

Information session

Introduction TLS 1.3

16 May 2023



1. Introduction

Mirjam van der Horst

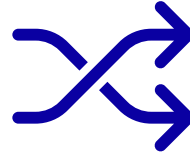
Agenda

1. Introduction (Mirjam van der Horst)
2. What is TLS? (John van der Stap)
3. Why go from TLS 1.2 to TLS 1.3? (John van der Stap)
4. Which changes accompany TLS 1.3?
 - a. General (John van der Stap)
 - b. Central systems EDSN (Jurjan Woltman)
 - c. Central systems TenneT (Jan Heerschop)
5. Organisation & planning (Amanda Zachariasse)
6. Documentation & communication (Amanda Zachariasse)

Aim of the information session



What is TLS?



Why go from TLS 1.2 to TLS 1.3? What will change?



Central systems:
system readiness



Insight into planning
and transition criteria



Documentation &
communication



2. What is TLS 1.3?

John van der Stap

What is TLS?

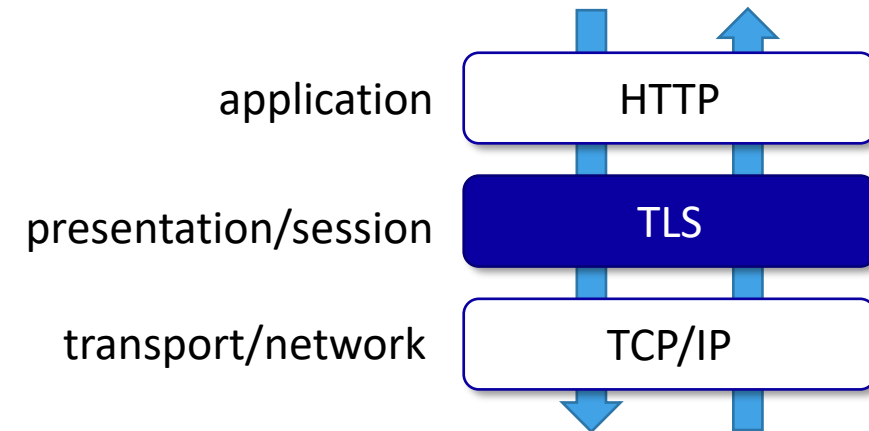
Transport Layer Security – secure connection thanks to encryption and authentication

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





What is TLS?

Transport Layer Security – secure connection thanks to encryption and authentication

TLS

- TLS is a protocol that aims to ensure secure connections via the internet.
- TLS 1.2 has existed since 2008. The security level of this protocol is declining. In January 2021, the National Cyber Security Center (NCSC) lowered the rating of this protocol from **good** to **sufficient**.
- Its successor, namely TLS 1.3, is available but has not yet been implemented everywhere.

TLS within the energy sector

- Since 2016, TLS 1.2 has been used to send messages within the sector.
- To make sure that information in the sector is exchanged securely, TLS 1.3 was incorporated into issue TC043. This issue was approved by the NEDU General Meeting of Members on 11 November 2020.



3. Why go from TLS 1.2 to TLS 1.3?

John van der Stap



Why go from TLS 1.2 to TLS 1.3?

Ensure secure data exchange across the whole sector



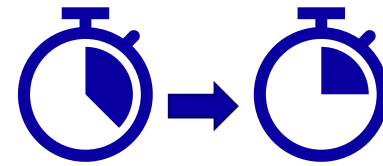
Urgency

TLS 1.2 is 'outdated', has not new developments and there is *increasing* chance of vulnerabilities



Security

More reliable and safer than TLS 1.2.



Speed

Improved handshake



Agreement

- ✓ Issue TC043 has been approved
 - ✓ 31-12-2023 all systems switched to TLS 1.3
- ✓ Introduction plan has been approved in MFF General Meeting of Members



Why go from TLS 1.2 to TLS 1.3?

