BILAG

TLS-konfiguration

November 2026

Styrelsen for
Samfundssikkerhed

TLS Konfigurationsparametre

#	Emne for retningslinjer	Værdi	Sikkerhedsniveau
1	TLS-versioner	TLS 1.3	God
		TLS 1.2	Tilstrækkelig
		TLS 1.1 TLS 1.0 SSL 3.0 SSL 2.0 SSL 1.0	Utilstrækkelig
2	Algoritmer til nøgleudveksling	X25519MLKEM768 SecP256r1MLKEM768 SecP384r1MLKEM1024	God
		ECDHE	Tilstrækkelig
		DHE RSA DH ECDH KRB5 NULL PSK SRP	Utilstrækkelig
3	Algoritmer til autentificering	ECDSA RSA (RSA-PSS) EdDSA	Tilstrækkelig
		DSS EXPORT-* PSK Anon NULL KRB5	Utilstrækkelig

#	Emne for retningslinjer	Værdi	Sikkerhedsniveau
4	Algoritmer til bulk-kryptering	AES-256-GCM ChaCha20-Poly1305	God
		AES-256-CCM AES-128-GCM AES-128-CCM	Tilstrækkelig
		AES-256-CBC AES-128-CBC CAMELLIA ARIA 3DES SEED AES-256-CCM_8 AES-128-CCM_8 IDEA DES RC4 NULL	Utilstrækkelig
5	Hash-funktioner	SHA-512 SHA-384 SHA-256	God
		SHA-224 SHA-1 MD5	Utilstrækkelig
6	RSA Nøglelængder[1]	Mindst 3072	Tilstrækkelig
		Mindre end 3072	Utilstrækkelig
7	RSA Padding scheme	RSA-PSS	Tilstrækkelig
		RSA-PKCS#1 v1.5	Utilstrækkelig
8	Elliptiske kurver	secp521r1 secp384r1 secp256r1 Curve448[2] Curve25519[3] brainpoolP512r1 brainpoolP384r1 brainpoolP256r1	Tilstrækkelig
		secp224r1 Andre kurver	Utilstrækkelig
9	Edwards kurver	Ed448 Ed25519	Tilstrækkelig
		Andre kurver	Utilstrækkelig

[1] Kun til brug med signaturer, ikke til nøgleudveksling
[2] Kun til brug med ECDHE
[3] Kun til brug med ECDHE

#	Emne for retningslinjer	Værdi	Sikkerhedsniveau
10	”Finite field” grupper	Samtlige grupper	Utilstrækkelig
11	Komprimering	TLS 1.3: N/A TLS 1.2: Ingen komprimering	God
		TLS 1.2: TLS-komprimering[4]	Utilstrækkelig
12	Klient-initierede genforhandling (Client initiated renegotiation)	TLS 1.3: N/A TLS 1.2: No renegotiation	God
		TLS 1.2: Limited secure renegotiation	Tilstrækkelig
		TLS 1.2: Unlimited secure renegotiation TLS 1.2: Insecure renegotiation	Utilstrækkelig
13	Genoptag session (resume session)	No resumption TLS 1.3: Session tickets	God
		TLS 1.2: Session tickets + additional security measures TLS 1.2: Session-ID’s + additional security measures	Tilstrækkelig
		Andet	Utilstrækkelig
14	0-RTT	TLS 1.3: No 0-RTT TLS 1.2: N/A	God
		TLS 1.3: Using 0-RTT	Utilstrækkelig

[4] Komprimering kan også forekomme ved ”application-level”, hvilket ikke er et TLS konfigurationsparameter. Det er dog relevant at sikre, at application-level komprimering ikke fører til en sårbarhed.

Styrelsen for
Samfundssikkerhed

Datavej 20
3460 Birkerød
+45 45 16 16 66

Rådgivning
Kontakt til Styrelsen for Samfundssikkerhed angående rådgivning om sikkerhed, cybersikkerhed, beredskabsplanlægning og forsyningssikkerhed: raadgivning@samsik.dk