QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > personal.metrobankdirect.com > 210.213.81.109

SSL Report: personal.metrobankdirect.com (210.213.81.109)

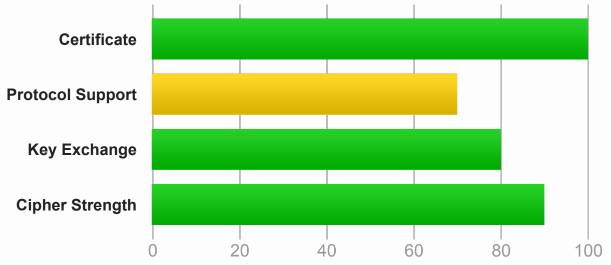
Assessed on: Fri, 27 Nov 2015 15:36:14 UTC | Clear cache

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 »

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

Subject	personal.metrobankdirect.com Fingerprint SHA1: 0a75f58ab3a79d51e262e3b56e6146551d5bbc32 Pin SHA256: Hcly9AT8Qae54SLoGqkXy/IhKLfZ8TE/5naLYGY8upA=
Common names	personal.metrobankdirect.com
Alternative names	ebirpersonal.metrobankdirect.com personal.metrobankdirect.com
Prefix handling	Not required for subdomains
Valid from	Mon, 07 Sep 2015 00:00:00 UTC
Valid until	Tue, 06 Dec 2016 23:59:59 UTC (expires in 1 year)
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	2 (3116 bytes)
Chain issues	None

#2

Subject	Symantec Class 3 EV SSL CA - G3 Fingerprint SHA1: e3fc0ad84f2f5a83ed6f86f567f8b14b40dcbf12 Pin SHA256: gMxWOrX4PMQesK9qFNbYBxjBfjUvlkn/vN1n+L9lE5E=
Valid until	Mon, 30 Oct 2023 23:59:59 UTC (expires in 7 years and 11 months)
Key	RSA 2048 bits (e 65537)
Issuer	VeriSign Class 3 Public Primary Certification Authority - G5
Signature algorithm	SHA256withRSA

Certification Paths

Path #1: Trusted

1	Sent by server	personal.metrobankdirect.com Fingerprint SHA1: 0a75f58ab3a79d51e262e3b56e6146551d5bbc32 Pin SHA256: Hcly9AT8Qae54SLoGqkXy/IhKLfZ8TE/5naLYGY8upA= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	Symantec Class 3 EV SSL CA - G3 Fingerprint SHA1: e3fc0ad84f2f5a83ed6f86f567f8b14b40dcbf12 Pin SHA256: gMxWOrX4PMQesK9qFNbYBxjBfjUvlkn/vN1n+L9lE5E= RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	VeriSign Class 3 Public Primary Certification Authority - G5 Self-signed Fingerprint SHA1: 4eb6d578499b1ccf5f581ead56be3d9b6744a5e5 Pin SHA256: JbQbUG5JMJUoI6brnx0x3vZF6jilxsapbXGVfjhN8Fg= 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_GCM_SHA384 (0x9f) DH 1024 bits (p: 128, g: 1, Ys: 128) FS **WEAK**	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 1024 bits (p: 128, g: 1, Ys: 128) FS **WEAK**	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 1024 bits (p: 128, g: 1, Ys: 128) FS **WEAK**	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits (p: 128, g: 1, Ys: 128) FS **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_AES_256_GCM_SHA384 (0x9d)	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH 256 bits (eq. 3072 bits RSA) FS	128

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH 256 bits (eq. 3072 bits RSA) FS	112

Handshake Simulation

Android 2.3.7 No SNI [2]	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Android 4.0.4	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Android 4.1.1	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Android 4.2.2	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Android 4.3	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Android 4.4.2	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) FS	256
Android 5.0.0	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) FS	128
Baidu Jan 2015	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
BingPreview Jan 2015	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) FS	256
Chrome 45 / OS X R	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) FS	128
Firefox 31.3.0 ESR / Win 7	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Firefox 41 / OS X R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Googlebot Feb 2015	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) 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_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_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) FS	256
IE 11 / Win 8.1 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) 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_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) FS	256
IE 11 / Win 10 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) FS	256
Edge / Win 10 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) FS	256
Java 6u45 No SNI [2]	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Java 7u25	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Java 8u31	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) FS	128
OpenSSL 0.9.8y	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
OpenSSL 1.0.1l R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) FS	256
OpenSSL 1.0.2 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) FS	256
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Safari 6 / iOS 6.0.1 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Safari 7 / iOS 7.1 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Safari 7 / OS X 10.9 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Safari 8 / iOS 8.4 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Safari 8 / OS X 10.10 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Safari 9 / iOS 9 R	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) No FS	256
Safari 9 / OS X 10.11 R	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) No FS	256
Apple ATS 9 / iOS 9 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) FS	256
Yahoo Slurp Jan 2015	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) FS	256
YandexBot Jan 2015	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) 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: 0x39
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	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
HSTS Preloading	Not in: Chrome Edge Firefox IE Tor personal.metrobankdirect.com
Public Key Pinning (HPKP)	No
Public Key Pinning Report-Only	No
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
SSL 2 handshake compatibility	Yes

Miscellaneous

Test date	Fri, 27 Nov 2015 15:32:37 UTC
Test duration	101.530 seconds
HTTP status code	200
HTTP server signature	IBM_HTTP_Server
Server hostname	personal.metrobankdirect.com

SSL Report v1.20.28

Terms and Conditions