

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

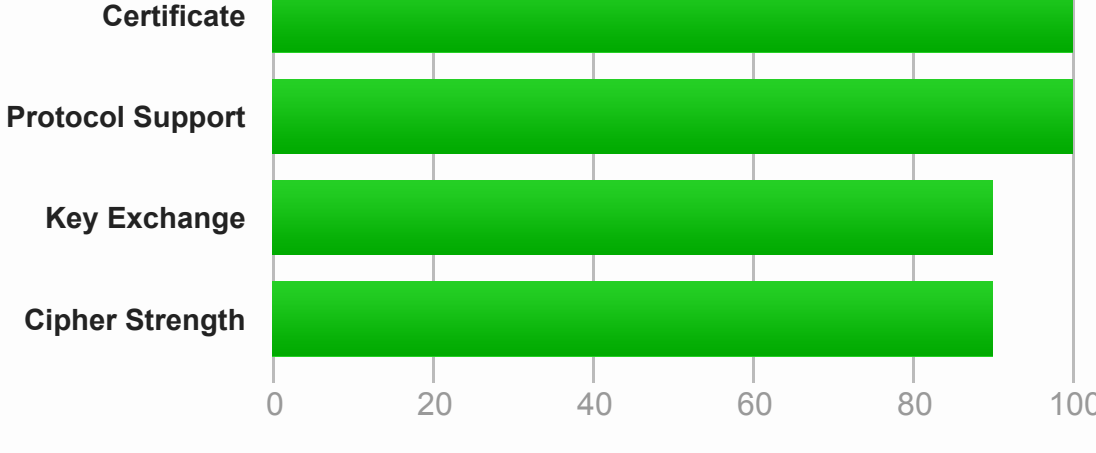
## SSL Report: netfiles.de (213.95.202.206)

Assessed on: Tue, 02 Apr 2024 06:18:15 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 >](#)

### Certificate #1: RSA 4096 bits (SHA256withRSA)

Server Key and Certificate #1	
<b>Subject</b>	netfiles.de Fingerprint SHA256: 14d8aa5207bad33093499196266d1f5986b1e12b73205c2f6a3965942562 Pn SHA256: 93MB7zVjH2GhmUa9Pfd02Tq7UOPh8p3vX4d4q+
<b>Common names</b>	netfiles.de
<b>Alternative names</b>	netfiles.de www.netfiles.de app.netfiles.de stp.netfiles.de webdav.netfiles.de analytics.netfiles.de help.netfiles.de netfiles.com www.netfiles.com analytics.netfiles.com help.netfiles.com
<b>Serial Number</b>	23738975a13777bec74f501685e65f65
<b>Valid from</b>	Wed, 02 Aug 2023 08:36:13 UTC
<b>Valid until</b>	Thu, 01 Aug 2024 23:59:59 UTC (expires in 3 months and 30 days)
<b>Key</b>	RSA 4096 bits (e 65537)
<b>Weak key (Debian)</b>	No
<b>Issuer</b>	Telekom Security ServerID EV Class 3 CA AIA: http://crl.serverid.telesec.de/crl/Telekom_Security_ServerID_EV_Class_3_CA.crl
<b>Signature algorithm</b>	SHA256withRSA
<b>Extended Validation</b>	Yes
<b>Certificate Transparency</b>	Yes (certificate)
<b>OCSF Must Staple</b>	No
<b>Revocation information</b>	CRL: http://crl.serverid.telesec.de/crl/Telekom_Security_ServerID_EV_Class_3_CA.crl OCSF: http://ocsp.serverid.telesec.de/ocsp
<b>Revocation status</b>	Good (not revoked)
<b>DNS CAA</b>	No (more info)
<b>Trusted</b>	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)	
<b>Certificates provided</b>	4 (7498 bytes)
<b>Chain issues</b>	Incorrect order, Extra certs, Contains anchor
<b>#2</b>	netfiles.de Fingerprint SHA256: 14d8aa5207bad33093499196266d1f5986b1e12b73205c2f6a3965942562 Pn SHA256: 93MB7zVjH2GhmUa9Pfd02Tq7UOPh8p3vX4d4q+
<b>Valid until</b>	Thu, 01 Aug 2024 23:59:59 UTC (expires in 3 months and 30 days)
<b>Key</b>	RSA 4096 bits (e 65537)
<b>Issuer</b>	Telekom Security ServerID EV Class 3 CA
<b>Signature algorithm</b>	SHA256withRSA
<b>#3</b>	Telekom Security ServerID EV Class 3 CA Fingerprint SHA256: 5092cab63702549561c34623b546f7c333a110633c14711290a2b96986a230 Pn SHA256: sLVg_e1nMBJmUuVZ047BMMc6EhI+ezBvAduzBM+
<b>Valid until</b>	Mon, 02 Aug 2027 23:59:59 UTC (expires in 3 years and 4 months)
<b>Key</b>	RSA 3072 bits (e 65537)
<b>Issuer</b>	T-TeleSec GlobalRoot Class 3
<b>Signature algorithm</b>	SHA256withRSA
<b>#4</b>	T-TeleSec GlobalRoot Class 3 In trust store Fingerprint SHA256: 1073dad31e644f16430efcc0d9e97106f9c9875ca7a31707a703e966d522bd Pn SHA256: jKZ3ZLPL2g5nQzqHv1Nn9z8V9PL3ctkHwRk3s9
<b>Valid until</b>	Sat, 01 Oct 2033 23:59:59 UTC (expires in 9 years and 5 months)
<b>Key</b>	RSA 2048 bits (e 65537)
<b>Issuer</b>	T-TeleSec GlobalRoot Class 3 Self-signed
<b>Signature algorithm</b>	SHA256withRSA

