Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > www.alpha.gr

# SSL Report: www.alpha.gr (193.193.184.47)

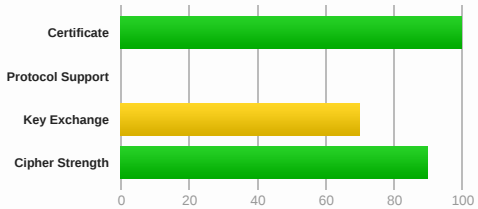
**Assessed on:** Mon, 25 Feb 2019 16:03:37 UTC | Hide | Clear cache

**Scan Another »**

## Summary

Overall Rating

F




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

This server is vulnerable to the Return Of Bleichenbacher's Oracle Threat (ROBOT) vulnerability. Grade set to F. MORE INFO »

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

This site works only in browsers with SNI support.

Renegotiation test has been disabled temporarily due to an Apache httpd 2.4.37 bug. MORE INFO »

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

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

### Server Key and Certificate #1

| | |
|---|---|
| Subject | www.alpha.gr<br>Fingerprint SHA256: 35bbfae464c9d873d964eb51699077e22938bbeacaf6f736140872af2b06f2ea<br>Pin SHA256: SY6iu+DtORiF+PzC+TCrp9N9Efh6KTbN84Er/0GT7tg= |
| Common names | www.alpha.gr |
| Alternative names | www.alpha.gr alpha.gr |
| Serial Number | 06e608f671c8f44e62b439003d364857 |
| Valid from | Mon, 13 Aug 2018 00:00:00 UTC |
| Valid until | Mon, 28 Oct 2019 12:00:00 UTC (expires in 8 months and 2 days) |
| Key | RSA 2048 bits (e 65537) |
| Weak key (Debian) | No |
| Issuer | DigiCert SHA2 Extended Validation Server CA<br>AIA: http://cacerts.digicert.com/DigiCertSHA2ExtendedValidationServerCA.crt |
| Signature algorithm | SHA256withRSA |
| Extended Validation | Yes |
| Certificate Transparency | Yes (certificate) |
| OCSP Must Staple | No |
| Revocation information | CRL, OCSP<br>CRL: http://crl3.digicert.com/sha2-ev-server-g2.crl<br>OCSP: http://ocsp.digicert.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 | 2 (2911 bytes) |
| Chain issues | None |

### Additional Certificates (if supplied)

#### #2

| | |
|---|---|
| **Subject** | DigiCert SHA2 Extended Validation Server CA<br>Fingerprint SHA256: 403e062a2653059113285baf80a0d4ae422c848c9f78fad01fc94bc5b87fef1a<br>Pin SHA256: RRM1dGqnDFsCJXBTHky16vi1obOlCgFFn/yOhl/y+ho= |
| **Valid until** | Sun, 22 Oct 2028 12:00:00 UTC (expires in 9 years and 7 months) |
| **Key** | RSA 2048 bits (e 65537) |
| **Issuer** | DigiCert High Assurance EV Root CA |
| **Signature algorithm** | SHA256withRSA |

### 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 |

For TLS 1.3 tests, we only support RFC 8446.

### Cipher Suites

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

| | |
|---|---|
| TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK** | 256 |
| TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK** | 128 |
| TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) **WEAK** | 256 |
| TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) **WEAK** | 128 |
| TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK** | 256 |
| TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK** | 128 |

### Handshake Simulation

| | | | |
|---|---|---|---|
| Android 4.4.2 | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_GCM_SHA384 No FS |
| Android 5.0.0 | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_128_GCM_SHA256 No FS |
| Android 6.0 | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_128_GCM_SHA256 No FS |
| Android 7.0 | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_GCM_SHA384 No FS |
| BingPreview Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_GCM_SHA384 No FS |
| Chrome 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_128_GCM_SHA256 No FS |
| Chrome 69 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_GCM_SHA384 No FS |
| Chrome 70 / Win 10 | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_GCM_SHA384 No FS |
| Firefox 31.3.0 ESR / Win 7 | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA No FS |
| Firefox 47 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA No FS |
| Firefox 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA No FS |
| Firefox 62 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA No FS |
| Googlebot Feb 2018 | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_GCM_SHA384 No FS |
| IE 11 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_GCM_SHA384 No FS |
| IE 11 / Win 8.1 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_GCM_SHA384 No FS |
| IE 11 / Win Phone 8.1 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA256 No FS |
| IE 11 / Win Phone 8.1 Update R | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_GCM_SHA384 No FS |
| IE 11 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_GCM_SHA384 No FS |
| Edge 15 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_GCM_SHA384 No FS |
| Edge 13 / Win Phone 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_GCM_SHA384 No FS |
| Java 8u161 | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_GCM_SHA384 No FS |

## Handshake Simulation

| | | | |
|---|---|---|---|
| OpenSSL 1.0.1l R | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_GCM_SHA384 No FS |
| OpenSSL 1.0.2e R | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_GCM_SHA384 No FS |
| Safari 6 / iOS 6.0.1 | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA256 No FS |
| Safari 7 / iOS 7.1 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA256 No FS |
| Safari 7 / OS X 10.9 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA256 No FS |
| Safari 8 / iOS 8.4 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA256 No FS |
| Safari 8 / OS X 10.10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA256 No FS |
| Safari 9 / iOS 9 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_GCM_SHA384 No FS |
| Safari 9 / OS X 10.11 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_GCM_SHA384 No FS |
| Safari 10 / iOS 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_GCM_SHA384 No FS |
| Safari 10 / OS X 10.12 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_GCM_SHA384 No FS |
| Apple ATS 9 / iOS 9 R | Server closed connection | | |
| Yahoo Slurp Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_GCM_SHA384 No FS |
| YandexBot Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_256_GCM_SHA384 No 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

| | |
|---|---|
| **DROWN** | No, server keys and hostname not seen elsewhere with SSLv2<br>**(1) For a better understanding of this test, please read this longer explanation**<br>(2) Key usage data kindly provided by the Censys network search engine; original DROWN website here<br>(3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete |
| **BEAST attack** | Mitigated server-side (more info) |
| **POODLE (SSLv3)** | No, SSL 3 not supported (more info) |
| **POODLE (TLS)** | No (more info) |
| **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) |
| **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)** | **Yes, but oracle is weak** (more info) |
| **Forward Secrecy** | **No WEAK** (more info) |
| **ALPN** | No |
| **NPN** | No |
| **Session resumption (caching)** | Yes |
| **Session resumption (tickets)** | No |
| **OCSP stapling** | No |
| **Strict Transport Security (HSTS)** | **Yes**<br>max-age=31536000; includeSubDomains |
| **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, ECDHE suites not supported |

## Protocol Details

| | |
|---|---|
| Supported Named Groups | - |
| SSL 2 handshake compatibility | No |

## HTTP Requests

1 https://www.alpha.gr/ (HTTP/1.1 200 OK)

## Miscellaneous

| | |
|---|---|
| Test date | Mon, 25 Feb 2019 16:01:47 UTC |
| Test duration | 109.868 seconds |
| HTTP status code | 200 |
| HTTP server signature | |
| Server hostname | 184a47 |

SSL Report v1.32.16