

QUESTIONS & ANSWERS

INTRODUCTION TLS 1.3

Date last update: 2 June 2023
Version: 1.0

1	ABOUT TLS	2
1.1	WHAT IS TLS?	2
1.2	FOR WHAT IS TLS USED IN THE ENERGY SECTOR?	2
2	SCOPE INTRODUCTION TLS 1.3	3
2.1	WHICH CENTRAL SYSTEMS ARE IN SCOPE FOR THE 'INTRODUCTION TLS 1.3' PROJECT?	3
2.1.1	<i>How do I know which central system already supports TLS 1.3?</i>	4
2.2	QUESTIONS RELATING TO THE SCOPE	4
2.2.1	<i>Are the central systems of GTS also in scope?</i>	4
2.2.2	<i>Do the arrangements also apply to (internal) notifications via the internet, such as e.g. an app for customers?</i>	4
2.2.3	<i>When making the systems TLS 1.3-ready, will EDSN also be implementing notification modifications, like e.g. the transition from SOAP to REST?</i>	4
3	INTRODUCTION TLS 1.3	5
3.1	WHY IS IT NECESSARY TO INTRODUCE TLS 1.3?	5
3.1.1	<i>What is perfect forward secrecy?</i>	5
3.2	IS THE INTRODUCTION OF TLS 1.3 COMPULSORY?	5
3.3	WHAT IS THE SCHEDULE FOR INTRODUCING TLS 1.3?	5
3.3.1	<i>Can I already switch to TLS 1.3?</i>	5
3.3.2	<i>Must I wait until all central systems are ready for TLS 1.3 before I implement it?</i>	5
3.3.3	<i>What is the final date for introducing TLS 1.3?</i>	6
3.3.4	<i>What happens if I have not introduced TLS 1.3 on time?</i>	6
3.3.5	<i>Once the switch to TLS 1.3 has been realised, are market parties advised to deactivate TLS 1.2 when communicating with central systems?</i>	6
3.3.6	<i>Will it be clear before 1 July 2023 which end points will be modified at TenneT and EDSN?</i>	6
3.3.7	<i>Will the central systems continue to support TLS 1.2 for a particular period of time?</i>	6
3.3.8	<i>What is the latest date until which TLS 1.2 can be used?</i>	6
4	SUPPORT INTRODUCTION TLS 1.3	7
4.1	WHAT SUPPORT IS AVAILABLE FOR THE INTRODUCTION OF TLS 1.3?	7
	• Help desk EDSN	7
	• Help desk TenneT	7
4.1.1	<i>Who will help me to introduce TLS 1.3?</i>	7
4.1.2	<i>Where can I find more information?</i>	7
4.1.3	<i>Will there also be a testing environment that only supports TLS 1.3, so it is certain that a fall-back to TLS 1.2 will not be used?</i>	7
4.2	WHAT IF	7
4.2.1	<i>What happens if my software supplier has not sorted out its systems on time?</i>	7
4.2.2	<i>Will market parties be actively informed if the monitoring process shows that they have switched to TLS 1.3?</i>	7
5	OTHER QUESTIONS	8
5.1	WHEN WILL THERE BE AN UPDATE FOR DOCUMENT '230412 – INTRODUCTION TLS 1.3 – EXECUTION AND COMMUNICATION PLAN – DEFINITIVE', WHICH ALSO INCLUDES THE APPENDIX 4.4.2 "CENTRAL SYSTEMS MANAGED BY TENNET"?	8
5.2	IF THE ACCEPTANCE CRITERION IS 66.66% WEIGHTED MARKET SHARE AND TLS 1.2 IS LATER NO LONGER SUPPORTED, SURELY THIS CAN BE REGARDED AS A MARKET DISRUPTION?	8

1 About TLS

1.1 What is TLS?

Transport Layer Security (TLS) is an encryption protocol that has been designed to ensure secure communication between web browsers and servers. It is currently used in almost all apps. Many IP-based protocols, such as HTTPS, SMTP, POP3 and FTP, support TLS. This helps to ensure secure data transfer.

1.2 For what is TLS used in the energy sector?

TLS (currently version 1.2) is used in the energy sector to securely exchange data between the systems of market parties (local systems) and the central systems operated by TenneT and EDSN.

More information about TLS and how it works is presented in the online information session called 'Introduction TLS 1.3'.

This can be found via mijnMFFBAS: [2. Information session TLS 1.3 16 May 2023](#)

2 Scope introduction TLS 1.3

2.1 Which central systems are in scope for the 'Introduction TLS 1.3' project?

It applies to every application in your organisation's landscape that communicates with central systems as part of national market processes. In addition, it may also be necessary to modify the underlying software that the application relies on. Examples include database systems (DBMS's) and gateways.

Tip: consult your organisation's architects and technical administrators about this!

Central systems that are in scope for Introduction TLS 1.3 have been listed in the table below. For each system, it has been mentioned who is responsible for operating the system. TenneT or EDSN can be contacted in case of questions.

