SSL Report: www.nys.go.ke (102.210.149.88)

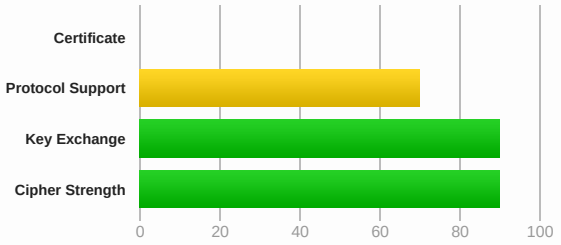
Assessed on: Sun, 25 Oct 2026 11:26:53 UTC | **HIDDEN** | Clear cache

Scan Another »

Summary

Overall Rating

F



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server's certificate is not trusted, see below for details.

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

This server does not support TLS 1.3. MORE INFO »

This site works only in browsers with SNI support.

This server does not support PQC (Post-Quantum Cryptography) key exchange.

Certificate #1: RSA 2048 bits (SHA384withRSA)

Server Key and Certificate #1

Subject	*.nys.go.ke Fingerprint SHA256: d5849b9b981fd57081c71d7e2f11f07a1063efb7f2b80683d5f73405c799d3df Pin SHA256: A5fpB6pkoMqCpxV6Q1D+6aj9oMp56cB8SCH7iKo4MkA=
Common names	*.nys.go.ke
Alternative names	*.nys.go.ke www.nys.go.ke nys.go.ke
Serial Number	21520191fea86ca86c6ca4d66d8811
Valid from	Thu, 03 Sep 2026 13:42:19 UTC
Valid until	Wed, 02 Dec 2026 13:42:19 UTC (expires in 1 month and 7 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	EM DV TLS CA - G2A-1 AIA: http://repository.emsign.com/certs/EMDVTLSCAG2A1EE.p7c
Signature algorithm	SHA384withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.emsign.com?EMDVTLSCAG2A1.crl OCSP: http://ocsp-a.emsign.com
Revocation status	Revoked **INSECURE**

Server Key and Certificate #1

DNS CAA	No (more info)
Trusted	No **NOT TRUSTED** (Why?) **Mozilla Apple Android Java Windows**

Additional Certificates (if supplied)

Certificates provided	4 (5968 bytes)
Chain issues	Contains anchor

#2

Subject	EM DV TLS CA - G2A-1 Fingerprint SHA256: 3f13597d3355d341bd09328aee567d7f4e002d9919b986f9962daff197ea75d1 Pin SHA256: zrUpja649ZJ5SAtGACyJ93Vcw6FpUUsRuBC+/BlaANg=
Valid until	Mon, 28 May 2040 07:16:12 UTC (expires in 13 years and 7 months)
Key	RSA 4096 bits (e 65537)
Issuer	emSign Root TLS CA - G1
Signature algorithm	SHA384withRSA

#3

Subject	emSign Root TLS CA - G1 Fingerprint SHA256: 9b913476eab476e21e0887dbcde44345d1359d28116b83b7cd3e87bd807ebf68 Pin SHA256: 7OKONSic6GIcckB5SeUFAFKtRgfMMy6vm1RgKarL+3o=
Valid until	Sat, 09 Jul 2039 18:30:00 UTC (expires in 12 years and 8 months)
Key	RSA 4096 bits (e 65537)
Issuer	emSign Root CA - G1
Signature algorithm	SHA256withRSA

#4

Subject	emSign Root CA - G1 In trust store Fingerprint SHA256: 40f6af0346a99aa1cd1d555a4e9cce62c7f9634603ee406615833dc8c8d00367 Pin SHA256: N2oacIKlk9zMINVh0Rnpq40w8RzDIdCjf6QfDfKE4Bw=
Valid until	Wed, 18 Feb 2043 18:30:00 UTC (expires in 16 years and 3 months)
Key	RSA 2048 bits (e 65537)
Issuer	emSign Root CA - G1 Self-signed
Signature algorithm	SHA256withRSA

