# SSL Report: dcdndoor04.sdcc.bnl.gov (2620:0:210:2:0:0:0:44)

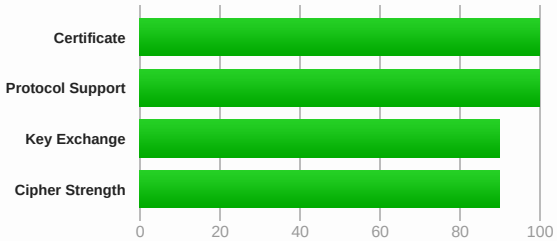
**Assessed on:** Mon, 26 Oct 2026 08:24:34 UTC | **HIDDEN** | Clear cache

Scan Another »

## Summary

Overall Rating

B




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

This server's certificate chain is incomplete. Grade capped to B.

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 4096 bits (SHA384withRSA)

### Server Key and Certificate #1

| | |
|---|---|
| **Subject** | dcdndoor04.sdcc.bnl.gov<br>Fingerprint SHA256: c0ad027d86cc5e3677b8bfc39caf91a0938ae56c109f993173cc14dc73a9f894<br>Pin SHA256: RL1aWhAVSN9YC99ooRyLphBEjDcWNj/ZBW1QrPvRyRE= |
| **Common names** | dcdndoor04.sdcc.bnl.gov |
| **Alternative names** | dcdndoor04.sdcc.bnl.gov dcdndoor.sdcc.bnl.gov |
| **Serial Number** | 00a9c5d4f76ec74e1df97290d53e3292 |
| **Valid from** | Mon, 19 Oct 2026 12:53:39 UTC |
| **Valid until** | Thu, 06 May 2027 12:53:39 UTC (expires in 6 months and 10 days) |
| **Key** | RSA 4096 bits (e 65537) |
| **Weak key (Debian)** | No |
| **Issuer** | InCommon RSA IGTF Server CA 4<br>AIA: http://repository.emsign.com/certs/EEEMIncommonIGTFOVG2C.crt |
| **Signature algorithm** | SHA384withRSA |
| **Extended Validation** | No |
| **Certificate Transparency** | **Yes (certificate)** |
| **OCSP Must Staple** | No |
| **Revocation information** | CRL, OCSP<br>CRL: http://crl-c.emsign.com/?EEEMIncommonIGTFOVG2C.crl<br>OCSP: http://ocsp-c.emsign.com |
| **Revocation status** | Good (not revoked) |
| **DNS CAA** | No (more info) |

### Server Key and Certificate #1

| | |
|---|---|
| Trusted | Yes<br>Mozilla Apple Android Java Windows |

### Additional Certificates (if supplied)

| | |
|---|---|
| Certificates provided | 1 (2320 bytes) |
| Chain issues | Incomplete |

### Certification Paths

Click here to expand

## Configuration

### Protocols

| | |
|---|---|
| TLS 1.3 | Yes |
| TLS 1.2 | Yes |
| 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_AES_128_GCM_SHA256 (0x1301) | ECDH x25519 (eq. 3072 bits RSA) FS | 128 |
| TLS_CHACHA20_POLY1305_SHA256 (0x1303) | ECDH x25519 (eq. 3072 bits RSA) FS | 256 |

**# TLS 1.2 (suites in server-preferred order)**

| | | |
|---|---|---|
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) | ECDH secp521r1 (eq. 15360 bits RSA) FS | 256 |
| TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) | ECDH secp521r1 (eq. 15360 bits RSA) FS | 256 |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) | ECDH secp521r1 (eq. 15360 bits RSA) FS | 128 |
| TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) | DH 2048 bits FS | 256 |
| TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa) | DH 2048 bits FS | 256 |
| TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) | DH 2048 bits FS | 128 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | ECDH secp521r1 (eq. 15360 bits RSA) FS **WEAK** | 256 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) | ECDH secp521r1 (eq. 15360 bits RSA) FS **WEAK** | 128 |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) | DH 2048 bits FS **WEAK** | 256 |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) | DH 2048 bits FS **WEAK** | 128 |