Ensure secure data exchange across the whole sector

Advantages

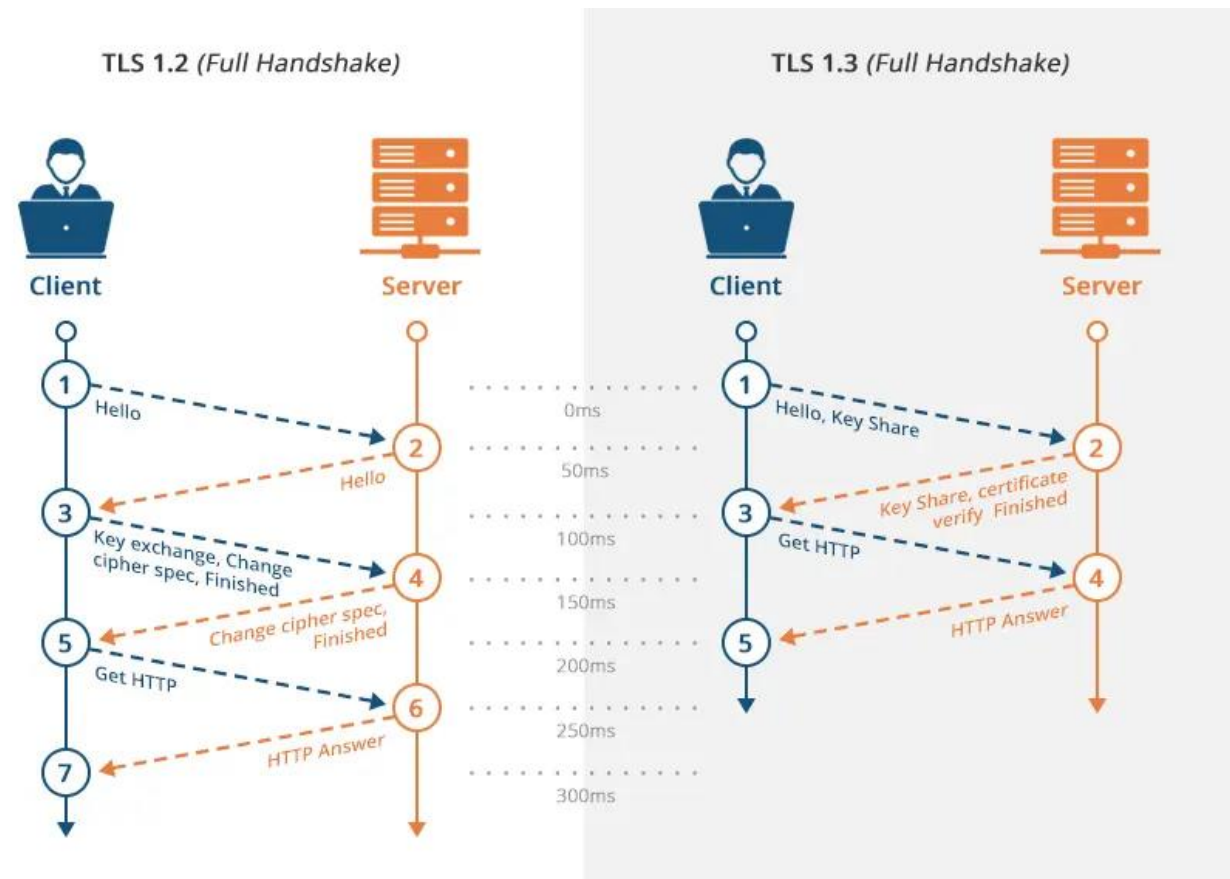
- TLS 1.3 makes it possible to improve the speed of messages, because the protocol contains fewer steps between the server and the client.
- TLS 1.3 offers more robust security and it has improved encryption algorithms that have no known weaknesses.
- In short: TLS 1.3 ensures faster exchange and more secure messages.

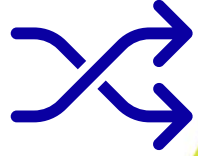
Sector agreements

- To make sure that information in the sector is exchanged securely, TLS 1.3 was incorporated into issue TC043. This issue was approved by the NEDU General Meeting of Members on 11 November 2020.
- On 9 March 2022, the NEDU General Meeting of Members decided that TLS 1.2 would no longer be permitted for the exchange of messages after the end of 2023.

Why go from TLS 1.2 to TLS 1.3?

