Qualys. SSL Labs

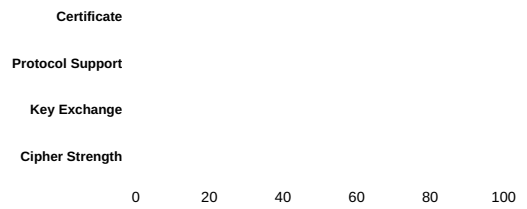


# SSL Report: api.tplinkra.com (44.195.227.47)

## Summary

**Overall Rating**

**A-**




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

There is no support for secure renegotiation. Grade reduced to A-. MORE INFO »

## Certificate #1: RSA 2048 bits (SHA256withRSA)

### Server Key and Certificate #1

| | |
|---|---|
| **Subject** | *.tplinkra.com<br>Fingerprint SHA256: 2e44a9bc3b7e04f99a958d4c0e50f70a8cdb553bf2866b8c2ef4802f3cbdc08b<br>Pin SHA256: P7zmM8ww7cnOoQ4cS9rmOupjskBvGBdvsyBoiOgTQYQ= |
| **Common names** | *.tplinkra.com |
| **Alternative names** | *.tplinkra.com tplinkra.com |
| **Serial Number** | 6be891ed6d0483ea |
| **Valid from** | Mon, 25 Mar 2024 02:31:30 UTC |
| **Valid until** | Sat, 26 Apr 2025 02:31:30 UTC (expires in 10 months and 9 days) |
| **Key** | RSA 2048 bits (e 65537) |
| **Weak key (Debian)** | No |
| **Issuer** | Go Daddy Secure Certificate Authority - G2<br>AIA: http://certificates.godaddy.com/repository/gdig2.crt |
| **Signature algorithm** | SHA256withRSA |
| **Extended Validation** | No |
| **Certificate Transparency** | Yes (certificate) |
| **OCSP Must Staple** | No |
| **Revocation information** | CRL, OCSP<br>CRL: http://crl.godaddy.com/gdig2s1-19154.crl<br>OCSP: http://ocsp.godaddy.com/ |
| **Revocation status** | Good (not revoked) |
| **DNS CAA** | No (more info) |
| **Trusted** | Yes<br>Mozilla Apple Android Java Windows |

### Additional Certificates (if supplied)

| | |
|---|---|
| **Certificates provided** | 4 (5101 bytes) |
| **Chain issues** | Contains anchor |

#### #2

| | |
|---|---|
| **Subject** | Go Daddy Secure Certificate Authority - G2<br>Fingerprint SHA256: 973a41276ffd01e027a2aad49e34c37846d3e976ff6a620b6712e33832041aa6<br>Pin SHA256: 8Rw90Ej3Ttt8RRkrg+WYDS9n7IS03bk5bjP/UXPtaY8= |
| **Valid until** | Sat, 03 May 2031 07:00:00 UTC (expires in 6 years and 10 months) |
| **Key** | RSA 2048 bits (e 65537) |
| **Issuer** | Go Daddy Root Certificate Authority - G2 |
| **Signature algorithm** | SHA256withRSA |

### Additional Certificates (if supplied)

#### #3

| | |
|---|---|
| **Subject** | Go Daddy Root Certificate Authority - G2<br>Fingerprint SHA256: 3a2fbe92891e57fe05d57087f48e730f17e5a5f53ef403d618e5b74d7a7e6ecb<br>Pin SHA256: Ko8tivDrEjiY90yGasP6ZpBU4jwXvHqVvQI0GS3GNdA= |
| **Valid until** | Fri, 30 May 2031 07:00:00 UTC (expires in 6 years and 11 months) |
| **Key** | RSA 2048 bits (e 65537) |
| **Issuer** | The Go Daddy Group, Inc. / Go Daddy Class 2 Certification Authority |
| **Signature algorithm** | SHA256withRSA |

