QUALYS SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > secure.handelsbanken.se

SSL Report: secure.handelsbanken.se (192.176.124.184)

Assessed on: Wed, 07 Oct 2015 11:37:46 UTC | Clear cache

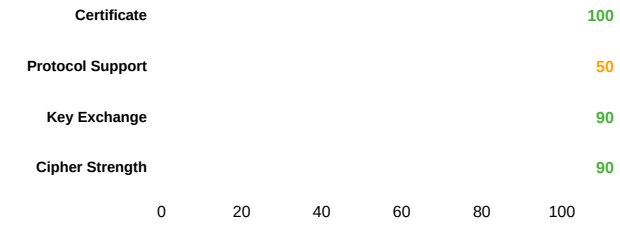
Scan Another »

Summary

Overall Rating

C

No support for TLS 1.2, which is the only secure protocol version. MORE »



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

Certificate uses a weak signature. When renewing, ensure you upgrade to SHA2. MORE INFO »

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

Authentication

Server Key and Certificate #1

Common names	secure.handelsbanken.se
Alternative names	secure.handelsbanken.se
Prefix handling	Not required for subdomains
Valid from	Mon, 01 Sep 2014 00:00:00 UTC
Valid until	Sat, 17 Oct 2015 23:59:59 UTC (expires in 10 days, 12 hours)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Symantec Class 3 EV SSL SGC CA - G2
Signature algorithm	SHA1withRSA **WEAK**
Extended Validation	Yes
Certificate Transparency	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes

Additional Certificates (if supplied)

Certificates provided	3 (4102 bytes)
Chain issues	Extra certs

#2

Subject	Symantec Class 3 EV SSL SGC CA - G2 Fingerprint: 378fe73e16e4f1e33949b760a3bd225149359025
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

Additional Certificates (if supplied)

Signature algorithm	SHA1withRSA **WEAK**

#3

Subject	VeriSign Class 3 Public Primary Certification Authority - G5 Fingerprint: 29b73d9f7501b8c0adfd5e4337a390d1ad205f48
Valid until	Sun, 07 Nov 2021 23:59:59 UTC (expires in 6 years and 1 month)
Key	RSA 2048 bits (e 65537)
Issuer	VeriSign / Class 3 Public Primary Certification Authority
Signature algorithm	SHA1withRSA **WEAK**

Certification Paths

Path #1: Trusted

1	Sent by server	secure.handelsbanken.se Fingerprint: 42fc804107b20009ccca2bc8e572d237d63a6389 RSA 2048 bits (e 65537) / SHA1withRSA **WEAK SIGNATURE**
2	Sent by server	Symantec Class 3 EV SSL SGC CA - G2 Fingerprint: 378fe73e16e4f1e33949b760a3bd225149359025 RSA 2048 bits (e 65537) / SHA1withRSA **WEAK SIGNATURE**
3	In trust store	VeriSign Class 3 Public Primary Certification Authority - G5 Self-signed Fingerprint: 4eb6d578499b1ccf5f581ead56be3d9b6744a5e5 RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

Configuration

Protocols

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

Cipher Suites (sorted by strength as the server has no preference; deprecated and SSL 2 suites at the end)

TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256

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_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 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	No FS	256
Android 5.0.0	TLS 1.0	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 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	No FS	256
Chrome 43 / OS X R	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	No FS	256
Firefox 31.3.0 ESR / Win 7	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
Firefox 39 / OS X R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
Googlebot Feb 2015	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
IE 6 / XP No FS [1] No SNI [2]	Protocol or cipher suite mismatch			Fail [3]
IE 7 / Vista	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128

Handshake Simulation

IE 8 / XP No FS [1] No SNI [2]	Protocol or cipher suite mismatch			Fail[3]
IE 8-10 / Win 7 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
IE 11 / Win 7 R	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	No FS	256
IE 11 / Win 8.1 R	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	No FS	256
IE 10 / Win Phone 8.0	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
IE 11 / Win Phone 8.1 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
IE 11 / Win Phone 8.1 Update R	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	No FS	256
Edge 12 / Win 10 (Build 10130) R	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	No 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_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
Java 8u31	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
OpenSSL 0.9.8y	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	No FS	256
OpenSSL 1.0.1l R	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	No FS	256
OpenSSL 1.0.2 R	TLS 1.0	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_128_CBC_SHA (0x2f)	No FS	128
Safari 6 / iOS 6.0.1 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
Safari 7 / iOS 7.1 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
Safari 7 / OS X 10.9 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
Safari 8 / iOS 8.4 R	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	No FS	256
Safari 8 / OS X 10.10 R	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	No FS	256
Yahoo Slurp Jan 2015	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	No FS	256
YandexBot Jan 2015	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.

(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: 0x2f
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)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	**Probably, but not exploitable** (investigate to confirm and patch) (more info)
Forward Secrecy	**No WEAK** (more info)
Next Protocol Negotiation (NPN)	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
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
Uses common DH primes	No, DHE suites not supported

Protocol Details

DH public server param (Ys) reuse	No, DHE suites not supported
SSL 2 handshake compatibility	Yes

Miscellaneous

Test date	Wed, 07 Oct 2015 11:36:40 UTC
Test duration	66.132 seconds
HTTP status code	403
HTTP server signature	
Server hostname	secure.handelsbanken.se

SSL Report v1.19.33