

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

SSL Report: www.cm-amarante.pt (188.93.227.91)

Assessed on: Tue, 09 Mar 2021 10:27:28 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating

B

Certificate

Protocol Support

Key Exchange

Cipher Strength

020406080100

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

This site works only in browsers with SNI support.

This server supports TLS 1.3.

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1

Subject	*.cm-amarante.pt Fingerprint SHA256: cc5525fac9492f173b6eeba13e8709174dcec4c73acf1a49bc3a53fb80b17b9b Pin SHA256: UwM7VFVT1i6ni8GTxvYWPRzU8/ymj/bbcUyDSFlsrBY=
Common names	*.cm-amarante.pt
Alternative names	*.cm-amarante.pt cm-amarante.pt
Serial Number	1d3128d9aad866023da84038a6048548
Valid from	Mon, 24 Aug 2020 00:00:00 UTC
Valid until	Wed, 25 Aug 2021 23:59:59 UTC (expires in 5 months and 16 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Sectigo RSA Domain Validation Secure Server CA AIA: http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://ocsp.sectigo.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 (3034 bytes)
-----------------------	----------------

Additional Certificates (if supplied)

Chain issues	None
#2	
Subject	Sectigo RSA Domain Validation Secure Server CA Fingerprint SHA256: 7fa4ff68ec04a99d7528d5085f94907f4d1dd1c5381bacdc832ed5c960214676 Pin SHA256: 4a6cPehl7OG6cuDZka5NDZ7FR8a60d3auda+sKfg4Ng=
Valid until	Tue, 31 Dec 2030 23:59:59 UTC (expires in 9 years and 9 months)
Key	RSA 2048 bits (e 65537)
Issuer	USERTrust RSA Certification Authority
Signature algorithm	SHA384withRSA



Certification Paths



Click here to expand

Certificate #2: RSA 2048 bits (SHA256withRSA) No SNI



Click here to expand

Configuration



Protocols

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

(*) Experimental: Server negotiated using No-SNI



Cipher Suites

# TLS 1.3 (server has no preference)			
TLS_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA) FS		128
TLS_AES_256_GCM_SHA384 (0x1302)	ECDH x25519 (eq. 3072 bits RSA) FS		256
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	ECDH x25519 (eq. 3072 bits RSA) FS		256
# TLS 1.2 (server has no preference)			
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	WEAK		128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits FS WEAK		128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	WEAK		128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 2048 bits FS WEAK		128
TLS_RSA_WITH_SEED_CBC_SHA (0x96)	WEAK		128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a)	DH 2048 bits FS WEAK		128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp521r1 (eq. 15360 bits RSA) FS WEAK		128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	WEAK		128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 2048 bits FS WEAK		128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	WEAK		128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 2048 bits FS		128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xba)	WEAK		128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xbe)	DH 2048 bits FS WEAK		128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp521r1 (eq. 15360 bits RSA) FS WEAK		128

