

Qualys[®] SSL Labs

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

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

SSL Report: www.cgd.pt (195.234.134.174)

Assessed on: Tue, 03 May 2022 14:33:19 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating

B

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](#).

This server does not support Forward Secrecy with the reference browsers. Grade capped to B. [MORE INFO »](#)

This server does not support Authenticated encryption (AEAD) cipher suites. Grade capped to B. [MORE INFO »](#)


This server supports TLS 1.0 and TLS 1.1. Grade capped to B. [MORE INFO »](#)

Certificate #1: RSA 4096 bits (SHA256withRSA)



Server Key and Certificate #1

Subject	www.cgd.pt Fingerprint SHA256: 9ca4367b1b7ca3241336af0817bbea4573928b21b9b5fca5c63d9dd4e49b4f3 Pin SHA256: 7Hacmx6/enpEywOyxzVGizUlti7ypB17w3iu4dhGNWFU=
Common names	www.cgd.pt
Alternative names	www.cgd.pt cgd.pt
Serial Number	0d2895cc8579b7939e96b1479fcb539b
Valid from	Thu, 25 Nov 2021 00:00:00 UTC
Valid until	Mon, 26 Dec 2022 23:59:59 UTC (expires in 7 months and 23 days)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	DigiCert SHA2 Extended Validation Server CA AIA: http://cacerts.digicert.com/DigiCertSHA2ExtendedValidationServerCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	Yes
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl3.digicert.com/sha2-ev-server-g3.crl OCSP: http://ocsp.digicert.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows



Additional Certificates (if supplied)

Certificates provided	3 (4250 bytes)
Chain issues	Contains anchor

https://www.ssllabs.com/ssltest/analyze.html?d=www.cgd.pt

1/5

Additional Certificates (if supplied)

#2

Subject	DigiCert SHA2 Extended Validation Server CA Fingerprint SHA256: 403e062a2653059113285baf80a0d4ae422c848c9f78fad01fc94bc5b87fef1a Pin SHA256: RRM1dGqnDFsCJXBTHky16vi1obOlCgFFnlyOhly+ho=
Valid until	Sun, 22 Oct 2028 12:00:00 UTC (expires in 6 years and 5 months)
Key	RSA 2048 bits (e 65537)
Issuer	DigiCert High Assurance EV Root CA
Signature algorithm	SHA256withRSA

#3

Subject	DigiCert High Assurance EV Root CA In trust store Fingerprint SHA256: 7431e5f4c3c1ce4690774f0b61e05440883ba9a01ed00ba6abd7806ed3b118cf Pin SHA256: WoIWRYlOVNa9ihaBciRSC7XHjiiYS9VwUGOlud4PB18=
Valid until	Mon, 10 Nov 2031 00:00:00 UTC (expires in 9 years and 6 months)
Key	RSA 2048 bits (e 65537)
Issuer	DigiCert High Assurance EV Root CA Self-signed
Signature algorithm	SHA1withRSA Weak, but no impact on root certificate



Certification Paths



Mozilla Apple Android Java Windows

Path #1: Trusted

1	Sent by server	www.cgd.pt Fingerprint SHA256: 9ca4367b1b7ca3241336af0817bbeea4573928b21b9b5fca5c63d9dd4e49b4f3 Pin SHA256: 7Hacmx6/enpEywOyxzVGlzUtl7ypB17w3iu4dhGfWfU= RSA 4096 bits (e 65537) / SHA256withRSA
2	Sent by server	DigiCert SHA2 Extended Validation Server CA Fingerprint SHA256: 403e062a2653059113285baf80a0d4ae422c848c9f78fad01fc94bc5b87fef1a Pin SHA256: RRM1dGqnDFsCJXBTHky16vi1obOlCgFFnlyOhly+ho= RSA 2048 bits (e 65537) / SHA256withRSA
3	Sent by server In trust store	DigiCert High Assurance EV Root CA Self-signed Fingerprint SHA256: 7431e5f4c3c1ce4690774f0b61e05440883ba9a01ed00ba6abd7806ed3b118cf Pin SHA256: WoIWRYlOVNa9ihaBciRSC7XHjiiYS9VwUGOlud4PB18= RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

Configuration



Protocols

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



Cipher Suites

TLS 1.2 (suites in server-preferred order)



TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) WEAK	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK	112

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 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Android 4.0.4	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 4.1.1	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 4.2.2	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 4.3	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 4.4.2	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Android 5.0.0	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 6.0	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 7.0	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 8.0	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 8.1	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 9.0	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Baidu Jan 2015	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
BingPreview Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Chrome 49 / XP SP3	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Chrome 69 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Chrome 70 / Win 10	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Chrome 80 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Firefox 31.3.0 ESR / Win 7	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Firefox 47 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Firefox 49 / XP SP3	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Firefox 62 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Firefox 73 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Googlebot Feb 2018	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 7 / Vista	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 8 / XP No FS ¹ No SNI ²	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA
IE 8-10 / Win 7 R	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 11 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
IE 11 / Win 8.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
IE 10 / Win Phone 8.0	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 11 / Win Phone 8.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
IE 11 / Win Phone 8.1 Update R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
IE 11 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Edge 15 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Edge 16 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Edge 18 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Edge 13 / Win Phone 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Java 6u45 No SNI ²	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Java 7u25	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Java 8u161	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Java 11.0.3	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Java 12.0.1	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
OpenSSL 0.9.8y	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
OpenSSL 1.0.1l R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
OpenSSL 1.0.2s R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
OpenSSL 1.1.0k R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
OpenSSL 1.1.1c R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 5.1.9 / OS X 10.6.8	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 6 / iOS 6.0.1	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 7 / iOS 7.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 7 / OS X 10.9 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 8 / iOS 8.4 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS

Handshake Simulation

Safari 8 / OS X 10.10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 9 / iOS 9 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 9 / OS X 10.11 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 10 / iOS 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 10 / OS X 10.12 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 12.1.1 / iOS 12.3.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Apple ATS 9 / iOS 9 R	Server sent fatal alert: handshake_failure		
Yahoo Slurp Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
YandexBot Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No 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
Secure Renegotiation	Supported	
Secure Client-Initiated Renegotiation	No	
Insecure Client-Initiated Renegotiation	No	
BEAST attack	Not mitigated server-side (more info)	TLS 1.0: 0x35
POODLE (SSLv3)	No, SSL 3 not supported (more info)	
POODLE (TLS)	No (more info)	
Zombie POODLE	No (more info)	TLS 1.2 : 0x0035
GOLDENDOODLE	No (more info)	TLS 1.2 : 0x0035
OpenSSL 0-Length	No (more info)	TLS 1.2 : 0x0035
Sleeping POODLE	No (more info)	TLS 1.2 : 0x0035
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)	
SSL/TLS compression	No	
RC4	No	
Heartbeat (extension)	Yes	
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	No WEAK (more info)	
ALPN	No	
NPN	No	
Session resumption (caching)	Yes	
Session resumption (tickets)	Yes	
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	

Protocol Details	
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, ECDHE suites not supported
Supported Named Groups	-
SSL 2 handshake compatibility	Yes



HTTP Requests	
1	https://www.cgd.pt/ (HTTP/1.1 302 Redirect)
2	https://www.cgd.pt/Pages/default_v2.aspx (HTTP/1.1 302 Found)
3	https://www.cgd.pt/Particulares/Pages/Particulares_v2.aspx (HTTP/1.1 200 OK)



Miscellaneous	
Test date	Tue, 03 May 2022 14:30:53 UTC
Test duration	146.662 seconds
HTTP status code	200
HTTP server signature	-
Server hostname	web1.cgd.pt