No.	System	Managed by
1	Axway API Gateway, Axway B2Bi, KONG gateway, Toestemmingsplatform, Energiedatalink Provider, CERES	EDSN
2	C-AR/Portal (incl. sector register, CER, PUD, MDD, MPR, SUP/DSO Register, TR, ADC, BU, GBU) (incoming)	EDSN
3	C-AR/Portal (incl. Sector register, CER, PUD, MDD, MPR, SUP/DSO Register, TR, ADC, BU, GBU) (outgoing: C-AR ==> application)	EDSN
4	C-ARM	EDSN
5	Data sharing platform	EDSN
6	EAN code book	EDSN
7	Gopacs (incoming)	EDSN
8	Nexus (outgoing)	EDSN
9	Portal CTS	EDSN
10	TMR (outgoing)	EDSN
11	CSS	EDSN
12	Gopacs (outgoing: Gopacs ==> Application)	EDSN
13	Nexus (incoming: Application ==> Nexus))	EDSN
14	TMR (incoming: Application ==> TMR)	EDSN
15	MMC Hub	TenneT
16	CPS	TenneT
17	TQF	TenneT
18	APFAS	TenneT
19	OSB for legacy websites	TenneT
20	CPB	TenneT
21	GOPACS adapter	TenneT
22	FCR web services	TenneT
23	B2B gateway	TenneT
24	API Gateway (KONG)	TenneT
25	MHS	TenneT

Table 1: Overview central systems in scope incl. operating party

2.1.1 How do I know which central system already supports TLS 1.3?

The 'Dashboard readiness Central Systems' is placed on mijnMFFBAS every two weeks. Link to folder:
[1. Dashboard readiness Central Systems](#)

2.2 Questions relating to the scope

2.2.1 Are the central systems of GTS also in scope?

No central systems of GTS are in scope. The NEXUS system, which is used to exchange allocation and reconciliation notifications gas, is operated by EDSN and is in scope.

2.2.2 Do the arrangements also apply to (internal) notifications via the internet, such as e.g. an app for customers?

No, this project only covers notifications concerning market processes for which MFFBAS is responsible and which take place between market parties and the central systems operated by EDSN and TenneT. As a result, notifications between a market party and, for example, your own customer app will not be in scope.

2.2.3 When making the systems TLS 1.3-ready, will EDSN also be implementing notification modifications, like e.g. the transition from SOAP to REST?

No. In order to protect the scope of the project, no notification modifications will be made because market parties will then have to implement these new notifications and this will become a 'traditional' sector release.

3 Introduction TLS 1.3

3.1 Why is it necessary to introduce TLS 1.3?

TLS 1.3 ensures faster exchange and more secure data-exchange messages. The National Cyber Security Center (NCSC) has lowered the rating of TLS 1.2 from 'good' to 'sufficient'. Research has shown that the number and algorithms used by TLS 1.2 contain encryption weaknesses, which may be susceptible to breach. And this could risk the continuity and security of exchanged messages. There is also a real chance that NCSC will further downgrade TLS 1.2 to 'insufficient'. In addition, TLS 1.3 makes it possible to improve the speed of messages, because the protocol contains fewer steps between the server and the client. The security offered by TLS 1.3 is also more robust - thus ensuring *perfect forward secrecy* - and has improved encryption algorithms that contain no known weaknesses.

3.1.1 What is perfect forward secrecy

Perfect forward secrecy is an encryption style that involves producing temporary private key exchanges between clients and servers. A unique session key is generated for every individual session that is started by the user. If one of these session keys is compromised, the data in other sessions will remain secure. This means that past sessions and the information they contain will be protected against future attacks. This encryption style is normally used by phone apps, web pages and messaging apps where the privacy of users is extremely important.

3.2 Is the introduction of TLS 1.3 compulsory?

Yes, in accordance with decisions made by the NEDU General Meeting of Members and the MFF General Meeting of Members, TLS 1.3 must be implemented in order to continue exchanging data within the energy sector.

No.	Date	Decision	Document number	Agenda point
1508	11 November 2020	The NEDU General Meeting of Members approves TC043 Introduction TLS 1.3.	NEDU General Meeting of Members 20201111-014.1	14.1
1638	9 March 2022	The NEDU General Meeting of Members decides that TLS 1.2 will no longer be permitted for the exchange of messages after the end of 2023.	NEDU General Meeting of Members 20220309-014.2	14.2

Table 2: Decisions NEDU General Meeting of Members and MFF General Meeting of Members

3.3 What is the schedule for introducing TLS 1.3?

Transition dates are part of the decisions mentioned in table 2. As of 1 July 2023, all central systems will support TLS 1.3. This will mark the start of the dual phase, where both TLS 1.2 and TLS 1.3 will be supported. All market parties are expected to have switched to TLS 1.3 by 31 December 2023. This means a proposal can be made to the MFF General Meeting of Members to end the support for TLS 1.2 offered by TenneT and EDSN.

