

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > www.bancobpi.pt

SSL Report: www.bancobpi.pt (185.26.46.11)

Assessed on: Tue, 03 May 2022 14:34:22 UTC | Hide | Clear cache

Scan Another »

Overall Rating 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. There is no support for secure renegotiation. Grade reduced to A-. MORE INFO > HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO >

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1

Cubinet	www.bancobpi.pt
Subject	Fingerprint SHA256: 3c4673b4d4c62d1de663e40ba94e4e3344f41046b086bc38e38cfc94445f2e8b Pin SHA256: Jfc02DfEkzTxkB/Qju8qyrd7dujxaLEhVgsM9Btqhyl=
Common names	www.bancobpi.pt
Alternative names	www.bancobpi.pt bancobpi.pt content.bancobpi.pt m.bancobpi.pt m.bpionline.pt net.bpipremio.pt questionario-bancobpi.pt repcontent.bancobpi.pt sim.bancobpi.pt www.acpmaster.com www.bpigestaoactivos.pt www.bpi-gestaodeactivos.pt www.bpiinvestimentos.pt www.bpionline.pt www.bpipremio.pt www.fundosbpi.pt www.gestaoactivos.pt www.gestaoactivosbpi.pt www.svb.bancobpi.pt
Serial Number	0cbdd3b8dfb92e256b36879fe3dbdb67
Valid from	Mon, 20 Dec 2021 00:00:00 UTC
Valid until	Tue, 20 Sep 2022 23:59:59 UTC (expires in 4 months and 17 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	COMODO RSA Organization Validation Secure Server CA AIA: http://crt.comodoca.com/COMODORSAOrganizationValidationSecureServerCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.comodoca.com/COMODORSAOrganizationValidationSecureServerCA.crl OCSP: http://ocsp.comodoca.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 (5206 bytes)

Additional Certificates (if supplied) Chain issues Contains anchor #2 COMODO RSA Organization Validation Secure Server CA Subject Fingerprint SHA256: 111006378afbe8e99bb02ba87390ca429fca2773f74d7f7eb5744f5ddf68014b Pin SHA256: EgNpQkIEUNXn9Nl6RoIOC532j1g5+EFw0ZpLxxJq9Ms= Valid until Sun, 11 Feb 2029 23:59:59 UTC (expires in 6 years and 9 months) Key RSA 2048 bits (e 65537) COMODO RSA Certification Authority Issuer Signature algorithm SHA384withRSA #3 COMODO RSA Certification Authority In trust store Subject Fingerprint SHA256: 52f0e1c4e58ec629291b60317f074671b85d7ea80d5b07273463534b32b40234 Pin SHA256: grX4Ta9HpZx6tSHkmCrvpApTQGo67CYDnvprLg5yRME= Valid until Mon, 18 Jan 2038 23:59:59 UTC (expires in 15 years and 8 months) RSA 4096 bits (e 65537) Key COMODO RSA Certification Authority Self-signed Issuer Signature algorithm SHA384withRSA



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





Handshake Simulation

Handshake Simulation			
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp384r1 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
Android 8.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Android 8.1	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Android 9.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 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 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Chrome 70 / Win 10	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Chrome 80 / Win 10 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_AES_128_GCM_SHA256 ECDH secp256r1 FS