Certification Paths

Click here to expand

Certificate #2: RSA 2048 bits (SHA384withRSA) No SNI

Click here to expand

Configuration

Protocols

TLS 1.3	No
TLS 1.2	Yes*
TLS 1.1	Yes
TLS 1.0	Yes*

Protocols

SSL 3	No
SSL 2	No

(*) Experimental: Server negotiated using No-SNI

Cipher Suites

# TLS 1.2 (suites in server-preferred order)				
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH x25519 (eq. 3072 bits RSA)	FS		256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 2048 bits	FS		256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)	ECDH x25519 (eq. 3072 bits RSA)	FS		256
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa)	DH 2048 bits	FS		256
TLS_DHE_RSA_WITH_AES_256_CCM (0xc09f)	DH 2048 bits	FS		256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc061)	ECDH x25519 (eq. 3072 bits RSA)	FS		256
TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc053)	DH 2048 bits	FS		256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH x25519 (eq. 3072 bits RSA)	FS		128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 2048 bits	FS		128
TLS_DHE_RSA_WITH_AES_128_CCM (0xc09e)	DH 2048 bits	FS		128
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc060)	ECDH x25519 (eq. 3072 bits RSA)	FS		128
TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc052)	DH 2048 bits	FS		128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH x25519 (eq. 3072 bits RSA)	FS	WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 2048 bits	FS	WEAK	256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (0xc077)	ECDH x25519 (eq. 3072 bits RSA)	FS	WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0xc4)	DH 2048 bits	FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH x25519 (eq. 3072 bits RSA)	FS	WEAK	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 2048 bits	FS	WEAK	128
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xc076)	ECDH x25519 (eq. 3072 bits RSA)	FS	WEAK	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xbe)	DH 2048 bits	FS	WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH x25519 (eq. 3072 bits RSA)	FS	WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits	FS	WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 2048 bits	FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH x25519 (eq. 3072 bits RSA)	FS	WEAK	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits	FS	WEAK	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 2048 bits	FS	WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)			WEAK	256
TLS_RSA_WITH_AES_256_CCM (0xc09d)			WEAK	256
TLS_RSA_WITH_ARIA_256_GCM_SHA384 (0xc051)			WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)			WEAK	128
TLS_RSA_WITH_AES_128_CCM (0xc09c)			WEAK	128
TLS_RSA_WITH_ARIA_128_GCM_SHA256 (0xc050)			WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)			WEAK	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0xc0)			WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)			WEAK	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xba)			WEAK	128
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_CBC_SHA (0x2f)			WEAK	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)			WEAK	128
TLS_DHE_RSA_WITH_AES_256_CCM_8 (0xc0a3)	DH 2048 bits	FS		256
TLS_DHE_RSA_WITH_AES_128_CCM_8 (0xc0a2)	DH 2048 bits	FS		128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a)	DH 2048 bits	FS	WEAK	128
TLS_RSA_WITH_AES_256_CCM_8 (0xc0a1)			WEAK	256
TLS_RSA_WITH_AES_128_CCM_8 (0xc0a0)			WEAK	128

Cipher Suites

TLS_RSA_WITH_SEED_CBC_SHA (0x96)	**WEAK**	128

 # TLS 1.1 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits FS **WEAK**	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 2048 bits FS **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits FS **WEAK**	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 2048 bits FS **WEAK**	128
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_CBC_SHA (0x2f)	**WEAK**	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	**WEAK**	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a)	DH 2048 bits FS **WEAK**	128
TLS_RSA_WITH_SEED_CBC_SHA (0x96)	**WEAK**	128
TLS_RSA_WITH_IDEA_CBC_SHA (0x7)	**WEAK**	128

 # TLS 1.0 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits FS **WEAK**	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 2048 bits FS **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits FS **WEAK**	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 2048 bits FS **WEAK**	128
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_CBC_SHA (0x2f)	**WEAK**	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	**WEAK**	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a)	DH 2048 bits FS **WEAK**	128
TLS_RSA_WITH_SEED_CBC_SHA (0x96)	**WEAK**	128
TLS_RSA_WITH_IDEA_CBC_SHA (0x7)	**WEAK**	128

Handshake Simulation

Android 2.3.7 No SNI [2]	Incorrect certificate because this client doesn't support SNI RSA 2048 (SHA384) | TLS 1.0 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA | DH 2048			
Android 4.0.4	RSA 2048 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
Android 4.1.1	RSA 2048 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
Android 4.2.2	RSA 2048 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
Android 4.3	RSA 2048 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
Android 4.4.2	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Android 5.0.0	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 6.0	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 7.0	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Android 8.0	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Android 8.1	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Android 9.0	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Baidu Jan 2015	RSA 2048 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
BingPreview Jan 2015	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDH secp256r1 FS
Chrome 69 / Win 7 R	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Chrome 70 / Win 10	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Chrome 80 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS

