# SSL Report: ctb.rajbhasha.gov.in (164.100.252.48)

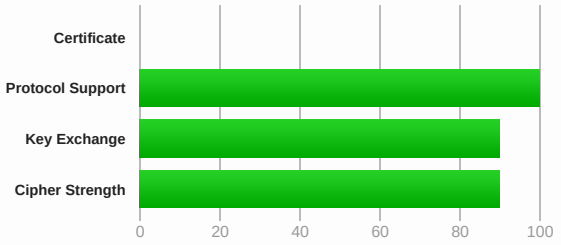
**Assessed on:** Sat, 24 Oct 2026 05:53:40 UTC | **HIDDEN** | Clear cache

**Scan Another »**

## Summary

Overall Rating

F




Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server's certificate is not trusted, see below for details.

This server supports TLS 1.3. MORE INFO »

This server supports PQC (Post-Quantum Cryptography) key exchange.

DNS Certification Authority Authorization (CAA) Policy found for this domain. MORE INFO »

## Certificate #1: RSA 2048 bits (SHA384withRSA)

### Server Key and Certificate #1

| | |
|---|---|
| **Subject** | *.rajbhasha.gov.in<br>Fingerprint SHA256: 13f96c04b335325364e9214ffc0576494a1f2fa6e8e54d0d8dcc932c795a3a18<br>Pin SHA256: iJCP/CQj7x1PtXthIVa0UzTvPh+DFt5UlWohjSVElEg= |
| **Common names** | *.rajbhasha.gov.in |
| **Alternative names** | *.rajbhasha.gov.in |
| **Serial Number** | 670e7e2d774953d7a6365bc5fa15be |
| **Valid from** | Mon, 17 Aug 2026 03:11:31 UTC |
| **Valid until** | Sun, 15 Nov 2026 03:11:31 UTC (expires in 21 days, 21 hours) |
| **Key** | RSA 2048 bits (e 65537) |
| **Weak key (Debian)** | No |
| **Issuer** | EM DV TLS CA - G2A-1<br>AIA: http://repository.emsign.com/certs/EMDVTLSCAG2A1EE.p7c |
| **Signature algorithm** | SHA384withRSA |
| **Extended Validation** | No |
| **Certificate Transparency** | **Yes (certificate)** |
| **OCSP Must Staple** | No |
| **Revocation information** | CRL, OCSP<br>CRL: http://crl.emsign.com?EMDVTLSCAG2A1.crl<br>OCSP: http://ocsp-a.emsign.com |
| **Revocation status** | Revoked **INSECURE** |
| **DNS CAA** | **Yes**<br>policy host: rajbhasha.gov.in<br>issue: emsign.com flags:0 |

## Server Key and Certificate #1

| | |
|---|---|
| | issuewild: emudra.com flags:0<br>issue: emudra.com flags:0<br>issue: letsencrypt.org flags:0<br>issuewild: emsign.com flags:0 |
| **Trusted** | No **NOT TRUSTED** (Why?)<br>**Mozilla Apple Android Java Windows** |

## Additional Certificates (if supplied)

| | |
|---|---|
| **Certificates provided** | 6 (8460 bytes) |
| **Chain issues** | **Contains anchor** |

### #2

| | |
|---|---|
| **Subject** | EM DV TLS CA - G2A-1<br>Fingerprint SHA256: 122a5433d8a2a8c501d5e680ab216885a6019326a189df91e8895f8b5ad488dd<br>Pin SHA256: zrUpja649ZJ5SAtGACyJ93Vcw6FpUUsRuBC+/BlaANg= |
| **Valid until** | Sun, 31 Dec 2028 23:59:59 UTC (expires in 2 years and 2 months) |
| **Key** | RSA 4096 bits (e 65537) |
| **Issuer** | AAA Certificate Services |
| **Signature algorithm** | SHA256withRSA |

### #3

| | |
|---|---|
| **Subject** | AAA Certificate Services In trust store<br>Fingerprint SHA256: d7a7a0fb5d7e2731d771e9484ebcdef71d5f0c3e0a2948782bc83ee0ea699ef4<br>Pin SHA256: vRU+17BDT2iGsXvOi76E7TQMcTLXAqj0+jGPdW7L1vM= |
| **Valid until** | Sun, 31 Dec 2028 23:59:59 UTC (expires in 2 years and 2 months) |
| **Key** | RSA 2048 bits (e 65537) |
| **Issuer** | AAA Certificate Services Self-signed |
| **Signature algorithm** | SHA1withRSA Weak, but no impact on root certificate |

