QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > email.t-online.de

# SSL Report: email.t-online.de (62.153.158.211)

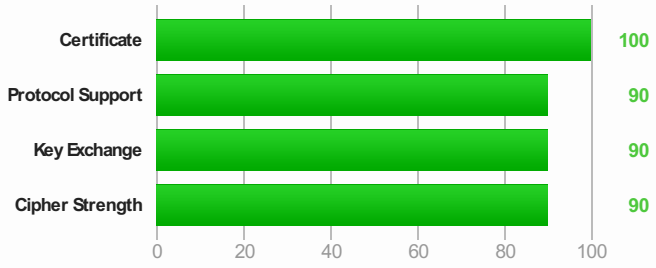
**Assessed on:** Mon Jun 23 08:07:45 UTC 2014 | Clear cache

**Scan Another »**

## Summary

Overall Rating

A+




Documentation: SSL/TLS Deployment Best Practices, SSL Server Rating Guide, and OpenSSL Cookbook.

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. MORE INFO »

This server is not vulnerable to the Heartbleed attack.

Experimental: This server is not vulnerable to the OpenSSL CCS vulnerability (CVE-2014-0224).

## Authentication

### Server Key and Certificate #1

| | |
|---|---|
| Common names | email.t-online.de |
| Alternative names | email.t-online.de |
| Prefix handling | Not required for subdomains |
| Valid from | Fri Mar 28 13:34:11 UTC 2014 |
| Valid until | Sat Mar 28 23:59:59 UTC 2015 (expires in 9 months and 8 days) |
| Key | RSA 2048 bits |
| Weak key (Debian) | No |
| Issuer | TeleSec ServerPass Extended Validation Class 3 CA |
| Signature algorithm | SHA256withRSA |
| Extended Validation | Yes |
| Revocation information | CRL, OCSP |
| Revocation status | Good (not revoked) |
| Trusted | Yes |

### Additional Certificates (if supplied)

| | |
|---|---|
| Certificates provided | 3 (4484 bytes) |
| Chain issues | Contains anchor |

#### #2

| | |
|---|---|
| Subject | TeleSec ServerPass Extended Validation Class 3 CA<br>SHA1: c6d43f5978e02e1fc64cf6fa94ac4b4d3adc8593 |
| Valid until | Sun Feb 11 23:59:59 UTC 2024 (expires in 9 years and 7 months) |

| | |
|---|---|
| **Key** | RSA 2048 bits |
| **Issuer** | T-TeleSec GlobalRoot Class 3 |
| **Signature algorithm** | SHA256withRSA |

### #3

| | |
|---|---|
| **Subject** | T-TeleSec GlobalRoot Class 3 In trust store<br>SHA1: 55a6723ecbf2eccdc3237470199d2abe11e381d1 |
| **Valid until** | Sat Oct 01 23:59:59 UTC 2033 (expires in 19 years and 3 months) |
| **Key** | RSA 2048 bits |
| **Issuer** | T-TeleSec GlobalRoot Class 3 Self-signed |
| **Signature algorithm** | SHA256withRSA |

### Certification Paths

#### Path #1: Trusted

| | | |
|---|---|---|
| 1 | Sent by server | email.t-online.de<br>SHA1: 43f7a752d54fd1fa2a56cf70285c0e619632a35f<br>RSA 2048 bits / SHA256withRSA |
| 2 | Sent by server | TeleSec ServerPass Extended Validation Class 3 CA<br>SHA1: c6d43f5978e02e1fc64cf6fa94ac4b4d3adc8593<br>RSA 2048 bits / SHA256withRSA |
| 3 | Sent by server<br>In trust store | T-TeleSec GlobalRoot Class 3<br>SHA1: 55a6723ecbf2eccdc3237470199d2abe11e381d1<br>RSA 2048 bits / SHA256withRSA |

## Configuration

### Protocols

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

### Cipher Suites (SSL 3+ suites in server-preferred order, then SSL 2 suites where used)

| | |
|---|---|
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH 256 bits (eq. 3072 bits RSA) FS | 256 |
| TLS_RSA_WITH_AES_256_CBC_SHA (0x35) | 256 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH 256 bits (eq. 3072 bits RSA) FS | 128 |
| TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) ECDH 256 bits (eq. 3072 bits RSA) FS | 128 |
| TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) | 128 |
| TLS_RSA_WITH_RC4_128_SHA (0x5) | 128 |

### Handshake Simulation

| | | | |
|---|---|---|---|
| Android 2.3.7 No SNI [2] | TLS 1.0 | TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS | 128 |
| Android 4.0.4 | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| Android 4.1.1 | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| Android 4.2.2 | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| Android 4.3 | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| Android 4.4.2 | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| BingBot Dec 2013 No SNI [2] | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| BingPreview Dec 2013 | TLS 1.0 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| Chrome 34 / OS X R | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |

| | | | |
|---|---|---|---|
| Firefox 24.2.0 ESR / Win 7 | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| Firefox 29 / OS X R | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| Googlebot Oct 2013 | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| IE 6 / XP No FS [1] No SNI [2] | SSL 3 | TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4 | 128 |
| IE 7 / Vista | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| IE 8 / XP No FS [1] No SNI [2] | TLS 1.0 | TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4 | 128 |
| IE 8-10 / Win 7 R | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| IE 11 / Win 7 R | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| IE 11 / Win 8.1 R | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| IE Mobile 10 / Win Phone 8.0 | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| IE Mobile 11 / Win Phone 8.1 | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| Java 6u45 No SNI [2] | TLS 1.0 | TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS | 128 |
| Java 7u25 | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS | 128 |
| Java 8b132 | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS | 128 |
| OpenSSL 0.9.8y | TLS 1.0 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| OpenSSL 1.0.1e | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| Safari 5.1.9 / OS X 10.6.8 | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| Safari 6 / iOS 6.0.1 R | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| Safari 7 / iOS 7.1 R | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| Safari 6.0.4 / OS X 10.8.4 R | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| Safari 7 / OS X 10.9 R | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| Yahoo Slurp Oct 2013 | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS | 256 |
| YandexBot May 2014 | TLS 1.0 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |

(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.
(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).

## Protocol Details

| | |
|---|---|
| **Secure Renegotiation** | **Supported** |
| **Secure Client-Initiated Renegotiation** | No |
| **Insecure Client-Initiated Renegotiation** | No |
| **BEAST attack** | Not mitigated server-side (more info) SSL 3: 0xc014, TLS 1.0: 0xc014 |
| **TLS compression** | No |
| **RC4** | Yes (not with TLS 1.1 and newer) (more info) |
| **Heartbeat (extension)** | No |
| **Heartbleed (vulnerability)** | No (more info) |
| **OpenSSL CCS vuln. (CVE-2014-0224)** | No |
| **Forward Secrecy** | With modern browsers (more info) |
| **Next Protocol Negotiation** | No |
| **Session resumption (caching)** | Yes |
| **Session resumption (tickets)** | No |
| **OCSP stapling** | No |
| **Strict Transport Security (HSTS)** | **Yes** max-age=31536000 |
| **Long handshake intolerance** | No |
| **TLS extension intolerance** | No |
| **TLS version intolerance** | No |
| **SSL 2 handshake compatibility** | Yes |

## Miscellaneous

| | |
|---|---|
| **Test date** | Mon Jun 23 08:06:44 UTC 2014 |
| **Test duration** | 61.342 seconds |

| | |
|---|---|
| **HTTP status code** | 200 |
| **HTTP server signature** | Apache |
| **Server hostname** | - |
| **PCI compliant** | Yes |
| **FIPS-ready** | No |

SSL Report v1.10.11