

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > pilierpublic.com

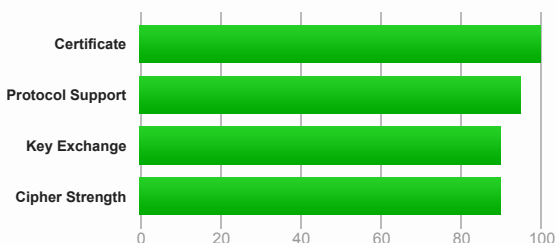
SSL Report: pilierpublic.com (185.61.152.27)

Assessed on: Tue, 21 Mar 2017 08:24:57 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This site works only in browsers with SNI support.

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1



Subject	salyens.com Fingerprint SHA1: bad2485cb94f022021e5e3c1859e45219a5cc3df Pin SHA256: 3zwc9n94YSHhpgZR7IKPvZ7aT7I4Lfgf757z28MGM1g=
Common names	salyens.com
Alternative names	itafel.com lifestoeeasy.com neokai.com pilierpublic.com salyens.com secure.salyens.com smartfolyo.com tokango.com vietropfacile.com www.itafel.com www.lifestoeeasy.com www.neokai.com www.pilierpublic.com www.salyens.com www.smartfolyo.com www.tokango.com www.vietropfacile.com
Valid from	Thu, 02 Feb 2017 01:43:00 UTC
Valid until	Wed, 03 May 2017 01:43:00 UTC (expires in 1 month and 11 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Let's Encrypt Authority X3 AIA: http://cert.int-x3.letsencrypt.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://ocsp.int-x3.letsencrypt.org/
Revocation status	Good (not revoked)
DNS CAA	No
Trusted	Yes



Additional Certificates (if supplied)



Certificates provided	2 (2739 bytes)
Chain issues	None

#2

Subject	Let's Encrypt Authority X3 Fingerprint SHA1: e6a3b45b062d509b3382282d196efe97d5956ccb Pin SHA256: YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMKBgFF2Fuihg=
Valid until	Wed, 17 Mar 2021 16:40:46 UTC (expires in 3 years and 11 months)
Key	RSA 2048 bits (e 65537)

Additional Certificates (if supplied)

Issuer	DST Root CA X3
Signature algorithm	SHA256withRSA



Certification Paths

[Click here to expand](#)

Certificate #2: RSA 2048 bits (SHA256withRSA) No SNI

[Click here to expand](#)

Configuration



Protocols

TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No



Cipher Suites

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)		256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)		256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)		256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)		128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)		128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)		128
TLS_RSA_WITH_SEED_CBC_SHA (0x96)		128
TLS_RSA_WITH_IDEA_CBC_SHA (0x7)		128

TLS 1.1 (suites in server-preferred order)

TLS 1.0 (suites in server-preferred order)



Handshake Simulation

Android 2.3.7 No SNI ²	Incorrect certificate because this client doesn't support SNI		
	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA
Android 4.0.4	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.2.2	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.3	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS

Handshake Simulation

Android 7.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Baidu Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Chrome 51 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Firefox 49 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Googlebot Feb 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 6 / XP No FS ¹ No SNI ²	Server closed connection				
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 8 / XP No FS ¹ No SNI ²	Server sent fatal alert: handshake_failure				
IE 8-10 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Edge 13 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Java 6u45 No SNI ²	Incorrect certificate because this client doesn't support SNI				
	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA		
Java 7u25	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Java 8u31	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA	No FS	
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
OpenSSL 1.0.2e R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).



Protocol Details

	IP Address	Port	Export	Special	Status
DROWN	199.188.203.137	443	Yes	No	handshake_failure
	192.64.116.214	443	Yes	No	handshake_failure
	198.154.104.189	443	Yes	No	handshake_failure
	199.188.204.209	443	Yes	No	handshake_failure
	199.188.203.130	443	Yes	Yes	handshake_failure
	198.154.104.180	443	Yes	No	handshake_failure
	64.22.89.64	443	Yes	Yes	handshake_failure

- (1) For a better understanding of this test, please read [this longer explanation](#)
(2) Key usage data kindly provided by the [Censys](#) network search engine; original DROWN test [here](#)
(3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and incomplete
(4) We perform real-time key reuse checks, but stop checking after first confirmed vulnerability
(5) The "Special" column indicates vulnerable OpenSSL version; "Export" refers to export cipher suites

Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc014
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
Forward Secrecy	With modern browsers (more info)
ALPN	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No
Public Key Pinning Report-Only	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No
Supported EC Named Curves	secp256r1
SSL 2 handshake compatibility	Yes



HTTP Requests



1 <https://pillarpublic.com/> (HTTP/1.1 200 OK)



Miscellaneous

Test date	Tue, 21 Mar 2017 08:22:14 UTC
Test duration	163.731 seconds
HTTP status code	200
HTTP server signature	Apache
Server hostname	s131.web-hosting.com