### #4

| | |
|---|---|
| **Subject** | EM DV TLS CA - G2A-1<br>Fingerprint SHA256: 3f13597d3355d341bd09328aee567d7f4e002d9919b986f9962daff197ea75d1<br>Pin SHA256: zrUpja649ZJ5SAtGACyJ93Vcw6FpUUsRuBC+/BlaANg= |
| **Valid until** | Mon, 28 May 2040 07:16:12 UTC (expires in 13 years and 7 months) |
| **Key** | RSA 4096 bits (e 65537) |
| **Issuer** | emSign Root TLS CA - G1 |
| **Signature algorithm** | SHA384withRSA |

### #5

| | |
|---|---|
| **Subject** | emSign Root TLS CA - G1<br>Fingerprint SHA256: 9b913476eab476e21e0887dbcde44345d1359d28116b83b7cd3e87bd807ebf68<br>Pin SHA256: 7OKONSic6GIcckB5SeUFAFKtRgfMMy6vm1RgKarL+3o= |
| **Valid until** | Sat, 09 Jul 2039 18:30:00 UTC (expires in 12 years and 8 months) |
| **Key** | RSA 4096 bits (e 65537) |
| **Issuer** | emSign Root CA - G1 |
| **Signature algorithm** | SHA256withRSA |

### #6

| | |
|---|---|
| **Subject** | emSign Root CA - G1 In trust store<br>Fingerprint SHA256: 40f6af0346a99aa1cd1d555a4e9cce62c7f9634603ee406615833dc8c8d00367<br>Pin SHA256: N2oacIKlk9zMINVh0Rnpq40w8RzDIdCjf6QfDfKE4Bw= |
| **Valid until** | Wed, 18 Feb 2043 18:30:00 UTC (expires in 16 years and 3 months) |
| **Key** | RSA 2048 bits (e 65537) |
| **Issuer** | emSign Root CA - G1 Self-signed |
| **Signature algorithm** | SHA256withRSA |

## Certification Paths

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 |

### Cipher Suites

| # TLS 1.3 (suites in server-preferred order) | | |
|---|---|---|
| TLS_AES_256_GCM_SHA384 (0x1302) | X25519MLKEM768 (eq. 3072 bits RSA) FS | 256 |
| TLS_CHACHA20_POLY1305_SHA256 (0x1303) | X25519MLKEM768 (eq. 3072 bits RSA) FS | 256 |
| TLS_AES_128_GCM_SHA256 (0x1301) | X25519MLKEM768 (eq. 3072 bits RSA) FS | 128 |

| # TLS 1.2 (suites in server-preferred order) | | |
|---|---|---|
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) | ECDH x25519 (eq. 3072 bits RSA) FS | 256 |
| TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) | DH 2048 bits FS | 256 |
| TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) | ECDH x25519 (eq. 3072 bits RSA) FS | 256 |
| TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa) | DH 2048 bits FS | 256 |
| TLS_DHE_RSA_WITH_AES_256_CCM (0xc09f) | DH 2048 bits FS | 256 |
| TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc061) | ECDH x25519 (eq. 3072 bits RSA) FS | 256 |
| TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc053) | DH 2048 bits FS | 256 |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) | ECDH x25519 (eq. 3072 bits RSA) FS | 128 |
| TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) | DH 2048 bits FS | 128 |
| TLS_DHE_RSA_WITH_AES_128_CCM (0xc09e) | DH 2048 bits FS | 128 |
| TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc060) | ECDH x25519 (eq. 3072 bits RSA) FS | 128 |
| TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc052) | DH 2048 bits FS | 128 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) | ECDH x25519 (eq. 3072 bits RSA) FS **WEAK** | 256 |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) | DH 2048 bits FS **WEAK** | 256 |
| TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (0xc077) | ECDH x25519 (eq. 3072 bits RSA) FS **WEAK** | 256 |
| TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0xc4) | DH 2048 bits FS **WEAK** | 256 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) | ECDH x25519 (eq. 3072 bits RSA) FS **WEAK** | 128 |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) | DH 2048 bits FS **WEAK** | 128 |
| TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xc076) | ECDH x25519 (eq. 3072 bits RSA) FS **WEAK** | 128 |
| TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xbe) | DH 2048 bits FS **WEAK** | 128 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | ECDH x25519 (eq. 3072 bits RSA) FS **WEAK** | 256 |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) | DH 2048 bits FS **WEAK** | 256 |
| TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) | DH 2048 bits FS **WEAK** | 256 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) | ECDH x25519 (eq. 3072 bits RSA) FS **WEAK** | 128 |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) | DH 2048 bits FS **WEAK** | 128 |
| TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) | DH 2048 bits FS **WEAK** | 128 |
| TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK** | | 256 |
| TLS_RSA_WITH_AES_256_CCM (0xc09d) **WEAK** | | 256 |
| TLS_RSA_WITH_ARIA_256_GCM_SHA384 (0xc051) **WEAK** | | 256 |
| TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK** | | 128 |
| TLS_RSA_WITH_AES_128_CCM (0xc09c) **WEAK** | | 128 |