Cipher Suites		
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp521r1 (eq. 15360 bits RSA) FS	128
TLS_RSA_WITH_ARIA_128_GCM_SHA256 (0xc050) WEAK		128
TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc052)	DH 2048 bits FS	128
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc060)	ECDH secp521r1 (eq. 15360 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xc076) WEAK	ECDH secp521r1 (eq. 15360 bits RSA) FS	128
TLS_RSA_WITH_AES_128_CCM (0xc09c) WEAK		128
TLS_DHE_RSA_WITH_AES_128_CCM (0xc09e)	DH 2048 bits FS	128
TLS_RSA_WITH_AES_128_CCM_8 (0xc0a0) WEAK		128
TLS_DHE_RSA_WITH_AES_128_CCM_8 (0xc0a2)	DH 2048 bits FS	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK		256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) WEAK	DH 2048 bits FS	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) WEAK		256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) WEAK	DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) WEAK	ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) WEAK		256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) WEAK	DH 2048 bits FS	256
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK		256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 2048 bits FS	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0xc0) WEAK		256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0xc4) WEAK	DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) WEAK	ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_RSA_WITH_ARIA_256_GCM_SHA384 (0xc051) WEAK		256
TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc053)	DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc061)	ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (0xc077) WEAK	ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_RSA_WITH_AES_256_CCM (0xc09d) WEAK		256
TLS_DHE_RSA_WITH_AES_256_CCM (0xc09f)	DH 2048 bits FS	256
TLS_RSA_WITH_AES_256_CCM_8 (0xc0a1) WEAK		256
TLS_DHE_RSA_WITH_AES_256_CCM_8 (0xc0a3)	DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0ca8)	ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0caa)	DH 2048 bits FS	256
# TLS 1.1 (server has no preference)		
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK		128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) WEAK	DH 2048 bits FS	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) WEAK		128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) WEAK	DH 2048 bits FS	128
TLS_RSA_WITH_SEED_CBC_SHA (0x96) WEAK		128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a) WEAK	DH 2048 bits FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) WEAK	ECDH secp521r1 (eq. 15360 bits RSA) FS	128
TLS_RSA_WITH_IDEA_CBC_SHA (0x7) WEAK		128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK		256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) WEAK	DH 2048 bits FS	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) WEAK		256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) WEAK	DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) WEAK	ECDH secp521r1 (eq. 15360 bits RSA) FS	256
# TLS 1.0 (server has no preference)		
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK		128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) WEAK	DH 2048 bits FS	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) WEAK		128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) WEAK	DH 2048 bits FS	128
TLS_RSA_WITH_SEED_CBC_SHA (0x96) WEAK		128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a) WEAK	DH 2048 bits FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) WEAK	ECDH secp521r1 (eq. 15360 bits RSA) FS	128

Cipher Suites

TLS_RSA_WITH_IDEA_CBC_SHA (0x7)	WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits FS WEAK	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 2048 bits FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp521r1 (eq. 15360 bits RSA) FS WEAK	256



Handshake Simulation

Android 2.3.7	No SNI ²	Incorrect certificate because this client doesn't support SNI		
RSA 2048 (SHA256) TLS 1.0 TLS_RSA_WITH_AES_128_CBC_SHA				
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 secp521r1 FS
Android 4.2.2		RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Android 4.3		RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Android 4.4.2		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS
Android 5.0.0		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 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_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 8.0		RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 8.1		-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 9.0		-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
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 secp521r1 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_128_GCM_SHA256 ECDH x25519 FS
Chrome 70 / Win 10		-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Chrome 80 / Win 10	R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 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 62 / Win 7	R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Firefox 73 / Win 10	R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Googlebot Feb 2018		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
IE 7 / Vista		RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No 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_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
IE 11 / Win 8.1	R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
IE 10 / Win Phone 8.0		RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 11 / Win Phone 8.1	R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA256 No FS
IE 11 / Win Phone 8.1 Update	R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 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 15 / Win 10	R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Edge 16 / Win 10	R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Edge 18 / Win 10	R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 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	Incorrect certificate because this client doesn't support SNI		
RSA 2048 (SHA256) TLS 1.0 TLS_RSA_WITH_AES_128_CBC_SHA				
Java 7u25		RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Java 8u161		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Java 11.0.3		-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 12.0.1		-	TLS 1.3	TLS_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 1.0.1j	R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS
OpenSSL 1.0.2s	R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS

Handshake Simulation

OpenSSL 1.1.0k R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519	FS
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519	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_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
Safari 12.1.2 / MacOS 10.14.6 Beta R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519	FS
Safari 12.1.1 / iOS 12.3.1 R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519	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 secp521r1	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

	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 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: 0x2f
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2: 0x002f
GOLDENDOODLE	No (more info) TLS 1.2: 0x002f
OpenSSL 0-Length	No (more info) TLS 1.2: 0x002f
Sleeping POODLE	No (more info) TLS 1.2: 0x002f
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	With some browsers (more info)
ALPN	Yes http/1.1
NPN	No
Session resumption (caching)	Yes

Protocol Details	
Session resumption (tickets)	Yes
OCSP stapling	Yes
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, x25519, x448 (Server has no preference)
SSL 2 handshake compatibility	Yes
0-RTT enabled	No



HTTP Requests +	
1	https://www.cm-amarante.pt/ (HTTP/1.1 200 OK)



Miscellaneous	
Test date	Tue, 09 Mar 2021 10:24:25 UTC
Test duration	183.259 seconds
HTTP status code	200
HTTP server signature	Apache
Server hostname	globaz-01.ibername.com

SSL Report v2.1.8