QUALYS SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > privat.ib.seb.se

# SSL Report: privat.ib.seb.se (129.178.53.85)

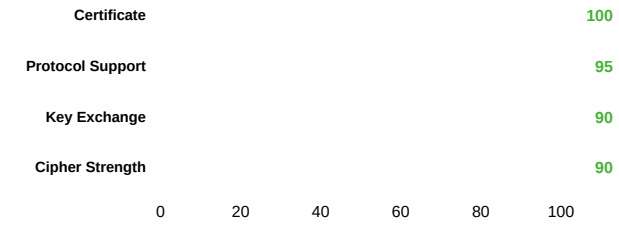
**Assessed on:** Wed, 07 Oct 2015 11:35:19 UTC | Clear cache

Scan Another »

## Summary

**Overall Rating**

**A-**




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

The server does not support Forward Secrecy with the reference browsers. Grade reduced to A-. MORE INFO »

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

## Authentication

### Server Key and Certificate #1

| | |
|---|---|
| **Common names** | privat.ib.seb.se |
| **Alternative names** | privat.ib.seb.se privat-in.ib.seb.se |
| **Prefix handling** | Not required for subdomains |
| **Valid from** | Wed, 04 Feb 2015 00:00:00 UTC |
| **Valid until** | Sat, 04 Feb 2017 23:59:59 UTC (expires in 1 year and 3 months) |
| **Key** | RSA 2048 bits (e 65537) |
| **Weak key (Debian)** | No |
| **Issuer** | Symantec Class 3 EV SSL CA - G3 |
| **Signature algorithm** | SHA256withRSA |
| **Extended Validation** | **Yes** |
| **Certificate Transparency** | **Yes (certificate)** |
| **Revocation information** | CRL, OCSP |
| **Revocation status** | Good (not revoked) |
| **Trusted** | **Yes** |

### Additional Certificates (if supplied)

| | |
|---|---|
| **Certificates provided** | 3 (4378 bytes) |
| **Chain issues** | **Contains anchor** |

#2

| | |
|---|---|
| **Subject** | Symantec Class 3 EV SSL CA - G3<br>Fingerprint: e3fc0ad84f2f5a83ed6f86f567f8b14b40dcbf12 |
| **Valid until** | Mon, 30 Oct 2023 23:59:59 UTC (expires in 8 years) |
| **Key** | RSA 2048 bits (e 65537) |
| **Issuer** | VeriSign Class 3 Public Primary Certification Authority - G5 |
| **Signature algorithm** | SHA256withRSA |

### Additional Certificates (if supplied)

#3

| | |
|---|---|
| **Subject** | VeriSign Class 3 Public Primary Certification Authority - G5 In trust store<br>Fingerprint: 4eb6d578499b1ccf5f581ead56be3d9b6744a5e5 |
| **Valid until** | Wed, 16 Jul 2036 23:59:59 UTC (expires in 20 years and 9 months) |
| **Key** | RSA 2048 bits (e 65537) |
| **Issuer** | VeriSign Class 3 Public Primary Certification Authority - G5 Self-signed |
| **Signature algorithm** | SHA1withRSA Weak, but no impact on root certificate |

### Certification Paths

#### Path #1: Trusted

| | | |
|---|---|---|
| **1** | Sent by server | privat.ib.seb.se<br>Fingerprint: eda7e337f33f123d2e4af0c2db27797de70c151d<br>RSA 2048 bits (e 65537) / SHA256withRSA |
| **2** | Sent by server | Symantec Class 3 EV SSL CA - G3<br>Fingerprint: e3fc0ad84f2f5a83ed6f86f567f8b14b40dcbf12<br>RSA 2048 bits (e 65537) / SHA256withRSA |
| **3** | Sent by server<br>In trust store | VeriSign Class 3 Public Primary Certification Authority - G5 Self-signed<br>Fingerprint: 4eb6d578499b1ccf5f581ead56be3d9b6744a5e5<br>RSA 2048 bits (e 65537) / SHA1withRSA<br>Weak or insecure signature, but no impact on root certificate |

