

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > netfiles.de

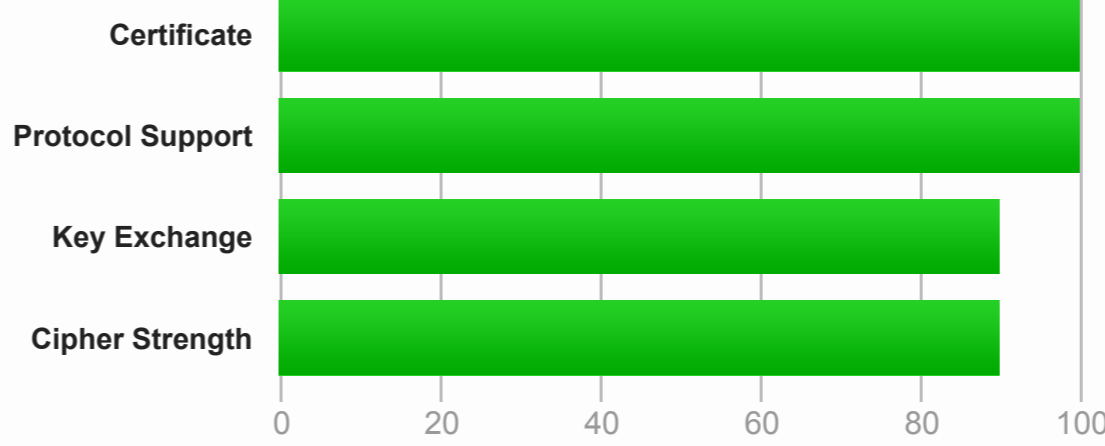
SSL Report: netfiles.de (213.95.202.206)

Assessed on: Mon, 01 Jul 2024 07:30:32 UTC | [Hide](#) | [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**.

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: 4d8eeaf5207ba330034991982058e10598b61e12b732f05c265a39b5942562 Pin SHA256: 95MBf7zqH42Ghm9GFI0z27u7UOPfB3vXk494+
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
Serial Number	23738975a13777bec74f501685e85b5
Valid from	Wed, 02 Aug 2023 08:36:13 UTC
Valid until	Thu, 01 Aug 2024 23:59:59 UTC (expires in 1 month)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	Telekom Security ServerID EV Class 3 CA AUA: http://rol.servid.telesec.de/rol/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://rol.servid.telesec.de/rol/Telekom_Security_ServerID_EV_Class_3_CA.crl OCSP: http://ocsp.servid.telesec.de/ocsp
Revocation status	Good (not revoked)
DNS CAA	Yes policy host: netfiles.de issuewild: letsencrypt.org flags:128 issuewild: godaddy.com flags:128 issuewild: telesec.de flags:128
Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)											
Certificates provided	4 (7498 bytes)										
Chain issues	Incorrect order, Extra certs, Contains anchor										
#2	<table border="1"> <tr> <td>Subject</td> <td>netfiles.de Fingerprint SHA256: 4d8eeaf5207ba330034991982058e10598b61e12b732f05c265a39b5942562 Pin SHA256: 95MBf7zqH42Ghm9GFI0z27u7UOPfB3vXk494+</td> </tr> <tr> <td>Valid until</td> <td>Thu, 01 Aug 2024 23:59:59 UTC (expires in 1 month)</td> </tr> <tr> <td>Key</td> <td>RSA 4096 bits (e 65537)</td> </tr> <tr> <td>Issuer</td> <td>Telekom Security ServerID EV Class 3 CA</td> </tr> <tr> <td>Signature algorithm</td> <td>SHA256withRSA</td> </tr> </table>	Subject	netfiles.de Fingerprint SHA256: 4d8eeaf5207ba330034991982058e10598b61e12b732f05c265a39b5942562 Pin SHA256: 95MBf7zqH42Ghm9GFI0z27u7UOPfB3vXk494+	Valid until	Thu, 01 Aug 2024 23:59:59 UTC (expires in 1 month)	Key	RSA 4096 bits (e 65537)	Issuer	Telekom Security ServerID EV Class 3 CA	Signature algorithm	SHA256withRSA
Subject	netfiles.de Fingerprint SHA256: 4d8eeaf5207ba330034991982058e10598b61e12b732f05c265a39b5942562 Pin SHA256: 95MBf7zqH42Ghm9GFI0z27u7UOPfB3vXk494+										
Valid until	Thu, 01 Aug 2024 23:59:59 UTC (expires in 1 month)										
Key	RSA 4096 bits (e 65537)										
Issuer	Telekom Security ServerID EV Class 3 CA										
Signature algorithm	SHA256withRSA										
#3	<table border="1"> <tr> <td>Subject</td> <td>Telekom Security ServerID EV Class 3 CA Fingerprint SHA256: 5052ce0c3f7026169561c3462365467f3331f18633c14741290e28e986a230 Pin SHA256: sLVjLr1nMLJMBUwVZ0H78BMAC6eH+e2BmAdjzB8M+</td> </tr> <tr> <td>Valid until</td> <td>Mon, 02 Aug 2027 23:59:59 UTC (expires in 3 years and 1 month)</td> </tr> <tr> <td>Key</td> <td>RSA 3072 bits (e 65537)</td> </tr> <tr> <td>Issuer</td> <td>T-TeleSec GlobalRoot Class 3</td> </tr> <tr> <td>Signature algorithm</td> <td>SHA256withRSA</td> </tr> </table>	Subject	Telekom Security ServerID EV Class 3 CA Fingerprint SHA256: 5052ce0c3f7026169561c3462365467f3331f18633c14741290e28e986a230 Pin SHA256: sLVjLr1nMLJMBUwVZ0H78BMAC6eH+e2BmAdjzB8M+	Valid until	Mon, 02 Aug 2027 23:59:59 UTC (expires in 3 years and 1 month)	Key	RSA 3072 bits (e 65537)	Issuer	T-TeleSec GlobalRoot Class 3	Signature algorithm	SHA256withRSA
Subject	Telekom Security ServerID EV Class 3 CA Fingerprint SHA256: 5052ce0c3f7026169561c3462365467f3331f18633c14741290e28e986a230 Pin SHA256: sLVjLr1nMLJMBUwVZ0H78BMAC6eH+e2BmAdjzB8M+										
Valid until	Mon, 02 Aug 2027 23:59:59 UTC (expires in 3 years and 1 month)										
Key	RSA 3072 bits (e 65537)										
Issuer	T-TeleSec GlobalRoot Class 3										
Signature algorithm	SHA256withRSA										
#4	<table border="1"> <tr> <td>Subject</td> <td>T-TeleSec GlobalRoot Class 3 In trust store Fingerprint SHA256: 1673dad31c6441b43b6f6cc0a9671060c9875eca7e31707a9e96522bbf Pin SHA256: jXZ3LzPLgShq2c9qVhRn2zGRVfPL3dvdhRk3S+</td> </tr> <tr> <td>Valid until</td> <td>Sat, 01 Oct 2033 23:59:59 UTC (expires in 9 years and 3 months)</td> </tr> <tr> <td>Key</td> <td>RSA 2048 bits (e 65537)</td> </tr> <tr> <td>Issuer</td> <td>T-TeleSec GlobalRoot Class 3 Self-signed</td> </tr> <tr> <td>Signature algorithm</td> <td>SHA256withRSA</td> </tr> </table>	Subject	T-TeleSec GlobalRoot Class 3 In trust store Fingerprint SHA256: 1673dad31c6441b43b6f6cc0a9671060c9875eca7e31707a9e96522bbf Pin SHA256: jXZ3LzPLgShq2c9qVhRn2zGRVfPL3dvdhRk3S+	Valid until	Sat, 01 Oct 2033 23:59:59 UTC (expires in 9 years and 3 months)	Key	RSA 2048 bits (e 65537)	Issuer	T-TeleSec GlobalRoot Class 3 Self-signed	Signature algorithm	SHA256withRSA
Subject	T-TeleSec GlobalRoot Class 3 In trust store Fingerprint SHA256: 1673dad31c6441b43b6f6cc0a9671060c9875eca7e31707a9e96522bbf Pin SHA256: jXZ3LzPLgShq2c9qVhRn2zGRVfPL3dvdhRk3S+										
Valid until	Sat, 01 Oct 2033 23:59:59 UTC (expires in 9 years and 3 months)										
Key	RSA 2048 bits (e 65537)										
Issuer	T-TeleSec GlobalRoot Class 3 Self-signed										
Signature algorithm	SHA256withRSA										

