

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [chase.com](#) > 159.53.224.21

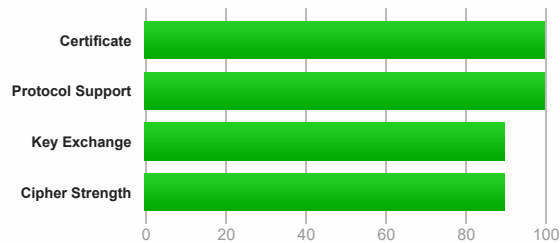
SSL Report: [chase.com](#) (159.53.224.21)

Assessed on: Fri, 22 Oct 2021 15:38:14 UTC | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



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

DNS Certification Authority Authorization (CAA) Policy found for this domain. [MORE INFO »](#)

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1



Subject	www.chase.com Fingerprint SHA256: 8b04b35c44725659b9be3d82b2b8cff3682c5b16a6d4f02d9234d0302faf1944 Pin SHA256: BeL5Ls9s5uD/2tgEQ0kMBYwZsg8VIOeahmkFyNmFbs=
Common names	www.chase.com
Alternative names	www.chase.com chase.com
Serial Number	6903d3016948046029983ac3d142d1
Valid from	Thu, 18 Feb 2021 10:56:34 UTC
Valid until	Fri, 18 Feb 2022 10:56:33 UTC (expires in 3 months and 26 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	Yes policy host: chase.com issue: entrust.net flags:0 issue: digicert.com flags:0
Trusted	Yes Mozilla Apple Android Java Windows



Additional Certificates (if supplied)



Certificates provided	3 (4252 bytes)
Chain issues	Contains anchor
#2	
Subject	Entrust Certification Authority - L1M Fingerprint SHA256: 75c5b3f01fd1f51a2c447ab7c785d72e69fa9c472c08571e7eadf3b8eabae70c Pin SHA256: VYZwGJkq3NN01YRI2RGIST11mqTWG8zDcRf1/KAN6l=
Valid until	Tue, 15 Oct 2030 15:55:03 UTC (expires in 8 years and 11 months)
Key	RSA 2048 bits (e 65537)
Issuer	Entrust Root Certification Authority - G2
Signature algorithm	SHA256withRSA

#3	
Subject	Entrust Root Certification Authority - G2 In trust store Fingerprint SHA256: 43df5774b03e7fef5fe40d931a7bedf1bb2e6b42738c4e6d3841103d3aa7f339 Pin SHA256: du6FkDdMcVQ3u8prumAo6t3i3G27uMP2EOhR8R0at/U=
Valid until	Sat, 07 Dec 2030 17:55:54 UTC (expires in 9 years and 1 month)
Key	RSA 2048 bits (e 65537)
Issuer	Entrust Root Certification Authority - G2 Self-signed
Signature algorithm	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_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA)	FS		256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)			WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)			WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)			WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)			WEAK	256



Handshake Simulation

Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS

Handshake Simulation

Android 7.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 8.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 8.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 9.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Chrome 69 / Win 7 ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Chrome 70 / Win 10	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Chrome 80 / Win 10 ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 47 / Win 7 ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 62 / Win 7 ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 73 / Win 10 ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
IE 11 / Win 7 ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	FS
IE 11 / Win 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 ^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_128_CBC_SHA256	ECDH secp256r1	FS
IE 11 / Win 10 ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Edge 15 / Win 10 ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Edge 16 / Win 10 ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Edge 18 / Win 10 ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Edge 13 / Win Phone 10 ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Java 11.0.3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Java 12.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
OpenSSL 1.0.1l ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
OpenSSL 1.0.2s ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
OpenSSL 1.1.0k ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
OpenSSL 1.1.1c ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	FS
Safari 7 / iOS 7.1 ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	FS
Safari 7 / OS X 10.9 ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	FS
Safari 8 / iOS 8.4 ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	FS
Safari 8 / OS X 10.10 ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	FS
Safari 9 / iOS 9 ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Safari 9 / OS X 10.11 ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Safari 10 / iOS 10 ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Safari 10 / OS X 10.12 ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Safari 12.1.2 / MacOS 10.14.6 Beta ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Safari 12.1.1 / iOS 12.3.1 ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Apple ATS 9 / iOS 9 ^R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	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.

Handshake Simulation

(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	
Secure Renegotiation	Supported	
Secure Client-Initiated Renegotiation	No	
Insecure Client-Initiated Renegotiation	No	
BEAST attack	Mitigated server-side	(more info)
POODLE (SSLv3)	No, SSL 3 not supported	(more info)
POODLE (TLS)	No	(more info)
Zombie POODLE	No	(more info) TLS 1.2 : 0xc027
GOLDENDOODLE	No	(more info) TLS 1.2 : 0xc027
OpenSSL 0-Length	No	(more info) TLS 1.2 : 0xc027
Sleeping POODLE	No	(more info) TLS 1.2 : 0xc027
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	(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)	No	
OCSP stapling	No	
Strict Transport Security (HSTS)	No	
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, 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, secp384r1 (server preferred order)	
SSL 2 handshake compatibility	Yes	



HTTP Requests



[1](#) <https://chase.com/> (HTTP/1.0 301 Moved Permanently)



Miscellaneous

Test date	Fri, 22 Oct 2021 15:28:27 UTC
Test duration	73.1 seconds
HTTP status code	301
HTTP forwarding	https://www.chase.com
HTTP server signature	BigIP
Server hostname	-

SSL Report v2.1.8

Copyright © 2009-2021 [Qualys, Inc.](#) All Rights Reserved.

[Terms and Conditions](#)

[Try Qualys for free!](#) Experience the award-winning [Qualys Cloud Platform](#) and the entire collection of [Qualys Cloud Apps](#), including [certificate security](#) solutions.