

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.nos.pt](#) > 212.113.183.252

SSL Report: [www.nos.pt](#) (212.113.183.252)

Assessed on: Tue, 03 May 2022 23:37:08 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 supports TLS 1.1. Grade capped to B. [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

Subject	*.nos.pt Fingerprint SHA256: b105efb4a5f28c9719ba1105f71270ef9a85fc1ba44a9ad439d33d7081fb5be6 Pin SHA256: li6SN0ZaXjg5Re9Yzitl3WYVMsXs1P0tpTFRf6JTVStk=
Common names	*.nos.pt
Alternative names	*.nos.pt nos.pt
Serial Number	1b760f51e0343a268c32284658f06256
Valid from	Thu, 21 Apr 2022 00:00:00 UTC
Valid until	Fri, 21 Apr 2023 23:59:59 UTC (expires in 11 months and 18 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	MarketWare - Soluções para Mercados Digitais, Lda. RSA DV CA AIA: http://crt.usertrust.com/MarketWareSolucoesparaMercadosDigitaisLdaRSADVCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.usertrust.com/MarketWareSolucoesparaMercadosDigitaisLdaRSADVCA.crl OCSP: http://ocsp.usertrust.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 (4743 bytes)
Chain issues	None

#2

Additional Certificates (if supplied)

Subject	MarketWare - Soluções para Mercados Digitais, Lda. RSA DV CA Fingerprint SHA256: 722d50874da45496d0299627409777603a87341a5f943b889c32e7b9280a8f71 Pin SHA256: 0xxElcXteNs+TYPZ7GyhN/WFNSBPpaBsyCLFCdhQQY0=
Valid until	Mon, 10 Nov 2025 23:59:59 UTC (expires in 3 years and 6 months)
Key	RSA 2048 bits (e 65537)
Issuer	USERTrust RSA Certification Authority
Signature algorithm	SHA384withRSA

#3

Subject	USERTrust RSA Certification Authority Fingerprint SHA256: 68b9c761219a5b1f0131784474665db61bbdb109e00f05ca9f74244ee5f5f52b Pin SHA256: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4ITdO/nEW/Td4=
Valid until	Sun, 31 Dec 2028 23:59:59 UTC (expires in 6 years and 7 months)
Key	RSA 4096 bits (e 65537)
Issuer	AAA Certificate Services
Signature algorithm	SHA384withRSA



Certification Paths



Click here to expand

Configuration



Protocols

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



Cipher Suites

# TLS 1.2 (suites in server-preferred order)			
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp384r1 (eq. 7680 bits RSA) FS		256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp384r1 (eq. 7680 bits RSA) FS		128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp384r1 (eq. 7680 bits RSA) FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp384r1 (eq. 7680 bits RSA) FS	WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp384r1 (eq. 7680 bits RSA) FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp384r1 (eq. 7680 bits RSA) FS	WEAK	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 4096 bits FS		256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 4096 bits FS	WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 4096 bits FS	WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 4096 bits FS	WEAK	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 4096 bits FS		128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 4096 bits FS	WEAK	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 4096 bits FS	WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)		WEAK	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)		WEAK	256
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_GCM_SHA256 (0x9c)		WEAK	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)		WEAK	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		WEAK	128

Cipher Suites

TLS 1.1 (suites in server-preferred order)



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 secp384r1	FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Android 8.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Android 8.1	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Android 9.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	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 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS
Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Chrome 70 / Win 10	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Chrome 80 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Firefox 73 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1	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 secp384r1	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 secp384r1	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 secp384r1	FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Java 11.0.3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Java 12.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
OpenSSL 1.0.1l 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 secp384r1	FS
OpenSSL 1.1.0k R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
OpenSSL 1.1.1c R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1	FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1	FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1	FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1	FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1	FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Safari 12.1.1 / iOS 12.3.1 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	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 (Protocol mismatch)

Handshake Simulation

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

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	Mitigated server-side	(more info)
POODLE (SSLv3)	No, SSL 3 not supported	(more info)
POODLE (TLS)	No	(more info)
Zombie POODLE	No	(more info) TLS 1.2 : 0xc027
GOLDENDOODLE	No	(more info) TLS 1.2 : 0xc027
OpenSSL 0-Length	No	(more info) TLS 1.2 : 0xc027
Sleeping POODLE	No	(more info) TLS 1.2 : 0xc027
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	Yes	h2 http/1.1
NPN	Yes	h2 http/1.1
Session resumption (caching)	No (IDs assigned but not accepted)	
Session resumption (tickets)	No	
OCSP stapling	Yes	
Strict Transport Security (HSTS)	Yes	max-age=31536000
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	secp384r1	
SSL 2 handshake compatibility	Yes	



HTTP Requests



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



Miscellaneous

Test date	Tue, 03 May 2022 23:34:46 UTC
Test duration	142.307 seconds
HTTP status code	200
HTTP server signature	Microsoft-IIS
Server hostname	a212-113-183-252.netcabo.pt

SSL Report v2.1.10