[Click here to expand](#)

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

[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_CHACHA20_POLY1305_SHA256 (0xc0a8)	ECDH x25519 (eq. 3072 bits RSA) FS 256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH x25519 (eq. 3072 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 secp256r1 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 x25519 FS
Android 8.0	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_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
Bit9 Preview Jan 2015	RSA 4096 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS
Chrome 69 / Win 7 R	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_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	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 secp256r1 FS
Firefox 49 / XP SP3	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS
Firefox 62 / Win 7 R	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Firefox 73 / Win 10 R	- TLS 1.3 TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Googlebot Feb 2018	RSA 4096 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_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 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Edge 16 / Win 10 R	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Edge 18 / Win 10 R	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Edge 19 / Win 10 R	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Java 8u161	RSA 4096 (SHA256) 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 1.0.11 R	RSA 4096 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
OpenSSL 1.0.2a R	RSA 4096 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
OpenSSL 1.0.0a R	RSA 4096 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
OpenSSL 1.1.1g 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 / iOS X 10.9 R	Server sent fatal alert: handshake_failure
Safari 8 / iOS 8.4 R	Server sent fatal alert: handshake_failure
Safari 8 / iOS 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 secp256r1 FS
Safari 9 / iOS X 10.11 R	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 10 / iOS X 10.12 R	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 12.1.2 / Mac OS 10.14.6	- TLS 1.3 TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Beja 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 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 4096 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
YandexBot Jan 2015	RSA 4096 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 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 rely with a lower protocol version.
 (R) Denotes a reference browser or client, with which we expect better effective security.
 (A) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).
 (A!) 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)
Ticklebleed (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)
ROBUST Security	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
OCSP Transport Security (HSTS)	Yes max-age=6307200; includeSubDomains; preload
HSTS Preloading	Chrome Edge Firefox IE (more info)
Public Key Pinning (HPKP)	No
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://netfiles.de/ (HTTP/1.1 301 Moved Permanently)

Miscellaneous	
Test date	Mon, 01 Jul 2024 07:29:13 UTC
Test duration	79.781 seconds
HTTP status code	301
HTTP forwarding	https://www.netfiles.de
HTTP server signature	Apache
Server hostname	-