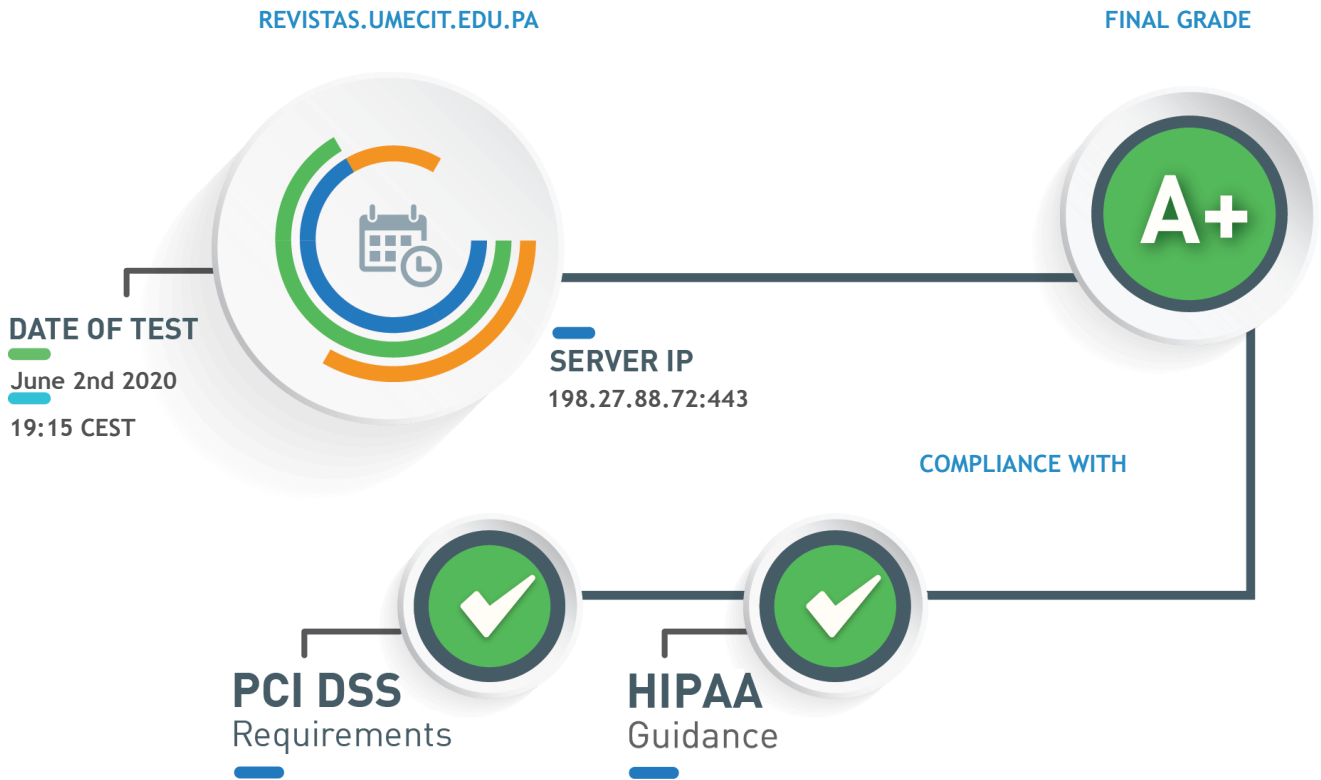


Test SSL/TLS implementation of any service on any port for compliance with PCI DSS requirements, HIPAA guidance and NIST guidelines.



## Summary of revistas.umecit.edu.pa:443 (HTTPS)

The server configuration supports only TLSv1.2 protocol, precluding users with older browsers from accessing your website. Information

# SSL Certificate Analysis

## RSA CERTIFICATE INFORMATION

<b>Issuer</b>	Let's Encrypt Authority X3
<b>Trusted</b>	Yes
<b>Common Name</b>	revistas.umecit.edu.pa
<b>Key Type/Size</b>	RSA 2048 bits
<b>Signature Algorithm</b>	sha256WithRSAEncryption
<b>Subject Alternative Names</b>	DNS:revistas.umecit.edu.pa
<b>Transparency</b>	Yes
<b>Validation Level</b>	DV
<b>CRL</b>	No
<b>OCSP</b>	http://ocsp.int-x3.letsencrypt.org
<b>OCSP Must-Staple</b>	No
<b>Supports OCSP Stapling</b>	Yes
<b>Valid From</b>	May 3rd 2020, 01:13 CEST
<b>Valid To</b>	August 1st 2020, 01:13 CEST

## CERTIFICATE CHAIN

### DST Root CA X3

Self-signed

Root CA

Key Type/Size	<b>RSA 2048 bits</b>
Signature Algorithm	<b>sha1WithRSAEncryption</b>
SHA256	<b>0687260331a72403d909f105e69bcf0d32e1bd2493ffc6d9206d11bcd6770739</b>
PIN	<b>Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys=</b>
Expires in	<b>485 days</b>

