QUALYS SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > internetbanken.privat.nordea.se

SSL Report: internetbanken.privat.nordea.se (193.234.187.12)

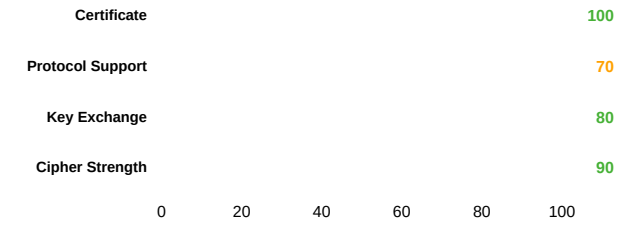
Assessed on: Wed, 07 Oct 2015 11:48:20 UTC | Clear cache

Scan Another »

Summary

Overall Rating

B



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

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

Intermediate certificate has a weak signature. When renewing, ensure you upgrade to an all-SHA2 chain. MORE INFO »

This server accepts the RC4 cipher, which is weak. Grade capped to B. MORE INFO »

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

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

Authentication

Server Key and Certificate #1

Common names	internetbanken.privat.nordea.se
Alternative names	internetbanken.privat.nordea.se
Prefix handling	Not required for subdomains
Valid from	Wed, 21 Jan 2015 00:00:00 UTC
Valid until	Mon, 14 Mar 2016 23:59:59 UTC (expires in 5 months and 7 days)
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 (4236 bytes)
Chain issues	Extra certs

#2

Subject	Symantec Class 3 EV SSL CA - G3 Fingerprint: e3fc0ad84f2f5a83ed6f86f567f8b14b40dcbf12

Additional Certificates (if supplied)

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

#3

Subject	VeriSign Class 3 Public Primary Certification Authority - G5 Fingerprint: 32f30882622b87cf8856c63db873df0853b4dd27
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	internetbanken.privat.nordea.se Fingerprint: 65f7e1b59f823c649da4ca2feba2c202c51062a6 RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	Symantec Class 3 EV SSL CA - G3 Fingerprint: e3fc0ad84f2f5a83ed6f86f567f8b14b40dcbf12 RSA 2048 bits (e 65537) / SHA256withRSA
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	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_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 1024 bits (p: 128, g: 1, Ys: 128) FS **WEAK**	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 1024 bits (p: 128, g: 1, Ys: 128) FS **WEAK**	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 1024 bits (p: 128, g: 1, Ys: 128) FS **WEAK**	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a) DH 1024 bits (p: 128, g: 1, Ys: 128) FS **WEAK**	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 1024 bits (p: 128, g: 1, Ys: 128) FS **WEAK**	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_SEED_CBC_SHA (0x96)	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	128
TLS_RSA_WITH_RC4_128_SHA (0x5) **WEAK**	128
TLS_RSA_WITH_RC4_128_MD5 (0x4) **WEAK**	128
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits (p: 128, g: 1, Ys: 128) FS **WEAK**	112
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112

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 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) 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_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) FS	256
BingPreview Jan 2015	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) 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_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) 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]
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_RC4_128_SHA (0x5) No FS RC4	128
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_SHA256 (0x3d) No FS	256
IE 11 / Win 8.1 R	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) 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_SHA256 (0x3d) No FS	256
IE 11 / Win Phone 8.1 Update R	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) No FS	256
Edge 12 / Win 10 (Build 10130) R	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) 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 1.2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) 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 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) FS	256
OpenSSL 1.0.2 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) 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_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) 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_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) FS	256
Safari 7 / OS X 10.9 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) FS	256
Safari 8 / iOS 8.4 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) FS	256
Safari 8 / OS X 10.10 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) FS	256
Yahoo Slurp Jan 2015	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) FS	256
YandexBot Jan 2015	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) 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	**Supported DoS DANGER** (more info)
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0x88
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	**Yes WEAK** (more info)

Protocol Details

Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	**With some browsers** (more info)
Next Protocol Negotiation (NPN)	No
Session resumption (caching)	Yes
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
Uses common DH primes	**Yes** Replace with custom DH parameters if possible (more info)
DH public server param (Ys) reuse	No
SSL 2 handshake compatibility	Yes

Miscellaneous

Test date	Wed, 07 Oct 2015 11:46:18 UTC
Test duration	121.611 seconds
HTTP status code	403
HTTP server signature	-
Server hostname	-

SSL Report v1.19.33