SSL Report: www.portaldasfinancas.gov.pt (213.13.158.243)

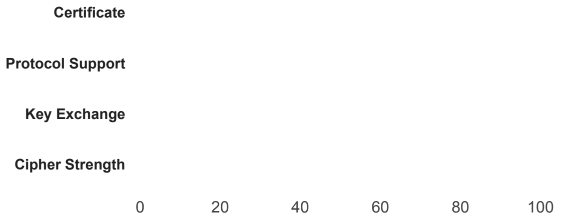
Assessed on: Sat, 24 Feb 2018 23:00:08 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A-



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 will be capped to B from March 2018. **MORE INFO »**

This server does not support Authenticated encryption (AEAD) cipher suites. Grade will be capped to B from March 2018. **MORE INFO »**

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	*.portaldasfinancas.gov.pt Fingerprint SHA256: 8f18efc9bf1a2ac72ecc33dc045b8a7486fe4f1c168b1509c14ddf5366af9c03 Pin SHA256: r04m3OS7bppGiE+dIpjNZJhpvC2TB0YHAdH46yk1ChM=
Common names	*.portaldasfinancas.gov.pt
Alternative names	*.portaldasfinancas.gov.pt
Serial Number	398ecada20115b125a15aad788c96337
Valid from	Wed, 22 Nov 2017 16:50:31 UTC
Valid until	Thu, 22 Nov 2018 16:50:32 UTC (expires in 8 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	4 (5009 bytes)
Chain issues	**Contains anchor**

#2

Additional Certificates (if supplied)

Subject	ECCE 001 Fingerprint SHA256: daab2e4504fd54ef7f99bb49e14c3d63a6ddff8af5604d5ba1d01f312b5204e4 Pin SHA256: V2bSTg2mjUVZ8Kpwrs5ZQj4uDn2hsDXDPy8GH3JMEX0=
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

#3

Subject	ECRaizEstado Fingerprint SHA256: 36b8b44851cca333959d6c8006cfddabf5b855e4a9b6ce51a7a8b4934886bac3 Pin SHA256: rTBMiEpdN2vRlSCaFMOeB/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

#4

Subject	Baltimore CyberTrust Root In trust store Fingerprint SHA256: 16af57a9f676b0ab126095aa5ebadef22ab31119d644ac95cd4b93dbf3f26aeb Pin SHA256: Y9mvm0exBk1JoQ57f9Vm28jKo5lFm/woKcVxrYxu80o=
Valid until	Mon, 12 May 2025 23:59:00 UTC (expires in 7 years and 2 months)
Key	RSA 2048 bits (e 65537)
Issuer	Baltimore CyberTrust Root Self-signed
Signature algorithm	SHA1withRSA Weak, but no impact on root certificate

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_RSA_WITH_AES_256_CBC_SHA256 (0x3d) **WEAK**	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
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 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Android 4.0.4	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS

Handshake Simulation

Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 4.2.2	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 4.3	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Baidu Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Chrome 57 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Firefox 53 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Googlebot Feb 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No 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_RSA_WITH_AES_256_CBC_SHA No FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Edge 13 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Java 6u45 No SNI [2]	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Java 7u25	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Java 8u31	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA256 No FS
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
OpenSSL 1.0.2e R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Apple ATS 9 / iOS 9 R	Server closed connection		
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS

# Not simulated clients (Protocol mismatch) ⊟

IE 6 / XP No FS [1] No SNI [2]	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	Yes
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)
Downgrade attack prevention	No, TLS_FALLBACK_SCSV not 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	No WEAK (more info)
ALPN	No
NPN	No
Session resumption (caching)	No (IDs assigned but not accepted)
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	TLS 2.152
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.portaldasfinancas.gov.pt/ (HTTP/1.1 301 Moved Permanently)

Miscellaneous

Test date	Sat, 24 Feb 2018 22:58:09 UTC
Test duration	119.117 seconds
HTTP status code	301
HTTP forwarding	http://www.portaldasfinancas.gov.pt PLAINTEXT
HTTP server signature	-
Server hostname	-

SSL Report v1.30.8