

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

# SSL Report: www.bmo.com (23.38.229.51)

Assessed on: Tue, 16 Oct 2018 18:49:51 UTC | **HIDDEN** | [Clear cache](#)

[Scan Another »](#)

## Summary

Overall Rating

# A

Certificate

Protocol Support

Key Exchange

Cipher Strength



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

## Certificate #1: RSA 2048 bits (SHA256withRSA)



### Server Key and Certificate #1

<b>Subject</b>	www.bmo.com Fingerprint SHA256: ec50684bc4d7c4282d72412b8b631f7104b54d067d74e9f6aa93722d9250162b Pin SHA256: 7C/J1dKBDsUVBsltcS7X6Ev8g0KXNAs9CwMabbH5e2s=
<b>Common names</b>	www.bmo.com
<b>Alternative names</b>	bmo.com bmobullion.com depositedge.bmoharris.com depositedge.mibank.com findit.bmo.com findit.prod.bmo.com m.bmo.com m.bmoharris.com m.bmoinvestorline.com m.bmolignedaction.com m.harrisbank.com m.mibank.com mibankrewards.com mimaap.com mobile.bmo.com mobile.bmoinvestorline.com mobile.bmolignedaction.com mv.mibank.com resourcecenter.bmoharris.com resources.bmo.com ressources.bmo.com www.bankofmontreal.com www.bmo.ca www.bmo.com www.bmo.hk www.bmo.mobi www.bmoassurance.com www.bmobanquepriveeharris.com www.bmobullion.com www.bmocm.com www.bmoespacemerge.com www.bmoetfs.hk www.bmoflex.com www.bmofundsus.com www.bmogamus.com www.bmogma.com www.bmoharris.com www.bmoharrisfinancialadvisors.com www.bmoharrisprivatebanking.com www.bmoinsurance.com www.bmomarginoutlook.com www.bmonb.com www.bmonesbittburns.com www.bmonotforprofitservices.com www.bmoretirementservices.com www.bmotaft-hartleyservices.com www.bmotrustandcustodyservices.com www.ctcmycfo.com www.harrisbank.com www.harrismycfo.com www.harrisprivatebankstability.com www.mibank.com www.mibank.mobi www.mibankrewards.com www.micapitalmarkets.com www.mimaap.com www.miretirement.com www.mitrust.com www.miwealth.com www.miwebflex.com www.mybmoretirement.com www.mycfo.com www.prod.bmo.com www.prod.bmoharris.com www4.bmo.com www4.harrisbank.com
<b>Serial Number</b>	035070766102dc2bce4dafa3f2b4d4d7
<b>Valid from</b>	Thu, 05 Jul 2018 00:00:00 UTC
<b>Valid until</b>	Sun, 05 Jul 2020 12:00:00 UTC (expires in 1 year and 8 months)
<b>Key</b>	RSA 2048 bits (e 65537)
<b>Weak key (Debian)</b>	No
<b>Issuer</b>	DigiCert Global CA G2 AIA: http://cacerts.digicert.com/DigiCertGlobalCAG2.crt
<b>Signature algorithm</b>	SHA256withRSA
<b>Extended Validation</b>	Yes
<b>Certificate Transparency</b>	Yes (certificate)
<b>OCSP Must Staple</b>	No

**Server Key and Certificate #1**

<b>Revocation information</b>	CRL, OCSP CRL: <a href="http://crl3.digicert.com/DigiCertGlobalCAG2.crl">http://crl3.digicert.com/DigiCertGlobalCAG2.crl</a> OCSP: <a href="http://ocsp.digicert.com">http://ocsp.digicert.com</a>
<b>Revocation status</b>	Good (not revoked)
<b>DNS CAA</b>	No ( <a href="#">more info</a> )
<b>Trusted</b>	<b>Yes</b> Mozilla Apple Android Java Windows



**Additional Certificates (if supplied)**

<b>Certificates provided</b>	2 (4389 bytes)
<b>Chain issues</b>	None

**#2**

<b>Subject</b>	DigiCert Global CA G2 Fingerprint SHA256: 8fac576439c9fd3ef153b51f9edd0d381b5df7b87559cebeca04297dd44a639b Pin SHA256: njN4rRG+22dNXAI+yb8e3UMypgzPUPHlv4+foULw1fg=
<b>Valid until</b>	Tue, 01 Aug 2028 12:00:00 UTC (expires in 9 years and 9 months)
<b>Key</b>	RSA 2048 bits (e 65537)
<b>Issuer</b>	DigiCert Global Root G2
<b>Signature algorithm</b>	SHA256withRSA



**Certification Paths**



[Click here to expand](#)

**Configuration**



**Protocols**

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
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 secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0a8)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256 <sup>P</sup>
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_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	<b>WEAK</b>	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	<b>WEAK</b>	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	<b>WEAK</b>	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	<b>WEAK</b>	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	<b>WEAK</b>	256

## Cipher Suites

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x2F) **WEAK**

128

## # TLS 1.1 (suites in server-preferred order)



(P) This server prefers ChaCha20 suites with clients that don't have AES-NI (e.g., Android devices)



## Handshake Simulation

<a href="#">Android 4.4.2</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	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 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Android 7.0</a>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDH secp256r1	FS
<a href="#">BingPreview Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Chrome 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2 > h2	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 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Chrome 70 / Win 10</a>	RSA 2048 (SHA256)	TLS 1.2 > h2	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 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2 > h2	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 > h2	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_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">IE 11 / Win 8.1</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">IE 11 / Win Phone 8.1</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	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 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">IE 11 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	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 > h2	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 > h2	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 1.0.1l</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	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_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 7 / iOS 7.1</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 7 / OS X 10.9</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 8 / iOS 8.4</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 8 / OS X 10.10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 9 / iOS 9</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	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 > h2	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 > h2	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 > h2	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 > h2	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 secp256r1	FS
<a href="#">YandexBot Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS

## # Not simulated clients (Protocol mismatch)

[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



## Protocol Details

	No, server keys and hostname not seen elsewhere with SSLv2
<b>DROWN</b>	(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
<b>Secure Renegotiation</b>	<b>Supported</b>
Secure Client-Initiated Renegotiation	No
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> )
<b>Downgrade attack prevention</b>	<b>Yes, TLS_FALLBACK_SCSV supported</b> ( <a href="#">more info</a> )
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</b> ( <a href="#">more info</a> )
ALPN	Yes h2 h2-14 http/1.1
NPN	Yes http/1.1 http/1.0
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
<b>OCSP stapling</b>	<b>Yes</b>
Strict Transport Security (HSTS)	No
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
ECDH public server param reuse	No
Supported Named Groups	secp256r1, x25519 (server preferred order)
SSL 2 handshake compatibility	Yes



## HTTP Requests



1 <https://www.bmo.com/> (HTTP/1.1 302 Moved Temporarily)

2 <https://www.bmo.com/main/personal> (HTTP/1.1 200 OK)



## Miscellaneous

Test date	Tue, 16 Oct 2018 18:48:39 UTC
Test duration	71.933 seconds
HTTP status code	200
HTTP server signature	-
Server hostname	a23-38-229-51.deploy.static.akamaitechnologies.com

SSL Report v1.32.6

Copyright © 2009-2018 [Qualys, Inc.](#) All Rights Reserved.

[Terms and Conditions](#)

Qualys is the leading provider of integrated [infrastructure security](#), [cloud infrastructure security](#), [endpoint security](#), [devsecops](#), [compliance](#) and [web app security](#) solutions.