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

Summary of revia.areandina.edu.co:443 (HTTPS)

The server configuration supports only TLSv1.2 protocol, precluding users with older browsers from accessing your website.
### 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>revia.areandina.edu.co</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:revia.areandina.edu.co</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>Yes</td>
</tr>
<tr>
<td><strong>Valid From</strong></td>
<td>April 18th 2020, 23:03 CEST</td>
</tr>
<tr>
<td><strong>Valid To</strong></td>
<td>July 17th 2020, 23:03 CEST</td>
</tr>
</tbody>
</table>

### CERTIFICATE CHAIN

#### DST Root CA X3

- **Key Type/Size**: RSA 2048 bits
- **Signature Algorithm**: sha1WithRSAEncryption
- **SHA256**: 0687260331a72403d909f105e69bcf0d32e1bd2493ffe6d9206d11b6d707739
- **PIN**: Vjs8r4z+80wjNcr1YKepWQboSRI63WsxWxhIMN+eWys=
- **Expires in**: 484 days

#### Let's Encrypt Authority X3

- **Key Type/Size**: RSA 2048 bits
- **Signature Algorithm**: sha256WithRSAEncryption
- **SHA256**: 25847d668eb4f04fdd40b12b6b0740c567da7d024308eb6c2c96fe41d9de218d
- **PIN**: YLh1dUR9y6Kja30RrAn7JKnbQG/uElLMkBF2Fulhg=
- **Expires in**: 287 days

#### revia.areandina.edu.co

- **Key Type/Size**: RSA 2048 bits
- **Signature Algorithm**: sha256WithRSAEncryption
SHA256          9bc70b921b30a77f1c5cad46c03937861d974dea6d12de9306eaeace7967d2db
PIN                T4DtQRhVdfhouMHqoKSae3wRcn+3ERzz6SMqmUvoc=
Expires in     44 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.

### 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_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_GCM_SHA256</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</td>
<td>Good configuration</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 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>secp256k1 (256 bits)</td>
<td>Good configuration</td>
</tr>
<tr>
<td>P-384 (secp384r1) (384 bits)</td>
<td>Good configuration</td>
</tr>
<tr>
<td>P-521 (secp521r1) (521 bits)</td>
<td>Good configuration</td>
</tr>
<tr>
<td>P-256 (prime256v1) (256 bits)</td>
<td>Good configuration</td>
</tr>
<tr>
<td>K-283 (sect283k1) (281 bits)</td>
<td>Good configuration</td>
</tr>
<tr>
<td>B-283 (sect283r1) (282 bits)</td>
<td>Good configuration</td>
</tr>
<tr>
<td>K-409 (sect409k1) (407 bits)</td>
<td>Good configuration</td>
</tr>
<tr>
<td>B-409 (sect409r1) (409 bits)</td>
<td>Good configuration</td>
</tr>
<tr>
<td>K-571 (sect571k1) (570 bits)</td>
<td>Good configuration</td>
</tr>
<tr>
<td>B-571 (sect571r1) (570 bits)</td>
<td>Good configuration</td>
</tr>
<tr>
<td>brainpoolP256r1 (256 bits)</td>
<td>Good configuration</td>
</tr>
<tr>
<td>brainpoolP384r1 (384 bits)</td>
<td>Good configuration</td>
</tr>
<tr>
<td>brainpoolP512r1 (512 bits)</td>
<td>Good configuration</td>
</tr>
</tbody>
</table>

## POODLE OVER TLS
The server is not vulnerable to POODLE over TLS.

**GOLDENDOODLE**
The server is not vulnerable to GOLDENDOODLE.

**ZOMBIE POODLE**
The server is not vulnerable to Zombie POODLE.

**SLEEPING POODLE**
The server is not vulnerable to Sleeping POODLE.

**0-LENGTH OPENSSL**
The server is not vulnerable 0-Length OpenSSL.

**CVE-2016-2107**
The server is not vulnerable to OpenSSL padding-oracle flaw (CVE-2016-2107).

**SERVER DOES NOT SUPPORT CLIENT-INITIATED INSECURE RENEGOTIATION**
The server does not support client-initiated insecure renegotiation.

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

**HEARTBLEED**
The server version of OpenSSL is not vulnerable to Heartbleed attack.

**CVE-2014-0224**
The server is not vulnerable to CVE-2014-0224 (OpenSSL CCS flaw).
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.  

**SERVER SUPPORTS OCSP STAPLING**

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

**SUPPORTED PROTOCOLS**

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

- **TLSv1.2**

**SUPPORTED CIPHERS**

List of all cipher suites supported by the server:

- **TLSv1.2**
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

**DIFFIE-HELLMAN PARAMETER SIZE**

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

**SUPPORTED ELLIPTIC CURVES**

List of all elliptic curves supported by the server:

- secp256k1 (256 bits)
- P-384 (secp384r1) (384 bits)
- P-521 (secp521r1) (521 bits)
- P-256 (prime256v1) (256 bits)
- K-283 (sect283k1) (281 bits)
- B-283 (sect283r1) (282 bits)
- K-409 (sect409k1) (407 bits)
- B-409 (sect409r1) (409 bits)
- K-571 (sect571k1) (570 bits)
- B-571 (sect571r1) (570 bits)
- brainpoolP256r1 (256 bits)
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.  

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

**SUPPORTED CIPHERS**
List of all cipher suites supported by the server:

**TLSv1.2**
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLSv1.2

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

**DIFFIE-HELLMAN PARAMETER SIZE**
Diffie-Hellman parameter size: 2048 bits

**SUPPORTED ELLIPTIC CURVES**
List of all elliptic curves supported by the server:

- secp256k1 (256 bits)
- P-384 (secp384r1) (384 bits)
- P-521 (secp521r1) (521 bits)
- P-256 (prime256v1) (256 bits)
- K-283 (sect283k1) (281 bits)
- B-283 (sect283r1) (282 bits)
- K-409 (sect409k1) (407 bits)
- B-409 (sect409r1) (409 bits)
- K-571 (sect571k1) (570 bits)
- B-571 (sect571r1) (570 bits)
- brainpoolP256r1 (256 bits)
Server does not support 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.

Server does not support extended master secret
The server does not support Extended Master Secret extension for TLS versions ≤ 1.2.

EC_POINT_FORMAT extension
The server supports the EC_POINT_FORMAT TLS extension.

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.

Server does not support 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.

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.

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:
63072000 seconds

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.