### ↳ Let's Encrypt Authority X3

Intermediate CA

Key Type/Size	<b>RSA 2048 bits</b>
Signature Algorithm	<b>sha256WithRSAEncryption</b>
SHA256	<b>25847d668eb4f04fdd40b12b6b0740c567da7d024308eb6c2c96fe41d9de218d</b>
PIN	<b>YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg=</b>
Expires in	<b>288 days</b>

### ↳ revistas.umecit.edu.pa

Server certificate

Key Type/Size	<b>RSA 2048 bits</b>
Signature Algorithm	<b>sha256WithRSAEncryption</b>

SHA256	58b47c69499f00b98a8631146252ff40c3dec57062d1ab3602f65ea303524d8e
PIN	067iYbCqDL0xI8k9EIKM+jA7oHOZpJDk1bWRg/p6Ocg=
Expires in	<b>59 days</b>

# 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\_GCM\_SHA256

Good configuration

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

## DIFFIE-HELLMAN PARAMETER SIZE

Diffie-Hellman parameter size: 2048 bits

Good configuration

## SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

secp256k1 (256 bits)

Good configuration

P-384 (secp384r1) (384 bits)

Good configuration

P-521 (secp521r1) (521 bits)

Good configuration

P-256 (prime256v1) (256 bits)

Good configuration

K-283 (sect283k1) (281 bits)

Good configuration

B-283 (sect283r1) (282 bits)

Good configuration

K-409 (sect409k1) (407 bits)

Good configuration

B-409 (sect409r1) (409 bits)

Good configuration

K-571 (sect571k1) (570 bits)

Good configuration

B-571 (sect571r1) (570 bits)

Good configuration

brainpoolP256r1 (256 bits)

Good configuration

brainpoolP384r1 (384 bits)

Good configuration

brainpoolP512r1 (512 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 OPENSLL**

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.

### X.509 CERTIFICATES ARE IN VERSION 3

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

Good configuration

### SERVER SUPPORTS OCSP STAPLING

The server supports OCSP stapling, which allows better verification of the certificate validation status.

Good configuration

### SUPPORTED PROTOCOLS

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

TLSv1.2

Good configuration

### SUPPORTED CIPHERS

List of all cipher suites supported by the server:

#### TLSV1.2

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\_GCM\_SHA256

Good configuration

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

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:

secp256k1 (256 bits)

Good configuration

P-384 (secp384r1) (384 bits)

Good configuration

P-521 (secp521r1) (521 bits)

Good configuration

P-256 (prime256v1) (256 bits)

Good configuration

K-283 (sect283k1) (281 bits)

Good configuration

B-283 (sect283r1) (282 bits)

Good configuration

K-409 (sect409k1) (407 bits)

Good configuration

B-409 (sect409r1) (409 bits)

Good configuration

K-571 (sect571k1) (570 bits)

Good configuration

B-571 (sect571r1) (570 bits)

Good configuration

brainpoolP256r1 (256 bits)

Good configuration

brainpoolP384r1 (384 bits)

Good configuration

brainpoolP512r1 (512 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 2 - Section 3

### X.509 CERTIFICATES ARE IN VERSION 3

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

Good configuration

### SERVER SUPPORTS OCSP STAPLING

The server supports OCSP stapling, which allows better verification of the certificate validation status.

Good configuration

### SUPPORTED CIPHERS

List of all cipher suites supported by the server:

#### TLSV1.2

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\_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

### DIFFIE-HELLMAN PARAMETER SIZE

Diffie-Hellman parameter size: 2048 bits

Good configuration

### SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

secp256k1 (256 bits)

Good configuration

P-384 (secp384r1) (384 bits)

Good configuration

P-521 (secp521r1) (521 bits)

Good configuration

P-256 (prime256v1) (256 bits)

Good configuration

K-283 (sect283k1) (281 bits)

Good configuration

B-283 (sect283r1) (282 bits)

Good configuration

K-409 (sect409k1) (407 bits)

Good configuration

B-409 (sect409r1) (409 bits)

Good configuration

K-571 (sect571k1) (570 bits)

Good configuration

B-571 (sect571r1) (570 bits)

Good configuration

brainpoolP256r1 (256 bits)

Good configuration



brainpoolP384r1 (384 bits)

Good configuration

brainpoolP512r1 (512 bits)

Good configuration

**SERVER DOES NOT SUPPORT OF TLSV1.3**

The server does not support TLSv1.3 which is the only version of TLS that currently has no known flaws or exploitable weaknesses.

Information

**SERVER DOES NOT SUPPORT EXTENDED MASTER SECRET**

The server does not support Extended Master Secret extension for TLS vresions  $\leq$  1.2.

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

**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

**SERVER DOES NOT SUPPORT OF TLSV1.3**

The server does not support TLSv1.3 which is the only version of TLS that currently has no known flaws or exploitable weaknesses.

Misconfiguration or weakness

**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

**ALWAYS-ON SSL**

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

Good configuration

**SERVER PROVIDES HSTS WITH LONG DURATION**

The server provides HTTP Strict Transport Security for more than 6 months:

63072000 seconds

Good configuration

**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 supports secure server-initiated renegotiation.

Good configuration

**SERVER DOES NOT SUPPORT TLS COMPRESSION**

TLS compression is not supported by the server.

Good configuration