**Certification Paths** [+](#)

[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	
<b># TLS 1.3 (suites in server-preferred order)</b>	<a href="#">+</a>
TLS_AES_256_GCM_SHA384 (0xc1302) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0xc1303) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_AES_128_GCM_SHA256 (0xc1301) ECDH x25519 (eq. 3072 bits RSA) FS	128
<b># TLS 1.2 (suites in server-preferred order)</b>	<a href="#">+</a>
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	
<a href="#">Android 4.4.2</a>	RSA 4096 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">Android 5.0.0</a>	Server sent fatal alert: handshake_failure
<a href="#">Android 6.0</a>	Server sent fatal alert: handshake_failure
<a href="#">Android 7.0</a>	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS
<a href="#">Android 8.0</a>	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS
<a href="#">Android 8.1</a>	- TLS 1.3 TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">Android 9.0</a>	- TLS 1.3 TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">BingPreview Jan 2015</a>	RSA 4096 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">Chrome 49 / XP SP3</a>	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS
<a href="#">Chrome 69 / Win 7 R</a>	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS
<a href="#">Chrome 70 / Win 10</a>	- TLS 1.3 TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">Chrome 80 / Win 10 R</a>	- TLS 1.3 TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">Firefox 31.3.0 ESR / Win 7</a>	Server sent fatal alert: handshake_failure
<a href="#">Firefox 47 / Win 7 R</a>	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS
<a href="#">Firefox 49 / XP SP3</a>	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS
<a href="#">Firefox 62 / Win 7 R</a>	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS
<a href="#">Firefox 73 / Win 10 R</a>	- TLS 1.3 TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">Googlebot Feb 2018</a>	RSA 4096 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS
<a href="#">IE 11 / Win 8.1 R</a>	Server sent fatal alert: handshake_failure
<a href="#">IE 11 / Win Phone 8.1 R</a>	Server sent fatal alert: handshake_failure
<a href="#">IE 11 / Win Phone 8.1 Update R</a>	Server sent fatal alert: handshake_failure
<a href="#">IE 11 / Win 10 R</a>	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">Edge 15 / Win 10 R</a>	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">Edge 18 / Win 10 R</a>	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">Edge 19 / Win 10 R</a>	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">Edge 13 / Win Phone 10 R</a>	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">Java 8u161</a>	RSA 4096 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">Java 11.0.3</a>	- TLS 1.3 TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">Java 12.0.1</a>	- TLS 1.3 TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">OpenSSL 1.0.1j R</a>	RSA 4096 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">OpenSSL 1.0.2a R</a>	RSA 4096 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">OpenSSL 1.0.0h R</a>	RSA 4096 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS
<a href="#">OpenSSL 1.1.1c R</a>	- TLS 1.3 TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">Safari 6 / OS 6.0.1</a>	Server sent fatal alert: handshake_failure
<a href="#">Safari 7 / OS 7.1 R</a>	Server sent fatal alert: handshake_failure
<a href="#">Safari 7 / OS X 10.8 R</a>	Server sent fatal alert: handshake_failure
<a href="#">Safari 8 / OS 8.4 R</a>	Server sent fatal alert: handshake_failure
<a href="#">Safari 8 / OS X 10.10 R</a>	Server sent fatal alert: handshake_failure
<a href="#">Safari 9 / OS 9 R</a>	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">Safari 10 / OS X 10.11 R</a>	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">Safari 10 / OS 10 R</a>	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">Safari 10 / OS X 10.12 R</a>	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">Safari 12.1.2 / MacOS 10.14.6 Beta R</a>	- TLS 1.3 TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">Safari 12.1.1 / OS 12.3.1 R</a>	- TLS 1.3 TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">Apple ATS 9 / OS 9 R</a>	RSA 4096 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">Yahoo Slurp Jan 2015</a>	RSA 4096 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<a href="#">YandexBot Jan 2015</a>	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 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	
<b>Secure Renegotiation</b>	Supported
Securo 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)
<b>Downgrade attack prevention</b>	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)
<b>Forward Secrecy</b>	Yes (with most browsers) ROBUST (more info)
ALPN	Yes h2 http/1.1
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
<b>OCSF stapling</b>	Yes
<b>Strict Transport Security (HSTS)</b>	Yes max-age=63072000; includeSubDomains; preload
<b>HSTS Preloading</b>	Chrome Edge Firefox IE (more info)
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	
<a href="#">1</a> <a href="https://netfiles.de/">https://netfiles.de/</a> (HTTP/1.1 301 Moved Permanently)	

Miscellaneous	
<b>Test date</b>	Tue, 02 Apr 2024 06:16:59 UTC
<b>Test duration</b>	76.409 seconds
<b>HTTP status code</b>	301
<b>HTTP forwarding</b>	https://www.netfiles.de
<b>HTTP server signature</b>	Apache
<b>Server hostname</b>	-