Qualys. SSL Labs

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > www.credit-suisse.com

# SSL Report: www.credit-suisse.com (23.6.65.160)

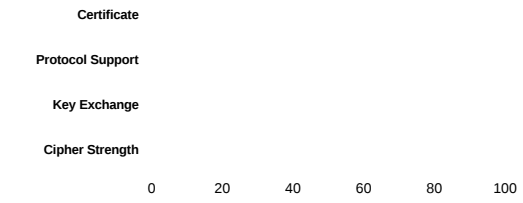
**Assessed on:** Mon, 19 Feb 2018 16:54:25 UTC | Hide | Clear cache

Scan Another »

## Summary

**Overall Rating**

**A+**




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

This server's certificate will be distrusted by Google and Mozilla from September 2018. 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.credit-suisse.com<br>Fingerprint SHA256: 94721fa9bc2de0e025d662558c645cb1c21eb2b224ebd1904d27e8672fdf1996<br>Pin SHA256: wQq8szRwXqfZWQAGCoxviBpv+0MK0DAYP4WPXnZvBUI= |
| **Common names** | www.credit-suisse.com |
| **Alternative names** | www.credit-suisse-securities-moscow.ru www.bank-credit-suisse-moscow.ru cdnext.credit-suisse.com cdn.credit-suisse.com www.credit-suisse.com credit-suisse.com |
| **Serial Number** | 4f36aa9c4990f2f3bef18697568fdc64 |
| **Valid from** | Fri, 24 Mar 2017 00:00:00 UTC |
| **Valid until** | Sun, 24 Mar 2019 23:59:59 UTC (expires in 1 year and 1 month) |
| **Key** | RSA 2048 bits (e 65537) |
| **Weak key (Debian)** | No |
| **Issuer** | Symantec Class 3 EV SSL CA - G3<br>AIA: http://sr.symcb.com/sr.crt |
| **Signature algorithm** | SHA256withRSA |
| **Extended Validation** | Yes |
| **Certificate Transparency** | Yes (certificate) |
| **OCSP Must Staple** | No |
| **Revocation information** | CRL, OCSP<br>CRL: http://sr.symcb.com/sr.crl<br>OCSP: http://sr.symcd.com |
| **Revocation status** | Good (not revoked) |
| **DNS CAA** | No (more info) |
| **Trusted** | Yes<br>Mozilla Apple Android Java Windows |

### Additional Certificates (if supplied)

### Additional Certificates (if supplied)

| | |
|---|---|
| **Certificates provided** | 2 (3244 bytes) |
| **Chain issues** | None |

#2

| | |
|---|---|
| **Subject** | Symantec Class 3 EV SSL CA - G3<br>Fingerprint SHA256: 9e6bc5f9ecc52460e8edc02c644d1be1cb9f2316f41daf3b616a0b2058294b31<br>Pin SHA256: gMxWOrX4PMQesK9qFNbYBxjBfjUvlkn/vN1n+L9lE5E= |
| **Valid until** | Mon, 30 Oct 2023 23:59:59 UTC (expires in 5 years and 8 months) |
| **Key** | RSA 2048 bits (e 65537) |
| **Issuer** | VeriSign Class 3 Public Primary Certification Authority - G5 |
| **Signature algorithm** | SHA256withRSA |

