

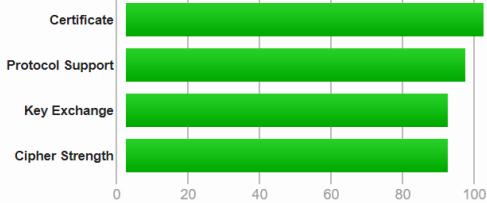
You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > www.bmbf.de

SSL Report: www.bmbf.de (93.191.166.200)

Assessed on: Fri, 22 Feb 2019 00:29:13 UTC | [Hide](#) | [Clear cache](#)[Scan Another »](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

Renegotiation test has been disabled temporarily due to an Apache httpd 2.4.37 bug. [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.bmbf.de Fingerprint SHA256: 322830b709f103835599a9c31327698f91ec89eb6c6f44d0cf3fc5ec0dac5e4 Pin SHA256: LznbCY7lwNFhXg8WeMIDwlBsEjrCVURjJgkM05lUH2l=
Common names	www.bmbf.de
Alternative names	www.bmbf.de bmbf.de
Serial Number	40383d0b492b2d61b227540a
Valid from	Wed, 17 Jan 2018 09:41:57 UTC
Valid until	Sat, 18 Jan 2020 09:41:57 UTC (expires in 10 months and 27 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	AlphaSSL CA - SHA256 - G2 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 CRL: http://crl2.alphassl.com/gs/gsalphasha2g2.crl OCSP: http://ocsp.globalsign.com/gsalphasha2g2
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows



Additional Certificates (if supplied)



Certificates provided	2 (2863 bytes)
Chain issues	None
#2	
Subject	AlphaSSL CA - SHA256 - G2 Fingerprint SHA256: ee793643199474ed800efdc8ccde4d37445921863593aa751bbf8ee491a391e97 Pin SHA256: amMeV6gb9QNxDZf7FJ19WaI2b7KpCF/1n2Js3UuSU=
Valid until	Tue, 20 Feb 2024 10:00:00 UTC (expires in 4 years and 11 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	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

For TLS 1.3 tests, we only support RFC 8446.



Cipher Suites



TLS 1.2 (suites in server-preferred order)

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_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 2048 bits FS	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	WEAK	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 2048 bits FS	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	WEAK	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccab)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CCM_8 (0xc0a3)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CCM (0xc09f)	DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_128_CCM_8 (0xc0a2)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_128_CCM (0xc09e)	DH 2048 bits FS	128
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (0xc077)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0xc4)	DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xc076)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xbe)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 2048 bits FS	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	WEAK	256
TLS_RSA_WITH_AES_256_CCM_8 (0xc0a1)	WEAK	256
TLS_RSA_WITH_AES_256_CCM (0xc09d)	WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	WEAK	128
TLS_RSA_WITH_AES_128_CCM_8 (0xc0a0)	WEAK	128
TLS_RSA_WITH_AES_128_CCM (0xc09c)	WEAK	128
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0xc0e)	WEAK	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	WEAK	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	WEAK	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	WEAK	128

TLS 1.1 (suites in server-preferred order)



TLS 1.0 (suites in server-preferred order)





Handshake Simulation

Android 2.3.7	No SNI ²	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 2048 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		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Android 5.0.0		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 6.0		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 7.0		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA 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		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Chrome 49 / XP SP3		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Chrome 69 / Win 7 R		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Chrome 70 / Win 10		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Firefox 31.3.0 ESR / Win 7		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Firefox 47 / Win 7 R		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Firefox 49 / XP SP3		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Firefox 62 / Win 7 R		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Googlebot Feb 2018		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA 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 FS¹ No SNI²			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		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
IE 11 / Win 8.1 R		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_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		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
IE 11 / Win 10 R		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Edge 15 / Win 10 R		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Edge 13 / Win Phone 10 R		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Java 6u45 No SNI²		RSA 2048 (SHA256) TLS 1.0 TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 2048	Client does not support DH parameters > 1024 bits	
Java 7u25		RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Java 8u161		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
OpenSSL 0.9.8y		RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 2048 FS
OpenSSL 1.0.1 R		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
OpenSSL 1.0.2e R		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_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		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_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		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 7 / OS X 10.9 R		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 8 / iOS 8.4 R		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 8 / OS X 10.10 R		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 9 / iOS 9 R		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 9 / OS X 10.11 R		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 10 / iOS 10 R		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 10 / OS X 10.12 R		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Apple ATS 9 / iOS 9 R		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Yahoo Slurp Jan 2015		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
YandexBot Jan 2015		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS

Not simulated clients (Protocol mismatch)



[IE 6 / XP No FS¹ No SNI²](#) 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 (1) For a better understanding of this test, please read this longer explanation (2) Key usage data kindly provided by the Censys network search engine; original DROWN website here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
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	Yes (with most browsers) ROBUST (more info)
ALPN	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	Yes max-age=16000000; includeSubDomains; preload;
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	secp256r1
SSL 2 handshake compatibility	Yes



HTTP Requests



1 <https://www.bmbf.de/> (HTTP/1.1 200 OK)



Miscellaneous

Test date	Fri, 22 Feb 2019 00:26:39 UTC
Test duration	153.72 seconds
HTTP status code	200
HTTP server signature	Apache
Server hostname	www.bmbf.de