You are here: Home > Projects > SSL Server Test > digitalcollections.lib.utk.edu > 52.35.121.117

SSL Report: digitalcollections.lib.utk.edu (52.35.121.117)

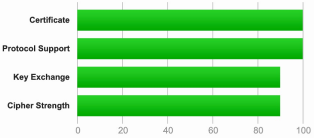
Assessed on: Thu, 01 Aug 2024 18:01:44 UTC | Hide | Clear cache

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 site works only in browsers with SNI support.

This server supports TLS 1.3.

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	digitalcollections.lib.utk.edu Fingerprint SHA256: 7fdd27380009c7b0589daf870b3ea60fc5bfde88409ce4575254ff9ec9f486ae Pin SHA256: gUICnS2V8Me78tlwTYPx+vohA9ZcTpNbOAudP6ZOXbs=
Common names	digitalcollections.lib.utk.edu
Alternative names	digitalcollections.lib.utk.edu
Serial Number	00a332aee52c3b0e77216c5bd04b0d3ea6
Valid from	Wed, 26 Jul 2023 00:00:00 UTC
Valid until	Sun, 25 Aug 2024 23:59:59 UTC (expires in 24 days, 5 hours)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	InCommon RSA Server CA 2 AIA: http://crt.sectigo.com/InCommonRSAServerCA2.crt
Signature algorithm	SHA384withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.sectigo.com/InCommonRSAServerCA2.crl OCSP: http://ocsp.sectigo.com
Revocation status	Good (not revoked) **CRL ERROR: IOException occurred**
DNS CAA	No (more info)
Trusted	**Yes** **Mozilla Apple Android Java Windows**

Additional Certificates (if supplied)

Certificates provided	1 (1775 bytes)
Chain issues	**Incomplete**

Certification Paths

Mozilla Apple Android Java Windows

Path #1: Trusted

1	Sent by server	digitalcollections.lib.utk.edu Fingerprint SHA256: 7fdd27380009c7b0589daf870b3ea60fc5bfde88409ce4575254ff9ec9f486ae Pin SHA256: gUICnS2V8Me78tlwTYPx+vohA9ZcTpNbOAudP6ZOXbs= RSA 2048 bits (e 65537) / SHA384withRSA **CRL ERROR: IOException occurred**
2	Extra download	InCommon RSA Server CA 2 Fingerprint SHA256: 87e01cc4dd0c9d92a3dbd49092ff13f9cd387445cdc57e5b984e1b7721b5b029 Pin SHA256: nIUvrOVzCyKOqY+U4sofEeIMk94Dt/WuMgaesi8NITk= RSA 3072 bits (e 65537) / SHA384withRSA **CRL ERROR: IOException occurred**
3	In trust store	USERTrust RSA Certification Authority Self-signed Fingerprint SHA256: e793c9b02fd8aa13e21c31228accb08119643b749c898964b1746d46c3d4cbd2 Pin SHA256: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4lTdO/nEW/Td4= RSA 4096 bits (e 65537) / SHA384withRSA

Path #2: Trusted

1	Sent by server	digitalcollections.lib.utk.edu Fingerprint SHA256: 7fdd27380009c7b0589daf870b3ea60fc5bfde88409ce4575254ff9ec9f486ae Pin SHA256: gUICnS2V8Me78tlwTYPx+vohA9ZcTpNbOAudP6ZOXbs= RSA 2048 bits (e 65537) / SHA384withRSA **CRL ERROR: IOException occurred**
2	Extra download	InCommon RSA Server CA 2 Fingerprint SHA256: 87e01cc4dd0c9d92a3dbd49092ff13f9cd387445cdc57e5b984e1b7721b5b029 Pin SHA256: nIUvrOVzCyKOqY+U4sofEeIMk94Dt/WuMgaesi8NITk= RSA 3072 bits (e 65537) / SHA384withRSA **CRL ERROR: IOException occurred**
3	Extra download	USERTrust RSA Certification Authority Fingerprint SHA256: 68b9c761219a5b1f0131784474665db61bbdb109e00f05ca9f74244ee5f5f52b Pin SHA256: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4lTdO/nEW/Td4= RSA 4096 bits (e 65537) / SHA384withRSA **CRL ERROR: IOException occurred**
4	In trust store	AAA Certificate Services Self-signed Fingerprint SHA256: d7a7a0fb5d7e2731d771e9484ebcdef71d5f0c3e0a2948782bc83ee0ea699ef4 Pin SHA256: vRU+17BDT2iGsXvOi76E7TQMcTLXAqj0+jGPdW7L1vM= RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

