Quick Reference Card: TLS 1.3

Version 11 – November 2023

TLS 1.3

What is TLS?
Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network. Infosheet NCSC about TLS (in Dutch).

Why TLS 1.3?
TLS 1.2 is 'outdated' and is becoming more vulnerable. TLS 1.3 is safer, faster, and future-proof. The market agreed on applying TLS 1.3.

Information overview

Direct link 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

Support

Please make sure that the subject of every e-mail contains 'TLS 1.3' and the application it concerns.

EDSN - servicedesk@edsn.nl
Questions directly related to the systems supported by EDSN.

TenneT - tennetccc@tennet.eu
Questions directly related to the systems supported by TenneT.

MFFBAS - projecten@mffbas.nl
General questions about planning and organization.

Systems within CMF-landscape

EDSN
End date TLS 1.2: 01-04-2023
14 central systems in CMF-landscape

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

TenneT
End date TLS 1.2: 01-04-2024
11 central systems in landscape

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

The systems mentioned above are the main systems. The connections and related systems can be found on myMFFBAS under: '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 • 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			

All settings can also be found in the presentation of the information session.