### Certification Paths

Click here to expand

## Certificate #2: EC 256 bits (SHA256withECDSA)

### Server Key and Certificate #1

| | |
|---|---|
| **Subject** | www.credit-suisse.com<br>Fingerprint SHA256: 26090f653d58069459e05575c154fc12eddfeb98a918b37e7f67504509b5ed80<br>Pin SHA256: B1yHEBKauc9VqxPcduJfm2dpih7P6Uh4NrFvj7T3yYE= |
| **Common names** | www.credit-suisse.com |
| **Alternative names** | credit-suisse.com www.credit-suisse-securities-moscow.ru cdn.credit-suisse.com cdnext.credit-suisse.com www.bank-credit-suisse-moscow.ru www.credit-suisse.com |
| **Serial Number** | 2339175617dcfb63831cf3568cb30299 |
| **Valid from** | Fri, 24 Mar 2017 00:00:00 UTC |
| **Valid until** | Sun, 24 Mar 2019 23:59:59 UTC (expires in 1 year and 1 month) |
| **Key** | EC 256 bits |
| **Weak key (Debian)** | No |
| **Issuer** | Symantec Class 3 ECC 256 bit EV CA - G2<br>AIA: http://rd.symcb.com/rd.crt |
| **Signature algorithm** | SHA256withECDSA |
| **Extended Validation** | Yes |
| **Certificate Transparency** | Yes (certificate) |
| **OCSP Must Staple** | No |
| **Revocation information** | CRL, OCSP<br>CRL: http://rd.symcb.com/rd.crl<br>OCSP: http://rd.symcd.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 (2653 bytes) |
| **Chain issues** | None |

#2

| | |
|---|---|
| **Subject** | Symantec Class 3 ECC 256 bit EV CA - G2<br>Fingerprint SHA256: 663636c03fd0b5b171f2b04407c3df767b349c8a990d87ce485898166e2b5120<br>Pin SHA256: PtK3zjOppRxW+hXzyuP7gC8Nt8hPS735XLgT+lQ1KTo= |
| **Valid until** | Sun, 11 May 2025 23:59:59 UTC (expires in 7 years and 2 months) |
| **Key** | EC 256 bits |
| **Issuer** | VeriSign Class 3 Public Primary Certification Authority - G5 |

### Additional Certificates (if supplied)

| | |
|---|---|
| **Signature algorithm** | SHA256withRSA |

### Certification Paths

Click here to expand

## Configuration

### Protocols

| | |
|---|---|
| TLS 1.3 | No |
| TLS 1.2 | Yes |
| TLS 1.1 | Yes |
| TLS 1.0 | Yes |
| 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_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) | ECDH secp256r1 (eq. 3072 bits RSA) FS | 256 |
| TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) | ECDH secp256r1 (eq. 3072 bits RSA) FS | 128 |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) | ECDH secp256r1 (eq. 3072 bits RSA) FS | 256 |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) | ECDH secp256r1 (eq. 3072 bits RSA) FS | 128 |
| TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) | ECDH secp256r1 (eq. 3072 bits RSA) FS | 256(P) |
| TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) | ECDH secp256r1 (eq. 3072 bits RSA) FS | 256(P) |
| TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) | ECDH secp256r1 (eq. 3072 bits RSA) FS | 256 |
| TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) | ECDH secp256r1 (eq. 3072 bits RSA) FS | 128 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) | ECDH secp256r1 (eq. 3072 bits RSA) FS | 256 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) | ECDH secp256r1 (eq. 3072 bits RSA) FS | 128 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | ECDH secp256r1 (eq. 3072 bits RSA) FS | 256 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) | ECDH secp256r1 (eq. 3072 bits RSA) FS | 128 |
| 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 |

**# TLS 1.1 (suites in server-preferred order)**

**# TLS 1.0 (suites in server-preferred order)**

(P) This server prefers ChaCha20 suites with clients that don't have AES-NI (e.g., Android devices)

### Handshake Simulation

| | | | |
|---|---|---|---|
| Android 2.3.7 No SNI [2] | RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_AES_128_CBC_SHA No FS |
| Android 4.0.4 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS |
| Android 4.1.1 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS |
| Android 4.2.2 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS |
| Android 4.3 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS |
| Android 4.4.2 | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Android 5.0.0 | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |

