

Qualys. SSL Labs

[Home](#) [Projects](#) [Qualys Free Trial](#) [Contact](#)

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > www.bankofindia.co.in

SSL Report: www.bankofindia.co.in (49.50.92.254)

Assessed on: Tue, 26 Feb 2019 17:19:32 UTC | [Hide](#) | [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](#).


Renegotiation test has been disabled temporarily due to an Apache httpd 2.4.37 bug. [MORE INFO »](#)

Certificate #1: RSA 2048 bits (SHA256withRSA)




Server Key and Certificate #1

Subject	bankofindia.co.in Fingerprint SHA256: a787924f6b14de410ad5a5835044aaf980332e944200c5fbc87061c95672cbea Pin SHA256: z6KTBZICOE6N0gNFO3iIndQYi7gIFqASvYsA5AwVxz8=
Common names	bankofindia.co.in
Alternative names	bankofindia.co.in www.bankofindia.co.in bankofindia.com bankofindia.com.hk bankofindia.fr bankofindia.co.bw bankofindia.co.nz bankofindia.co.za bankofindia.uk.com boijapan.com boikenya.com boitanzania.co.tz boiugan da.co.ug boiusa.com test.bankofindia.co.in
Serial Number	19a5ab2e3313ce980000000054cf4873
Valid from	Thu, 20 Dec 2018 12:04:23 UTC
Valid until	Tue, 08 Oct 2019 12:34:21 UTC (expires in 7 months and 11 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Entrust Certification Authority - L1M AIA: http://aia.entrust.net/l1m-chain256.cer
Signature algorithm	SHA256withRSA
Extended Validation	Yes
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.entrust.net/level1m.crl OCSP: http://ocsp.entrust.net
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows




Additional Certificates (if supplied)

Certificates provided	6 (8954 bytes)
-----------------------	----------------

Additional Certificates (if supplied)	
Chain issues	Extra certs, Contains anchor
#2	
Subject	Entrust Certification Authority - L1M Fingerprint SHA256: 75c5b3f01fd1f51a2c447ab7c785d72e69fa9c472c08571e7eadf3b8eabae70c Pin SHA256: VYZwGJkq3NN01YRI2RGIST1mqTWG8zDcRf1J/KAN6I=
Valid until	Tue, 15 Oct 2030 15:55:03 UTC (expires in 11 years and 7 months)
Key	RSA 2048 bits (e 65537)
Issuer	Entrust Root Certification Authority - G2
Signature algorithm	SHA256withRSA
#3	
Subject	Entrust Root Certification Authority - G2 <span>In trust store</span> Fingerprint SHA256: 43df5774b03e7fef5fe40d931a7bedf1bb2e6b42738c4e6d3841103d3aa7f339 Pin SHA256: du6FKdMcVQ3u8prumAo6t3i3G27uMP2EOhR8R0at/U=
Valid until	Sat, 07 Dec 2030 17:55:54 UTC (expires in 11 years and 9 months)
Key	RSA 2048 bits (e 65537)
Issuer	Entrust Root Certification Authority - G2 <span>Self-signed</span>
Signature algorithm	SHA256withRSA
#4	
Subject	bankofindia.co.in Fingerprint SHA256: a787924f6b4de410ad5a5835044aa1980332e944200c5fbc87061c95672cbea Pin SHA256: z6KTBZICOE6N0gNFO3iINdQYi7gIFqASvYsA5AwVxz8=
Valid until	Tue, 08 Oct 2019 12:34:21 UTC (expires in 7 months and 11 days)
Key	RSA 2048 bits (e 65537)
Issuer	Entrust Certification Authority - L1M
Signature algorithm	SHA256withRSA
#5	
Subject	Entrust Certification Authority - L1M Fingerprint SHA256: 75c5b3f01fd1f51a2c447ab7c785d72e69fa9c472c08571e7eadf3b8eabae70c Pin SHA256: VYZwGJkq3NN01YRI2RGIST1mqTWG8zDcRf1J/KAN6I=
Valid until	Tue, 15 Oct 2030 15:55:03 UTC (expires in 11 years and 7 months)
Key	RSA 2048 bits (e 65537)
Issuer	Entrust Root Certification Authority - G2
Signature algorithm	SHA256withRSA
#6	
Subject	Entrust Root Certification Authority - G2 <span>In trust store</span> Fingerprint SHA256: 43df5774b03e7fef5fe40d931a7bedf1bb2e6b42738c4e6d3841103d3aa7f339 Pin SHA256: du6FKdMcVQ3u8prumAo6t3i3G27uMP2EOhR8R0at/U=
Valid until	Sat, 07 Dec 2030 17:55:54 UTC (expires in 11 years and 9 months)
Key	RSA 2048 bits (e 65537)
Issuer	Entrust Root Certification Authority - G2 <span>Self-signed</span>
Signature algorithm	SHA256withRSA
<div><div></div><div>Certification Paths<div><div>+</div></div></div></div>	
<div>Click here to expand</div>	

