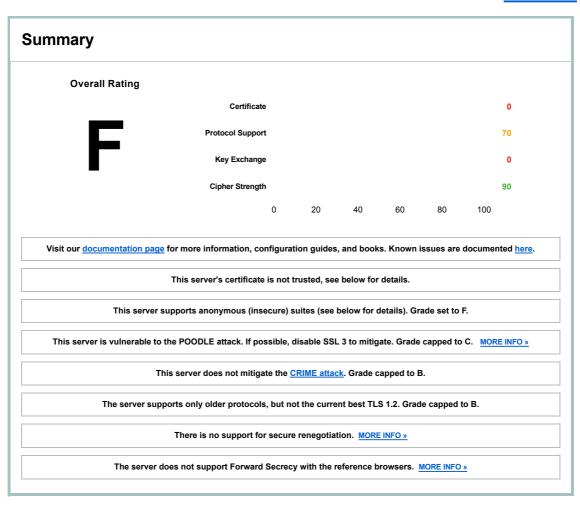
Projects

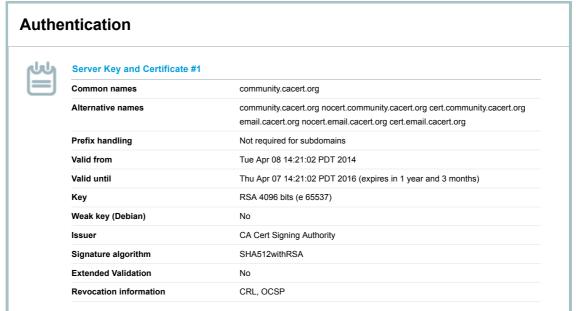
Assessed on: Sun Dec 14 03:30:57 PST 2014 | Clear cache