TLS 1.3 is faster than TLS 1.2





4. What will change with TLS 1.3?

a. General

John van der Stap

What will change with TLS 1.3? - General

Overall impact



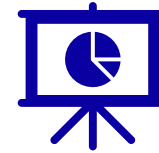
Scope

- All interfaces between central and local systems
- For an overview of the central systems, see slides: 21-24 (EDSN) and 25-37 (TenneT)



Change

- No certificate exchange needed
- In principle, end points will remain the same
- Dual period from at least 1-7-2023 to 31-12-2023



Transition

- Monitoring of central systems
- Please note: market parties can immediately start implementing TLS 1.3 Testing communication with central systems that are TLS 1.3-ready



What will change with TLS 1.3? - General

Overall impact

Scope

- All interfaces between central and local systems are in scope.

Change

- A certificate exchange is not needed for the introduction of TLS 1.3.
- In principle, there is no change in end points: current end points support TLS 1.2 and TLS 1.3.
- The dual period for each system in the CMF landscape will start before 1 July 2023.

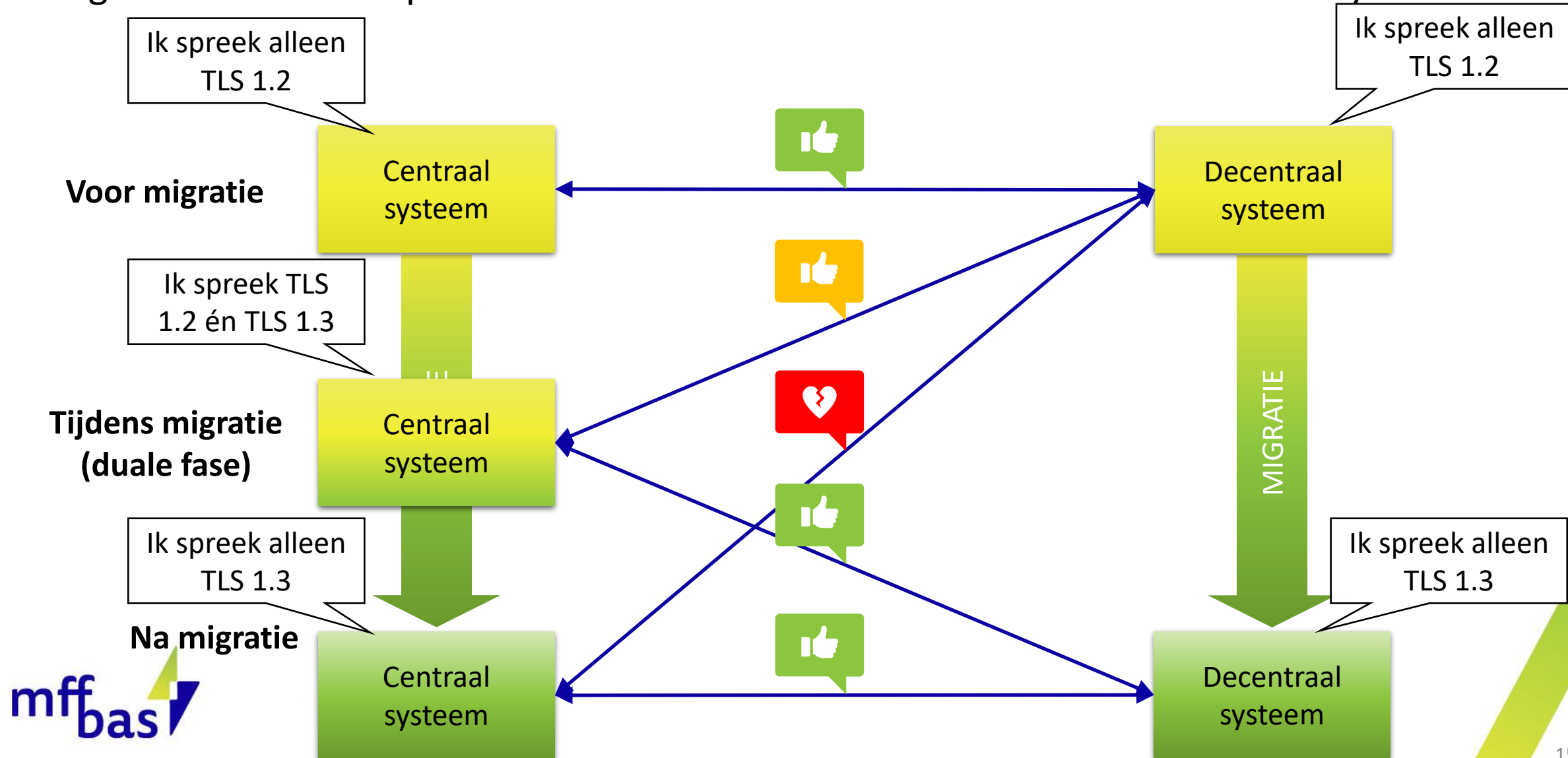
Transition

- Market parties need not wait until all central systems have switched to TLS 1.3.
- Market parties must first test the transition to TLS 1.3 on the testing environments of the central systems.
