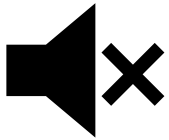
BAS B.V. // 18 January 2024 // AMERSFOORT

# Information session TLS 1.3
# Testing acceptance environment

18 January 2024

# Welcome to the information session TLS 1.3 Testing acceptance environment

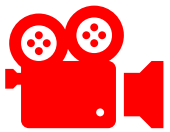


**Mute** your microphone.

Turn **off** your camera.

Ask questions via **the chat feature.** We are working with a moderator.

Presentation on **mijnMFFBAS.**



**The session is being recorded.**

The session will be **available** for 4 weeks. E-mail projecten@mffbas.nl

Recording is taking place for interested parties, with your approval.


All questions and answers will be placed on mijnMFFBAS.

# TLS 1.3

End dual phase 1 April 2024

# 1. Introduction

Mirjam van der Horst

# Agenda

1. Introduction (Mirjam van der Horst)
2. An overview of TLS 1.3 (Arjan Visser)
3. EDSN – Testing on acceptance environment (Leander Hiele)
4. TenneT – Testing on acceptance environment (Gerwin Bruynooge)
5. References (Amanda Zachariasse)

# 2. An overview of TLS 1.3

Arjan Visser

# What is TLS?

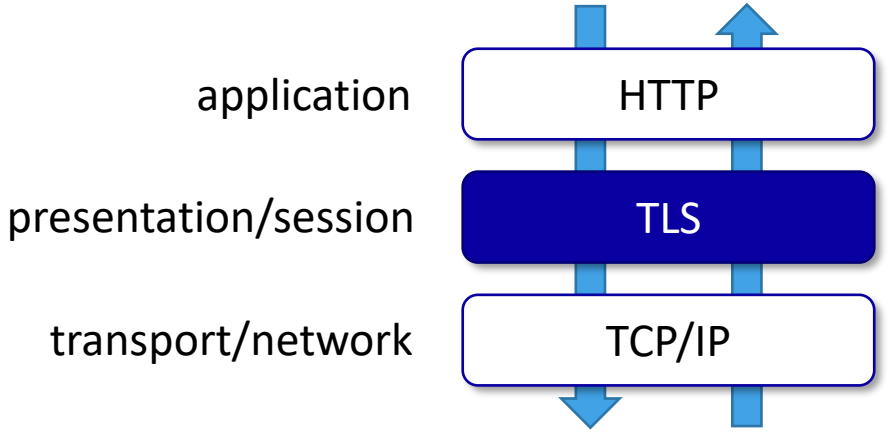
Transport Layer Security – secure connection thanks to encryption and authentication

**What is TLS?**

- ✓ TLS (Transport Layer Security) is a security protocol for data security
- ✓ Secure HTTP(S) connection thanks to encryption and authentication
- ✓ Between HTTP and TCP/IP

**History**

- ✓ TLS 1.2 has existed since 2008, TLS 1.3 since 2018
- ✓ Energy sector has worked with TLS 1.2 since 2016



# Why go from TLS 1.2 to TLS 1.3?

Ensure secure data exchange across the whole sector

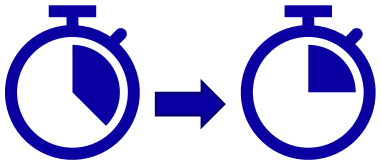
**Urgency**

TLS 1.2 is ‘outdated’, and there is *increasing* chance of vulnerabilities.
The security offered by TLS 1.3 is more robust and has improved encryption algorithms that feature no known shortcomings.

**Security**

TLS 1.3 is more reliable and safer than TLS 1.2.

In January 2021, the National Cyber Security Center (NCSC) downgraded TLS 1.2 from **good** to **sufficient**.



**Speed**

TLS 1.3 improves the speed of messages because the protocol contains fewer steps between the server and the client

**Agreement**

- ✓ Issue TC043 was approved by the NEDU GMM on 11/11/20
- ✓ All systems will switch to TLS 1.3 by 31-3-2024
- ✓ Introduction plan has been approved in MFF General Meeting of Members

# 3. EDSN – Testing on acceptance environment

Leander Hiele

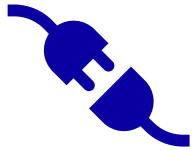
# Testing on **acceptance** environment

## Systems and sub-systems

| System | URL acceptance | Period only TLSv1.3 |
|---|---|---|
| Axway API Gateway, Axway B2Bi, KONG gateway, Toestemmingsplatform, Energiedatalink Provider, CERES | b2b.gateway-acc.edsn.nl / gateway-acc.edsn.nl | Available as of 22-1-2024 09:00 o'clock |
| C-AR/Portal | portaal-act.edsn.nl | Available as of 22-1-2024 09:00 o'clock |
| C-ARM | arm-act2.edsn.nl | Available as of 22-1-2024 09:00 o'clock |
| Data sharing platform | api.acc.mijnenergiedata.nl<br>www.acc.mijnenergiedata.nl | Available as of 22-1-2024 09:00 o'clock |
| EAN code book | b2b.gateway-acc.edsn.nl / gateway-acc.edsn.nl | Available as of 22-1-2024 09:00 o'clock |
| Gopacs | N/A | N/A |
| Nexus | N/A | N/A |
| Portal CTS | pp4-test.edsn.nl | Available as of 22-1-2024 09:00 o'clock |
| TMR | N/A | N/A |
| CSS | https://css-dat3.edsn.nl/css/ | Is already live due to another end point. |

# Support

## Connect, test, support



**Connection**

- Only CSS has another end point; other systems will retain the existing one;
- A test certificate may be needed for testing. If this is not present or has expired, then send a test certificate request to: servicedesk@edsn.nl

**Testing**

- Testing can be carried out in the usual manner, and at your own convenience. Support for the mentioned systems will be available to you if necessary.