+

	SSL	SCIVCI ICSI. WWW.	Dalicoopi.pt (Fowered by Quarys 33L Labs	,,	
Handshake Simulation					
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 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS	
Firefox 73 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS	
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS	
<u>IE 11 / Win 7</u> R	Server closed conn	ection			
<u>IE 11 / Win 8.1</u> R	Server closed conn	ection			
IE 11 / Win Phone 8.1 R	Server closed conn	ection			
IE 11 / Win Phone 8.1 Update F	Server closed conn	ection			
<u>IE 11 / Win 10</u> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS	
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS	
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS	
Edge 18 / 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	
<u>Java 8u161</u>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS	
Java 11.0.3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS	
Java 12.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS	
OpenSSL 1.0.1I R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS	
OpenSSL 1.0.2s R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS	
OpenSSL 1.1.0k R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS	
OpenSSL 1.1.1c R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS	
Safari 6 / iOS 6.0.1	Server closed conn	ection			
Safari 7 / iOS 7.1 R	Server closed conn	ection			
Safari 7 / OS X 10.9 R	Server closed conn	ection			
Safari 8 / iOS 8.4 R	Server closed conn	ection			
Safari 8 / OS X 10.10 R	Server closed conn	ection			
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	
<u>Safari 12.1.2 / MacOS 10.14.6</u> <u>Beta</u> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS	
Safari 12.1.1 / iOS 12.3.1 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 secp384r1 FS	
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS	
# Not simulated clients (Proto	ocol mismatch)				4

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.
- (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

	No, server keys and hostname not seen elsewhere with SSLv2
DROWN	(1) For a better understanding of this test, please read this longer explanation
	(2) Key usage data kindly provided by the <u>Censys</u> network search engine; original DROWN website <u>here</u>
	(3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	Not supported ACTION NEEDED (more info)
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)

