



You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > server.segtor.tr

SSL Report: server.segtor.tr (45.43.154.103)

Assessed on: Sun, 05 Jul 2026 20:30:44 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating

A

Certificate

Protocol Support

Key Exchange

Cipher Strength

0 20 40 60 80 100

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server supports TLS 1.3. [MORE INFO »](#)

This server does not support PQC (Post-Quantum Cryptography) key exchange.

Certificate #1: EC 256 bits (SHA384withECDSA)



Server Key and Certificate #1

server.segtor.tr	
Subject	Fingerprint SHA256: a0a87ad417a8715a8d0aeb16e0560c312c42b90bcb1116c3ec4df11020f15212
	Pin SHA256: oLDFyu3xGrhpFk56gW2jL0rDIIHsSuWToYkobiohs1w=
Common names	server.segtor.tr
Alternative names	server.segtor.tr
Serial Number	065ffc18ac8359c9f132495beddfbd629edf
Valid from	Wed, 13 May 2026 04:18:50 UTC
Valid until	Tue, 11 Aug 2026 04:18:49 UTC (expires in 1 month and 5 days)
Key	EC 256 bits
Weak key (Debian)	No
Issuer	E8
	AlA: http://e8.i.lencr.org/
Signature algorithm	SHA384withECDSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL
	CRL: http://e8.c.lencr.org/96.crl
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes
	Mozilla Apple Android Java Windows



Additional Certificates (if supplied)

Certificates provided	2 (2025 bytes)
Chain issues	None

#2

Additional Certificates (if supplied)

Subject	E8
	Fingerprint SHA256: 83624fd338c8d9b023c18a67cb7a9c0519da43d11775b4c6cbdad45c3d997c52
	Pin SHA256: iFvwVyJSxnQdyaUvUERIf+8qk7gRze3612JMwoO3zdU=
Valid until	Fri, 12 Mar 2027 23:59:59 UTC (expires in 8 months and 7 days)
Key	EC 384 bits
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA



Certification Paths



[Click here to expand](#)

Certificate #2: RSA 2048 bits (SHA256withRSA) No SNI



[Click here to expand](#)

Configuration



Protocols

TLS 1.3	Yes
TLS 1.2	Yes*
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

(*) Experimental: Server negotiated using No-SNI



Cipher Suites

# TLS 1.3 (server has no preference)			
TLS_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA) FS		128
TLS_AES_256_GCM_SHA384 (0x1302)	ECDH x25519 (eq. 3072 bits RSA) FS		256
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	ECDH x25519 (eq. 3072 bits RSA) FS		256
# TLS 1.2 (server has no preference)			
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	ECDH secp521r1 (eq. 15360 bits RSA) FS		128
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	ECDH secp521r1 (eq. 15360 bits RSA) FS		256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc030)	ECDH secp521r1 (eq. 15360 bits RSA) FS		256



Handshake Simulation

Android 4.4.2	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp521r1 FS
Android 5.0.0	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp521r1 FS
Android 6.0	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp521r1 FS
Android 7.0	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDH x25519 FS
Android 8.0	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDH x25519 FS
Android 8.1	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519 FS
Android 9.0	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519 FS
BingPreview Jan 2015	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp521r1 FS
Chrome 49 / XP SP3	Server sent fatal alert: handshake_failure			
Chrome 69 / Win 7 R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519 FS

Handshake Simulation

Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519	FS
Chrome 131 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519	FS
Firefox 31.3.0 ESR / Win 7	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 47 / Win 7 R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 49 / XP SP3	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 62 / Win 7 R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH x25519	FS
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519	FS
Firefox 135 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519	FS
Googlebot Feb 2018	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH x25519	FS
IE 11 / Win 7 R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
IE 11 / Win 8.1 R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
IE 11 / Win Phone 8.1 R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
IE 11 / Win Phone 8.1 Update R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
IE 11 / Win 10 R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Edge 15 / Win 10 R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH x25519	FS
Edge 16 / Win 10 R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH x25519	FS
Edge 18 / Win 10 R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH x25519	FS
Edge 131 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519	FS
Edge 13 / Win Phone 10 R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Java 8u161	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Java 11.0.3	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1	FS
Java 12.0.1	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1	FS
OpenSSL 1.0.1l R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp521r1	FS
OpenSSL 1.0.2s R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
OpenSSL 1.1.0k R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH x25519	FS
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519	FS
Opera 117 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519	FS
Safari 6 / iOS 6.0.1	Server sent fatal alert: handshake_failure				
Safari 7 / iOS 7.1 R	Server sent fatal alert: handshake_failure				
Safari 7 / OS X 10.9 R	Server sent fatal alert: handshake_failure				
Safari 8 / iOS 8.4 R	Server sent fatal alert: handshake_failure				
Safari 8 / OS X 10.10 R	Server sent fatal alert: handshake_failure				
Safari 9 / iOS 9 R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Safari 9 / OS X 10.11 R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Safari 10 / iOS 10 R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Safari 10 / OS X 10.12 R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519	FS
Safari 12.1.1 / iOS 12.3.1 R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519	FS
Apple ATS 9 / iOS 9 R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Yahoo Slurp Jan 2015	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
YandexBot Jan 2015	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp521r1	FS

Not simulated clients (Protocol mismatch)



[Click here to expand](#)

- (1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.
- (2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.
- (3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.
- (R) Denotes a reference browser or client, with which we expect better effective security.
- (All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).
- (All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.**



Protocol Details

Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No

Protocol Details

BEAST attack	Mitigated server-side (more info)
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info)
GOLDENDOODLE	No (more info)
OpenSSL 0-Length	No (more info)
Sleeping POODLE	No (more info)
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
ALPN	Yes http/1.1
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No
Supported Named Groups	x25519, secp256r1, x448, secp521r1, secp384r1, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 (server preferred order)
PQC Key Exchange	Not Supported
Supported PQC Groups	-
SSL 2 handshake compatibility	No
0-RTT enabled	No



HTTP Requests

1 https://server.segtor.tr/ (HTTP/1.1 200 OK)





Miscellaneous

Test date	Sun, 05 Jul 2026 20:29:25 UTC
Test duration	79.592 seconds
HTTP status code	200
HTTP server signature	Apache
Server hostname	server.segtor.tr