## Handshake Simulation

| | | | |
|---|---|---|---|
| Android 6.0 | EC 256 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Android 7.0 | EC 256 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS |
| Baidu Jan 2015 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS |
| BingPreview Jan 2015 | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Chrome 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Chrome 57 / Win 7 R | EC 256 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Firefox 31.3.0 ESR / Win 7 | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Firefox 47 / Win 7 R | EC 256 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Firefox 49 / XP SP3 | EC 256 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Firefox 53 / Win 7 R | EC 256 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Googlebot Feb 2015 | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| IE 7 / Vista | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS |
| IE 8 / XP No FS [1] No SNI [2] | Server sent fatal alert: handshake_failure | | |
| IE 8-10 / Win 7 R | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS |
| IE 11 / Win 7 R | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| IE 11 / Win 8.1 R | EC 256 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| IE 10 / Win Phone 8.0 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS |
| IE 11 / Win Phone 8.1 R | EC 256 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| IE 11 / Win Phone 8.1 Update R | EC 256 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| IE 11 / Win 10 R | EC 256 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Edge 13 / Win 10 R | EC 256 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Edge 13 / Win Phone 10 R | EC 256 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Java 6u45 No SNI [2] | RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_AES_128_CBC_SHA No FS |
| Java 7u25 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| Java 8u31 | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| OpenSSL 0.9.8y | RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_AES_256_CBC_SHA No FS |
| OpenSSL 1.0.1l R | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| OpenSSL 1.0.2e R | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Safari 5.1.9 / OS X 10.6.8 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS |
| Safari 6 / iOS 6.0.1 | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS |
| Safari 6.0.4 / OS X 10.8.4 R | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS |
| Safari 7 / iOS 7.1 R | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS |
| Safari 7 / OS X 10.9 R | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS |
| Safari 8 / iOS 8.4 R | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS |
| Safari 8 / OS X 10.10 R | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS |
| Safari 9 / iOS 9 R | EC 256 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Safari 9 / OS X 10.11 R | EC 256 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Safari 10 / iOS 10 R | EC 256 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Safari 10 / OS X 10.12 R | EC 256 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Apple ATS 9 / iOS 9 R | EC 256 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Yahoo Slurp Jan 2015 | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| YandexBot Jan 2015 | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |

### # Not simulated clients (Protocol mismatch)

| | |
|---|---|
| IE 6 / XP No FS [1] No SNI [2] | Protocol mismatch (not simulated) |

(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** |

## Protocol Details

| | |
|---|---|
| | (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** | Yes |
| **Insecure Client-Initiated Renegotiation** | No |
| **BEAST attack** | Not mitigated server-side (more info) TLS 1.0: 0xc014 |
| **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) |
| **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** | With modern browsers (more info) |
| **ALPN** | Yes http/1.1 |
| **NPN** | Yes http/1.1 http/1.0 |
| **Session resumption (caching)** | Yes |
| **Session resumption (tickets)** | Yes |
| **OCSP stapling** | **Yes** |
| **Strict Transport Security (HSTS)** | **Yes**<br>max-age=31536000 |
| **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 |
| **Supported Named Groups** | secp256r1, x25519 (server preferred order) |
| **SSL 2 handshake compatibility** | Yes |

## HTTP Requests

1. **https://www.credit-suisse.com/** (HTTP/1.1 302 Moved Temporarily)
2. **https://www.credit-suisse.com/index.html** (HTTP/1.1 302 Moved Temporarily)
3. **https://www.credit-suisse.com/mvc.do/rootRedirect** (HTTP/1.1 302 Moved Temporarily)
4. **https://www.credit-suisse.com/us/en.html** (HTTP/1.1 200 OK)

## Miscellaneous

| | |
|---|---|
| **Test date** | Mon, 19 Feb 2018 16:52:31 UTC |
| **Test duration** | 113.898 seconds |
| **HTTP status code** | 200 |
| **HTTP server signature** | - |
| **Server hostname** | a23-6-65-160.deploy.static.akamaitechnologies.com |

SSL Report v1.30.8