**Support**

- EDSN service desk (servicedesk@edsn.nl) ready to assist you. Mention the following as subject: TLS 1.3 - <Application name> - Problem/question

# 4. TenneT – Testing on acceptance environment

Gerwin Bruynooge

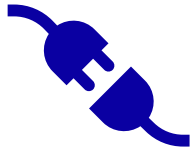
# Testing on **acceptance** environment

## Systems and sub-systems

| System (Acceptance) | Only TLS 1.3 | Per date |
|---|---|---|
| MMC Hub | YES | 1 February 2024 |
| CPS | Mail system; will continue to support TLS 1.2 | 1 February 2024 |
| TQF | Back-end system | 1.3 ready |
| APFAS | Back-end system | |
| OSB for legacy websites | Back-end system | 1.3 ready |
| CBP | Back-end system | 1.3 ready |
| GOPACS adapter | Back-end system | 1.3 ready |
| FCR web services | Back-end system | 1.3 ready |
| API Gateway (KONG) / TMAC | Back-end system | 1.3 ready |
| MHS | Back-end system | 1.3 ready |
| TIPCO | Back-end system | |
| My.TenneT.eu | YES | 1 February 2024 |

# Support

## Connect, test, support



**Connection**

- TenneT will retain the existing end points to connect with the applications.

**Testing**

- Testing can be carried out in the usual manner, and at your own convenience.

**Support**

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

- Content-related questions should be sent to the PO
- General questions should be sent to BAS

# 5. References

Amanda Zachariasse

# Remain up-to-date

## All relevant documents can be found on mijnMFFBAS

Mijn MFFBAS

**SharePoint**
Relevant documentation can be accessed via mijnMFFBAS. Request access, also for non-members

**Updates**
Updates will be placed in the SharePoint environment mijnMFFBAS. For example, about converting the acceptance environments.

**Newsletter**
A regular update will be provided via the newsletter

**Monitoring**
All market parties can test on the acceptance environment of EDSN and TenneT when it suits them.

**Phone calls**
All market parties will be approached by phone in order to create an inventory for market readiness. Make sure that the contact details are up-to-date via Partners in Energie.

**Cut-off point market readiness**
In February, a final request will be sent via e-mail, where market parties will have the chance to say that they are NOT ready.

# Quick Reference Card: TLS 1.3

Version 1.2 – November 2023

## TLS 1.3

*What is TLS?*
Transport Layer Security is a security protocol for data security.
Info sheet NCSC about TLS – download here
*Why TLS 1.3?*
TLS 1.2 is becoming more vulnerable. TLS 1.3 is faster, securer and more future-proof. Market agreements have been made to implement TLS 1.3.

## Information overview

Directly to all documents: https://mffbas.sharepoint.com/sites/TLS1.3

- ❑ 1. Dashboard readiness central systems and market parties
- ❑ 2. Information session TLS 1.3 16 May 2023 (presentation, questions & answers)
- ❑ 3. Settings and end points

## Help desk

Always mention 'TLS 1.3' in the e-mail subject and, wherever possible, also the name of the application.

*EDSN* - servicedesk@edsn.nl
Content-related questions and questions about the systems of EDSN.

*TenneT* - tennetccc@tennet.eu
Content-related questions and questions about the systems of TenneT.

*MFFBAS* - projecten@mffbas.nl
Questions about planning and organisation.

## Systems within CMF landscape

### EDSN
End date TLS 1.2: 01-04-2024
14 central systems in CMF landscape

1. Axway API Gateway
2. C-AR (incoming)
3. C-AR (outgoing)
4. C-ARM
5. Data sharing platform
6. EAN code book
7. Gopacs
8. Nexus (outgoing)
9. Portal CTS
10. TMR (outgoing)
11. CSS
12. Gopacs (outgoing)
13. Nexus (incoming)
14. TMR (incoming)

### TenneT
End date TLS 1.2: 01-04-2024
10 central systems in CMF landscape

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

The systems above are the main systems. The connections and underlying systems can be found in the documentation on mijnMFFBAS: 1. dashboard or 2. information session.

## Settings

| NCSC rating | Key exchange | Certificate-verification | Bulk encryption and hashing | Elliptical functions | Finite-field groups | RSA key length |
|---|---|---|---|---|---|---|
| Good | • ECDHE | • ECDSA<br>• RSA | • TLS-AES256-GCM-SHA256<br>• TLS-AES256-GCM-SHA384<br>• TLS-CHACHA20-POLY1305-SHA256 | • Sep384r1<br>• Sep256r1<br>• X448<br>• X25519 | | • > 3072 bit |
| Sufficient | • DHE | | | | • ffdhe4096<br>• ffdhe3072 | • 2048 – 3071 bit |
| Insufficient | | | • TLS-AES128-CM-SHA256 | | | |

The settings can also be found in the presentation for the online information session, and under settings.