### Cipher Suites

| | | |
|---|---|---|
| TLS_RSA_WITH_ARIA_128_GCM_SHA256 (0xc050) | **WEAK** | 128 |
| TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) | **WEAK** | 256 |
| TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0xc0) | **WEAK** | 256 |
| TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) | **WEAK** | 128 |
| TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xba) | **WEAK** | 128 |
| TLS_RSA_WITH_AES_256_CBC_SHA (0x35) | **WEAK** | 256 |
| TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) | **WEAK** | 256 |
| TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) | **WEAK** | 128 |
| TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) | **WEAK** | 128 |

### Handshake Simulation

| | | | | | |
|---|---|---|---|---|---|
| Android 4.4.2 | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Android 5.0.0 | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Android 6.0 | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Android 7.0 | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 | FS |
| Android 8.0 | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 | FS |
| Android 8.1 | - | TLS 1.3 | TLS_AES_256_GCM_SHA384 | ECDH x25519 | FS |
| Android 9.0 | - | TLS 1.3 | TLS_AES_256_GCM_SHA384 | ECDH x25519 | FS |
| BingPreview Jan 2015 | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Chrome 49 / XP SP3 | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 | ECDH secp256r1 | FS |
| Chrome 69 / Win 7 R | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 | FS |
| Chrome 70 / Win 10 | - | TLS 1.3 | TLS_AES_256_GCM_SHA384 | ECDH x25519 | FS |
| Chrome 80 / Win 10 R | - | TLS 1.3 | TLS_AES_256_GCM_SHA384 | ECDH x25519 | FS |
| Chrome 131 / Win 10 R | - | TLS 1.3 | TLS_AES_256_GCM_SHA384 | PQC X25519MLKEM768 | FS |
| Firefox 31.3.0 ESR / Win 7 | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Firefox 47 / Win 7 R | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 | ECDH secp256r1 | FS |
| Firefox 49 / XP SP3 | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Firefox 62 / Win 7 R | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 | FS |
| Firefox 73 / Win 10 R | - | TLS 1.3 | TLS_AES_256_GCM_SHA384 | ECDH x25519 | FS |
| Firefox 135 / Win 10 R | - | TLS 1.3 | TLS_AES_256_GCM_SHA384 | PQC X25519MLKEM768 | FS |
| Googlebot Feb 2018 | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 | FS |
| IE 11 / Win 7 R | RSA 2048 (SHA384) | TLS 1.2 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | DH 2048 | FS |
| IE 11 / Win 8.1 R | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | DH 2048 | FS |
| IE 11 / Win Phone 8.1 R | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | ECDH secp256r1 | FS |
| IE 11 / Win Phone 8.1 Update R | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | DH 2048 | FS |
| IE 11 / Win 10 R | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Edge 15 / Win 10 R | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 | FS |
| Edge 16 / Win 10 R | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 | FS |
| Edge 18 / Win 10 R | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 | FS |
| Edge 131 / Win 10 R | - | TLS 1.3 | TLS_AES_256_GCM_SHA384 | PQC X25519MLKEM768 | FS |
| Edge 13 / Win Phone 10 R | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Java 8u161 | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Java 11.0.3 | - | TLS 1.3 | TLS_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Java 12.0.1 | - | TLS 1.3 | TLS_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| OpenSSL 1.0.1l R | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| OpenSSL 1.0.2s R | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| OpenSSL 1.1.0k R | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_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_256_GCM_SHA384 | PQC X25519MLKEM768 | FS |
| Safari 6 / iOS 6.0.1 | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 | FS |
| Safari 7 / iOS 7.1 R | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 | FS |

