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

The server configuration supports only TLSv1.2 and TLSv1.3 protocols, precluding users with older browsers from accessing your website.

The server supports the most recent and secure TLS protocol version of TLS 1.3.
# SSL Certificate Analysis

## RSA Certificate Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Issuer</strong></td>
<td>Let's Encrypt Authority X3</td>
</tr>
<tr>
<td><strong>Trusted</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Common Name</strong></td>
<td>uexternado2.metarevistas.org</td>
</tr>
<tr>
<td><strong>Key Type/Size</strong></td>
<td>RSA 2048 bits</td>
</tr>
<tr>
<td><strong>Signature Algorithm</strong></td>
<td>sha256WithRSAEncryption</td>
</tr>
<tr>
<td><strong>Subject Alternative Names</strong></td>
<td>DNS:revistas.uexternado.edu.co, DNS:uexternado2.metarevistas.org</td>
</tr>
<tr>
<td><strong>Transparency</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Validation Level</strong></td>
<td>DV</td>
</tr>
<tr>
<td><strong>CRL</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>OCSP</strong></td>
<td><a href="http://ocsp.int-x3.letsencrypt.org">http://ocsp.int-x3.letsencrypt.org</a></td>
</tr>
<tr>
<td><strong>OCSP Must-Staple</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Supports OCSP Stapling</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Valid From</strong></td>
<td>April 23rd 2020, 02:43 CEST</td>
</tr>
<tr>
<td><strong>Valid To</strong></td>
<td>July 22nd 2020, 02:43 CEST</td>
</tr>
</tbody>
</table>

## Certificate Chain

**DST Root CA X3**
- **Key Type/Size**: RSA 2048 bits
- **Signature Algorithm**: sha1WithRSAEncryption
- **SHA256**: 0687260331a72403d909f105e69b6c0d32e1bd2493ff6c6d9206d11bcd6770739
- **PIN**: Vjs8r4z+80wjNcr1YKepWQboSIRi63WsxWxhMN+eWys=
- **Expires in**: 483 days

**Let's Encrypt Authority X3**
- **Key Type/Size**: RSA 2048 bits
- **Signature Algorithm**: sha256WithRSAEncryption
- **SHA256**: 25847d668eb4f04fdd40b12b6b0740c567da7d024308eb6c2c96fe41d9de218d
- **PIN**: YLh1dUR9y6Kja30RrAn7JKnbQG/uElLMkBF2Fuihg=
- **Expires in**: 286 days

**uexternado2.metarevistas.org**
- **Key Type/Size**: RSA 2048 bits
- **Signature Algorithm**: sha256WithRSAEncryption
SHA256: 537d71c2e7735d2f347e719d1d5df751c3b5b0341a17e2150a68eb26ce4636eb
PIN: wDVCxPp+ranMk4jq2Vj6sm6KO22Aq9JURl9TpWFGfOI=
Expires in: 47 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:

<table>
<thead>
<tr>
<th>Cipher Suite</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_AES_256_GCM_SHA384</td>
<td>Good config</td>
</tr>
<tr>
<td>TLS_CHACHA20_POLY1305_SHA256</td>
<td>Good config</td>
</tr>
<tr>
<td>TLS_AES_128_GCM_SHA256</td>
<td>Good config</td>
</tr>
</tbody>
</table>

### SUPPORTED PROTOCOLS

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

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLSv1.2</td>
<td>Good config</td>
</tr>
</tbody>
</table>
## TLSv1.3

### 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-256 (prime256v1) (256 bits)**
  **Good configuration**

- **P-521 (secp521r1) (521 bits)**
  **Good configuration**

- **P-384 (secp384r1) (384 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 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 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:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLSv1.2</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLSv1.3</td>
<td>Good configuration</td>
</tr>
</tbody>
</table>

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

<table>
<thead>
<tr>
<th>Cipher Suite</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_AES_256_GCM_SHA384</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_CHACHA20_POLY1305_SHA256</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_AES_128_GCM_SHA256</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_128_GCM_SHA256</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_GCM_SHA384</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_GCM_SHA256</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_GCM_SHA256</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_GCM_SHA384</td>
<td>Good configuration</td>
</tr>
</tbody>
</table>
### Good configuration

**DIFFIE-HELLMAN PARAMETER SIZE**

Diffie-Hellman parameter size: **2048 bits**

**SUPPORTED ELLIPTIC CURVES**

List of all elliptic curves supported by the server:

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

**EC_POINT_FORMAT EXTENSION**

The server supports the EC_POINT_FORMAT TLS extension.
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 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_256_GCM_SHA384 Good configuration
- TLS_CHACHA20_POLY1305_SHA256 Good configuration
- TLS_AES_128_GCM_SHA256 Good configuration

**TLSV1.2**
- 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_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_128_CBC_SHA Good configuration
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 Good configuration
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA Good configuration
- TLS_RSA_WITH_AES_128_GCM_SHA256 Good configuration
- TLS_RSA_WITH_AES_256_GCM_SHA384 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_CBC_SHA Good configuration
- TLS_RSA_WITH_AES_256_CBC_SHA Good configuration

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

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLSv1.2</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLSv1.3</td>
<td>Good configuration</td>
</tr>
</tbody>
</table>

**DIFFIE-HELLMAN PARAMETER SIZE**

Diffie-Hellman parameter size: **2048 bits**

**SUPPORTED ELLIPTIC CURVES**

List of all elliptic curves supported by the server:

<table>
<thead>
<tr>
<th>Curve</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-256 (prime256v1) (256 bits)</td>
<td>Good configuration</td>
</tr>
<tr>
<td>P-521 (secp521r1) (521 bits)</td>
<td>Good configuration</td>
</tr>
<tr>
<td>P-384 (secp384r1) (384 bits)</td>
<td>Good configuration</td>
</tr>
<tr>
<td>X25519 (253 bits)</td>
<td>Good configuration</td>
</tr>
<tr>
<td>X448 (448 bits)</td>
<td>Good configuration</td>
</tr>
</tbody>
</table>

**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.

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

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

SERVER HAS CIPHER PREFERENCE
The server enforces cipher suites preference.

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

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Cipher Suite</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLSv1.2</td>
<td>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>TLSv1.2</td>
<td>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>TLSv1.3</td>
<td>TLS_AES_256_GCM_SHA384</td>
</tr>
<tr>
<td>TLSv1.3</td>
<td>TLS_AES_256_GCM_SHA384</td>
</tr>
</tbody>
</table>

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

ALWAYS-ON SSL
The HTTP version of the website redirects to the HTTPS version.

SERVER PROVIDES HSTS WITH LONG DURATION
The server provides HTTP Strict Transport Security for more than 6 months: 31536000 seconds

TLS_FALLBACK_SCSV
The server supports TLS_FALLBACK_SCSV extension for protocol downgrade attack prevention.

SERVER DOES NOT SUPPORT CLIENT-INITIATED SECURE RENEGOTIATION
The server does not support client-initiated secure renegotiation.

SERVER-INITIATED SECURE RENEGOTIATION
The server supports secure server-initiated renegotiation.

SERVER DOES NOT SUPPORT TLS COMPRESSION
TLS compression is not supported by the server.
Good configuration