Certificate #2: RSA 2048 bits (SHA256withRSA) **No SNI**

Server Key and Certificate #1

Subject	Kubernetes Ingress Controller Fake Certificate Fingerprint SHA256: 0277a3825cbaa0cdaf7ac5cab8b7782cfb32344a1a6cc2bce6bab1f0788d7d6f Pin SHA256: w7rw77IG/hJ315I0HVJB7WgwB/NVI2XJKG7Zmz7ZauI=
Common names	Kubernetes Ingress Controller Fake Certificate
Alternative names	ingress.local **MISMATCH**
Serial Number	0084b05ca5e0f3867c1f847c391a43111b
Valid from	Sun, 28 Jul 2024 02:19:35 UTC
Valid until	Mon, 28 Jul 2025 02:19:35 UTC (expires in 11 months and 26 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Kubernetes Ingress Controller Fake Certificate Self-signed
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No

Revocation information	None
Trusted	No **NOT TRUSTED** **Mozilla Apple Android Java Windows**

Additional Certificates (if supplied)

Certificates provided	1 (884 bytes)
Chain issues	None

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

(*) Experimental: Server negotiated using No-SNI

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 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)	ECDH x25519 (eq. 3072 bits RSA) FS	256

Handshake Simulation

Android 4.4.2	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	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 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Android 8.0	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	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 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Chrome 69 / Win 7 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	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
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 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 62 / Win 7 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Googlebot Feb 2018	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
IE 11 / Win 7 R	Server sent fatal alert: handshake_failure			

IE 11 / Win 8.1 R	Server sent fatal alert: handshake_failure			
IE 11 / Win Phone 8.1 R	Server sent fatal alert: handshake_failure			
IE 11 / Win Phone 8.1 Update R	Server sent fatal alert: handshake_failure			
IE 11 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Edge 15 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Edge 16 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Edge 18 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Java 8u161	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	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 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
OpenSSL 1.0.2s R	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
OpenSSL 1.1.0k R	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Safari 6 / iOS 6.0.1	Server sent fatal alert: handshake_failure			
Safari 7 / iOS 7.1 R	Server sent fatal alert: handshake_failure			
Safari 7 / OS X 10.9 R	Server sent fatal alert: handshake_failure			
Safari 8 / iOS 8.4 R	Server sent fatal alert: handshake_failure			
Safari 8 / OS X 10.10 R	Server sent fatal alert: handshake_failure			
Safari 9 / iOS 9 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	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 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
YandexBot Jan 2015	RSA 2048 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_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

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)
GOLDENDOODLE	No (more info)
OpenSSL 0-Length	No (more info)
Sleeping POODLE	No (more info)
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 h2 http/1.1
NPN	No
Session resumption (caching)	**No (IDs assigned but not accepted)**
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	**Yes** max-age=15724800; includeSubDomains
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, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No
Supported Named Groups	x25519, secp256r1, x448, secp521r1, secp384r1 (server preferred order)
SSL 2 handshake compatibility	No
0-RTT enabled	No

HTTP Requests

1 **https://digitalcollections.lib.utk.edu/** (HTTP/1.1 401 Unauthorized)

Miscellaneous

Test date	Thu, 01 Aug 2024 17:59:40 UTC
Test duration	40.721 seconds
HTTP status code	401
HTTP server signature	-
Server hostname	ec2-52-35-121-117.us-west-2.compute.amazonaws.com

SSL Report v2.3.0

Copyright © 2009-2024 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.