### Handshake Simulation

| | | | | |
|---|---|---|---|---|
| Android 4.4.2 | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp521r1 FS |
| Android 5.0.0 | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp521r1 FS |
| Android 6.0 | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Android 7.0 | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 FS |
| Android 8.0 | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 FS |
| 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 |
| BingPreview Jan 2015 | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp521r1 FS |

## Handshake Simulation

| | | | | | |
|---|---|---|---|---|---|
| Chrome 49 / XP SP3 | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 | ECDH secp256r1 | FS |
| Chrome 69 / Win 7 R | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 | FS |
| 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 31.3.0 ESR / Win 7 | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Firefox 47 / Win 7 R | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 | ECDH secp256r1 | FS |
| Firefox 49 / XP SP3 | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Firefox 62 / Win 7 R | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 | FS |
| 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 |
| Googlebot Feb 2018 | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 | FS |
| IE 11 / Win 7 R | RSA 4096 (SHA384) | TLS 1.2 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | DH 2048 | FS |
| IE 11 / Win 8.1 R | RSA 4096 (SHA384) | TLS 1.2 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | DH 2048 | FS |
| IE 11 / Win Phone 8.1 R | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp256r1 | FS |
| IE 11 / Win Phone 8.1 Update R | RSA 4096 (SHA384) | TLS 1.2 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | DH 2048 | FS |
| IE 11 / Win 10 R | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Edge 15 / Win 10 R | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 | FS |
| Edge 16 / Win 10 R | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 | FS |
| Edge 18 / Win 10 R | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 | FS |
| Edge 131 / Win 10 R | - | TLS 1.3 | TLS_AES_256_GCM_SHA384 | ECDH x25519 | FS |
| Edge 13 / Win Phone 10 R | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Java 8u161 | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Java 11.0.3 | - | TLS 1.3 | TLS_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Java 12.0.1 | - | TLS 1.3 | TLS_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| OpenSSL 1.0.1l R | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp521r1 | FS |
| OpenSSL 1.0.2s R | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| OpenSSL 1.1.0k R | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 | FS |
| 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 6 / iOS 6.0.1 | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp256r1 | FS |
| Safari 7 / iOS 7.1 R | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp256r1 | FS |
| Safari 7 / OS X 10.9 R | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp256r1 | FS |
| Safari 8 / iOS 8.4 R | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp256r1 | FS |
| Safari 8 / OS X 10.10 R | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp256r1 | FS |
| Safari 9 / iOS 9 R | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Safari 9 / OS X 10.11 R | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Safari 10 / iOS 10 R | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Safari 10 / OS X 10.12 R | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Safari 12.1.2 / MacOS 10.14.6 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 |
| Apple ATS 9 / iOS 9 R | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Yahoo Slurp Jan 2015 | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp384r1 | FS |
| YandexBot Jan 2015 | RSA 4096 (SHA384) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp521r1 | 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.

## Handshake Simulation

(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** | 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 : `0xc014` |
| **GOLDENDOODLE** | No (more info) TLS 1.2 : `0xc014` |
| **OpenSSL 0-Length** | No (more info) TLS 1.2 : `0xc014` |
| **Sleeping POODLE** | No (more info) TLS 1.2 : `0xc014` |
| **Downgrade attack prevention** | No, TLS_FALLBACK_SCSV not 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** | No |
| **NPN** | No |
| **Session resumption (caching)** | **No (IDs assigned but not accepted)** |
| **Session resumption (tickets)** | Yes |
| **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) |
| **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** | secp256r1, secp384r1, secp521r1, x25519, x448, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 (Server has no preference) |
| **PQC Key Exchange** | Not Supported |
| **Supported PQC Groups** | - |
| **SSL 2 handshake compatibility** | No |
| **0-RTT enabled** | Test failed |

## HTTP Requests

1 **https://dcdndoor04.sdcc.bnl.gov/** (HTTP/1.1 401 login failed)

## Miscellaneous

| | |
|---|---|
| **Test date** | Mon, 26 Oct 2026 08:23:28 UTC |
| **Test duration** | 66.280 seconds |
| **HTTP status code** | 401 |
| **HTTP server signature** | dCache/11.2.7 |
| **Server hostname** | dcdndoor04.sdcc.bnl.gov |

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.