Summary of eprocurement.jmto.co.id:443 (HTTPS) SSL Security Test

jmto.co.id was tested 1 time during the last 12 months.

Date/Time:	Sep 1st, 2023 12:55:15 GMT+7
Source IP/Port:	34.128.98.159:443
Type:	HTTPS

Your final score

A

B

C

F

A+

Compliance Test	COMPLIANT
HIPAA Compliance Test	3 ISSUES FOUND
NIST Compliance Test	3 ISSUES FOUND
Industry Best Practices	NO MAJOR ISSUES FOUND
External Content Security	82 LINKS FOUND

The server supports the most recent and secure TLS protocol version of TLS 1.3. Good configuration

SSL Certificate Analysis

RSA CERTIFICATE INFORMATION

Issuer	DigiCert TLS RSA SHA256 2020 CA1
Trusted	Yes
Common Name	*.jmto.co.id
Key Type/Size	RSA 2048 bits
Serial Number	12966041546951268292624759963915797329
Signature Algorithm	sha256WithRSAEncryption
Subject Alternative Names	DNS:*.jmto.co.id, DNS:jmto.co.id
Transparency	Yes
Validation Level	OV
CRL	http://crl3.digicert.com/DigiCertTLSRSASHA2562020CA1-4.crl
OCSP	http://ocsp.digicert.com
OCSP Must-Staple	No
Supports OCSP Stapling	No
Valid From	September 20, 2022 01:00 CET
Valid To	October 22, 2023 00:59 CET

CERTIFICATE CHAIN

Server sends an unnecessary root certificate. Misconfiguration or weakness

Root CA	**DigiCert Global Root CA**
Type/Size	RSA 2048 bits
Serial Number	10944719598952040374951832963794454346
Signature	sha1WithRSAEncryption
SHA256	4348a0e9444c78cb26...257f8934a443c70161
PIN	r/mIkG3eEpVdm+u/ko...1bk4TyHIlByibiA5E=
Expires in	2,992 days
Comment	Self-signed

Intermediate CA	**DigiCert TLS RSA SHA256 2020 CA1**
Type/Size	RSA 2048 bits
Serial Number	9101305761976670746388865003982847684
Signature	sha256WithRSAEncryption
SHA256	52274c57ce4dee3b49...25a86fb4430182fe14
PIN	RQeZkB42znUfsDIIFW... 7nHwNFwWCrnMMJbVc=
Expires in	2,782 days

Comment	Extended Validation

Server certificate	***.jmto.co.id**
Type/Size	RSA 2048 bits
Serial Number	12966041546951268292624759963915797329
Signature	sha256WithRSAEncryption
SHA256	ba6844681c11f78b61…cb68492b03fa882b0a
PIN	K8wwKPk7/NSBY19Y0H… 1J1HnoQ/rPEqbkwcc=
Expires in	51 days
Comment	-

PCI DSS Compliance Test

Reference: PCI DSS 3.2.1, 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_CHACHA20_POLY1305_SHA256	Good configuration
TLS_AES_256_GCM_SHA384	Good configuration
TLS_AES_128_GCM_SHA256	Good configuration

TLSV1.2

TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	Good configuration
TLS_RSA_WITH_CAMELLIA_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_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_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

SUPPORTED PROTOCOLS

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

TLSv1.2	Good configuration
TLSv1.3	Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-384 (secp384r1) (384 bits)	Good configuration
P-521 (secp521r1) (521 bits)	Good configuration

P-256 (prime256v1) (256 bits)	Good configuration
X25519 (253 bits)	Good configuration
X448 (448 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 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 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 CCS Injection. Not vulnerable

CVE-2021-3449

The server is not vulnerable to CVE-2021-3449 (OpenSSL Maliciously Crafted Renegotiation Vulnerability). Not vulnerable

HIPAA and NIST Compliance Test

Reference: HIPAA, Security Rule (Ref. NIST SP 800-52: "Guidelines for the Selection and Use of TLS Implementations")

X.509 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 is not configured to support OCSP stapling for its RSA certificate that allows better verification of the certificate validation status. Reconfigure or upgrade your web server to enable OCSP stapling. **Non-compliant with NIST guidelines**

SUPPORTED CIPHERS

Consider dropping support for all non-compliant protocols. List of all cipher suites supported by the server:

TLSV1.3

TLS_CHACHA20_POLY1305_SHA256	Good configuration
TLS_AES_256_GCM_SHA384	Good configuration
TLS_AES_128_GCM_SHA256	Good configuration

TLSV1.2

TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	Non-compliant with NIST guidelines
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	Non-compliant with NIST guidelines
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_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

SUPPORTED PROTOCOLS

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

TLSv1.2	Good configuration
TLSv1.3	Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-384 (secp384r1) (384 bits)	Good configuration
P-521 (secp521r1) (521 bits)	Good configuration
P-256 (prime256v1) (256 bits)	Good configuration
X25519 (253 bits)	Good configuration
X448 (448 bits)	Good configuration

EC_POINT_FORMAT EXTENSION

The server supports the EC_POINT_FORMAT TLS extension.	Good configuration

Please wait. Data is loading...