- There will be no sector tests. However, the standard testing environments of systems in the CMF landscape are available for testing.
- Continuous monitoring is carried out to see how many parties (per market role and other parties) communicate via TLS 1.3 for each system in the CMF landscape.
- The dual period will end on 1 January 2024 at the latest. In consultation with the MFF General Meeting of Members, a decision can be made to extend the dual period.
- TLS 1.2 will be phased out following decision-making in the MFF General Meeting of Members.



What will change with TLS 1.3? - General

Migration and consequences for communication between central and local systems



What will change with TLS 1.3? - General

What if updating to TLS 1.3 is not supported or requires a lot of work?



Problem

- Insufficient time or capacity
- Software not TLS 1.3-ready



Solution

- Install a proxy server

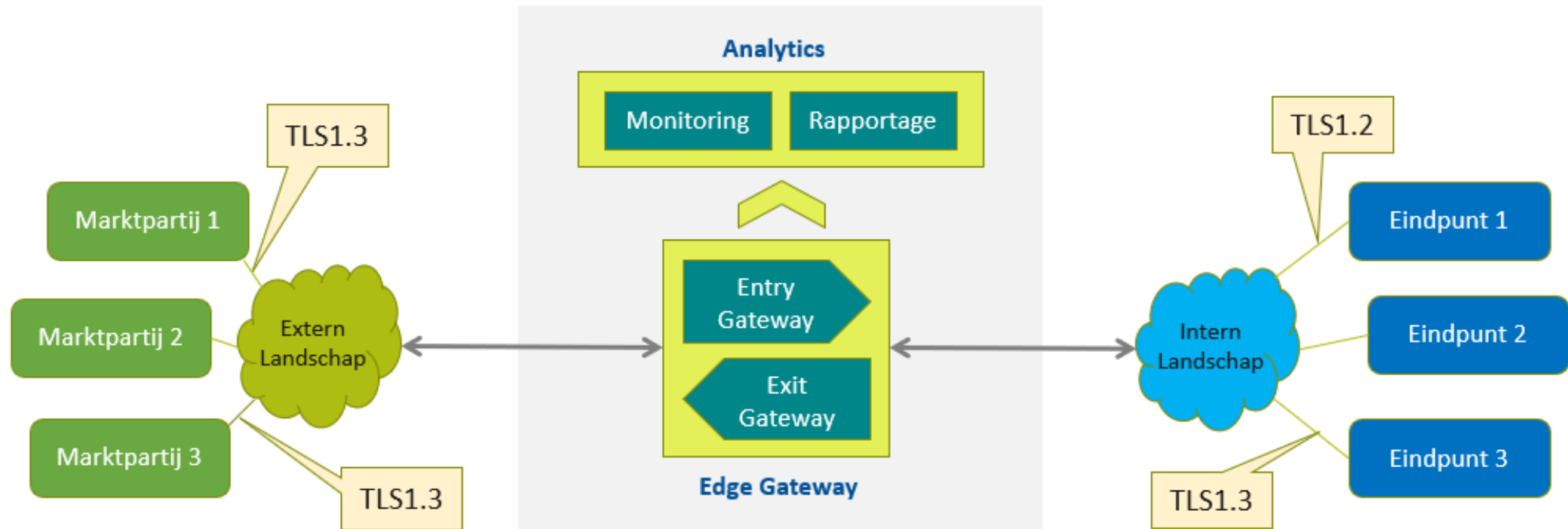


Advantages

- Continuation data exchange
- Upgrade systems to TLS 1.3 in own time

What will change with TLS 1.3? - General

Example for use of proxy server (practical example EDSN)





What will change with TLS 1.3? - General

What if updating to TLS 1.3 is not supported or requires a lot of work?

