

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

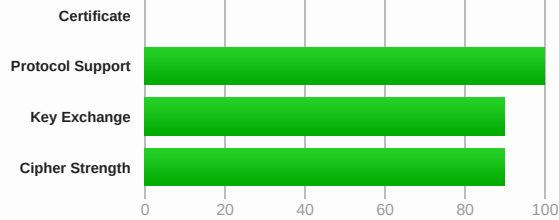
SSL Report: digitalpolicecitizenservices.gov.in (164.100.54.170)

Assessed on: Mon, 26 Oct 2026 08:53:29 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.

DNS Certification Authority Authorization (CAA) Policy found for this domain. [MORE INFO »](#)

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1



Subject	digitalpolicecitizenservices.gov.in Fingerprint SHA256: 6728fe347933b7ece19bd2fe9ef60949a7deba3399335a307551e647f5957a78 Pin SHA256: ZAcF/VW+g9bJrFZhDQ78FWE8707IT7u6bUmT/IVGE3U=
Common names	digitalpolicecitizenservices.gov.in
Alternative names	www.digitalpolicecitizenservices.gov.in digitalpolicecitizenservices.gov.in
Serial Number	00e49b2980da8467604d01313c56233a
Valid from	Fri, 19 Dec 2025 04:55:38 UTC
Valid until	Tue, 12 Jan 2027 10:20:16 UTC (expires in 2 months and 17 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	emSign SSL CA - G1 AIA: http://repository.emsign.com/certs/emSignSSLCAG1.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.emsign.com?emSignSSLCAG1.crl OCSP: http://ocsp.emsign.com
Revocation status	Revoked INSECURE
DNS CAA	Yes policy host: digitalpolicecitizenservices.gov.in issue: emsign.com flags:0



Trusted

No **NOT TRUSTED** ([Why?](#))
[Mozilla](#) [Apple](#) [Android](#) [Java](#) [Windows](#)



Additional Certificates (if supplied)



Certificates provided	2 (2824 bytes)
Chain issues	None
#2	
Subject	emSign SSL CA - G1 Fingerprint SHA256: 47b2efbc3670e7db4b41f22c51fc02ee84fb2dbf3082a49f2c2688122e9210a1 Pin SHA256: qvzNg6+PS7JbCFR+FL+eAfFZOiN6pXXsH1tc9auHIF8=
Valid until	Fri, 18 Feb 2033 18:30:00 UTC (expires in 6 years and 3 months)
Key	RSA 2048 bits (e 65537)
Issuer	emSign Root CA - G1
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_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_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_128_CCM_SHA256 (0x1304)	ECDH x25519 (eq. 3072 bits RSA) FS	128



Handshake Simulation

Android 8.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519	FS
Android 9.0	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519	FS
Chrome 69 / Win 7 R		Server sent fatal alert: protocol_version			
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519	FS
Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519	FS
Chrome 131 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519	FS
Firefox 62 / Win 7 R		Server sent fatal alert: protocol_version			
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519	FS
Firefox 135 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519	FS
Edge 131 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519	FS
Java 11.0.3	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH secp256r1	FS

Handshake Simulation

Java 12.0.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH secp256r1	FS
OpenSSL 1.1.0k	R	Server sent fatal alert: protocol_version			
OpenSSL 1.1.1c	R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Opera 117 / Win 10	R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Safari 12.1.2 / MacOS 10.14.6		-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Beta	R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Safari 12.1.1 / iOS 12.3.1	R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	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)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Supported Named Groups	x25519, secp256r1, x448, secp521r1, secp384r1, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 (server preferred order)
PQC Key Exchange	Not Supported
Supported PQC Groups	-
SSL 2 handshake compatibility	No
0-RTT enabled	No



HTTP Requests



1 <https://digitalpolicecitizenservices.gov.in/> (HTTP/1.1 302 Found)



Miscellaneous

Test date	Mon, 26 Oct 2026 08:52:40 UTC
Test duration	49.612 seconds
HTTP status code	302
HTTP forwarding	https://www.digitalpolicecitizenservices.gov.in
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