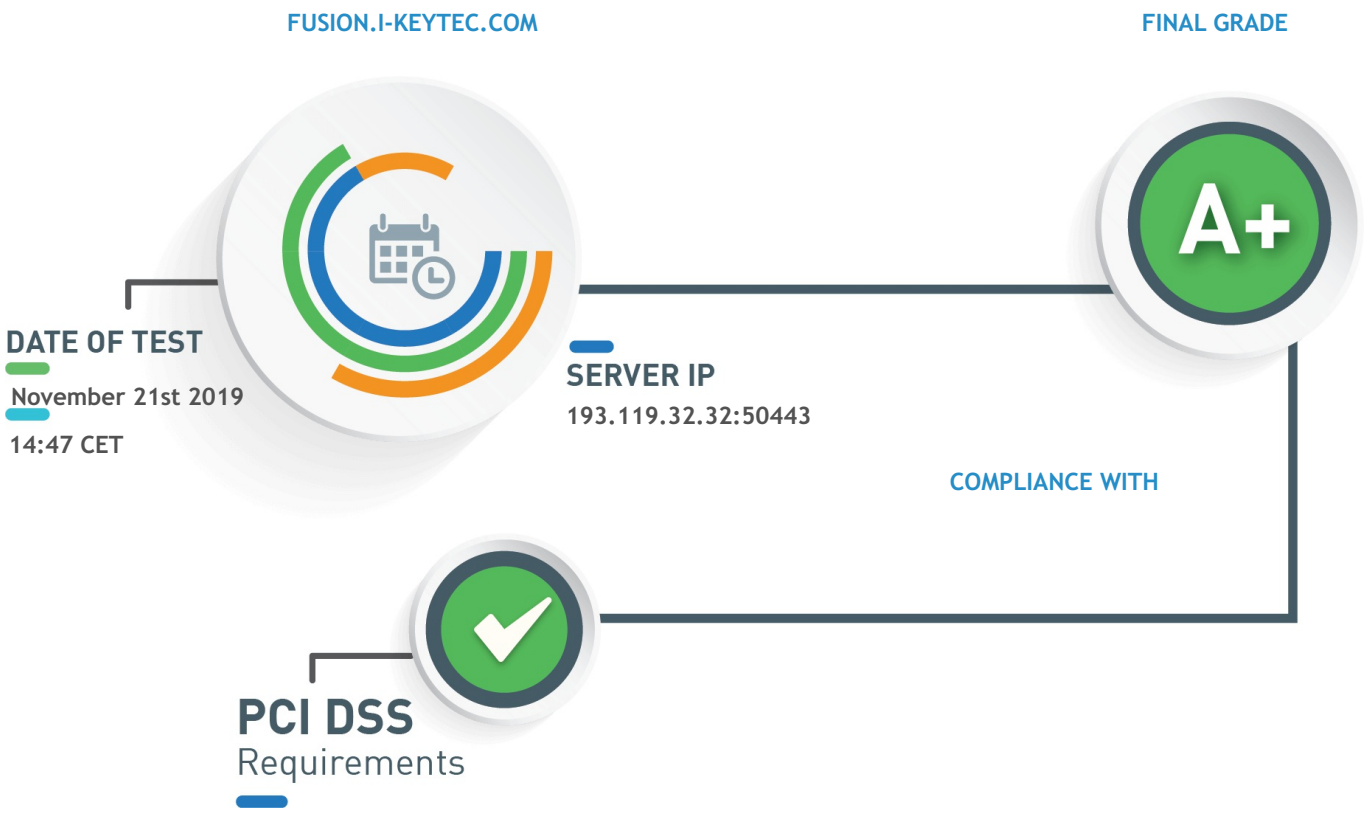
Test SSL/TLS implementation of any service on any port for compliance with PCI DSS requirements, HIPAA guidance and NIST guidelines.



Summary of fusion.i-keytec.com:50443 (N/A) SSL Security Test

The server supports cipher suites that are not approved by HIPAA guidance and NIST guidelines.	Non-compliant with HIPAA and NIST
The server configuration supports only TLSv1.2 and TLSv1.3 protocols, precluding users with older browsers from accessing your website.	Information
The tested service seems to be a N/A.	Information
The server supports the most recent and secure TLS protocol version of TLS 1.3.	Good configuration
The server prefers cipher suites supporting Perfect-Forward-Secrecy.	Good configuration

SSL Certificate Analysis

RSA CERTIFICATE INFORMATION

Issuer	Sectigo RSA Domain Validation Secure Server CA
Trusted	Yes
Common Name	fusion.i-keytec.com
Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
Subject Alternative Names	DNS:fusion.i-keytec.com, DNS:www.fusion.i-keytec.com
Transparency	Yes
Validation Level	DV
CRL	No
OCSP	http://ocsp.sectigo.com
OCSP Must-Staple	No
Supports OCSP Stapling	No
Valid From	November 14th 2019, 01:00 CET
Valid To	November 14th 2021, 00:59 CET

CERTIFICATE CHAIN

Intermediate certificate is not provided by the server. Misconfiguration or weakness

AddTrust External CA Root

Self-signed Root CA

Key Type/Size	**RSA 2048 bits**
Signature Algorithm	**sha1WithRSAEncryption**
SHA256	**687fa451382278fff0c8b11f8d43d576671c6eb2bceab413fb83d965d06d2ff2**
PIN	**ICppFqbkrlJ3EcVFAkeip0+44VaoJUymbnOaEUk7tEU=**
Expires in	**191 days**