3.3.1 Can I already switch to TLS 1.3?

Yes, definitely! The majority of central systems already support TLS 1.3. So you can start testing how TLS 1.3 communicates with these central system. And then you can start using TLS 1.3 to communicate with these central systems.

3.3.2 Must I wait until all central systems are ready for TLS 1.3 before I implement it?

No. It is recommended to already start with the central systems that already support TLS 1.3.

3.3.3 What is the final date for introducing TLS 1.3?

The deadline has been set to 31 December 2023.

3.3.4 What happens if I have not introduced TLS 1.3 on time?

Once the 66% weighted market share per market role (TSO and DSO 100%) has been reached for all market parties, the project will report this to the MFF General Meeting of Members. The MFF General Meeting of Members must then decide when support for TLS 1.2 will be ended. And once that decision has been made, and TLS 1.2 has actually been phased out, local systems will no longer be able to connect to central systems via TLS 1.2.

3.3.5 Once the switch to TLS 1.3 has been realised, are market parties advised to deactivate TLS 1.2 when communicating with central systems?

TLS 1.2 should preferably be deactivated immediately, unless the concerned system is also used for interfaces with other systems that are based on TLS 1.2.

3.3.6 Will it be clear before 1 July 2023 which end points will be modified at TenneT and EDSN?

EDSN and TenneT do not have any plans to modify end points at this moment in time. Should it be necessary, this will be communicated via the newsletter and mijnMFFBAS.

3.3.7 Will the central systems continue to support TLS 1.2 for a particular period of time?

Yes, this is called the dual period where central systems will support TLS 1.2 as well as TLS 1.3. This will end as soon as the MFF General Meeting of Members decides to no longer support TLS 1.2 and makes it possible for operators of central systems to deactivate TLS 1.2.

3.3.8 What is the latest date until which TLS 1.2 can be used?

This has yet to be determined. The main priority is to make sure that TLS 1.3 is used when communicating with central systems. The deadline for this has been set to 31 December 2023. In the autumn of 2023, we will see how the switch to TLS 1.3 is progressing and will make a proposal to the MFF General Meeting of Members about when support for TLS 1.2 can be ended. The final decision will be made by the MFF General Meeting of Members.

4 Support introduction TLS 1.3

4.1 What support is available for the Introduction of TLS 1.3?

You can rely on:

- *Help desk EDSN*

Send an e-mail to: servicedesk@edsn.nl, with the subject: TLS1.3 - <Application name> - Problem/question.

- *Help desk TenneT*

Send an e-mail to TenneT Customer Care Center: tennetccc@tennet.eu.

4.1.1 Who will help me to introduce TLS 1.3?

The operators of central systems, namely EDSN and TenneT, are ready to answer your questions. The contact details of both parties have been mentioned above.

4.1.2 Where can I find more information?

Additional information can be found on mijnMFFBAS under 'TLS 1.3' (<https://mffbas.sharepoint.com/sites/TLS1.3>). What support does MFFBAS offer for the Introduction of TLS 1.3? Support is provided by sharing acquired knowledge of TLS 1.3 and explaining the potential impact for organisations, such as:

- Settings for configuring TLS 1.3
- Insight into versions of standard software commonly used in the market
- Alternatives

4.1.3 Will there also be a testing environment that only supports TLS 1.3, so it is certain that a fall-back to TLS 1.2 will not be used?

This is not being offered by EDSN or TenneT. Only a testing environment that supports both TLS 1.2 and TLS 1.3 will be available, just like the production environments of EDSN and TenneT, which also support both versions.

4.2 What if....

4.2.1 What happens if my software supplier has not sorted out its systems on time?

Then you can place these systems on a proxy server, which will make it possible to run external traffic via TLS 1.3, while not all systems are TLS 1.3-ready internally. What this looks like and what you must do has been presented in the online information session called 'Introduction TLS 1.3'. This can be found via mijnMFFBAS: [2. Information session TLS 1.3 16 May 2023](#).

4.2.2 Will market parties be actively informed if the monitoring process shows that they have switched to TLS 1.3?

The responsibility for switching to TLS 1.3 lies with the market parties. Monitoring is primarily aimed at gaining an insight into how the transition to TLS 1.3 is progressing at sector level. If there are doubts whether the switch to TLS 1.3 has been successful, market parties can contact the help desk of EDSN or TenneT depending on the system to which the question relates. See table 1 and question 4.1.

5 Other questions

5.1 When will there be an update for document '230412 – Introduction TLS 1.3 – Execution and Communication plan – Definitive', which also includes the appendix 4.4.2 "Central systems managed by TenneT"?

This update cannot be provided. The concerned systems can be found in the information session and on the Dashboard readiness Central Systems. Both have been published and can be accessed via mijnMFFBAS.

5.2 If the acceptance criterion is 66.66% weighted market share and TLS 1.2 is later no longer supported, surely this can be regarded as a market disruption?

Yes, and that is why support for TLS 1.2 cannot be ended at a whim. This decision will only be made in the MFF General Meeting of Members based on the available information and the impact of the decision.