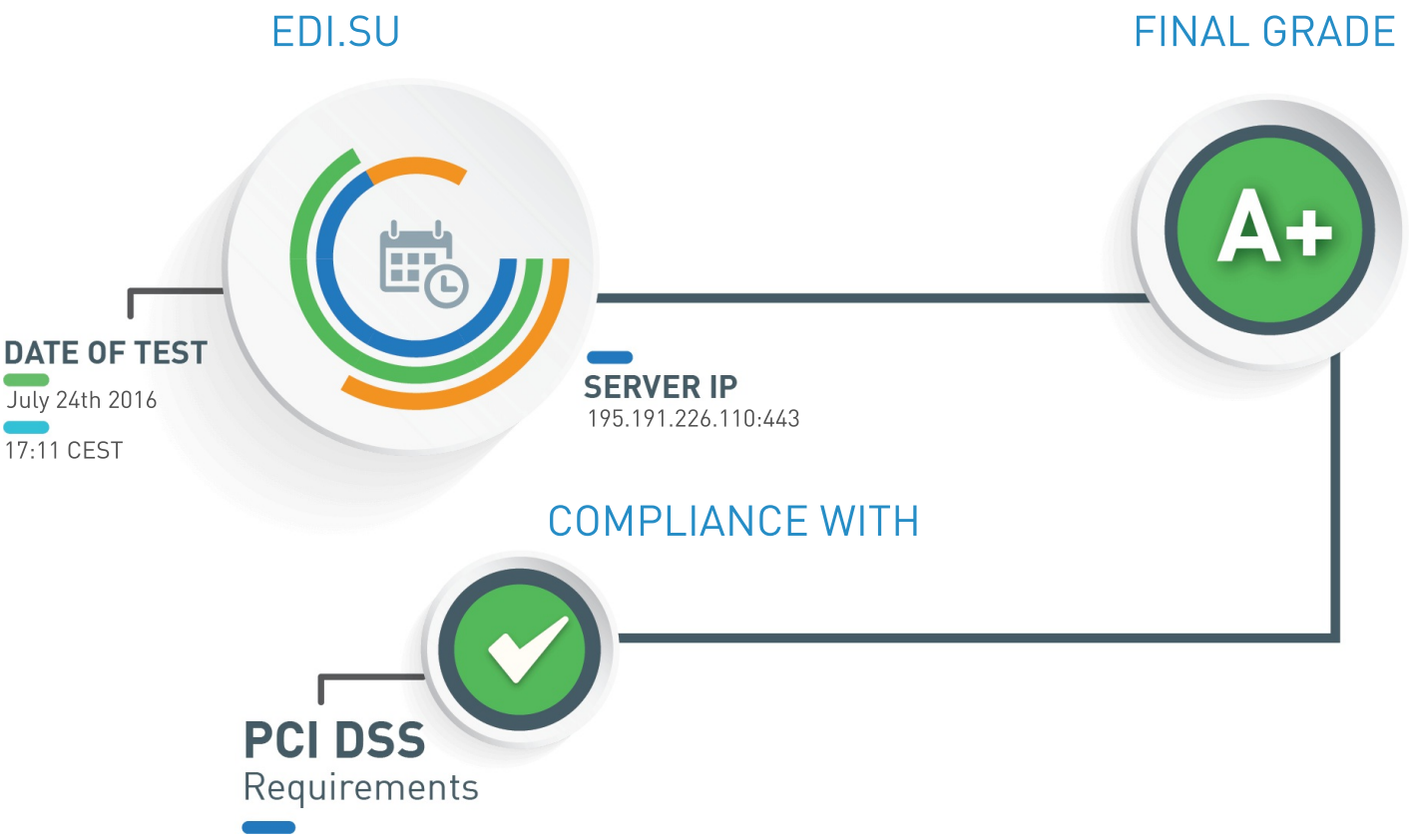
SSL/TLS Security Assessment of e-vo.ru

Test SSL/TLS implementation of any service on any port for compliance with industry best-practices, NIST guidelines and PCI DSS requirements.



