

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

## SSL Report: libreduca.com (192.81.217.8)

Assessed on: Tue Oct 15 13:03:22 UTC 2013 | [Clear cache](#)

[Scan Another »](#)

### Summary

#### Overall Rating

A

Certificate	100
Protocol Support	90
Key Exchange	80
Cipher Strength	90

0   20   40   60   80   100

Documentation: [SSL/TLS Deployment Best Practices](#), [SSL Server Rating Guide](#), and [OpenSSL Cookbook](#).

### Authentication



#### Server Key and Certificate #1

Common names	*.libreduca.com
Alternative names	*.libreduca.com libreduca.com
Prefix handling	Both (with and without WWW)
Valid from	Mon Jan 14 00:00:00 UTC 2013
Valid until	Wed Feb 12 23:59:59 UTC 2014 (expires in 3 months and 30 days)
Key	RSA 2048 bits
Weak key (Debian)	No
Issuer	EssentialSSL CA
Signature algorithm	SHA1withRSA
Extended Validation	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
<b>Trusted</b>	<b>Yes</b>



#### Additional Certificates (if supplied)

Certificates provided	4 (4992 bytes)
Chain issues	None

#### #2

Subject	EssentialSSL CA SHA1: 73820a20f8f47a457cd0b54cc4e4e31cefa5c1e7
Valid until	Tue Dec 31 23:59:59 UTC 2019 (expires in 6 years and 2 months)
Key	RSA 2048 bits
Issuer	COMODO Certification Authority
Signature algorithm	SHA1withRSA

#### #3

<b>Subject</b>	COMODO Certification Authority SHA1: 4e154acb683efd5578001432b92afe896812b85e
<b>Valid until</b>	Sat May 30 10:48:38 UTC 2020 (expires in 6 years and 7 months)
<b>Key</b>	RSA 2048 bits
<b>Issuer</b>	UTN - DATACorp SGC
<b>Signature algorithm</b>	SHA1withRSA

#4

<b>Subject</b>	UTN - DATACorp SGC SHA1: 9e99817d12280c9677674430492eda1dce2e4c63
<b>Valid until</b>	Sat May 30 10:48:38 UTC 2020 (expires in 6 years and 7 months)
<b>Key</b>	RSA 2048 bits
<b>Issuer</b>	AddTrust External CA Root
<b>Signature algorithm</b>	SHA1withRSA



## Certification Paths

### Path #1: Trusted

			*.libreduca.com
1	Sent by server		SHA1: 8ecea8cb7ae8a701bb14e0bdb89276536a6c2ef6 RSA 2048 bits / SHA1withRSA
2	Sent by server		EssentialSSL CA SHA1: 73820a20f8f47a457cd0b54cc4e4e31cefa5c1e7 RSA 2048 bits / SHA1withRSA
3	In trust store		COMODO Certification Authority SHA1: 6631bf9ef74f9eb6c9d5a60cba6abed1f7bdef7b RSA 2048 bits / SHA1withRSA

### Path #2: Trusted

			*.libreduca.com
1	Sent by server		SHA1: 8ecea8cb7ae8a701bb14e0bdb89276536a6c2ef6 RSA 2048 bits / SHA1withRSA
2	Sent by server		EssentialSSL CA SHA1: 73820a20f8f47a457cd0b54cc4e4e31cefa5c1e7 RSA 2048 bits / SHA1withRSA
3	Sent by server		COMODO Certification Authority SHA1: 4e154acb683efd5578001432b92afe896812b85e RSA 2048 bits / SHA1withRSA
4	In trust store		UTN - DATACorp SGC SHA1: 58119f0e128287ea50fdd987456f4f78dcfad6d4 RSA 2048 bits / SHA1withRSA

### Path #3: Trusted

			*.libreduca.com
1	Sent by server		SHA1: 8ecea8cb7ae8a701bb14e0bdb89276536a6c2ef6 RSA 2048 bits / SHA1withRSA
2	Sent by server		EssentialSSL CA SHA1: 73820a20f8f47a457cd0b54cc4e4e31cefa5c1e7 RSA 2048 bits / SHA1withRSA
3	Sent by server		COMODO Certification Authority SHA1: 4e154acb683efd5578001432b92afe896812b85e RSA 2048 bits / SHA1withRSA
4	Sent by server		UTN - DATACorp SGC SHA1: 9e99817d12280c9677674430492eda1dce2e4c63 RSA 2048 bits / SHA1withRSA
5	In trust store		AddTrust External CA Root SHA1: 02faf3e291435468607857694df5e45b68851868 RSA 2048 bits / SHA1withRSA

# Configuration



## Protocols

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



## Cipher Suites (SSL 3+ suites in server-preferred order, then SSL 2 suites where used)

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 1024 bits (p: 128, g: 1, Ys: 128) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 1024 bits (p: 128, g: 1, Ys: 128) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 1024 bits (p: 128, g: 1, Ys: 128) FS	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 1024 bits (p: 128, g: 1, Ys: 128) FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a)	DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_RSA_WITH_RC4_128_SHA (0x5)		128



## Handshake Simulation

<a href="#">Chrome 30 / Win 7</a>	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) FS	256
<a href="#">Firefox 10.0.12 ESR / Win 7</a>	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
<a href="#">Firefox 17.0.7 ESR / Win 7</a>	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
<a href="#">Firefox 21 / Fedora 19</a>	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
<a href="#">Firefox 24 / Win 7</a>	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
<a href="#">IE 6 / XP</a> No FS *	SSL 3	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS	128
<a href="#">IE 7 / Vista</a>	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS	128
<a href="#">IE 8 / XP</a> No FS *	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS	128
<a href="#">IE 8-10 / Win 7</a>	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS	128
<a href="#">IE 11 / Win 8.1</a>			Fail**
<a href="#">Java 6u45</a>	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
<a href="#">Java 7u25</a>	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
<a href="#">OpenSSL 0.9.8y</a>	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
<a href="#">OpenSSL 1.0.1e</a>	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) FS	256
<a href="#">Opera 12.15 / Win 7</a>	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
<a href="#">Opera 16 / Win 7</a>	TLS 1.1	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
<a href="#">Safari 5.1.9 / OS X 10.6.8</a>	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
<a href="#">Safari 6 / iOS 6.0.1</a>	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) FS	256
<a href="#">Safari 6.0.4 / OS X 10.8.4</a>	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
<a href="#">Safari 7 / OS X 10.9</a>	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) FS	256

\* Browsers that do not support Forward Secrecy are excluded when determining support for it.

\*\* Only first connection attempt simulated. Browsers are likely to retry with a lower protocol version or other tweaks.



## Protocol Details

Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No

Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side ( <a href="#">more info</a> ) SSL 3: 0x39, TLS 1.0: 0x39
TLS compression	No
RC4	Yes NOT DESIRABLE ( <a href="#">more info</a> )
Forward Secrecy	With some browsers ( <a href="#">more info</a> )
Next Protocol Negotiation	No
Session resumption	Yes
Session tickets	Yes
OCSP stapling	No
Strict Transport Security	Yes max-age=31536000
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	TLS 2.98
SSL 2 handshake compatibility	Yes



#### Miscellaneous

Test date	Tue Oct 15 13:02:42 UTC 2013
Test duration	40.39 seconds
HTTP status code	200
HTTP server signature	Apache/2.2.22 (Ubuntu)
Server hostname	libreduca.com
PCI compliant	Yes
FIPS-ready	No