

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.bsnebiz.com.my](#) > 211.25.204.15

# SSL Report: [www.bsnebiz.com.my](#) (211.25.204.15)

Assessed on: Mon, 09 Aug 2021 03:24:18 UTC | [Clear cache](#)

[Scan Another »](#)

## Summary

Overall Rating

# A+

Certificate

Protocol Support

Key Exchange

Cipher Strength

0 20 40 60 80 100

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

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

<b>Subject</b>	www.bsnebiz.com.my Fingerprint SHA256: a2e0b80d620486a8feda45929c89a7c00076878ba3f12e2b25f61a8042605a8f Pin SHA256: B/P5utwdVjf3u1fX6RNIFc8l36PvNAzUXA35HqVmELE=
<b>Common names</b>	www.bsnebiz.com.my
<b>Alternative names</b>	www.bsnebiz.com.my bsnebiz.com.my
<b>Serial Number</b>	1210140590f4a0fcd0244256
<b>Valid from</b>	Wed, 16 Oct 2019 08:26:07 UTC
<b>Valid until</b>	Mon, 22 Nov 2021 08:24:57 UTC (expires in 3 months and 13 days)
<b>Key</b>	RSA 2048 bits (e 65537)
<b>Weak key (Debian)</b>	No
<b>Issuer</b>	GlobalSign Extended Validation CA - SHA256 - G3 AIA: http://secure.globalsign.com/cacert/gsexextendvalsha2g3r3.crt
<b>Signature algorithm</b>	SHA256withRSA
<b>Extended Validation</b>	Yes
<b>Certificate Transparency</b>	Yes (certificate)
<b>OCSP Must Staple</b>	No
<b>Revocation information</b>	OCSP OCSP: http://ocsp2.globalsign.com/gsexextendvalsha2g3r3
<b>Revocation status</b>	Good (not revoked)
<b>DNS CAA</b>	No (more info)
<b>Trusted</b>	Yes Mozilla Apple Android Java Windows



### Additional Certificates (if supplied)

<b>Certificates provided</b>	3 (3786 bytes)
<b>Chain issues</b>	Contains anchor

Additional Certificates (if supplied)

#2

<b>Subject</b>	GlobalSign Extended Validation CA - SHA256 - G3 Fingerprint SHA256: aed5dd9a5339685dfb029f6d89a14335a96512c3cacc52b2994af8b6b37fa4d2 Pin SHA256: 86fLJetopQLDNxYZ0uMI66Xp1fPfgLIHHn9v6KT0i4I=
<b>Valid until</b>	Mon, 21 Sep 2026 00:00:00 UTC (expires in 5 years and 1 month)
<b>Key</b>	RSA 2048 bits (e 65537)
<b>Issuer</b>	GlobalSign
<b>Signature algorithm</b>	SHA256withRSA

#3

<b>Subject</b>	GlobalSign <b>In trust store</b> Fingerprint SHA256: cbb522d7b7f127ad6a0113865bdf1cd4102e7d0759af635a7cf4720dc963c53b Pin SHA256: cGuxAXyFXfKwM61cF4HPWX8S0srS9j0aSqN0k4AP+4A=
<b>Valid until</b>	Sun, 18 Mar 2029 10:00:00 UTC (expires in 7 years and 7 months)
<b>Key</b>	RSA 2048 bits (e 65537)
<b>Issuer</b>	GlobalSign Self-signed
<b>Signature algorithm</b>	SHA256withRSA



Certification Paths



[Click here to expand](#)

## Configuration



Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No



Cipher Suites

# TLS 1.2 (suites in server-preferred order)



TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS <b>WEAK</b>	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS <b>WEAK</b>	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS <b>WEAK</b>	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS <b>WEAK</b>	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	<b>WEAK</b>	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	<b>WEAK</b>	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	<b>WEAK</b>	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	<b>WEAK</b>	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	<b>WEAK</b>	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	<b>WEAK</b>	256
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	<b>WEAK</b>	128
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	<b>WEAK</b>	256