↳ USERTrust RSA Certification Authority

Intermediate CA

Key Type/Size	**RSA 4096 bits**
Signature Algorithm	**sha384WithRSAEncryption**
SHA256	**1a5174980a294a528a110726d5855650266c48d9883bea692b67b6d726da98c5**
PIN	**x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4lTdO/nEW/Td4=**
Expires in	**191 days**

↳ Sectigo RSA Domain Validation Secure Server CA

Intermediate CA

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha384WithRSAEncryption
SHA256	7fa4ff68ec04a99d7528d5085f94907f4d1dd1c5381bacdc832ed5c960214676
PIN	4a6cPehI7OG6cuDZka5NDZ7FR8a60d3auda+sKfg4Ng=
Expires in	4,058 days

↳ **fusion.i-keytec.com** — Server certificate

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
SHA256	7639d0f939da7e6960b34274b1a9ed550a7e6e2a7a3d73362cf1a100b53a2b91
PIN	mQo1Q+wfWNM8ZBKeBo+iX01BhRidl53UwQx5UyMfWhE=
Expires in	723 days

CERTIFICATE CHAIN CONTINUED

USERTrust RSA Certification Authority — Self-signed, Root CA

Key Type/Size	RSA 4096 bits
Signature Algorithm	sha384WithRSAEncryption
SHA256	e793c9b02fd8aa13e21c31228accb08119643b749c898964b1746d46c3d4cbd2
PIN	x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4lTdO/nEW/Td4=
Expires in	6,633 days

↳ **Sectigo RSA Domain Validation Secure Server CA** — Intermediate CA

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha384WithRSAEncryption
SHA256	7fa4ff68ec04a99d7528d5085f94907f4d1dd1c5381bacdc832ed5c960214676
PIN	4a6cPehI7OG6cuDZka5NDZ7FR8a60d3auda+sKfg4Ng=
Expires in	4,058 days

↳ **fusion.i-keytec.com** — Server certificate

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
SHA256	7639d0f939da7e6960b34274b1a9ed550a7e6e2a7a3d73362cf1a100b53a2b91
PIN	mQo1Q+wfWNM8ZBKeBo+iX01BhRidl53UwQx5UyMfWhE=

Expires in	**723 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:

TLSV1.3

TLS_AES_128_GCM_SHA256	Information
TLS_AES_256_GCM_SHA384	Information
TLS_CHACHA20_POLY1305_SHA256	Information

TLSV1.2

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	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_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration

SUPPORTED PROTOCOLS

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

TLSv1.2	Good configuration
TLSv1.3	Information

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-256 (prime256v1) (256 bits)	Good configuration
P-384 (secp384r1) (384 bits)	Good configuration

POODLE OVER TLS

The server is not vulnerable to POODLE over TLS. Not vulnerable

GOLDENDOODLE

The server is not vulnerable to GOLDENDOODLE. Not vulnerable

ZOMBIE POODLE

The server is not vulnerable to Zombie POODLE. Not vulnerable

SLEEPING POODLE

The server is not vulnerable to Sleeping POODLE. Not vulnerable

0-LENGTH OPENSSL

The server is not vulnerable 0-Length OpenSSL. 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

ROBOT

The server is not vulnerable to ROBOT (Return Of Bleichenbacher's Oracle Threat) vulnerability. Not vulnerable

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 Guidance

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:

TLSv1.2	Good configuration
TLSv1.3	Information

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLSV1.3

TLS_AES_128_GCM_SHA256	Information
TLS_AES_256_GCM_SHA384	Information
TLS_CHACHA20_POLY1305_SHA256	Information

TLSV1.2

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Non-compliant with HIPAA guidance
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_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-256 (prime256v1) (256 bits)	Good configuration
P-384 (secp384r1) (384 bits)	Good configuration

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

NIST **Update to Current Use and Deprecation of TDEA** abrogates 3DES authorized in the NIST guidelines. — Information

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:

TLSV1.3

TLS_AES_128_GCM_SHA256	Information
TLS_AES_256_GCM_SHA384	Information
TLS_CHACHA20_POLY1305_SHA256	Information

TLSV1.2

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Non-compliant with NIST guidelines
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_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration

SUPPORTED PROTOCOLS

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

TLSv1.2	Good configuration
TLSv1.3	Information

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-256 (prime256v1) (256 bits)	Good configuration
P-384 (secp384r1) (384 bits)	Good configuration

EC_POINT_FORMAT EXTENSION

The server supports the EC_POINT_FORMAT TLS extension. — Good configuration

Test For Industry Best-Practices

DNSCAA

This domain does not have a Certification Authority Authorization (CAA) record.

Information

CERTIFICATES DO NOT PROVIDE EV

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

Information

TLSV1.3 SUPPORTED

The server supports TLSv1.3 which is the only version of TLS that currently has no known flaws or exploitable weaknesses.

Good configuration

SERVER HAS CIPHER PREFERENCE

The server enforces cipher suites preference.

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:

TLSv1.2

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

TLSv1.2

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

Good configuration

TLSv1.3 TLS_AES_128_GCM_SHA256

TLSv1.3 TLS_AES_128_GCM_SHA256

Information

SERVER PREFERS CIPHER SUITES PROVIDING PFS

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

Good configuration

TLS_FALLBACK_SCSV

TLS_FALLBACK_SCSV extension prevents protocol downgrade attacks. We advise to update your TLS engine to support it.

Misconfiguration or weakness

SERVER DOES NOT SUPPORT CLIENT-INITIATED SECURE RENEGOTIATION

The server does not support client-initiated secure renegotiation.

Good configuration

SERVER-INITIATED SECURE RENEGOTIATION

The server does not support secure server-initiated renegotiation.

Misconfiguration or weakness

SERVER DOES NOT SUPPORT TLS COMPRESSION

TLS compression is not supported by the server.

Good configuration