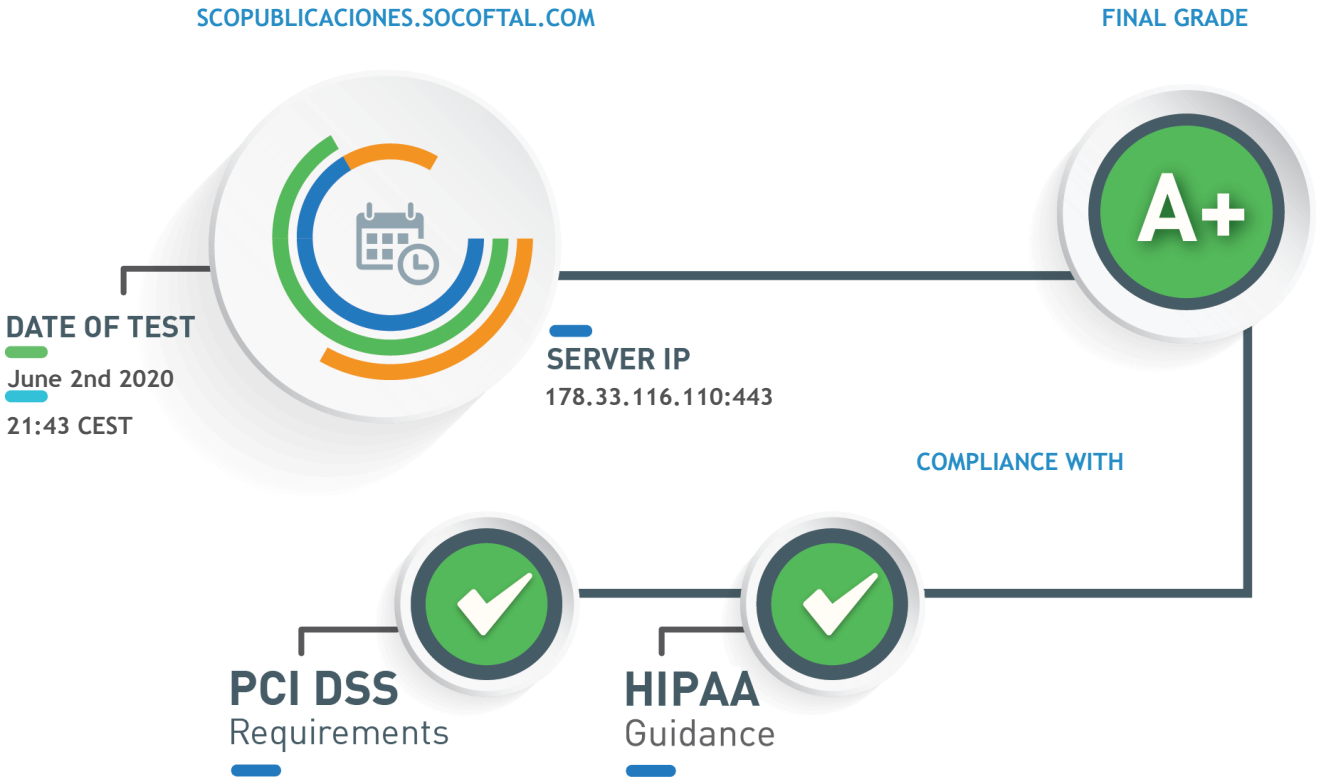
Test SSL/TLS implementation of any service on any port for compliance with PCI DSS requirements, HIPAA guidance and NIST guidelines.



Summary of scopublicaciones.socoftal.com: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

Issuer	Let's Encrypt Authority X3
Trusted	Yes
Common Name	scopublicaciones.socoftal.com
Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
Subject Alternative Names	DNS:scopublicaciones.socoftal.com, DNS:socoftal.metarevistas.org
Transparency	Yes
Validation Level	DV
CRL	No
OCSP	http://ocsp.int-x3.letsencrypt.org
OCSP Must-Staple	No
Supports OCSP Stapling	Yes
Valid From	May 19th 2020, 06:01 CEST
Valid To	August 17th 2020, 06:01 CEST

CERTIFICATE CHAIN

DST Root CA X3 — Self-signed — Root CA

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

↳ **Let's Encrypt Authority X3** — Intermediate CA

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

↳ **scopublicaciones.socoftal.com** — Server certificate

Key Type/Size	**RSA 2048 bits**
Signature Algorithm	**sha256WithRSAEncryption**

SHA256	6042afe29e05989bcdff044c36b2457e48901244b2c8056d69e2a47c4371d1d9
PIN	LIyW+SJBkQD6LUcKMH10E2J+zVGfGwuFGjt0ERVhC2g=
Expires in	75 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:

TLSV1.2

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:

P-256 (prime256v1) (256 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 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:

P-256 (prime256v1) (256 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:

P-256 (prime256v1) (256 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 ≤ 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