

# SSL Server Security Test of mail.networksec.de

Test SSL/TLS implementation of any service on any port for compliance with PCI DSS requirements, HIPAA guidance and NIST guidelines.

MAIL.NETWORKSEC.DE

FINAL GRADE

**DATE OF TEST**

January 28th 2017  
15:43 CET



**SERVER IP**  
144.76.73.70:995



COMPLIANCE WITH



**PCI DSS**  
Requirements

## Assessment Executive Summary

The tested service does not seem to be an HTTPS service.

Information

The server configuration seems to be good, but is not entirely compliant with NIST guidelines and HIPAA guidance.

Information

# SSL Certificate Overview

## RSA CERTIFICATE INFORMATION

Trusted	Yes
Common Name	networksec.de
Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
Subject Alternative Names	DNS:isp.nwsec.de, DNS:mail.networksec.de, DNS:networksec.de
Transparency	No
Extended Validation	No
CRL	No
OCSP	http://ocsp.int-x3.letsencrypt.org/
OCSP Must-Staple	No
Supports OCSP Stapling	No
Valid From	January 22nd 2017, 04:16 CET
Valid To	April 22nd 2017, 05:16 CEST

## CERTIFICATE CHAIN

### networksec.de

Server certificate

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
SHA256	7b9e57c747aa68464fb4fa52896f02c34b26bc1dbdc4b05cbabe1a2941004d03
PIN	ddAoHcAMuEI5m6dDVEydIlk2Ytx9+SOLav/ypmTStqw=
Expires in	84 days

### Let's Encrypt Authority X3

Intermediate CA

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
SHA256	de6da669c1368f77b7e9d695474ed9aa592423603bbbe6a546b8bd3c90c2f2fb
PIN	YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg=
Expires in	1,509 days

### DST Root CA X3

Self-signed Root CA

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha1WithRSAEncryption
SHA256	42444fdb056ee97612747572e390e7027719cf6a4441cd54fc2999265af24f71
PIN	Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys=
Expires in	1,706 days

# Test For Compliance With PCI DSS Requirements

Reference: PCI DSS 3.1 - Requirements 2.3 and 4.1

## CERTIFICATES ARE TRUSTED

All the certificates provided by the server are trusted.

Good configuration

## SUPPORTED CIPHERS

List of all cipher suites supported by the server:

### TLSV1.2

TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration

### TLSV1.1

TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration

### TLSV1.0

TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration

## SUPPORTED PROTOCOLS

List of all SSL/TLS protocols supported by the server:

TLSv1.0	Deprecated. Dropped in June 2018
TLSv1.1	Good configuration
TLSv1.2	Good configuration

## DIFFIE-HELLMAN PARAMETER SIZE

Diffie-Hellman parameter size: 2048 bits

Good configuration

## SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-384 (secp384r1) (384 bits)

Good configuration

### POODLE OVER TLS

The server is not vulnerable to POODLE over TLS.

Not vulnerable

### CVE-2016-2107

The server is not vulnerable to OpenSSL padding-oracle flaw (CVE-2016-2107).

Not vulnerable

### SERVER DOES NOT SUPPORT CLIENT-INITIATED INSECURE RENEGOTIATION

The server does not support client-initiated insecure renegotiation.

Good configuration

### HEARTBLEED

The server version of OpenSSL is not vulnerable to Heartbleed attack.

Not vulnerable

### CVE-2014-0224

The server is not vulnerable to CVE-2014-0224 (OpenSSL CCS flaw).

Not vulnerable

# Test For Compliance With HIPAA

Reference: HIPAA of 1996, Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.

## X509 CERTIFICATES ARE IN VERSION 3

All the X509 certificates provided by the server are in version 3.

Good configuration

## SERVER DOES NOT SUPPORT OCSP STAPLING

The server does not support OCSP stapling for its RSA certificate. Its support allows better verification of the certificate validation status.