Problem

There is not enough time or people to modify internal systems on time.

Or a software manufacturer has not yet modified its software to communicate via TLS 1.3.

Possible consequence

Firstly, it will not be possible to communicate with the central systems.

Solution

To place a proxy server between the local system and internet traffic.

If TLS 1.2 traffic is converted to TLS 1.3, the proxy server can improve the security of the traffic and makes sure that the client and the server both use the most recent security protocols.

Advantage

You can buy time to upgrade internal systems to TLS 1.3.

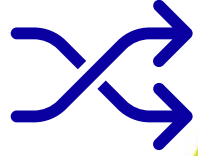


What will change with TLS 1.3? - General

Settings & cipher suites for TLS 1.3 – work effectively and sufficiently for TLS 1.3

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

For a detailed description of how to value settings, see the most recent [guidelines of the NCSC](#)



4. What will change with TLS 1.3?

b. Central systems EDSN

Jurjan Woltman



What will change with TLS 1.3? - EDSN

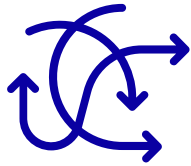
Systems and sub-systems

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.



What will change with TLS 1.3? - EDSN

Change, testing, support



Change

- Wherever possible, EDSN 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

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



What will change with TLS 1.3? - EDSN

Change, testing, support

Change

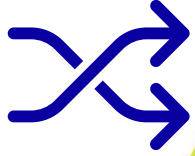
- Wherever possible, EDSN will retain the existing end points to connect with the applications (dual).

Testing

- Testing can be carried out at your own convenience using the testing/acceptance environment.

Support

- Should there be issues, the service desk of EDSN will be ready to assist you.
- If you are unable to make a connection using TLS 1.3, Send an e-mail to
 - servicedesk@edsn.nl
 - Mention the following as subject: TLS 1.3 - <Application name> - Problem/question
 - We will then contact you as soon as possible



