SSL Report: netfiles.de (213.95.202.206)

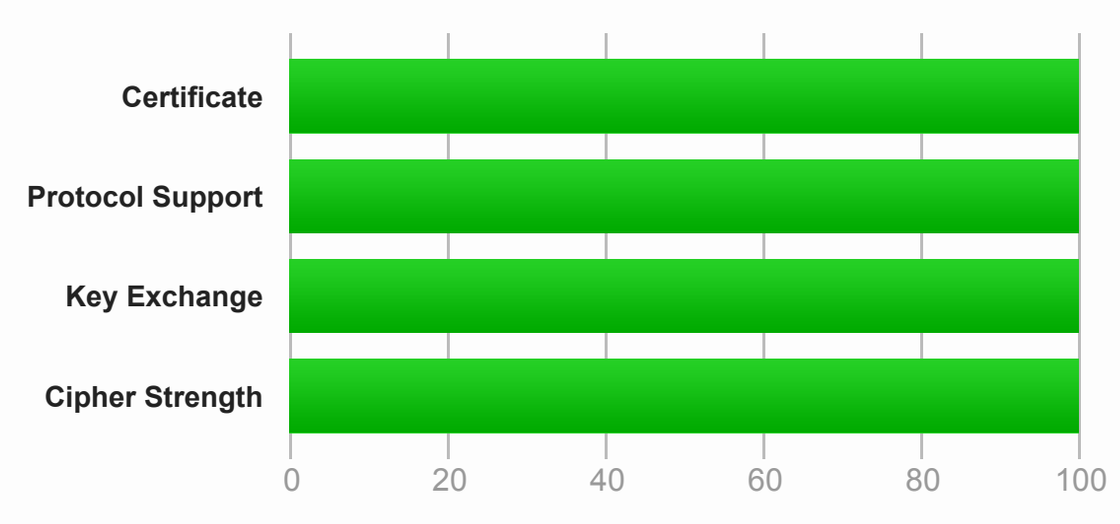
Assessed on: Wed, 04 Dec 2024 10:27:42 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A+



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

This server supports TLS 1.3.

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

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

Certificate #1: RSA 4096 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	netfiles.de Fingerprint SHA256: 4253df9819258ead4c0786f31af99de9cd2e7688413660d460664740216e9741 Pin SHA256: mTgNqC6IYffwpKxWh1j6836Y+uuVIG+OBB9XehMfADs=
Common names	netfiles.de
Alternative names	netfiles.de www.netfiles.de app.netfiles.de sftp.netfiles.de webdav.netfiles.de analytics.netfiles.de help.netfiles.de netfiles.com www.netfiles.com analytics.netfiles.com help.netfiles.com auth.netfiles.de web.netfiles.de
Serial Number	34feedb5b6f20000de5bec4d48ff7a18
Valid from	Mon, 22 Jul 2024 10:36:52 UTC
Valid until	Sat, 26 Jul 2025 23:59:59 UTC (expires in 7 months and 22 days)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	Telekom Security ServerID EV Class 3 CA AIA: http://crt.serverid.telesec.de/crt/Telekom_Security_ServerID_EV_Class_3_CA.crt
Signature algorithm	SHA256withRSA
Extended Validation	Yes
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.serverid.telesec.de/rl/Telekom_Security_ServerID_EV_Class_3_CA.crl OCSP: http://ocsp.serverid.telesec.de/ocspr
Revocation status	Good (not revoked)
DNS CAA	Yes policy host: netfiles.de issuewild: godaddy.com flags:128 issuewild: telesec.de flags:128 issuewild: letsencrypt.org flags:128
Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	3 (5093 bytes)
Chain issues	Contains anchor

#2

Subject	Telekom Security ServerID EV Class 3 CA Fingerprint SHA256: 5092ce0e3f70f2fd9561c34623b546f7d333ef1b633c147d1290e28de986a230 Pin SHA256: sLVgLe1nM8JMIbUmVZO+i7BiMeC6eHi+ezBmAduziBM=
Valid until	Mon, 02 Aug 2027 23:59:59 UTC (expires in 2 years and 7 months)
Key	RSA 3072 bits (e 65537)
Issuer	T-TeleSec GlobalRoot Class 3
Signature algorithm	SHA256withRSA

#3

Subject	T-TeleSec GlobalRoot Class 3 In trust store Fingerprint SHA256: fd73dad31c644ff1b43bef0ccdda96710b9cd9875eca7e31707af3e96d522bbd Pin SHA256: jXZ3ZLPL2giSnQcqIqVh9NzdG8V9PL3cIlxH0rR/kSI=
Valid until	Sat, 01 Oct 2033 23:59:59 UTC (expires in 8 years and 9 months)
Key	RSA 2048 bits (e 65537)
Issuer	T-TeleSec GlobalRoot Class 3 Self-signed
Signature algorithm	SHA256withRSA

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 (we could not determine if the server has a preference)

TLS_AES_256_GCM_SHA384 (0x1302) ECDH secp384r1 (eq. 7680 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH secp384r1 (eq. 7680 bits RSA) FS	256

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp521r1 (eq. 15360 bits RSA) FS	256

Handshake Simulation

Android 4.4.2	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS
Android 5.0.0	Server sent fatal alert: handshake_failure		
Android 6.0	Server sent fatal alert: handshake_failure		
Android 7.0	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp384r1 FS
Android 8.0	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp384r1 FS
Android 8.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp384r1 FS
Android 9.0	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp384r1 FS
BingPreview Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS
Chrome 49 / XP SP3	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp384r1 FS
Chrome 69 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp384r1 FS
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp384r1 FS
Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp384r1 FS
Firefox 31.3.0 ESR / Win 7	Server sent fatal alert: handshake_failure		
Firefox 47 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp521r1 FS
Firefox 49 / XP SP3	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp521r1 FS
Firefox 62 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp521r1 FS
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp384r1 FS
Googlebot Feb 2018	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp384r1 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 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Edge 15 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Edge 16 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Edge 18 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Edge 13 / Win Phone 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Java 8u161	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS
Java 11.0.3	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp384r1 FS
Java 12.0.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp384r1 FS
OpenSSL 1.0.1l R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS
OpenSSL 1.0.2s R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS
OpenSSL 1.1.0k R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp521r1 FS
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp521r1 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 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS
Safari 9 / OS X 10.11 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS
Safari 10 / iOS 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS
Safari 10 / OS X 10.12 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp384r1 FS
Safari 12.1.1 / iOS 12.3.1 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp384r1 FS
Apple ATS 9 / iOS 9 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS
Yahoo Slurp Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
YandexBot Jan 2015	RSA 4096 (SHA256)	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.
(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)	Yes
Session resumption (tickets)	Yes
OCSP stapling	Yes
Strict Transport Security (HSTS)	Yes max-age=63072000; includeSubDomains; preload
HSTS Preloading	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	secp521r1, secp384r1 (server preferred order)
SSL 2 handshake compatibility	No
0-RTT enabled	No

HTTP Requests

1 https://netfiles.de/ (HTTP/1.1 301 Moved Permanently)

Miscellaneous

Test date	Wed, 04 Dec 2024 10:26:30 UTC
Test duration	72.408 seconds
HTTP status code	301
HTTP forwarding	https://www.netfiles.de
HTTP server signature	Apache
Server hostname	-

SSL Report v2.3.0