

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > www.nerdrr.gov.in

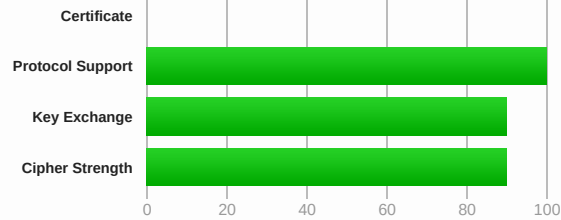
SSL Report: www.nerdrr.gov.in (103.99.184.80)

Assessed on: Sun, 25 Oct 2026 11:03:49 UTC | **HIDDEN** | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



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 1.3. [MORE INFO »](#)

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

Certificate #1: RSA 2048 bits (SHA384withRSA)



Server Key and Certificate #1



Subject	*.nerdrr.gov.in Fingerprint SHA256: dc606772481386001427b33b851bd4b8494c672534616851e536e72c343452e3 Pin SHA256: 5entwDzVF/l8ari6EF7+hjTl3aPw5FW00YF+kSKLg8g=
Common names	*.nerdrr.gov.in
Alternative names	nerdrr.gov.in *.nerdrr.gov.in
Serial Number	00e441f7b467c7d0fda36afb296bf66f
Valid from	Mon, 28 Sep 2026 05:48:21 UTC
Valid until	Wed, 02 Dec 2026 09:36:32 UTC (expires in 1 month and 6 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	EM DV TLS CA - G2A-1 AIA: http://repository.emsign.com/certs/EMDVTLSAG2A1EE.p7c
Signature algorithm	SHA384withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.emsign.com?EMDVTLSAG2A1.crl OCSP: http://ocsp-a.emsign.com
Revocation status	Revoked INSECURE
DNS CAA	No (more info)
Trusted	No NOT TRUSTED (Why?) Mozilla Apple Android Java Windows



Additional Certificates (if supplied)



Certificates provided	6 (8469 bytes)
Chain issues	Contains anchor
#2	
Subject	EM DV TLS CA - G2A-1 Fingerprint SHA256: 122a5433d8a2a8c501d5e680ab216885a6019326a189df91e8895f8b5ad488dd Pin SHA256: zrUpja649ZJ5SAIGACyJ93Vcw6FpUUsRuBC+/BlaAng=
Valid until	Sun, 31 Dec 2028 23:59:59 UTC (expires in 2 years and 2 months)
Key	RSA 4096 bits (e 65537)
Issuer	AAA Certificate Services
Signature algorithm	SHA256withRSA
#3	
Subject	AAA Certificate Services In trust store Fingerprint SHA256: d7a7a0fb5d7e2731d771e9484ebcdef71d5f0c3e0a2948782bc83ee0ea699ef4 Pin SHA256: vRU+17BDT2IGsXvOi76E7TQMCTLXAqJ0+GPdW7L1vM=
Valid until	Sun, 31 Dec 2028 23:59:59 UTC (expires in 2 years and 2 months)
Key	RSA 2048 bits (e 65537)
Issuer	AAA Certificate Services Self-signed
Signature algorithm	SHA1withRSA Weak, but no impact on root certificate
#4	
Subject	EM DV TLS CA - G2A-1 Fingerprint SHA256: 3f13597d3355d341bd09328aee567d7f4e002d9919b986f9962daff197ea75d1 Pin SHA256: zrUpja649ZJ5SAIGACyJ93Vcw6FpUUsRuBC+/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
#5	
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
#6	
Subject	emSign Root CA - G1 In trust store Fingerprint SHA256: 40f6af0346a99aa1cd1d555a4e9cce62c7f9634603ee406615833dc8c8d00367 Pin SHA256: N2oacIKlk9zMINVh0Rnpq40w8RzDldCjff6QIDfKE4Bw=
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](#)



Protocols

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



Cipher Suites

# TLS 1.3 (suites in server-preferred order)			
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



Handshake Simulation

Android 8.1	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519	FS
Android 9.0	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519	FS
Chrome 69 / Win 7	R	Server sent fatal alert: protocol_version			
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
Chrome 131 / Win 10	R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519 FS
Firefox 62 / Win 7	R	Server sent fatal alert: protocol_version			
Firefox 73 / Win 10	R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519 FS
Firefox 135 / Win 10	R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519 FS
Edge 131 / Win 10	R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519 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 1.1.0k	R	Server sent fatal alert: protocol_version			
OpenSSL 1.1.1c	R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519 FS
Opera 117 / Win 10	R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519 FS
Safari 12.1.2 / MacOS 10.14.6	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519	FS
Beta	R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519 FS
Safari 12.1.1 / iOS 12.3.1	R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519 FS

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

ROBOT (vulnerability)	No (more info)
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
ALPN	Yes http/1.1
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)

Protocol Details

Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Supported Named Groups	x25519, secp256r1, x448, secp521r1, secp384r1 (server preferred order)
PQC Key Exchange	Not Supported
Supported PQC Groups	-
SSL 2 handshake compatibility	No
0-RTT enabled	No



HTTP Requests



- 1 <https://www.nerdr.gov.in/> (HTTP/1.1 403 Forbidden)



Miscellaneous

Test date	Sun, 25 Oct 2026 11:03:08 UTC
Test duration	41.631 seconds
HTTP status code	403
HTTP server signature	Apache
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