COLDENDOODLE No (more info) OpenSSL 0-Length No (more info) Obersolated State prevention Vo (more info) Downgrade attack prevention Vo (more info) SSLTTLS compression No RC4 No Heartbeat (extension) No (more info) Heartbeat (vulnerability) No (more info) OpenSSL CSS vuln. (CVE-2014-0224) No (more info) OpenSSL Padding Oracle vuln. No (more info) C(VE-2016-2107) No (more info) ROBOT (vulnerability) No (more info) Forward Secrecy Yes (with most browsers) ROBUST (more info) ALPN Yes (with most browsers) ROBUST (more info) ALPN No (IDs empty) Session resumption (caching) No (IDs empty) Session resumption (tickots) No (IDs empty) Strict Transport Security (HSTS) Yes Public Key Pinning (HPKP) No (more info) Public Key Pinning (Static) No (more info) Long handshake intolerance No (more info) TLS extension intolerance TLS 2.152 Incorrect SNI alerts	Protocol Details	
Sleeping POODLE No (more info) Downgrade attack prevention Unknown (requires support for at least two protocols, excl. SSL2) SSLTLS compression No RC4 No Heartbele (xulnerability) No (more info) Ticketbleed (vulnerability) No (more info) OpenSSL CCS vuln. (CVE-2014-0224) No (more info) OpenSSL Padding Oracle vuln. (CVE-2014-0224) No (more info) CVE-2016-2107) No (more info) Forward Secrecy Yes (with most browsers) ROBUST (more info) ALPN Yes (with most browsers) ROBUST (more info) ALPN No Session resumption (caching) No (IDs empty) Session resumption (tickets) No OCSP stapling No Strict Transport Security (HSTS) Yes max age+31586000, includeSubDomains HSTS Preloading Not in: Chrome Edge Firefox IE Public Key Pinning (Static) No (more info) Long handshake intolerance No (more info) Long handshake intolerance No (more info) TLS version intolerance No (more info) Uses common DH primes <t< th=""><th>GOLDENDOODLE</th><th>No (more info)</th></t<>	GOLDENDOODLE	No (more info)
Downgrade attack prevention Unknown (requires support for at least two protocols, excl. SSL2) SSL/TLS compression No RC4 No Heartback (extension) No Heartback (vulnerability) No (more infg) OpenSSL CS vuln. (CVE-2014-0224) No (more infg) OpenSSL Padding Oracle vuln. (CVE-2014-0224) No (more infg) OpenSSL Padding Oracle vuln. (CVE-2016-2107) No (more infg) ROBOT (vulnerability) No (more infg) Forward Secrecy Yes (with most browsers) ROBUST (more infg) ALPN Yes (with most browsers) ROBUST (more infg) No (IDs empty) Session resumption (tackts) No (IDs empty) Session resumption (tickets) No (IDs empty) Sestict Transport Security (HSTS) Yes (max age-31550000) includeSubDomains HSTS Preloading Not in: Chrome Edge Firefox IE Public Key Pinning (HPKP) No (more infg) Public Key Pinning (Static) No (more infg) Long handshake intolerance No TLS extension intolerance No TLS version intolerance No TLS version intolerance	OpenSSL 0-Length	No (more info)
SSLITLS compression No RC4 No Heartbeat (extension) No Heartbead (extension) No (more info) Ticketbleed (vulnerability) No (more info) OpenSSL Padding Oracle vuln. (CVE-2014-0224) No (more info) OpenSSL Padding Oracle vuln. (CVE-2016-2107) No (more info) ROBOT (vulnerability) No (more info) ROBOT (vulnerability) No (more info) Forward Secrecy Yes (with most browsers) ROBUST (more info) ALPN No NPN No Session resumption (caching) No (IDS empty) Session resumption (tickets) No OCSP stapling No Strict Transport Security (HSTS) Yes max agera 3153000, include SubDomains HSTS Preloading Not in: Chrome Edge Firefox IE Public Key Pinning (HPKP) No (more info) Public Key Pinning (Static) No (more info) Long handshake intolerance No TLS extension intolerance No TLS extension intolerance No TLS extension intolerance No <	Sleeping POODLE	No (more info)
RC4 No Heartbeat (extension) No Heartbeat (extension) No Heartbeat (extension) No Heartbead (vulnerability) No (more info) Ticketbleed (vulnerability) No (more info) OpenSSL CCS vuln. (CVE-2014-0224) No (more info) OpenSSL Padding Oracle vuln. (CVE-2016-2017) No (more info) ROBOT (vulnerability) No (more info) ROBOT (vulnerability) No (more info) Forward Secrecy Yes (with most browsers) ROBUST (more info) ALPN Yes http:/.l.ht/2 NPN No Session resumption (caching) No (IDs empty) Session resumption (tickets) No OCSP stapling No CCSP stapling No CCSP stapling No Strict Transport Security (HSTS) Research (ESP) Interval (ESP) Interva	Downgrade attack prevention	Unknown (requires support for at least two protocols, excl. SSL2)
Heartbeat (extension) Heartblead (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) OpenSSL Padding Oracle vuln. (CVE-2016-2107) No (more info) OpenSSL Padding Oracle vuln. (CVE-2016-2107) No (more info) Forward Socrecy Yes (with most browsers) ROBUST (more info) ALPN Yes http://l hz NPN No Session resumption (caching) No (IDs empty) Session resumption (tickets) No OCSP stapling No OCSP stapling No OCSP stapling No (incre info) No (incre	SSL/TLS compression	No