4. What will change with TLS 1.3?

c. Central systems TenneT

Jan Heerschop



What will change with TLS 1.3? - TenneT

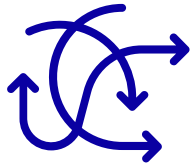
Systems and sub-systems

System	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



What will change with TLS 1.3? - TenneT

Change, testing, support



Change

- If possible, 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



5. Planning & organisation

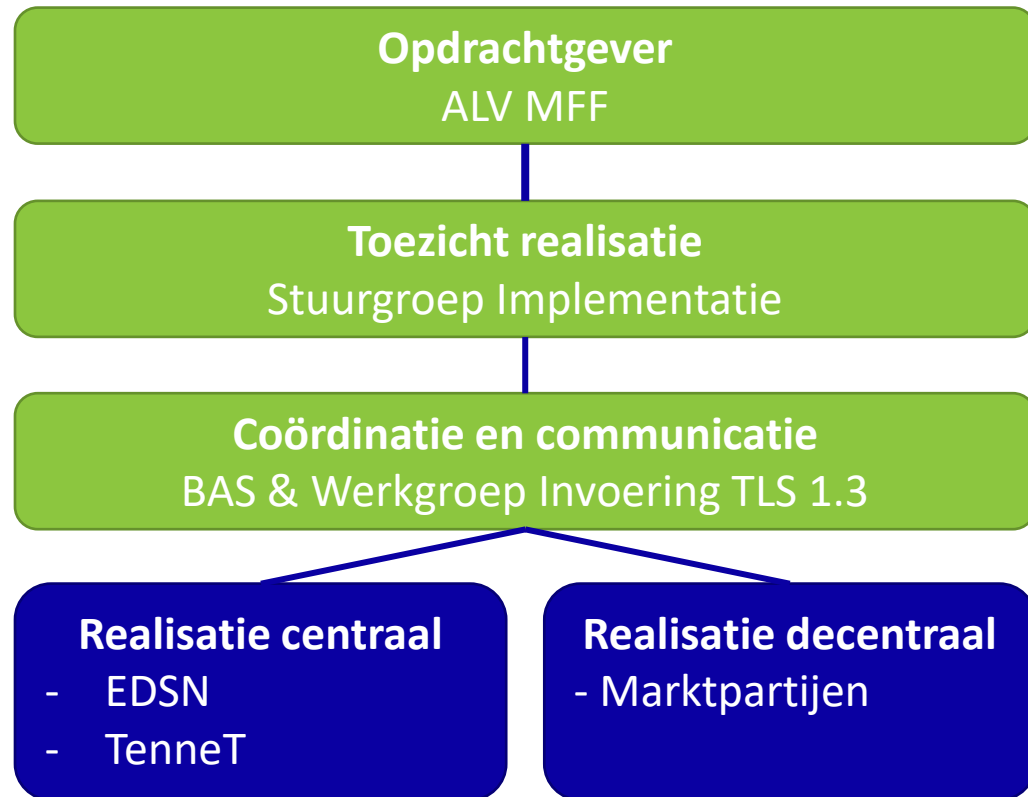
Amanda Zachariasse



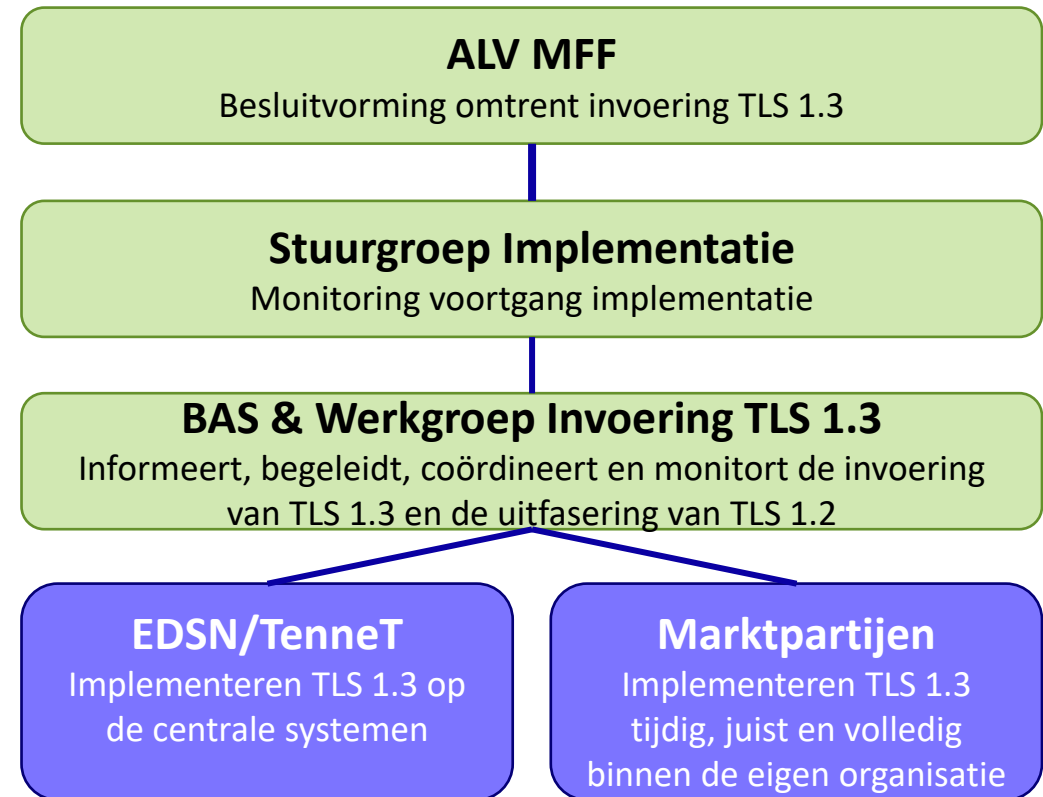
Planning & organisation

Organisation

Organisation structure



Responsibilities





Planning & organisation

Organisation

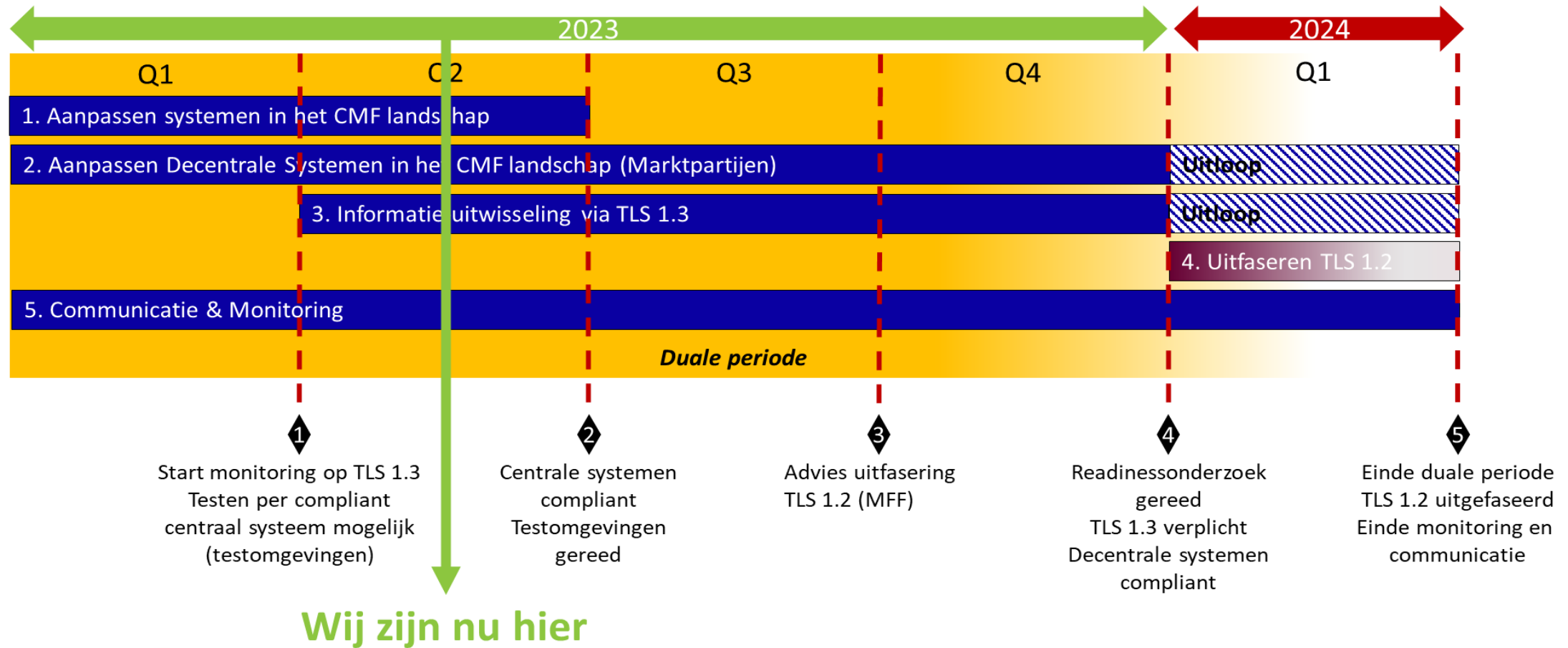
Working group members – Working group Introduction TLS 1.3

Name	Market role	Represented in team
Amanda Zachariasse	BAS	Project leader / Topic Manager
Tony Sloos	RNB / DSO – IT Services (EDSN)	Point of contact readiness central systems EDSN
Leander Hiele	RNB / DSO – IT Services (EDSN)	PL readiness central systems EDSN
Jan Heerschop	LNB / TSO E – TenneT	Point of contact readiness central systems TenneT
Jan Nienhuis	RNB / DSO – Stedin	Point of contact security
Mirjam van der Horst	BAS / Steering committee Implementation	Point of contact Steering committee Implementation
Bram van Straalen	BAS / CoP Secure Architecture	Point of contact BAS / CoP Secure Architecture
Jacco Hogeweg	BAS	Point of contact communication
Arjan Visser	BAS	Topic Manager

- BAS supplies information about, supports, coordinates and monitors the introduction of TLS 1.3 and the deactivation of TLS 1.2.
- Parties in the sector – members of MFF and others – are responsible for realising the transition to TLS 1.3 within their organisations in a timely, correct and complete manner.