Configuration

	Protocols	
	TLS 1.3	No
	TLS 1.2	Yes

Protocols

TLS 1.1	No
TLS 1.0	No
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_GCM_SHA384 (0xc030)	ECDH secp384r1 (eq. 7680 bits RSA)	FS		256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp384r1 (eq. 7680 bits RSA)	FS		128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp384r1 (eq. 7680 bits RSA)	FS		128



Handshake Simulation

<a href="#">Android 4.4.2</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
<a href="#">Android 5.0.0</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	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_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">BingPreview Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	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_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Chrome 70 / Win 10</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	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_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Firefox 62 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Googlebot Feb 2018</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">IE 11 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	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_SHA256	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_SHA256	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_SHA256	ECDH secp256r1	FS
<a href="#">IE 11 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Edge 15 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Edge 13 / Win Phone 10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Java 8u161</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">OpenSSL 1.0.1j</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
<a href="#">OpenSSL 1.0.2e</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	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_SHA256	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_SHA256	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_SHA256	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_SHA256	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_SHA256	ECDH secp256r1	FS
<a href="#">Safari 9 / iOS 9</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Safari 9 / OS X 10.11</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Safari 10 / iOS 10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Safari 10 / OS X 10.12</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Apple ATS 9 / iOS 9</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Yahoo Slurp Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
<a href="#">YandexBot Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS

# Not simulated clients (Protocol mismatch) [+]

Click here to expand

Handshake Simulation

- (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

	No, server keys and hostname not seen elsewhere with SSLv2
DROWN	(1) For a better understanding of this test, please read <a href="#">this longer explanation</a> (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
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> )
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> )
Forward Secrecy	Yes (with most browsers) ROBUST ( <a href="#">more info</a> )
ALPN	No
NPN	No
Session resumption (caching)	No (IDs assigned but not accepted)
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
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	TLS 2.152
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No
Supported Named Groups	secp256r1, secp384r1 (Server has no preference)
SSL 2 handshake compatibility	Yes



HTTP Requests



- 1 https://www.bankofindia.co.in/ (HTTP/1.1 200 OK)



Miscellaneous

Test date	Tue, 26 Feb 2019 17:17:36 UTC
Test duration	116.24 seconds
HTTP status code	200

Miscellaneous	
HTTP server signature	
Server hostname	rabbit.createstatements.net.92.50.49.in-addr.arpa
SSL Report v1.32.16	
Copyright © 2009-2019 <a href="#">Qualys, Inc.</a> . All Rights Reserved. <a href="#">Terms and Conditions</a>	
<a href="#">Try Qualys for free!</a> Experience the award-winning <a href="#">Qualys Cloud Platform</a> and the entire collection of <a href="#">Qualys Cloud Apps</a> , including <a href="#">certificate security</a> solutions.	