Hearbleed (vulnerability) No (more info) Ticketbleed (vulnerability) No (more info) OpenSSL CCS vuln. (CVE-2014-0224) No (more info) OpenSSL Padding Oracie vuln. (CVE-2016-2107) ROBOT (vulnerability) No (more info) ROBOT (vulnerability) No (more info) ROBOT (vulnerability) No (more info) Forward Secrecy Yes (with most browsers) ROBUST (more info) ALPN No No No No Session resumption (caching) No (IDs empty) Session resumption (tickets) No OCSP stapling No Strict Transport Security (HSTS) Yes max-agge=31536000; includeSubDomains HSTS Preloading Not in: Chrome Edge Firefox IE Public Key Pinning (HPKP) No (more info) Long handshake intolerance No TLS extension intolerance No TLS extension intolerance No, OHE sultes not supported DH public server param (vs) reuse No, DHE sultes not supported ECDH public server param reuse No Supported Named Groups Secp256f1, secp384f1 (Server has no preference)	RC4	No
Ticketbleed (vulnerability) No (more info) OpenSSL CCS vuln. (CVE-2014-0224) No (more info) OpenSSL Padding Oracle vuln. (CVE-2016-2107) ROBOT (vulnerability) No (more info) ROBOT (vulnerability) No (more info) Forward Secrecy Yes (with most browsers) ROBUST (more info) ALPN No Session resumption (caching) No (IDs empty) Session resumption (tickets) No OCSP stapling No Strict Transport Security (HSTS) Yes max-age=1558000: includeSubDomains HSTS Preloading No (imore info) No (more info) No (more info) Public Key Pinning (HPKP) No (more info) No (more info) TLS extension intolerance No TLS extension intolerance No TLS version intolerance No, DHE sultes not supported DH public server param (vs) reuse No, DHE sultes not supported ECDH public server param reuse No Supported Named Groups ROBUST (Server has no preference)	Heartbeat (extension)	No
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 hz NPN No Session resumption (caching) No (IDs empty) Session resumption (tickets) No OCSP stapling No Strict Transport Security (HSTS) Yes max-age=31538000; includeSubDomains 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 Strict Transport Security (AST) No	Heartbleed (vulnerability)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107) ROBOT (vulnerability) No (more info) Forward Secrecy Yes (with most browsers) ROBUST (more info) ALPN No Session resumption (caching) No (IDs empty) Session resumption (tickets) No OCSP stapling No Strict Transport Security (HSTS) **Pes** max-age=31539000; includeSubDomains HSTS Preloading Not in: Chrome Edge Firefox IE Public Key Pinning (HPKP) No (more info) Public Key Pinning (Static) No (more info) No (more info) Long handshake intolerance No TLS extension intolerance No TLS version intolerance TLS 2.152 Incorrect SNI alerts 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, secp384r1 (Server has no preference)	Ticketbleed (vulnerability)	No (more info)
ROBOT (vulnerability)	OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy Yes (with most browsers) ROBUST (more info) ALPN Yes http/1.1 h2 NPN No Session resumption (caching) No (IDs empty) Session resumption (tickets) No OCSP stapling No Strict Transport Security (HSTS) **max-age=31538000; includeSubDomains* HSTS Preloading Not in: Chrome Edge Firefox IE Public Key Pinning (HPKP) No (more info) Public Key Pinning (RPKP) No (more info) No (more info) Long handshake intolerance No TLS extension intolerance TLS 2.152 Incorrect SNI alerts No Uses common DH primes No, DHE suites not supported DH public server param (Ys) reuse No Supported Named Groups secp256r1, secp384r1 (Server has no preference)		No (more info)
ALPN Yes http/1.1 h2 NPN No Session resumption (caching) No (IDs empty) Session resumption (tickets) No OCSP stapling No Strict Transport Security (HSTS) Yes max-age=31536000; includeSubDomains Modern Info HSTS Preloading Not in: Chrome Edge Firefox IE Public Key Pinning (HPKP) No (more info) 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 Supported Named Groups secp256f1, secp384f1 (Server has no preference)	ROBOT (vulnerability)	No (more info)
NPN No (IDs empty) Session resumption (caching) No (IDs empty) Session resumption (tickets) No OCSP stapling No Strict Transport Security (HSTS) Yes max-age=31536000; includeSubDomains HSTS Preloading Not in: Chrome Edge Firefox IE Public Key Pinning (HPKP) No (more info) Public Key Pinning (RPKP) No (more info) 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 Supported Named Groups server param reuse No	Forward Secrecy	Yes (with most browsers) ROBUST (more info)