## Configuration

### Protocols

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

### Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites at the end)

| | |
|---|---|
| TLS_RSA_WITH_AES_256_CBC_SHA (0x35) | 256 |
| TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) | 256 |
| TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) | 112 |
| TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) | 128 |
| TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) | 128 |

### Handshake Simulation

| | | | |
|---|---|---|---|
| Android 2.3.7 No SNI [2] | TLS 1.0 | TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS | 112 |
| Android 4.0.4 | TLS 1.0 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| Android 4.1.1 | TLS 1.0 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| Android 4.2.2 | TLS 1.0 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| Android 4.3 | TLS 1.0 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| Android 4.4.2 | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| Android 5.0.0 | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| Baidu Jan 2015 | TLS 1.0 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| BingPreview Jan 2015 | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| Chrome 43 / OS X R | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| Firefox 31.3.0 ESR / Win 7 | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| Firefox 39 / OS X R | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| Googlebot Feb 2015 | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| IE 6 / XP No FS [1] No SNI [2] | Protocol or cipher suite mismatch | | Fail[3] |

## Handshake Simulation

| | | | |
|---|---|---|---|
| IE 7 / Vista | TLS 1.0 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| IE 8 / XP No FS [1] No SNI [2] | TLS 1.0 | TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS | 112 |
| IE 8-10 / Win 7 R | TLS 1.0 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| IE 11 / Win 7 R | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| IE 11 / Win 8.1 R | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| IE 10 / Win Phone 8.0 | TLS 1.0 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| IE 11 / Win Phone 8.1 R | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| IE 11 / Win Phone 8.1 Update R | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| Edge 12 / Win 10 (Build 10130) R | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| Java 6u45 No SNI [2] | TLS 1.0 | TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS | 112 |
| Java 7u25 | TLS 1.0 | TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS | 112 |
| Java 8u31 | TLS 1.2 | TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS | 112 |
| OpenSSL 0.9.8y | TLS 1.0 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| OpenSSL 1.0.1l R | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| OpenSSL 1.0.2 R | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| Safari 5.1.9 / OS X 10.6.8 | TLS 1.0 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| Safari 6 / iOS 6.0.1 R | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| Safari 6.0.4 / OS X 10.8.4 R | TLS 1.0 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| Safari 7 / iOS 7.1 R | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| Safari 7 / OS X 10.9 R | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| Safari 8 / iOS 8.4 R | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| Safari 8 / OS X 10.10 R | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| Yahoo Slurp Jan 2015 | TLS 1.2 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS | 256 |
| YandexBot Jan 2015 | TLS 1.2 | 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.

(3) Only first connection attempt simulated. Browsers tend to 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).

## Protocol Details

| | |
|---|---|
| **Secure Renegotiation** | **Supported** |
| **Secure Client-Initiated Renegotiation** | No |
| **Insecure Client-Initiated Renegotiation** | No |
| **BEAST attack** | Not mitigated server-side (more info) TLS 1.0: 0x35 |
| **POODLE (SSLv3)** | No, SSL 3 not supported (more info) |
| **POODLE (TLS)** | 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) |
| **OpenSSL CCS vuln. (CVE-2014-0224)** | No (more info) |
| **Forward Secrecy** | **No WEAK** (more info) |
| **Next Protocol Negotiation (NPN)** | No |
| **Session resumption (caching)** | **No (IDs assigned but not accepted)** |
| **Session resumption (tickets)** | No |
| **OCSP stapling** | No |
| **Strict Transport Security (HSTS)** | No |
| **Public Key Pinning (HPKP)** | No |
| **Long handshake intolerance** | No |
| **TLS extension intolerance** | No |
| **TLS version intolerance** | No |
| **Incorrect SNI alerts** | No |

## Protocol Details

| | |
|---|---|
| **Uses common DH primes** | No, DHE suites not supported |
| **DH public server param (Ys) reuse** | No, DHE suites not supported |
| **SSL 2 handshake compatibility** | Yes |


## Miscellaneous

| | |
|---|---|
| **Test date** | Wed, 07 Oct 2015 11:32:54 UTC |
| **Test duration** | 144.803 seconds |
| **HTTP status code** | 200 |
| **HTTP server signature** | - |
| **Server hostname** | privat.ib.seb.se |

SSL Report v1.19.33