Handshake Simulation

Chrome 131 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 47 / Win 7 R	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Firefox 62 / Win 7 R	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Firefox 73 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Firefox 135 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Googlebot Feb 2018	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
IE 7 / Vista	RSA 2048 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
IE 8 / XP No FS [1] No SNI [2]	Server sent fatal alert: handshake_failure			
IE 8-10 / Win 7 R	RSA 2048 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
IE 11 / Win 7 R	RSA 2048 (SHA384)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 2048 FS
IE 11 / Win 8.1 R	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 2048 FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA384)	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 (SHA384)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 2048 FS
IE 11 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Edge 15 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Edge 16 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Edge 18 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Edge 131 / Win 10 R	RSA 2048 (SHA384)	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 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Java 6u45 No SNI [2]	Client does not support DH parameters > 1024 bits RSA 2048 (SHA384) | TLS 1.0 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA | DH 2048			
Java 7u25	RSA 2048 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
Java 8u161	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Java 11.0.3	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Java 12.0.1	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
OpenSSL 0.9.8y	RSA 2048 (SHA384)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DH 2048 FS
OpenSSL 1.0.1l R	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
OpenSSL 1.0.2s R	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
OpenSSL 1.1.0k R	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
OpenSSL 1.1.1c R	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Opera 117 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA384)	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 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 9 / iOS 9 R	RSA 2048 (SHA384)	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 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 2048 (SHA384)	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 (SHA384)	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	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Safari 12.1.1 / iOS 12.3.1 R	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
YandexBot Jan 2015	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS

Handshake Simulation

 # 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

Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: `0xc014`
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)	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	**Yes (with most browsers) ROBUST** (more info)
ALPN	Yes http/1.1
NPN	No
Session resumption (caching)	**No (IDs empty)**
Session resumption (tickets)	Yes
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	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	x25519, secp256r1, secp384r1, secp521r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1 (server preferred order)
PQC Key Exchange	Not Supported
Supported PQC Groups	-
SSL 2 handshake compatibility	Yes

HTTP Requests

1 https://www.nys.go.ke/ (HTTP/1.1 200 OK)

Miscellaneous

Test date	Sun, 25 Oct 2026 11:22:37 UTC
Test duration	256.274 seconds
HTTP status code	200
HTTP server signature	nginx
Server hostname	-

Why is my certificate not trusted?

There are many reasons why a certificate may not be trusted. The exact problem is indicated on the report card in bright red. The problems fall into three categories:

1. Invalid certificate
2. Invalid configuration
3. Unknown Certificate Authority

1. Invalid certificate

A certificate is invalid if:

- It is used before its activation date
- It is used after its expiry date
- Certificate hostnames don't match the site hostname
- It has been revoked
- It has insecure signature
- It has been blacklisted

2. Invalid configuration

In some cases, the certificate chain does not contain all the necessary certificates to connect the web server certificate to one of the root certificates in our trust store. Less commonly, one of the certificates in the chain (other than the web server certificate) will have expired, and that invalidates the entire chain.

3. Unknown Certificate Authority

In order for trust to be established, we must have the root certificate of the signing Certificate Authority in our trust store. SSL Labs does not maintain its own trust store; instead we use the store maintained by Mozilla.

If we mark a web site as not trusted, that means that the average web user's browser will not trust it either. For certain special groups of users, such web sites can still be secure. For example, if you can securely verify that a self-signed web site is operated by a person you trust, then you can trust that self-signed web site too. Or, if you work for an organisation that manages its own trust, and you have their own root certificate already embedded in your browser. Such special cases do not work for the general public, however, and this is what we indicate on our report card.

4. Interoperability issues

In some rare cases trust cannot be established because of interoperability issues between our code and the code or configuration running on the server. We manually review such cases, but if you encounter such an issue please feel free to contact us. Such problems are very difficult to troubleshoot and you may be able to provide us with information that might help us determine the root cause.

SSL Report v2.4.3

Copyright © 2009-2026 Qualys, Inc. All Rights Reserved. Privacy Policy. Terms and Conditions

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