# SSL Report: doingbusinesskenya.go.ke (41.76.171.1)

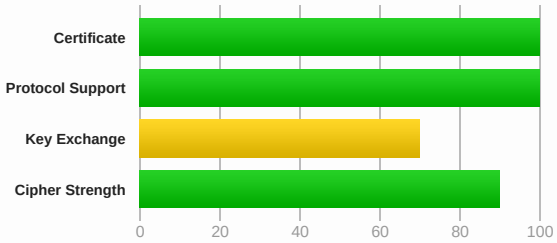
**Assessed on:** Mon, 26 Oct 2026 09:05:08 UTC | **HIDDEN** | Clear cache

**Scan Another »**

## Summary

Overall Rating

**B**




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

This server does not support Forward Secrecy with the reference browsers. Grade capped to B. MORE INFO »

HTTP request to this server failed, see below for details.

This site works only in browsers with SNI support.

This server supports TLS 1.3. MORE INFO »

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

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

### Server Key and Certificate #1

| | |
|---|---|
| **Subject** | *.doingbusinesskenya.go.ke<br>Fingerprint SHA256: af66998331151b1e0bc86065bd39dc14f7750e8ac9dfa328f7db6e4a59f43623<br>Pin SHA256: YKqClT0lc0EuAHbYO2rlIGAFSW8j46e1qaYSDkUNW4Y= |
| **Common names** | *.doingbusinesskenya.go.ke |
| **Alternative names** | doingbusinesskenya.go.ke *.doingbusinesskenya.go.ke |
| **Serial Number** | 0098b13a1a12d4105f166881288c0a7c |
| **Valid from** | Fri, 16 Oct 2026 09:03:49 UTC |
| **Valid until** | Wed, 13 Jan 2027 09:03:49 UTC (expires in 2 months and 17 days) |
| **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** | Good (not revoked) |

## Server Key and Certificate #1

| | |
|---|---|
| DNS CAA | No (more info) |
| Trusted | Yes<br>Mozilla Apple Android Java Windows |

## Additional Certificates (if supplied)

| | |
|---|---|
| Certificates provided | 6 (8517 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

## Certificate #2: RSA 2048 bits (SHA384withRSA) 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_RSA_WITH_AES_128_CBC_SHA (0x2f) | WEAK | 128 |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) | DH 2048 bits FS WEAK | 128 |
| TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) | WEAK | 128 |
| TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) | DH 2048 bits FS WEAK | 128 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) | ECDH secp521r1 (eq. 15360 bits RSA) FS WEAK | 128 |
| TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) | WEAK | 128 |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) | DH 2048 bits FS WEAK | 128 |
| TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) | WEAK | 128 |
| TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) | DH 2048 bits FS | 128 |
| TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xba) | WEAK | 128 |
| TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xbe) | DH 2048 bits FS WEAK | 128 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) | ECDH secp521r1 (eq. 15360 bits RSA) FS WEAK | 128 |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) | ECDH secp521r1 (eq. 15360 bits RSA) FS | 128 |
| TLS_RSA_WITH_ARIA_128_GCM_SHA256 (0xc050) | WEAK | 128 |
| TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc052) | DH 2048 bits FS | 128 |
| TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc060) | ECDH secp521r1 (eq. 15360 bits RSA) FS | 128 |
| TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xc076) | ECDH secp521r1 (eq. 15360 bits RSA) FS WEAK | 128 |
| TLS_RSA_WITH_AES_128_CCM (0xc09c) | WEAK | 128 |
| TLS_DHE_RSA_WITH_AES_128_CCM (0xc09e) | DH 2048 bits FS | 128 |
| TLS_RSA_WITH_AES_128_CCM_8 (0xc0a0) | WEAK | 128 |
| TLS_DHE_RSA_WITH_AES_128_CCM_8 (0xc0a2) | DH 2048 bits FS | 128 |
| TLS_RSA_WITH_AES_256_CBC_SHA (0x35) | WEAK | 256 |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) | DH 2048 bits FS WEAK | 256 |
| TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) | WEAK | 256 |
| TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) | DH 2048 bits FS WEAK | 256 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | ECDH secp521r1 (eq. 15360 bits RSA) FS WEAK | 256 |
| TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) | WEAK | 256 |

