Qualys. SSL Labs



# SSL Report: sp5pbe.rf.pl (83.144.113.166)

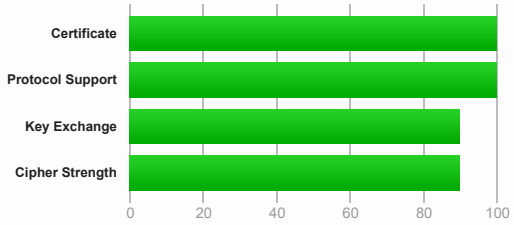
**Assessed on:** Mon, 07 May 2018 19:49:02 UTC | Hide | Clear cache

Scan Another »

## Summary

Overall Rating

A




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

## Certificate #1: RSA 4096 bits (SHA256withRSA)

### Server Key and Certificate #1

| | |
|---|---|
| Subject | *.rf.pl<br>Fingerprint SHA256: 996d41378485b1532225df5c9f2bfcc03e5e38a3da2a5bc14740e5633e7c4708<br>Pin SHA256: C6jpgjUqJsTiBE+avFTv8dnYhnpxtmbWI4cpX+5RJCc= |
| Common names | *.rf.pl |
| Alternative names | *.rf.pl rf.pl |
| Serial Number | 3721a45fb1ca571fc1381cf2 |
| Valid from | Sun, 18 Mar 2018 23:36:49 UTC |
| Valid until | Wed, 18 Mar 2020 23:36:49 UTC (expires in 1 year and 10 months) |
| Key | RSA 4096 bits (e 65537) |
| Weak key (Debian) | No |
| Issuer | AlphaSSL CA - SHA256 - G2<br>AIA: http://secure2.alphassl.com/cacert/gsalphasha2g2r1.crt |
| Signature algorithm | SHA256withRSA |
| Extended Validation | No |
| Certificate Transparency | Yes (certificate) |
| OCSP Must Staple | No |
| Revocation information | CRL, OCSP<br>CRL: http://crl2.alphassl.com/gs/gsalphasha2g2.crl<br>OCSP: http://ocsp2.globalsign.com/gsalphasha2g2 |
| 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 (2972 bytes) |
| Chain issues | None |

#### #2

| | |
|---|---|
| Subject | AlphaSSL CA - SHA256 - G2<br>Fingerprint SHA256: ee793643199474ed60efdc8ccde4d37445921683593aa751bbf8ee491a391e97<br>Pin SHA256: amMeV6gb9QNx0Zf7FtJ19Wa/t2B7KpCF/1n2Js3UuSU= |
| Valid until | Tue, 20 Feb 2024 10:00:00 UTC (expires in 5 years and 9 months) |
| Key | RSA 2048 bits (e 65537) |
| Issuer | GlobalSign 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 currently support draft version 18.

### Cipher Suites

| # TLS 1.2 (suites in server-preferred order) | | |
|---|---|---|
| TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) | ECDH x25519 (eq. 3072 bits RSA) FS | 256 |
| TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa) | DH 4096 bits FS | 256 |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) | ECDH x25519 (eq. 3072 bits RSA) FS | 256 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) | ECDH x25519 (eq. 3072 bits RSA) FS | 256 |
| TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) | DH 4096 bits FS | 256 |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) | DH 4096 bits FS | 256 |
| TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0xc4) | DH 4096 bits FS | 256 |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) | ECDH x25519 (eq. 3072 bits RSA) FS | 128 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) | ECDH x25519 (eq. 3072 bits RSA) FS | 128 |
| TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) | DH 4096 bits FS | 128 |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) | DH 4096 bits FS | 128 |
| TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xbe) | DH 4096 bits FS | 128 |

### Handshake Simulation

| | | | |
|---|---|---|---|
| Android 4.4.2 | RSA 4096 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Android 5.0.0 | RSA 4096 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Android 6.0 | RSA 4096 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Android 7.0 | RSA 4096 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS |
| BingPreview Jan 2015 | RSA 4096 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Chrome 49 / XP SP3 | RSA 4096 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS |
| Chrome 57 / Win 7 R | RSA 4096 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS |
| Firefox 31.3.0 ESR / Win 7 | RSA 4096 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Firefox 47 / Win 7 R | RSA 4096 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS |
| Firefox 49 / XP SP3 | RSA 4096 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS |
| Firefox 53 / Win 7 R | RSA 4096 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS |
| Googlebot Feb 2018 | RSA 4096 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS |
| IE 11 / Win 7 R | RSA 4096 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS |
| IE 11 / Win 8.1 R | RSA 4096 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS |
| IE 11 / Win Phone 8.1 R | RSA 4096 (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 4096 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS |
| IE 11 / Win 10 R | RSA 4096 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Edge 15 / Win 10 R | RSA 4096 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS |
| Edge 13 / Win Phone 10 R | RSA 4096 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Java 8u161 | RSA 4096 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| OpenSSL 1.0.1l R | RSA 4096 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| OpenSSL 1.0.2e R | RSA 4096 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Safari 6 / iOS 6.0.1 | RSA 4096 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS |
| Safari 7 / iOS 7.1 R | RSA 4096 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS |
| Safari 7 / OS X 10.9 R | RSA 4096 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS |
| Safari 8 / iOS 8.4 R | RSA 4096 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS |

## Handshake Simulation

| | | | | |
|---|---|---|---|---|
| Safari 8 / OS X 10.10 R | RSA 4096 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 FS |
| Safari 9 / iOS 9 R | RSA 4096 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Safari 9 / OS X 10.11 R | RSA 4096 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Safari 10 / iOS 10 R | RSA 4096 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Safari 10 / OS X 10.12 R | RSA 4096 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Apple ATS 9 / iOS 9 R | RSA 4096 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Yahoo Slurp Jan 2015 | RSA 4096 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| YandexBot Jan 2015 | RSA 4096 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | 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

| | |
|---|---|
| **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 |
| **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) |
| **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)** | No (more info) |
| **Forward Secrecy** | **Yes (with most browsers) ROBUST** (more info) |
| **ALPN** | Yes http/1.1 |
| **NPN** | No |
| **Session resumption (caching)** | Yes |
| **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 |
| **DH public server param (Ys) reuse** | No |
| **ECDH public server param reuse** | No |
| **Supported Named Groups** | x25519, secp256r1, secp384r1 (server preferred order) |
| **SSL 2 handshake compatibility** | Yes |

## HTTP Requests

1 **https://sp5pbe.rf.pl/** (HTTP/1.1 200 OK)

## Miscellaneous

| | |
|---|---|
| **Test date** | Mon, 07 May 2018 19:47:25 UTC |
| **Test duration** | 97.449 seconds |
| **HTTP status code** | 200 |
| **HTTP server signature** | Apache/2.4.33 (Unix) LibreSSL/2.7.2 PHP/7.0.29 |
| **Server hostname** | oxygen.sp5pbe.waw.pl |

SSL Report v1.31.0