### Handshake Simulation

| | | | | |
|---|---|---|---|---|
| Safari 7 / OS X 10.9 R | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 FS |
| Safari 8 / iOS 8.4 R | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 FS |
| Safari 8 / OS X 10.10 R | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 FS |
| Safari 9 / iOS 9 R | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Safari 9 / OS X 10.11 R | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Safari 10 / iOS 10 R | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Safari 10 / OS X 10.12 R | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Safari 12.1.2 / MacOS 10.14.6 Beta R | - | TLS 1.3 | TLS_AES_256_GCM_SHA384 | ECDH x25519 FS |
| Safari 12.1.1 / iOS 12.3.1 R | - | TLS 1.3 | TLS_AES_256_GCM_SHA384 | ECDH x25519 FS |
| Apple ATS 9 / iOS 9 R | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Yahoo Slurp Jan 2015 | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| YandexBot Jan 2015 | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 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 |
| **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) TLS 1.2 : 0xc027 |
| **GOLDENDOODLE** | No (more info) TLS 1.2 : 0xc027 |
| **OpenSSL 0-Length** | No (more info) TLS 1.2 : 0xc027 |
| **Sleeping POODLE** | No (more info) TLS 1.2 : 0xc027 |
| **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) |

### Protocol Details

| | |
|---|---|
| **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 |
| **DH public server param (Ys) reuse** | No |
| **ECDH public server param reuse** | No |
| **Supported Named Groups** | X25519MLKEM768, x25519, secp256r1, x448, secp384r1, secp521r1, ffdhe2048, ffdhe3072 (server preferred order) |
| **PQC Key Exchange** | **Supported** |
| **Supported PQC Groups** | X25519MLKEM768 |
| **SSL 2 handshake compatibility** | No |
| **0-RTT enabled** | No |

### HTTP Requests

1 **https://ctb.rajbhasha.gov.in/** (HTTP/1.1 200 OK)

### Miscellaneous

| | |
|---|---|
| **Test date** | Sat, 24 Oct 2026 05:50:10 UTC |
| **Test duration** | 209.496 seconds |
| **HTTP status code** | 200 |
| **HTTP server signature** | Apache/2.4.68 (Win64) OpenSSL/3.6.3 PHP/7.4.9 |
| **Server hostname** | - |

## Why is my certificate not trusted?

There are many reasons why a certificate may not be trusted. The exact problem is indicated on the report card in bright red. The problems fall into three categories:

1. Invalid certificate
2. Invalid configuration
3. Unknown Certificate Authority

**1. Invalid certificate**

A certificate is invalid if:

- It is used before its activation date
- It is used after its expiry date
- Certificate hostnames don't match the site hostname
- It has been revoked
- It has insecure signature
- It has been blacklisted

**2. Invalid configuration**

In some cases, the certificate chain does not contain all the necessary certificates to connect the web server certificate to one of the root certificates in our trust store. Less commonly, one of the certificates in the chain (other than the web server certificate) will have expired, and that invalidates the entire chain.

**3. Unknown Certificate Authority**

In order for trust to be established, we must have the root certificate of the signing Certificate Authority in our trust store. SSL Labs does not maintain its own trust store; instead we use the store maintained by Mozilla.

If we mark a web site as not trusted, that means that the average web user's browser will not trust it either. For certain special groups of users, such web sites can still be secure. For example, if you can securely verify that a self-signed web site is operated by a person you trust, then you can trust that self-signed web site too. Or, if you work for an organisation that manages its own trust, and you have their own root certificate already embedded in your browser. Such special cases do not work for the general public, however, and this is what we indicate on our report card.

**4. Interoperability issues**

In some rare cases trust cannot be established because of interoperability issues between our code and the code or configuration running on the server. We manually review such cases, but if you encounter such an issue please feel free to contact us. Such problems are very difficult to troubleshoot and you may be able to provide us with information that might help us determine the root cause.

SSL Report v2.4.3

Copyright © 2009-2026 Qualys, Inc. All Rights Reserved. Privacy Policy. Terms and Conditions

Try Qualys for free! Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps, including certificate security solutions.