

Qualys[®] SSL Labs

Home

Projects

Qualys.com

Contact

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.sns.gov.pt](#) > 188.138.57.39

SSL Report: [www.sns.gov.pt](#) (188.138.57.39)

Assessed on: Sat, 24 Feb 2018 23:01:08 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](#).


Server sent invalid HSTS policy. See below for further information.

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1

Subject	*.sns.gov.pt Fingerprint SHA256: d87ae04d5946721b7da4a12bf519bf2c24cbb003543ddd3bcb70c7e75cb1a7f0 Pin SHA256: 5TObzyPFEH6DwHaKUyCReA9S5F7hO+cNH2tz6uw8fg=
Common names	*.sns.gov.pt
Alternative names	sns.gov.pt *.sns.gov.pt
Serial Number	6cbbca80b7b479205a661c389f197357
Valid from	Mon, 22 Jan 2018 17:15:36 UTC
Valid until	Tue, 22 Jan 2019 17:16:39 UTC (expires in 10 months and 28 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	ECCE 001 AIA: http://trust.ecce.gov.pt/ecce-001.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crls.ecce.gov.pt/crls/crl-001.crl OCSP: http://ocsp.ecce.gov.pt
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows



Additional Certificates (if supplied)

Certificates provided	3 (4113 bytes)
Chain issues	Incorrect order

#2

https://www.ssllabs.com/ssltest/analyze.html?d=www.sns.gov.pt&s=188.138.57.39

1/5

Additional Certificates (if supplied)

Subject	ECRaizEstado
	Fingerprint SHA256: 36b8b44851cca333959d6c8006cfdabf5b855e4a9b6ce51a7a8b4934886bac3
	Pin SHA256: rTBMIEpdNZvRISCaFMoeB/DT9c+JPYArBT4bkm5V13Q=
Valid until	Fri, 30 Sep 2022 17:39:11 UTC (expires in 4 years and 7 months)
Key	RSA 4096 bits (e 65537)
Issuer	Baltimore CyberTrust Root
Signature algorithm	SHA256withRSA

#3

Subject	ECCE 001
	Fingerprint SHA256: daab2e4504fd54ef7f99bb49e14c3d63a6ddff8af5604d5ba1d01f312b5204e4
	Pin SHA256: V2bSTg2mjUVZ8Kpws5ZQj4uDn2hsDXDPy8GH3JMEX0=
Valid until	Thu, 24 Jun 2027 15:43:57 UTC (expires in 9 years and 3 months)
Key	RSA 2048 bits (e 65537)
Issuer	ECRaizEstado
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_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_DHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02e)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0xc02f)	DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0xc026)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0xc011)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0xc02b)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0xc012)	DH 2048 bits FS	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0xc03c)	WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0xc03d)	WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0xc03e)	WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0xc03f)	WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0xc02f)	WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0xc035)	WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0xc088)	DH 2048 bits FS	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0xc084)	WEAK	256

Cipher Suites

TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 2048 bits FS	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) 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 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_128_CBC_SHA ECDH secp256r1 FS
Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.2.2	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.3	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
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 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Baidu Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA 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 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 57 / Win 7 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 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 53 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 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_128_CBC_SHA ECDH secp256r1 FS
IE 8 / XP No FS ¹ No SNI ²	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA
IE 8-10 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 DH 2048 FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 DH 2048 FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_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_128_GCM_SHA256 DH 2048 FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 13 / 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 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_128_CBC_SHA DH 2048 FS
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.0.2e R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA 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 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA 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 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS

Handshake Simulation

Safari 10 / OS X 10.12 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Apple ATS 9 / iOS 9 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	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)

[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) <small>TLS 1.0: 0xc013</small>		
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)	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	Yes (with most browsers) ROBUST (more info)		
ALPN	No		
NPN	Yes <small>http/1.1</small>		
Session resumption (caching)	No (IDs assigned but not accepted)		
Session resumption (tickets)	Yes		
OCSP stapling	No		
Strict Transport Security (HSTS)	Invalid <small>Server provided more than one HSTS header</small>		
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		
SSL 2 handshake compatibility	Yes		



HTTP Requests

1 <https://www.sns.gov.pt/> (HTTP/1.1 200 OK)



Miscellaneous

Test date	Sat, 24 Feb 2018 22:57:56 UTC
Test duration	191.393 seconds
HTTP status code	200
HTTP server signature	nginx
Server hostname	backdoor.veks.net

SSL Report v1.30.8