## Handshake Simulation

<a href="#">Android 4.4.2</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Android 5.0.0</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Android 6.0</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Android 7.0</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Android 8.0</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Android 8.1</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Android 9.0</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">BingPreview Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Chrome 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Chrome 69 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Chrome 70 / Win 10</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Chrome 80 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 31.3.0 ESR / Win 7</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 47 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 62 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 73 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">GoogLebot Feb 2018</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">IE 11 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">IE 11 / Win 8.1</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">IE 11 / Win Phone 8.1</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">IE 11 / Win Phone 8.1 Update</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">IE 11 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Edge 15 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Edge 16 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Edge 18 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Edge 13 / Win Phone 10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Java 8u161</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Java 11.0.3</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Java 12.0.1</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">OpenSSL 1.0.1j</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">OpenSSL 1.0.2s</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">OpenSSL 1.1.0k</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">OpenSSL 1.1.1c</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Safari 6 / iOS 6.0.1</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">Safari 7 / iOS 7.1</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">Safari 7 / OS X 10.9</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">Safari 8 / iOS 8.4</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">Safari 8 / OS X 10.10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">Safari 9 / iOS 9</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Safari 9 / OS X 10.11</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Safari 10 / iOS 10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Safari 10 / OS X 10.12</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Safari 12.1.2 / MacOS 10.14.6 Beta</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Safari 12.1.1 / iOS 12.3.1</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Apple ATS 9 / iOS 9</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Yahoo Slurp Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">YandexBot Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS

# Not simulated clients (Protocol mismatch)



## Handshake Simulation

[Click here to expand](#)

- (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 <b>(1) For a better understanding of this test, please read <a href="#">this longer explanation</a></b> (2) Key usage data kindly provided by the <a href="#">Censys</a> network search engine; original DROWN website <a href="#">here</a> (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
<b>Secure Renegotiation</b>	<b>Supported</b>
Secure Client-Initiated Renegotiation	Yes
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side ( <a href="#">more info</a> )
POODLE (SSLv3)	No, SSL 3 not supported ( <a href="#">more info</a> )
POODLE (TLS)	No ( <a href="#">more info</a> )
Zombie POODLE	No ( <a href="#">more info</a> ) TLS 1.2 : 0xc013
GOLDENDOODLE	No ( <a href="#">more info</a> ) TLS 1.2 : 0xc013
OpenSSL 0-Length	No ( <a href="#">more info</a> ) TLS 1.2 : 0xc013
Sleeping POODLE	No ( <a href="#">more info</a> ) TLS 1.2 : 0xc013
Downgrade attack prevention	Unknown (requires support for at least two protocols, excl. SSL2)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No ( <a href="#">more info</a> )
Ticketbleed (vulnerability)	No ( <a href="#">more info</a> )
OpenSSL CCS vuln. (CVE-2014-0224)	No ( <a href="#">more info</a> )
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No ( <a href="#">more info</a> )
ROBOT (vulnerability)	No ( <a href="#">more info</a> )
<b>Forward Secrecy</b>	<b>Yes (with most browsers) ROBUST (<a href="#">more info</a>)</b>
ALPN	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	No
<b>Strict Transport Security (HSTS)</b>	<b>Yes</b> max-age=31536000; includeSubDomains; preload
HSTS Preloading	<b>Not in: Chrome Edge Firefox IE</b>
Public Key Pinning (HPKP)	No ( <a href="#">more info</a> )
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No ( <a href="#">more info</a> )
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
<b>ECDH public server param reuse</b>	<b>Yes</b>
Supported Named Groups	secp256r1, x25519, secp384r1 (server preferred order)
SSL 2 handshake compatibility	Yes



HTTP Requests



1 <https://www.bsnebiz.com.my/> (HTTP/1.1 200 OK)



Miscellaneous

Test date	Mon, 09 Aug 2021 03:19:17 UTC
Test duration	124.678 seconds
HTTP status code	200
HTTP server signature	-
Server hostname	-

SSL Report v2.1.8