Non-compliant with HIPAA guidance

## SUPPORTED PROTOCOLS

List of all SSL/TLS protocols supported by the server:

TLSv1.0

Good configuration

TLSv1.1

Good configuration

TLSv1.2

Good configuration

## SUPPORTED CIPHERS

List of all cipher suites supported by the server:

### TLSV1.2

TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

Good configuration

TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA

Good configuration

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

Good configuration

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA

Good configuration

TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256

Good configuration

TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256

Good configuration

TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

Good configuration

TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

Good configuration

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256

Good configuration

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384

Good configuration

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

Good configuration

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

Good configuration

### TLSV1.1

TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

Good configuration

TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA

Good configuration

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

Good configuration

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA

Good configuration

### TLSV1.0

TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

Good configuration

TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA

Good configuration

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

Good configuration

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA

Good configuration

## DIFFIE-HELLMAN PARAMETER SIZE

Diffie-Hellman parameter size: 2048 bits

Good configuration

## SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-384 [secp384r1] (384 bits)

Good configuration

## TLSV1.1 SUPPORTED

The server supports TLSv1.1 which is mandatory to comply with HIPAA guidance.

Good configuration

## TLSV1.2 SUPPORTED

The server supports TLSv1.2 which is the only SSL/TLS protocol that currently has no known flaws or exploitable weaknesses.

Good configuration

## MISSING MANDATORY CIPHERS

The support of these ciphers is mandatory according to HIPAA guidance:

### TLSV1.2

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

Non-compliant with HIPAA guidance

TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256

Non-compliant with HIPAA guidance

### TLSV1.1

TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

Non-compliant with HIPAA guidance

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

Non-compliant with HIPAA guidance

### TLSV1.0

TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

Non-compliant with HIPAA guidance

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

Non-compliant with HIPAA guidance

## EC\_POINT\_FORMAT EXTENSION

The server supports the EC\_POINT\_FORMAT TLS extension.

Good configuration

# Test For Compliance With NIST Guidelines

Reference: NIST Special Publication 800-52 Revision 1 - Section 3

## X509 CERTIFICATES ARE IN VERSION 3

All the X509 certificates provided by the server are in version 3.

Good configuration

## SERVER DOES NOT SUPPORT OCSP STAPLING

The server does not support OCSP stapling for its RSA certificate. Its support allows better verification of the certificate validation status.

Non-compliant with NIST guidelines

## SUPPORTED CIPHERS

List of all cipher suites supported by the server:

### TLSV1.2

TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration

### TLSV1.1

TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration

### TLSV1.0

TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration

## SUPPORTED PROTOCOLS

List of all SSL/TLS protocols supported by the server:

TLSv1.0	Good configuration
TLSv1.1	Good configuration
TLSv1.2	Good configuration

## DIFFIE-HELLMAN PARAMETER SIZE

Diffie-Hellman parameter size: 2048 bits

Good configuration

## SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-384 [secp384r1] [384 bits]

Good configuration

## TLSV1.1 SUPPORTED

The server supports TLSv1.1 which is mandatory to comply with NIST guidelines.

Good configuration

## TLSV1.2 SUPPORTED

The server supports TLSv1.2 which is the only SSL/TLS protocol that currently has no known flaws or exploitable weaknesses.

Good configuration

## MISSING MANDATORY CIPHERS

The support of these ciphers is mandatory according to NIST guidelines:

### TLSV1.2

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

Non-compliant with NIST guidelines

TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256

Non-compliant with NIST guidelines

### TLSV1.1

TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

Non-compliant with NIST guidelines

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

Non-compliant with NIST guidelines

### TLSV1.0

TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

Non-compliant with NIST guidelines

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

Non-compliant with NIST guidelines

## EC\_POINT\_FORMAT EXTENSION

The server supports the EC\_POINT\_FORMAT TLS extension.

Good configuration



# Test For Industry Best-Practices

## CERTIFICATES DO NOT PROVIDE EV

The RSA certificate provided is NOT an Extended Validation (EV) certificate.

Information

## SERVER DOES NOT HAVE CIPHER PREFERENCE

The server does not prefer cipher suites. We advise to enable this feature in order to enforce usage of the best cipher suites selected.

Misconfiguration or weakness

## TLS\_FALLBACK\_SCSV

The server supports TLS\_FALLBACK\_SCSV extension for protocol downgrade attack prevention.

Good configuration

## SERVER SUPPORTS CLIENT-INITIATED SECURE RENEGOTIATION

The server supports a client-initiated secure renegotiation that may be unsafe and allow Denial of Service attacks.

Misconfiguration or weakness

## SERVER-INITIATED SECURE RENEGOTIATION

The server supports secure server-initiated renegotiation.

Good configuration

## SERVER DOES NOT SUPPORT TLS COMPRESSION

TLS compression is not supported by the server.

Good configuration