### Cipher Suites

| | | |
|---|---|---|
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 2048 bits FS **WEAK** | | 256 |
| TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK** | | 256 |
| TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS | | 256 |
| TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0xc0) **WEAK** | | 256 |
| TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0xc4) DH 2048 bits FS **WEAK** | | 256 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp521r1 (eq. 15360 bits RSA) FS **WEAK** | | 256 |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp521r1 (eq. 15360 bits RSA) FS | | 256 |
| TLS_RSA_WITH_ARIA_256_GCM_SHA384 (0xc051) **WEAK** | | 256 |
| TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc053) DH 2048 bits FS | | 256 |
| TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc061) ECDH secp521r1 (eq. 15360 bits RSA) FS | | 256 |
| TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (0xc077) ECDH secp521r1 (eq. 15360 bits RSA) FS **WEAK** | | 256 |
| TLS_RSA_WITH_AES_256_CCM (0xc09d) **WEAK** | | 256 |
| TLS_DHE_RSA_WITH_AES_256_CCM (0xc09f) DH 2048 bits FS | | 256 |
| TLS_RSA_WITH_AES_256_CCM_8 (0xc0a1) **WEAK** | | 256 |
| TLS_DHE_RSA_WITH_AES_256_CCM_8 (0xc0a3) DH 2048 bits FS | | 256 |
| TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH secp521r1 (eq. 15360 bits RSA) FS | | 256 |
| TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa) DH 2048 bits FS | | 256 |

### Handshake Simulation

| | | | |
|---|---|---|---|
| Android 4.4.2 | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS |
| Android 5.0.0 | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 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_CHACHA20_POLY1305_SHA256 ECDH x25519 FS |
| Android 8.0 | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_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 | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS |
| Chrome 49 / XP SP3 | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Chrome 69 / Win 7 R | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS |
| Chrome 70 / Win 10 | - | TLS 1.3 | TLS_AES_128_GCM_SHA256 ECDH x25519 FS |
| 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 | 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_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Firefox 49 / XP SP3 | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Firefox 62 / Win 7 R | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_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 | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS |
| IE 11 / Win 7 R | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS |
| IE 11 / Win 8.1 R | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS |
| IE 11 / Win Phone 8.1 R | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_RSA_WITH_AES_128_CBC_SHA256 No FS |
| IE 11 / Win Phone 8.1 Update R | RSA 2048 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 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_128_GCM_SHA256 ECDH x25519 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_CBC_SHA384 ECDH secp256r1 FS |
| Java 11.0.3 | - | TLS 1.3 | TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS |

### Handshake Simulation

| | | | |
|---|---|---|---|
| Java 12.0.1 | - | TLS 1.3 | TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| OpenSSL 1.0.1l R | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 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_128_GCM_SHA256 ECDH x25519 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 |
| 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_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 | 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 secp384r1 FS |
| YandexBot Jan 2015 | RSA 2048 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_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 |
| **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 : 0x002f |
| **GOLDENDOODLE** | No (more info) TLS 1.2 : 0x002f |
| **OpenSSL 0-Length** | No (more info) TLS 1.2 : 0x002f |
| **Sleeping POODLE** | No (more info) TLS 1.2 : 0x002f |
| **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** | **With some browsers** (more info) |

## Protocol Details

| | |
|---|---|
| **ALPN** | Yes http/1.1 |
| **NPN** | No |
| **Session resumption (caching)** | Yes |
| **Session resumption (tickets)** | No |
| **OCSP stapling** | No |
| **Strict Transport Security (HSTS)** | Unknown (failed HTTP request?) |
| **HSTS Preloading** | Not in: Chrome Edge Firefox IE |
| **Public Key Pinning (HPKP)** | Unknown (failed HTTP request?) |
| **Public Key Pinning Report-Only** | Unknown (failed HTTP request?) |
| **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** | 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://doingbusinesskenya.go.ke/** (Request failed)

## Miscellaneous

| | |
|---|---|
| **Test date** | Mon, 26 Oct 2026 09:00:09 UTC |
| **Test duration** | 298.491 seconds |
| **HTTP status code** | Request failed |
| **HTTP server signature** | Unknown |
| **Server hostname** | - |

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.