

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > irfc.co.in

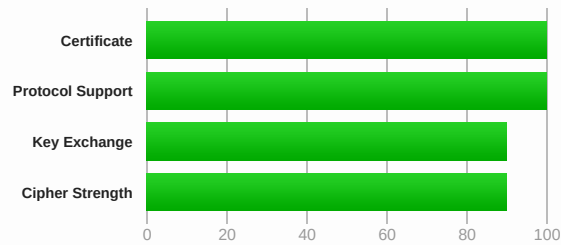
SSL Report: irfc.co.in (103.127.140.94)

Assessed on: Sun, 25 Oct 2026 09:40:50 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 supports TLS 1.3. [MORE INFO »](#)

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

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO »](#)

Certificate #1: RSA 2048 bits (SHA384withRSA)



Server Key and Certificate #1



Subject	irfc.co.in Fingerprint SHA256: cab25c93c19e804e3f5de8166807aedc8743a20a837660fc6b15f3f7861c351c Pin SHA256: 09JWfh4gbU2WQkjz2SQ6VHQ5IC/zd7uB4IAptPcJPpA=
Common names	irfc.co.in
Alternative names	www.irfc.co.in irfc.co.in
Serial Number	008a7becb2fb72fa905a451025248a7e
Valid from	Thu, 15 Oct 2026 22:33:29 UTC
Valid until	Tue, 12 Jan 2027 22:33:29 UTC (expires in 2 months and 18 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	EM DV TLS CA - G2A-1 AIA: http://repository.emsign.com/certs/EMDVTLSGAG2A1EE.p7c
Signature algorithm	SHA384withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.emsign.com?EMDVTLSGAG2A1.crl OCSP: http://ocsp-a.emsign.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows



Additional Certificates (if supplied)



Certificates provided	4 (5969 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: 7OKONSic6GicckB5SeUFAFKiRgfMMY6vm1RgKarL+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: N2oacIKlk9zMINVh0Rnpq40w8RzDldCjff6QfDfKE4Bw=
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](#)

Configuration



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 secp256r1 (eq. 3072 bits RSA) FS		128
TLS_AES_256_GCM_SHA384 (0x1302)	ECDH secp256r1 (eq. 3072 bits RSA) FS		256
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	ECDH secp256r1 (eq. 3072 bits RSA) FS		256
TLS_AES_128_CCM_SHA256 (0x1304)	ECDH secp256r1 (eq. 3072 bits RSA) FS		128



Handshake Simulation

Android 8.1	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 9.0	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1	FS
Chrome 69 / Win 7	R	Server sent fatal alert: handshake_failure			
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1	FS
Chrome 80 / Win 10	R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1 FS
Chrome 131 / Win 10	R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 62 / Win 7	R	Server sent fatal alert: handshake_failure			
Firefox 73 / Win 10	R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 135 / Win 10	R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1 FS
Edge 131 / Win 10	R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	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 1.1.0k	R	Server sent fatal alert: handshake_failure			
OpenSSL 1.1.1c	R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1 FS
Opera 117 / Win 10	R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1 FS
Safari 12.1.2 / MacOS 10.14.6	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1	FS
Beta	R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1 FS
Safari 12.1.1 / iOS 12.3.1	R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1 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	No
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	Yes max-age=31536000; includeSubDomains; preload
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)
Supported Named Groups	secp256r1, x25519, secp384r1, ffdhe2048, ffdhe3072, ffdhe4096 (server preferred order)
PQC Key Exchange	Not Supported
Supported PQC Groups	-
SSL 2 handshake compatibility	No
0-RTT enabled	No



HTTP Requests

[1 https://lirfc.co.in/ \(HTTP/1.1 302 Found\)](#)



Miscellaneous

Test date	Sun, 25 Oct 2026 09:40:07 UTC
Test duration	43.361 seconds
HTTP status code	200
HTTP server signature	-
Server hostname	-

SSL Report v2.4.3