Planning & organisation

All market parties and local/central systems will switch to TLS 1.3 in 2023



Planning & organisation

Calibration moments and acceptance criteria

Monitoring & reporting TLS 1.3-readiness



1 July 2023

Evaluation TLS 1.3-
readiness central systems



End Q3

Evaluation TLS 1.3-readiness
market parties (local systems)



Acceptance criteria

- 100% readiness central systems
- Local systems 66.66% weighted market share market parties



Planning & organisation

Calibration moments and acceptance criteria

- Evaluate readiness central systems 1 July 2023, report to MFF General Meeting of Members
- Evaluate readiness market parties end Q3, report to MFF General Meeting of Members
- The following acceptance criteria will be used so that TLS 1.2 can be phased out:
 - Systems in the CMF landscape, which are within scope, are subject to an acceptance criterion of 100% over op TLS 1.3.
 - All interfaces between local systems in the CMF landscape are subject to a weighted market share of 66% for those already on TLS 1.3.
 - A weighted market share cannot be issued for ODA's (Other Service Providers) and other market participants. In this case, 51% of the absolute market share applies.



6. Documentation & communication

Amanda Zachariasse



Documentation & communication

All relevant documents can be found on mijnMFFBAS

 Mijn MFFBAS

SharePoint

Relevant documentation can be accessed via mijnMFFBAS.

Request access, also for non-members



Dashboard

Monthly update for the readiness of central systems in the dashboard, also on mijnMFFBAS



Newsletter

A regular update will be provided via the newsletter



Monitoring

EDSN and TenneT monitor all central systems in order to monitor the transition of market parties to TLS 1.3



Documentation & communication

Communication links

- The issue document was approved on 12 November 2020 in the NEDU General Meeting of Members. The end date for TLS 1.2 was set on 9 March 2022 in the NEDU General Meeting of Members. The execution and communication plan was approved on 8 March 2023 in the MFF General Meeting of Members.
- The approved issue document, execution and communication plan, information session and Q&A can be found on mijnMFFBAS: Release/TLS 1.3. [TLS 1.3 - Introduction page \(sharepoint.com\)](#)
- RFC's or other important notifications are communicated via the newsletter. If you have not yet subscribed, subscribe to the free newsletter via communicatie@mffbas.nl
- If you, as a market party, have questions about this topic, please ask them via projecten@mffbas.nl
- The EDSN service desk (servicedesk@edsn.nl) is ready to assist you. Mention the following as subject: TLS1.3 - <Application name> - Problem/question.
- Via the TenneT Customer Care Center: tennetccc@tennet.eu

Summary Introduction TLS 1.3

The transition to TLS 1.3 can be initiated by each market party **as of now**, on all central systems that are TLS 1.3-ready.



What is TLS?

TLS (Transport Layer Security) is a security protocol for data security



Why TLS 1.3?

- ✓ TLS 1.2 is becoming more vulnerable
- ✓ Faster, safer and futureproof
- ✓ In accordance with Issue TC043



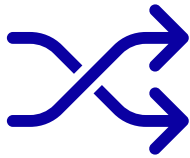
Planning

- ✓ 1-7-2023 Central Systems TLS 1.3-ready
- ✓ 31-12-2023 market parties TLS 1.3-ready



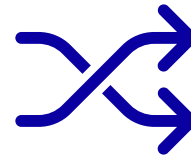
Documentation & communication

- ✓ Publications on mijnMFFBAS
- ✓ Newsletters



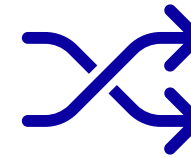
General

- All interfaces between central and local systems
- From TLS 1.2 to TLS 1.3 without certificate exchange



EDSN

- End points the same wherever possible
- Testing at your own convenience
- Help desk available for support



TenneT

- End points the same wherever possible
- Testing at your own convenience
- Help desk available for support