Session resumption (caching) No (IDs empty) Session resumption (tickets) No OCSP stapling No Strict Transport Security (HSTS) Yes max-age=31536000; includeSubDomains 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 Supported Named Groups Session resumption (tickets) No No Supported Named Groups	ALPN	Yes http/1.1 h2
Session resumption (tickets) No OCSP stapling No Strict Transport Security (HSTS) Wes max-age=31538000; includeSubDomains 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 version intolerance TLS version intolerance 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, secp384r1 (Server has no preference)	NPN	No
OCSP stapling No Strict Transport Security (HSTS) Yes max-age=31536000; includeSubDomains 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 Supported Named Groups secp256r1, secp384r1 (Server has no preference)	Session resumption (caching)	No (IDs empty)
Strict Transport Security (HSTS) Yes max-age=31536000; includeSubDomains 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 Supported Named Groups secp256r1, secp384r1 (Server has no preference)	Session resumption (tickets)	No
Strict Transport Security (HSTS) max-age=31536000; includeSubDomains 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 Supported Named Groups secp256r1, secp384r1 (Server has no preference)	OCSP stapling	No
Public Key Pinning (HPKP) No (more info) Public Key Pinning Report-Only No (more info) Public Key Pinning (Static) No (more info) Long handshake intolerance No TLS extension intolerance TLS 2.152 Incorrect SNI alerts No Uses common DH primes No, DHE suites not supported DH public server param (Ys) reuse ECDH public server param reuse No Supported Named Groups No (more info) No	Strict Transport Security (HSTS)	
Public Key Pinning Report-Only Public Key Pinning (Static) No (more info) Long handshake intolerance No TLS extension intolerance TLS 2.152 Incorrect SNI alerts No Uses common DH primes No, DHE suites not supported DH public server param (Ys) reuse No Supported Named Groups No No No No Supported Named Groups No No No No No No No Supported Named Groups No No No No No No No No No Supported Named Groups No No No No No No Supported Named Groups	HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (Static) Long handshake intolerance No TLS extension intolerance TLS 2.152 Incorrect SNI alerts No Uses common DH primes No, DHE suites not supported DH public server param (Ys) reuse No Supported Named Groups No (more info) No No Supported Named Groups No No Supported Named Groups No (more info) No No Supported Named Groups No Supported Named Groups No Supported Named Groups No No (more info) No No Supported Named Groups No No Supported Named Groups No No (more info) No Supported Named Groups No Supported Named Groups No Supported Named Groups	Public Key Pinning (HPKP)	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 Supported Named Groups secp256r1, secp384r1 (Server has no preference)	Public Key Pinning Report-Only	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 Supported Named Groups secp256r1, secp384r1 (Server has no preference)	Public Key Pinning (Static)	No (more info)
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 ECDH public server param reuse No Supported Named Groups TLS 2.152 No	Long handshake intolerance	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, secp384r1 (Server has no preference)	TLS extension intolerance	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, secp384r1 (Server has no preference)	TLS version intolerance	TLS 2.152
DH public server param (Ys) reuse No, DHE suites not supported ECDH public server param reuse No Supported Named Groups secp256r1, secp384r1 (Server has no preference)	Incorrect SNI alerts	No
ECDH public server param reuse No Supported Named Groups secp256r1, secp384r1 (Server has no preference)	Uses common DH primes	No, DHE suites not supported
Supported Named Groups secp256r1, secp384r1 (Server has no preference)	DH public server param (Ys) reuse	No, DHE suites not supported
	ECDH public server param reuse	No
SSL 2 handshake compatibility Yes	Supported Named Groups	secp256r1, secp384r1 (Server has no preference)
	SSL 2 handshake compatibility	Yes



HTTP Requests



- 1 https://www.bancobpi.pt/ (HTTP/1.1 301 Moved Permanently)
- 2 https://www.bancobpi.pt/particulares (HTTP/1.1 200 OK)



Miscellaneous

Test date	Tue, 03 May 2022 14:33:11 UTC
Test duration	70.657 seconds
HTTP status code	200
HTTP server signature	Oracle-HTTP-Server
Server hostname	

SSL Report v2.1.10

Copyright © 2009-2022 Qualys, Inc. All Rights Reserved.

Terms and Conditions

<u>Try Qualys for free!</u> Experience the award-winning <u>Qualys Cloud Platform</u> and the entire collection of <u>Qualys Cloud Apps</u>, including <u>certificate security</u> solutions.