Assessment Executive Summary

The server configuration seems to be good, but is not entirely compliant with NIST guidelines — Information

The server prefers cipher suites supporting Perfect-Forward-Secrecy — Good configuration

SSL Certificate Overview

RSA CERTIFICATE INFORMATION

Trusted	Yes
Common Name	***.e-vo.ru**
Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
Subject Alternative Names	DNS:*.edi.su, DNS:edi.su
Transparency	No
Extended Validation	No
Valid From	April 26th 2015, 11:47 CEST
Valid To	July 25th 2018, 23:37 CEST

CERTIFICATE CHAIN

***.edi.su** — Server certificate

Key Type/Size	**RSA 2048 bits**
Signature Algorithm	**sha256WithRSAEncryption**
SHA256	**0ca05f7bcba55f87d84b1347e7bf9b9b4e03e6d72b8b3bbcfbddb7dbee8394d2**
PIN	**e642SikM0VlJP1nuN5NE8Sg42uJ3El6BwSNLp829bXk=**
Expires in	**731 days**

RapidSSL SHA256 CA - G3 — Intermediate CA

Key Type/Size	**RSA 2048 bits**
Signature Algorithm	**sha256WithRSAEncryption**
SHA256	**6e37822b18adbba04ed1ed6f1d2b14f9a4d268516dd949736146f64d645e0617**
PIN	**6X0iNAQtPljXKEVcqZBwyMcRwq1yW60549axatu3oDE=**
Expires in	**2,126 days**

GeoTrust Global CA — Self-signed, Root CA

Key Type/Size	**RSA 2048 bits**
Signature Algorithm	**sha1WithRSAEncryption**
SHA256	**ad8255ac5a2894e7bbf034870d25d635418e8c74f7b936ae1ea29055dc81e2e9**
PIN	**h6801m+z8v3zbgkRHpq6L29Esgfzhj89C1SyUCOQmqU=**
Expires in	**2,127 days**

Test For Compliance With NIST Guidelines

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

DIFFIE-HELLMAN PARAMETER SIZE

The size of your Diffie-Hellman (DH) parameter:

2048 bits	Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-256 (prime256v1) (256 bits)	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

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	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_DHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	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_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Good configuration

MISSING MANDATORY CIPHERS

The support of these ciphers is mandatory according to NIST:

TLS_RSA_WITH_3DES_EDE_CBC_SHA	Non-compliant with NIST guidelines
TLS_RSA_WITH_AES_128_CBC_SHA	Non-compliant with NIST guidelines
TLS_RSA_WITH_AES_128_GCM_SHA256	Non-compliant with NIST guidelines

SERVER DOES NOT SUPPORT OCSP STAPLING

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

Non-compliant with NIST guidelines

Test For Compliance With PCI DSS Requirements

Reference: PCI DSS 3.1 - Requirements 2.3 and 4.1

DIFFIE-HELLMAN PARAMETER SIZE

The size of your Diffie-Hellman (DH) parameter:

2048 bits	Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-256 (prime256v1) (256 bits)	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

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	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_DHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	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_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Good configuration

POODLE

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 Industry Best-Practices

CERTIFICATE HAS BEEN SIGNED FOR MORE THAN 3 YEARS

The RSA certificate provided has been validated for more than 3 years. This means that the private key of the server will remain the same for more than 3 years. NIST guidelines suggest limiting certificate validity to 3 years maximum.

Misconfiguration or weakness

CERTIFICATE IS NOT EV

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

Information

SERVER SUPPORTS TLSV1.2

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

Good configuration

SERVER PREFERS PFS ENABLED CIPHER SUITES

For TLS family of protocols, the server prefers cipher suite(s) providing Perfect Forward Secrecy (PFS).

Good configuration

HTTP SITE DOES REDIRECT

The HTTP version of the website redirects to the HTTPS version.

Good configuration

SERVER DOES NOT PROVIDE HSTS

The server does not send the HTTP-Strict-Transport-Security. We advise to enable it to enforce the user to browse the website in HTTPS.

Misconfiguration or weakness

SERVER DOES NOT PROVIDE HPKP

The server does not send HTTP-Public-Key-Pinning header. We advise to enable HPKP in order to avoid Man-In-The-Middle attacks.

Information

SERVER SUPPORTS TLS FALLBACK SCSV EXTENSION

The server supports TLS_FALLBACK_SCSV extension for protocol downgrade attack prevention.

Good configuration

SERVER DOES NOT SUPPORT CLIENT-INITIATED SECURE RENEGOTIATION

The server does not support client-initiated secure renegotiation.

Good configuration

SECURE RENEGOCIATION SUPPORTED

The server supports secure server-initiated renegotiation.

Good configuration

TLS COMPRESSION SUPPORT

TLS compression is not supported by the server.

Good configuration

SERVER PREFERRED CIPHER SUITES

Preferred cipher suite for each protocol supported (except SSLv2). Expected configuration are ciphers allowed by PCI DSS and enabling PFS:

TLSv1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLSv1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLSv1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration