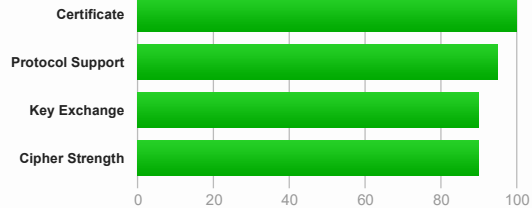


You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.ren.pt](#) > 185.165.104.164

SSL Report: [www.ren.pt](#) (185.165.104.164)

Summary

Overall Rating



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



Subject	*.ren.pt Fingerprint SHA256: 3f3bb86cf521dd0ad5311e667ba3a9672a428a698b043b0c60eb8e4c556989a7 Pin SHA256: ppw3Hcih5Kud3wXhAdTINvbyks+ixmBEA15Lueb0Xz8=
Common names	*.ren.pt
Alternative names	*.ren.pt ren.pt k2.intra.ren.pt
Serial Number	0e36e7214f9ef67b0e46bc579fdb9539
Valid from	Mon, 23 Mar 2015 00:00:00 UTC
Valid until	Sun, 27 May 2018 12:00:00 UTC (expires in 3 months and 3 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	DigiCert SHA2 Secure Server CA AIA: http://cacerts.digicert.com/DigiCertSHA2SecureServerCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl3.digicert.com/ssca-sha2-g4.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	2 (2496 bytes)
Chain issues	None
#2	
Subject	DigiCert SHA2 Secure Server CA Fingerprint SHA256: 154c433c491929c5ef686e838e323664a00e6a0d822ccc958fb4dab03e49a08f Pin SHA256: 5kVjNEMw0KjCAu7eXY5HZdvYCS13BbA0VJG1RSP91w=

Additional Certificates (if supplied)

Valid until

Wed, 08 Mar 2023 12:00:00 UTC (expires in 5 years)

Key


RSA 2048 bits (e 65537)

Issuer

DigiCert Global Root CA

Signature algorithm


SHA256withRSA



Certification Paths

Click here to expand


Configuration



Protocols

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

For TLS 1.3 tests, we currently support draft version 18.



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_DHE_RSA_WITH_AES_256_GCM_SHA384 (0xc09f)	DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0ca8)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0caa)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CCM_8 (0xc0a3)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CCM (0xc09f)	DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0xc09e)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_128_CCM_8 (0xc0a2)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_128_CCM (0xc09e)	DH 2048 bits FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0xc06b)	DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (0xc077)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0xc04)	DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0xc067)	DH 2048 bits FS	128
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xc076)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xcbe)	DH 2048 bits FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0xc39)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0xc88)	DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0xc33)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0xc45)	DH 2048 bits FS	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0xc9d)	WEAK	256
TLS_RSA_WITH_AES_256_CCM_8 (0xc0a1)	WEAK	256
TLS_RSA_WITH_AES_256_CCM (0xc09d)	WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0xc9c)	WEAK	128

2 of 6

23/02/2018, 18:43

Cipher Suites

TLS_RSA_WITH_AES_128_CCM_8 (0xc0a0)	WEAK	128
TLS_RSA_WITH_AES_128_CCM (0xc09c)	WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0xc3d)	WEAK	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0xc0)	WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0xc3c)	WEAK	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xba)	WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	WEAK	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	WEAK	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	WEAK	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a) DH 2048 bits FS		128
TLS_RSA_WITH_SEED_CBC_SHA (0x96)	WEAK	128

TLS 1.1 (suites in server-preferred order)



TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS		256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 2048 bits FS		256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 2048 bits FS		256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS		128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 2048 bits FS		128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 2048 bits FS		128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	WEAK	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	WEAK	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	WEAK	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a) DH 2048 bits FS		128
TLS_RSA_WITH_SEED_CBC_SHA (0x96)	WEAK	128
TLS_RSA_WITH_IDEA_CBC_SHA (0x7)	WEAK	128

TLS 1.0 (suites in server-preferred order)



TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS		256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 2048 bits FS		256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 2048 bits FS		256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS		128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 2048 bits FS		128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 2048 bits FS		128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	WEAK	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	WEAK	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	WEAK	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a) DH 2048 bits FS		128
TLS_RSA_WITH_SEED_CBC_SHA (0x96)	WEAK	128
TLS_RSA_WITH_IDEA_CBC_SHA (0x7)	WEAK	128



Handshake Simulation

Android 2.3.7 No SNI ²	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 2048 FS
Android 4.0.4	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.2.2	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.3	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 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 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS

Handshake Simulation

Baidu Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS
Chrome 57 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 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 > http/1.1	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Firefox 53 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Googlebot Feb 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
IE 8 / XP No FS ¹ No SNI ²	Server sent fatal alert: handshake_failure		
IE 8-10 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 2048 FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 2048 FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	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 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 2048 FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Edge 13 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Java 6u45 No SNI ²	Client does not support DH parameters > 1024 bits		
	RSA 2048 (SHA256)	TLS 1.0 TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 2048	
Java 7u25	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Java 8u31	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 2048 FS
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
OpenSSL 1.0.2e R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 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

Protocol Details**Secure Renegotiation**

Secure Client-Initiated Renegotiation
Insecure Client-Initiated Renegotiation

Supported

No
No
Not mitigated server-side ([more info](#)) TLS 1.0: 0xc014

POODLE (SSLv3)

No, SSL 3 not supported ([more info](#))

POODLE (TLS)

No ([more info](#))**Downgrade attack prevention****Yes, TLS_FALLBACK_SCSV supported** ([more info](#))

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

Yes http/1.1

NPN

No

Session resumption (caching)**No (IDs empty)**

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

TLS extension intolerance

No

TLS version intolerance

No

Incorrect SNI alerts

No

Uses common DH primes

No

DH public server param (Ys) reuse

No

ECDH public server param reuse

No

Supported Named Groups

secp256r1, secp384r1, secp521r1 (server preferred order)

SSL 2 handshake compatibility

Yes

**HTTP Requests****1** <https://www.ren.pt/> (HTTP/1.1 200 OK)**Miscellaneous**

Test date	Fri, 23 Feb 2018 18:36:17 UTC
Test duration	176.979 seconds
HTTP status code	200
HTTP server signature	Microsoft-IIS/7.5
Server hostname	-