CAPLIN

# Qualys SSL Labs: SSL report

**Host**
libtest.caplin.com

**Date**
Sun, 5 Jun 2022 09:03:38 UTC

**Liberator version**
7.1.24

**Liberator configuration**

```
# Disable TLS versions SSLv2, SSLv3, TLSv1, and TLSv1.1
# (retain TLSv1.2 and TLSv1.3)
https-ssl-options SSL_OP_NO_SSLv2|SSL_OP_NO_SSLv3|SSL_OP_NO_TLSv1|
SSL_OP_NO_TLSv1_1

# Set OpenSSL cipher list
https-cipher-list "ECDHE+TLSv1.2+AESGCM ECDHE+TLSv1.2+AESCCM
ECDHE+TLSv1.2+CHACHA20 DHE+TLSv1.2+AESGCM DHE+TLSv1.2+AESCCM
DHE+TLSv1.2+CHACHA20"

# Diffie-Hellman parameters file (required for DHE cipher support)
https-dhparams ${SSLCERT_PATH}/rttpd-dhparam-2048.pem
```

**Description**

- Suitable for modern TLS clients that support TLS 1.2 and/or TLS 1.3
- Protocol versions: TLS 1.2 and TLS 1.3
- TLS 1.3 ciphers: all mandatory ciphers
- TLS 1.2 ciphers: forward secrecy (ECDHE and DHE) ciphers that implement AES-GCM, AES-CCM, or CHACHA20 encryption
- Diffie-Hellman parameters file: 2048 bit

**References**

- Configure how Liberator handles HTTPS connections
- SSL Labs SSL and TLS deployment best practices
- SSL Labs server rating guide

# SSL Report: libtest.caplin.com (94.31.7.221)

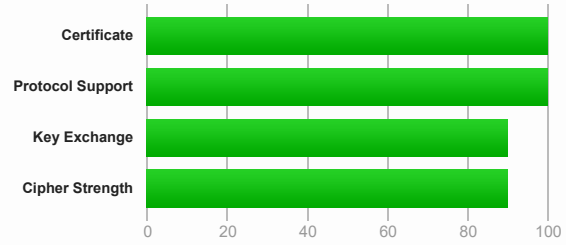
**Assessed on:** Sun, 05 Jun 2022 09:03:38 UTC | **HIDDEN** | Clear cache

Scan Another »

## Summary

Overall Rating

A+




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

This server supports TLS 1.3.

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 | *.caplin.com<br>Fingerprint SHA256: 6fcde2a6d98aa529ccff656f35f15a8da4c2f85ad5e37f7d8c39693ed0472f92<br>Pin SHA256: BQVGx9UINIzO5ifcgdEohLLOtSV/XMbRPgdP3cZYQ+8= |
| Common names | *.caplin.com |
| Alternative names | *.caplin.com caplin.com |
| Serial Number | 5716786e8f1f1b90 |
| Valid from | Wed, 16 Jun 2021 10:36:58 UTC |
| Valid until | Mon, 18 Jul 2022 10:36:58 UTC (expires in 1 month and 13 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/gdig2s1-3048.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 (5129 bytes) |
| Chain issues | Contains anchor |

#2

### Additional Certificates (if supplied)

| | |
|---|---|
| **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 8 years and 10 months) |
| **Key** | RSA 2048 bits (e 65537) |
| **Issuer** | Go Daddy Root Certificate Authority - G2 |
| **Signature algorithm** | SHA256withRSA |

#### #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 8 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 12 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 | Yes |
| TLS 1.2 | Yes |
| TLS 1.1 | No |
| TLS 1.0 | No |
| SSL 3 | No |
| SSL 2 | No |

### 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_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS | 128 |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp521r1 (eq. 15360 bits RSA) FS | 128 |
| TLS_DHE_RSA_WITH_AES_128_CCM (0xc09e) DH 2048 bits FS | 128 |
| TLS_DHE_RSA_WITH_AES_128_CCM_8 (0xc0a2) DH 2048 bits FS | 128 |
| TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS | 256 |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp521r1 (eq. 15360 bits RSA) FS | 256 |
| TLS_DHE_RSA_WITH_AES_256_CCM (0xc09f) DH 2048 bits FS | 256 |
| TLS_DHE_RSA_WITH_AES_256_CCM_8 (0xc0a3) DH 2048 bits FS | 256 |

## Cipher Suites

| | | |
|---|---|---|
| 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 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp521r1 FS |
| Android 5.0.0 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp521r1 FS |
| Android 6.0 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Android 7.0 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 | ECDH x25519 FS |
| Android 8.0 | RSA 2048 (SHA256) | TLS 1.2 | 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 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp521r1 FS |
| Chrome 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Chrome 69 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | 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 |
| Firefox 31.3.0 ESR / Win 7 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Firefox 47 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Firefox 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Firefox 62 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | 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 |
| Googlebot Feb 2018 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH x25519 FS |
| IE 11 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | DH 2048 FS |
| IE 11 / Win 8.1 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | DH 2048 FS |
| IE 11 / Win Phone 8.1 R | Server sent fatal alert: handshake_failure | | | |
| IE 11 / Win Phone 8.1 Update R | RSA 2048 (SHA256) | TLS 1.2 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | DH 2048 FS |
| IE 11 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Edge 15 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 FS |
| Edge 16 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 FS |
| Edge 18 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 FS |
| Edge 13 / Win Phone 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Java 8u161 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_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 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp521r1 FS |
| OpenSSL 1.0.2s R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| OpenSSL 1.1.0k R | RSA 2048 (SHA256) | 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 |
| 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 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Safari 9 / OS X 10.11 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Safari 10 / iOS 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Safari 10 / OS X 10.12 R | RSA 2048 (SHA256) | TLS 1.2 | 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 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Yahoo Slurp Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp384r1 FS |
| YandexBot Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp521r1 FS |

## Handshake Simulation

**# 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** | **Unable to perform this test due to an internal error.**<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<br>**INTERNAL ERROR: Connection refused (Connection refused)**<br>**INTERNAL ERROR: Connection refused (Connection refused)** |
| **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) |
| **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** | No |
| **NPN** | No |
| **Session resumption (caching)** | **No (IDs assigned but not accepted)** |
| **Session resumption (tickets)** | Yes |
| **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 |
| **DH public server param (Ys) reuse** | No |
| **ECDH public server param reuse** | No |
| **Supported Named Groups** | secp256r1, secp384r1, secp521r1, x25519, x448 (Server has no preference) |
| **SSL 2 handshake compatibility** | Yes |
| **0-RTT enabled** | No |

## HTTP Requests

1 https://libtest.caplin.com/ (HTTP/1.1 200 OK)

## Miscellaneous

| | |
|---|---|
| **Test date** | Sun, 05 Jun 2022 09:02:23 UTC |
| **Test duration** | 74.553 seconds |
| **HTTP status code** | 200 |
| **HTTP server signature** | unknown |
| **Server hostname** | 94.31.7.221.available.above.net |

SSL Report v2.1.10