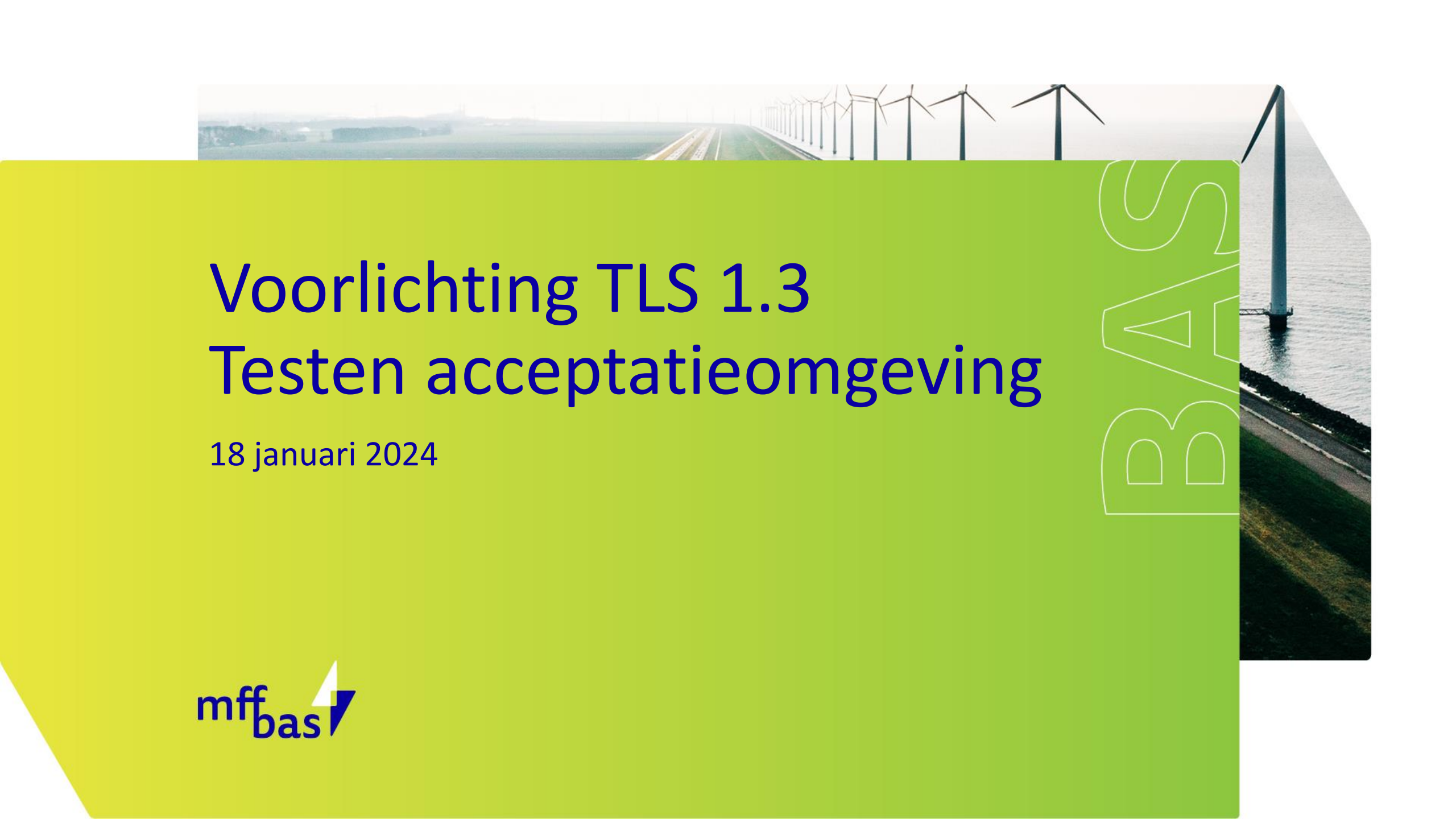


BAS

mff
bas





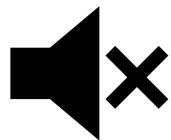
Voorlichting TLS 1.3

Testen acceptatieomgeving

18 januari 2024

Welkom bij de voorlichting TLS 1.3

Testen acceptatieomgeving



Zet je microfoon op **mute**.



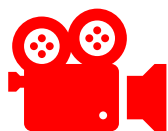
Zet je camera **uit**.



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 geïnteresseerden met jullie goedkeuring.



Alle vragen en antwoorden komen op **mijnMFFBAS**.

TLS 1.3

Einde duale fase 1 april 2024



1. Introductie

Mirjam van der Horst

Agenda

1. Introductie (Mirjam van der Horst)
2. TLS 1.3 in vogelvlucht (Arjan Visser)
3. EDSN – Testen op acceptatieomgeving (Leander Hiele)
4. TenneT – Testen op acceptatieomgeving (Gerwin Bruynooge)
5. Naslagwerk (Amanda Zachariasse)



2. TLS 1.3 in vogelvlucht

Arjan Visser

Wat is TLS?