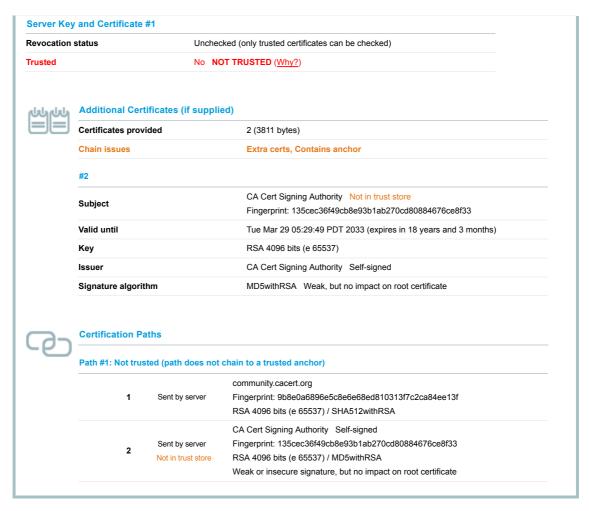
Scan Anoth

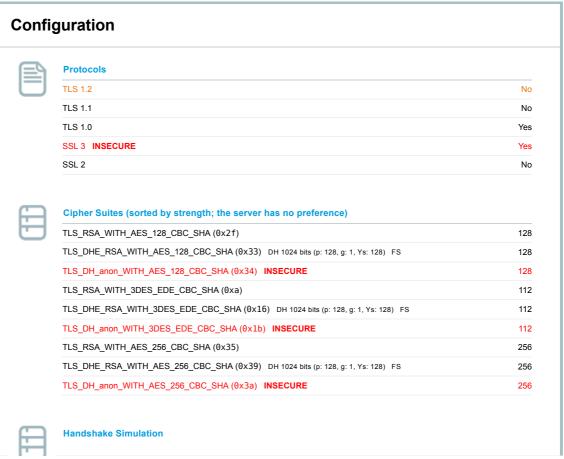
Qualys.com





14.12.2014 13:14 1 von 5





14.12.2014 13:14 2 von 5

Handshake Simulation	TI 0 4 2	TIO DOA WITH AFO 400 ODO ONA (0.25) N. 50	400
Android 2.3.7 No SNI ²	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Android 4.0.4	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Android 4.1.1	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Android 4.2.2	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Android 4.3	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Android 4.4.2	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
BingBot Dec 2013 No SNI 2	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
BingPreview Jun 2014	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Chrome 39 / OS X R	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Firefox 31.3.0 ESR / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Firefox 34 / OS X R	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Googlebot Jun 2014	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
IE 6 / XP No FS 1 No SNI 2	SSL 3	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112
IE 7 / Vista	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
IE 8 / XP No FS 1 No SNI 2	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112
<u>IE 8-10 / Win 7</u> R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
<u>IE 11 / Win 7</u> R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
IE 11 / Win 10 Preview R	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
<u>IE 11 / Win 8.1</u> R	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
IE Mobile 10 / Win Phone 8.0	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
IE Mobile 11 / Win Phone 8.1	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Java 6u45 No SNI ²	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Java 7u25	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Java 8b132	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
OpenSSL 0.9.8y	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
OpenSSL 1.0.1h	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Safari 6 / iOS 6.0.1 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Safari 7 / iOS 7.1 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Safari 8 / iOS 8.0 Beta R	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
<u>Safari 6.0.4 / OS X 10.8.4</u> R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Safari 7 / OS X 10.9 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Yahoo Slurp Jun 2014 No SNI ²	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
YandexBot Sep 2014	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
(1) Clients that do not support Ed		recy (FS) are excluded when determining support for it.	

- (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

Secure Renegotiation	Not supported ACTION NEEDED (more info)
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) SSL 3: 0x2f, TLS 1.0: 0x2f
POODLE (SSLv3)	Vulnerable INSECURE (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	No, TLS_FALLBACK_SCSV not supported (more info)
TLS compression	Yes INSECURE (more info)
RC4	No

14.12.2014 13:14 3 von 5

Heartbeat (
	(extension)	No
Heartbleed	(vulnerability)	No (more info)
OpenSSL 0	CCS vuln. (CVE-2014-0224)	No (more info)
Forward Se	ecrecy	With some browsers (more info)
Next Proto	col Negotiation (NPN)	No
Session re	sumption (caching)	Yes
Session re	sumption (tickets)	No
OCSP stap	ling	No
Strict Trans	sport Security (HSTS)	No
Public Key	Pinning (HPKP)	No
Long hand	shake intolerance	No
TLS extens	sion intolerance	No
TLS versio	n intolerance	TLS 2.98
SSL 2 hand	dshake compatibility	Yes
SSL 2 hand	Miscellaneous Test date	Yes Sun Dec 14 03:29:23 PST 2014
SSL 2 hand	Miscellaneous	Sun Dec 14 03:29:23 PST 2014 93.563 seconds
SSL 2 hand	Miscellaneous Test date	Sun Dec 14 03:29:23 PST 2014
SSL 2 hand	Miscellaneous Test date Test duration	Sun Dec 14 03:29:23 PST 2014 93.563 seconds
SSL 2 hand	Miscellaneous Test date Test duration HTTP status code	Sun Dec 14 03:29:23 PST 2014 93.563 seconds 302

Why is my certificate not trusted?

There are many reasons why a certificate may not be trusted. The exact problem is indicated on the report card in bright red. The problems fall interactegories:

- 1. Invalid certificate
- 2. Invalid configuration
- 3. Unknown Certificate Authority

1. Invalid certificate

A certificate is invalid if:

- It is used before its activation date
- It is used after its expiry date
- Certificate hostnames don't match the site hostname
- It has been revoked

2. Invalid configuration

In some cases, the certificate chain does not contain all the necessary certificates to connect the web server certificate to one of the root certificate our trust store. Less commonly, one of the certificates in the chain (other than the web server certificate) will have expired, and that invalidates the chain.

3. Unknown Certificate Authority

In order for trust to be established, we must have the root certificate of the signing Certificate Authority in our trust store. SSL Labs does not maint own trust store; instead we use the store maintained by Mozilla.

If we mark a web site as not trusted, that means that the average web user's browser will not trust it either. For certain special groups of users, sur sites can still be secure. For example, if you can securely verify that a self-signed web site is operated by a person you trust, then you can trust this self-signed web site too. Or, if you work for an organisation that manages its own trust, and you have their own root certificate already embedded i browser. Such special cases do not work for the general public, however, and this is what we indicate on our report card.

14.12.2014 13:14 4 von 5

4. Interoperability issues

In some rare cases trust cannot be established because of interoperability issues between our code and the code or configuration running on the seemanually review such cases, but if you encounter such an issue please feel free to contact us. Such problems are very difficult to troubleshoot you may be able to provide us with information that might help us determine the root cause.

SSL Report v1.11.1

Copyright © 2009-2014 Qualys, Inc. All Rights Reserved.

Terms and Con

14.12.2014 13:14 5 von 5