#### #4

| | |
|---|---|
| **Subject** | The Go Daddy Group, Inc. / Go Daddy Class 2 Certification Authority In trust store<br>Fingerprint SHA256: c3846bf24b9e93ca64274c0ec67c1ecc5e024ffcacd2d74019350e81fe546ae4<br>Pin SHA256: VjLZe/p3W/PJnd6lL8JVNBCGQBZynFLdZSTIqcO0SJ8= |
| **Valid until** | Thu, 29 Jun 2034 17:06:20 UTC (expires in 10 years) |
| **Key** | RSA 2048 bits (e 3) |
| **Issuer** | The Go Daddy Group, Inc. / Go Daddy Class 2 Certification Authority Self-signed |
| **Signature algorithm** | SHA1withRSA Weak, but no impact on root certificate |

### Certification Paths

Click here to expand

## Configuration

### Protocols

| | |
|---|---|
| TLS 1.3 | No |
| TLS 1.2 | Yes |
| TLS 1.1 | No |
| TLS 1.0 | No |
| SSL 3 | No |
| SSL 2 | No |

### Cipher Suites

**# TLS 1.2 (suites in server-preferred order)**

| | |
|---|---|
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS | 128 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK** | 128 |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS | 256 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK** | 256 |
| TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK** | 128 |
| TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) **WEAK** | 128 |
| TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK** | 256 |
| TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) **WEAK** | 256 |

### Handshake Simulation

| | | | | |
|---|---|---|---|---|
| Android 4.4.2 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Android 5.0.0 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Android 6.0 | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Android 7.0 | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Android 8.0 | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Android 8.1 | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Android 9.0 | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| BingPreview Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Chrome 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Chrome 69 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Chrome 70 / Win 10 | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Chrome 80 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Firefox 31.3.0 ESR / Win 7 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |

## Handshake Simulation

| | | | |
|---|---|---|---|
| Firefox 47 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Firefox 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Firefox 62 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Firefox 73 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Googlebot Feb 2018 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| IE 11 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS |
| IE 11 / Win 8.1 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS |
| IE 11 / Win Phone 8.1 R | RSA 2048 (SHA256) | 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 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS |
| IE 11 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Edge 15 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Edge 16 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Edge 18 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Edge 13 / Win Phone 10 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Java 8u161 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Java 11.0.3 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Java 12.0.1 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| OpenSSL 1.0.1l R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| OpenSSL 1.0.2s R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| OpenSSL 1.1.0k R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| OpenSSL 1.1.1c R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Safari 6 / iOS 6.0.1 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS |
| Safari 7 / iOS 7.1 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS |
| Safari 7 / OS X 10.9 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS |
| Safari 8 / iOS 8.4 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS |
| Safari 8 / OS X 10.10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS |
| Safari 9 / iOS 9 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Safari 9 / OS X 10.11 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Safari 10 / iOS 10 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Safari 10 / OS X 10.12 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Safari 12.1.2 / MacOS 10.14.6 Beta R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Safari 12.1.1 / iOS 12.3.1 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Apple ATS 9 / iOS 9 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Yahoo Slurp Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| YandexBot Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 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

| | |
|---|---|
| **Renegotiation** | Unknown |
| **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** | Unknown (requires support for at least two protocols, excl. SSL2) |
| **SSL/TLS compression** | No |
| **RC4** | No |
| **Heartbeat (extension)** | No |
| **Heartbleed (vulnerability)** | No (more info) |

## Protocol Details

| | |
|---|---|
| **Ticketbleed (vulnerability)** | No (more info) |
| **OpenSSL CCS vuln. (CVE-2014-0224)** | Unknown (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 h2 http/1.1 |
| **NPN** | Yes h2 http/1.1 |
| **Session resumption (caching)** | **No (IDs assigned but not accepted)** |
| **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** | - |
| **SSL 2 handshake compatibility** | Yes |

## HTTP Requests

1 **https://api.tplinkra.com/** (HTTP/1.1 200 OK)

## Miscellaneous

| | |
|---|---|
| **Test date** | Sun, 16 Jun 2024 17:28:11 UTC |
| **Test duration** | 117.351 seconds |
| **HTTP status code** | 200 |
| **HTTP server signature** | Jetty(tws) |
| **Server hostname** | ec2-44-195-227-47.compute-1.amazonaws.com |

SSL Report v2.3.0