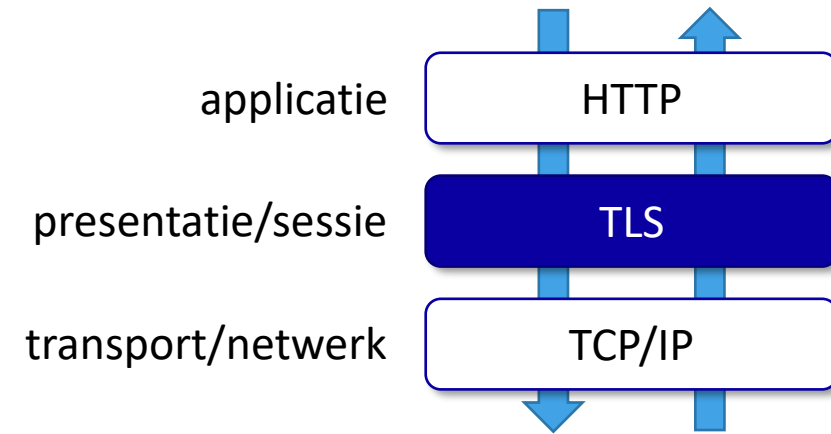
Transport Layer Security – veilige verbinding door encryptie en authenticatie

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



Waarom van TLS 1.2 naar TLS 1.3?

Sectorbreed waarborgen van veilige gegevensuitwisseling



Urgentie

TLS 1.2 is 'op leeftijd', en de kans op meer kwetsbaarheden neemt toe.

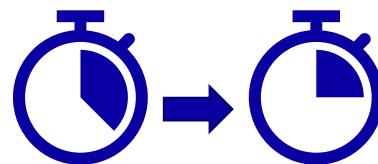
De security van TLS 1.3 is meer robuust en heeft verbeterde encryptie-algoritmen die geen bekende zwakheden bevatten.



Security

TLS 1.3 is betrouwbaarder en veiliger dan TLS 1.2.

Het Nationaal Cyber Security Center (NCSC) heeft TLS 1.2 in januari 2021 afgewaardeerd van **goed** naar **voldoende**.



Snelheid

TLS 1.3 geeft een verbetering in de snelheid van berichtenverkeer, doordat het protocol tussen server en client minder stappen bevat



Afgesproken

- ✓ Issue TC043 is 11/11/20 vastgesteld door ALV NEDU
- ✓ 31-3-2024 alle systemen over op TLS 1.3
- ✓ Invoeringsplan is vastgesteld in ALV MFF



3. EDSN – Testen op acceptatieomgeving

Leander Hiele

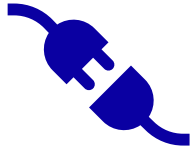
Testen op acceptatieomgeving

Systemen en subsystemen

Systeem	URL acceptatie	Periode alleen TLSv1.3
Axway API Gateway, Axway B2Bi , KONG gateway, Toestemmingsplatform, Energiedatalink Provider, CERES	b2b.gateway-acc.edsn.nl / gateway-acc.edsn.nl	Beschikbaar vanaf 22-1-2024 0 9:00 uur
C-AR/Portaal	portaal-act.edsn.nl	Beschikbaar vanaf 22-1-2024 0 9:00 uur
C-ARM	arm-act2.edsn.nl	Beschikbaar vanaf 22-1-2024 0 9:00 uur
Data delen platform	api.acc.mijnenergieedata.nl www.acc.mijnenergieedata.nl	Beschikbaar vanaf 22-1-2024 0 9:00 uur
EAN-codeboek	b2b.gateway-acc.edsn.nl / gateway-acc.edsn.nl	Beschikbaar vanaf 22-1-2024 0 9:00 uur
Gopacs	N.v.t	N.v.t
Nexus	N.v.t.	N.v.t.
Portaal CTS	pp4-test.edsn.nl	Beschikbaar vanaf 22-1-2024 0 9:00 uur
TMR	N.v.t.	N.v.t
CSS	https://css-dat3.edsn.nl/css/	Is al live i.v.m. andere endpoint.

Support

Connecteren, testen, support



Verbinden

- CSS heeft alleen een andere endpoint, overige systemen behouden de bestaande;
- Voor het testen is er mogelijk een test certificaat nodig. Als deze niet aanwezig is of verlopen is. Stuur dan een test-certificaat verzoek naar: servicedesk@edsn.nl



Testen

- Testen kan via de reguliere weg en op eigen gelegenheid. Eventuele support staat voor jullie klaar voor de benoemde systemen.



