Cryptographic Recommendations Smals

Creation date: 2025-10-28

WARNING: This document is generated in the context of experiments by Smals Research and has no authoritative value.

TLS (Transport Layer Security)

TLS versions

Version	Recommendation level	Use up to
TLSv1.0	insecure	
TLSv1.1	insecure	
TLSv1.2	secure	
TLSv1.3	recommended	

TLSv1.2

Cipher Suite	Recommendation level	Use up to	Remarks
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	recommended	2031-12-31+	
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	recommended	2031-12-31+	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	recommended	2031-12-31+	
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	recommended	2031-12-31+	
TLS_ECDHE_ECDSA_WITH_AES_256_CCM	secure	2031-12-31+	[0]
TLS_ECDHE_ECDSA_WITH_AES_128_CCM	secure	2031-12-31+	[0]
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	secure	2031-12-31+	[1]
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	secure	2031-12-31+	[1]
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	phase-out	2026-12-31	[2]
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	phase-out	2026-12-31	[2]
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	phase-out	2026-12-31	[2]
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	phase-out	2026-12-31	[2]
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	phase-out	2029-12-31	[3]
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	phase-out	2029-12-31	[3]
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	phase-out	2029-12-31	[3]
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	phase-out	2029-12-31	[3]
TLS_DH_DSS_WITH_AES_128_CBC_SHA256	phase-out	2026-12-31	[2]
TLS_DH_DSS_WITH_AES_256_CBC_SHA256	phase-out	2026-12-31	[2]
TLS_DH_DSS_WITH_AES_128_GCM_SHA256	phase-out	2026-12-31	[2]
TLS_DH_DSS_WITH_AES_256_GCM_SHA384	phase-out	2026-12-31	[2]
TLS_DH_RSA_WITH_AES_128_CBC_SHA256	phase-out	2026-12-31	[2]

TLS_DH_RSA_WITH_AES_256_CBC_SHA256	phase-out	2026-12-31	[2]
TLS_DH_RSA_WITH_AES_128_GCM_SHA256	phase-out	2026-12-31	[2]
TLS_DH_RSA_WITH_AES_256_GCM_SHA384	phase-out	2026-12-31	[2]
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	phase-out	2029-12-31	[4]
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	phase-out	2029-12-31	[4]
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	phase-out	2029-12-31	[4]
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	phase-out	2029-12-31	[4]
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	phase-out	2029-12-31	[4]
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	phase-out	2029-12-31	[4]
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	phase-out	2029-12-31	[4]
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	phase-out	2029-12-31	[4]
TLS_DHE_RSA_WITH_AES_128_CCM	phase-out	2029-12-31	[4]
TLS_ECCPWD_WITH_AES_128_GCM_SHA256	insecure		[5]
TLS_ECCPWD_WITH_AES_256_GCM_SHA384	insecure		[5]
TLS_ECCPWD_WITH_AES_128_CCM_SHA256	insecure		[5]
TLS_ECCPWD_WITH_AES_256_CCM_SHA384	insecure		[5]

TLSv1.3

Cipher Suite	Recommendation level	Use up to	Remarks
TLS_AES_256_GCM_SHA384	recommended	2031-12-31+	
TLS_AES_128_GCM_SHA256	recommended	2031-12-31+	
TLS_AES_128_CCM_SHA256	recommended	2031-12-31+	
TLS_CHACHA20_POLY1305_SHA256	secure	2031-12-31+	[6, 7, 8]
TLS_AES_128_CCM_8_SHA256	phase-out	2031-12-31	[9]
TLS_SHA256_SHA256	insecure		[10]
TLS_SHA384_SHA384	insecure		[10]
TLS_SM4_CCM_SM3	insecure		[11, 12]
TLS_SM4_GCM_SM3	insecure		[11, 12]

Conditions

[0] The security relies on choosing a unique nonce for every message encrypted

Remarks

[0] CCM is less widely used and tested compared to GCM

[1] Considered secure, but not recommended because it's less tested by experts, compared to AES-GCM

[2] No perfect forward secrecy (PFS)

[3] Enabling the TLS extension “Encrypt-then-MAC”, as soon as suitable implementations are available, upgrades this cipher suite to recommended.

[4] Cipher suites of the form TLS_DHE_* are set to be deprecated by the IETF (see https://datatracker.ietf.org/doc/draft-ietf-tls-deprecate-obsolete-kex/). These cipher suites are therefore only recommended until 2029.

[5] Password-based TLS suites (instead of certificate-based) lack expiration dates, which makes it unsuitable for use in government context

[6] Secure, but not recommended because it's less tested by experts, compared to AES-GCM. See https://fragdenstaat.de/anfrage/nicht-empfehlung-von-cipher-suite-tls-chacha20-poly1305-sha256-fuer-tls1-3-in-tr-02102-2/

[7] ChaCha20-Poly1305 has fast software performance, and without hardware acceleration, is usually faster than AES-GCM. See https://datatracker.ietf.org/doc/html/rfc8439#appendix-B

[8] Compared to AES-GCM, implementations of ChaCha20-Poly1305 are less vulnerable to timing attacks.

[9] Minimum tag length of 12 bytes is recommended

[10] This cipher suite uses no encryption at all. Hence, it does not provide confidentiality protection.

[11] ShangMi 4 Encryption: The ShangMi 4 (SM4) encryption algorithm is a chinese algorithm, which will be or is already mandatory for TLS encrypted connections in China. The security of this algorithm is not proven and its use is not recommended by the IETF

[12] The ShangMi 3 (SM3) hashing algorithm is a chinese algorithm, which will be or is already mandatory for TLS encrypted connections in China. The security of this algorithm is not proven and its use is not recommended by the IETF.

References