Support

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



4. TenneT – Testen op acceptatieomgeving

Gerwin Bruynooge

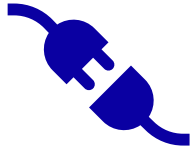
Testen op acceptatieomgeving

Systemen en subsystemen

System (Acceptatie)	Alleen TLS 1.3	Per datum
MMC Hub	YES	1-2-2024
CPS	Mailsysteem; blijft ook TLS 1.2 ondersteunen	1-2-2024
TQF	Back-end systeem	1.3 ready
APFAS	Back-end systeem	
OSB voor legacy websites	Back-end systeem	1.3 ready
CBP	Back-end systeem	1.3 ready
GOPACS adapter	Back-end systeem	1.3 ready
FCR webservices	Back-end systeem	1.3 ready
API Gateway (KONG) / TMAC	Back-end systeem	1.3 ready
MHS	Back-end systeem	1.3 ready
TIBCO	Back-end systeem	
My.TenneT.eu	Wegens technische storing is My.TenneT.eu tijdelijk niet beschikbaar voor testen met TLS 1.3	

Support

Connecteren, testen, support



Verbinden

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



Testen

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



Support

- Via het TenneT Customer Care Center:
tennetccc@tennet.eu
- Inhoudelijke vragen naar de PO
- Algemene vragen naar BAS



5. Naslagwerk

Amanda Zachariasse



Op de hoogte blijven

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



Updates

Updates zullen geplaatst worden in de SharePoint omgeving mijn MFFBAS.

Bijv. over de omzetting van de acceptatieomgevingen.



Nieuwsbrief

Regelmatig zal een update worden gegeven via de nieuwsbrief



Monitoring

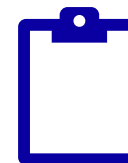
Alle marktpartijen kunnen op eigen gelegenheid testen op de acceptatieomgeving van EDSN en TenneT.



Bellen

Alle marktpartijen worden telefonisch benaderd om de market readiness te inventariseren.

Zorg ervoor dat de contactgegevens up-to-date zijn via Partners in Energie.



Uiterste market readiness

In februari zal nog een laatste uitvraag worden gedaan per mail, waarin marktpartijen kunnen aangeven dat zij NIET klaar zijn.

Quick Reference Card: TLS 1.3



TLS 1.3

Wat is TLS?

Transport Layer Security is een beveiligingsprotocol voor gegevensbeveiliging. Infosheet NCSC over TLS – [hier downloaden](#)

Waarom TLS 1.3?

TLS 1.2 wordt kwetsbaarder. TLS 1.3 is sneller, veiliger en toekomstbestendiger. Er zijn marktafspraken gemaakt om TLS 1.3 toe te passen.



Informatieoverzicht

Direct naar alle documenten: <https://mffbas.sharepoint.com/sites/TLS1.3>

- ☐ [1. Dashboard readiness centrale systemen en marktpartijen](#)
- ☐ [2. Voorlichtingssessie TLS 1.3 16 mei 2023](#) (presentatie, vraag & antwoord)
- ☐ [3. Instellingen en endpoints](#)



Helpdesk

Vermeld altijd in het onderwerp van de e-mail 'TLS 1.3' en waar mogelijk ook de naam van de applicatie.

EDSN - servicedesk@edsn.nl

Inhoudelijke vragen en vragen gerelateerd aan de systemen van EDSN.

TenneT - tennetccc@tennet.eu

Inhoudelijke vragen en vragen gerelateerd aan de systemen van TenneT.

MFFBAS - projecten@mffbas.nl

Vragen over planning en organisatie.



Systemen binnen CMF-landschap

EDSN

Einddatum TLS 1.2: 01-04-2024
14 centrale systemen in CMF-landschap

- | | |
|------------------------|-----------------------|
| 1. Axway API Gateway | (inkomend) |
| 2. C-AR (inkomend) | 8. Nexus (uitgaand) |
| 3. C-AR (uitgaand) | 9. Portaal CTS |
| 4. C-ARM | 10. TMR (uitgaand) |
| 5. Data delen platform | 11. CSS |
| 6. EAN-codeboek | 12. Gopacs (uitgaand) |
| 7. Gopacs | 13. Nexus (inkomend) |
| | 14. TMR (inkomend) |

TenneT

Einddatum TLS 1.2: 01-04-2024
10 centrale systemen in CMF-landschap

- | | |
|-----------------------------|------------------------|
| 1. MMC Hub | 7. GOPACS adapter |
| 2. CPS | 8. FCR webservices |
| 3. TQF | 9. B2B gateway |
| 4. APFAS | 10. API Gateway (KONG) |
| 5. OSB voor legacy websites | |
| 6. CPB | |

Bovenstaande systemen zijn de hoofdsystemen. De verbindingen en onderliggende systemen zijn terug te vinden in de documentatie op mijn MFFBAS onder: 1. dashboard of 2. voorlichting.



Instellingen

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			

De instellingen zijn ook terug te vinden in de presentatie van de online voorlichting en onder instellingen.