TLS Workflow

examples\testClient.c.clientBasicTest()--Line 13

# Initialization

load data\certs\tests\ecpCa.1024.key of type RSA Private Key ....

load data\certs\tests\ecpCa.1024.ca\_x509.pem of type X509 CERT ....

=== CERTIFICATE ISSUED TO ===

Common Name (CN): 127.0.0.1

Organization (O): TLS Zhijie Li Certificate Authority

Organizational Unit (OU): <Not Part Of Certificate>

=== CERTIFICATE ISSUED BY ===

Common Name (CN): 127.0.0.1

Organization (O): TLS Zhijie Li Certificate Authority

Organizational Unit (OU): <Not Part Of Certificate>

Not Before: Wed Nov 18 00:00:00 2015

Not After: Fri Jul 27 00:00:00 2029

RSA bitsize: 1024

Sig Type: SHA1

No.0 Cert of '127.0.0.1' has been added

examples\testClient.c.clientBasicTest()--Line 19

load data\certs\tests\ecpCA.1024.ca\_x509.pem of type X509 CA CERT ....

=== CERTIFICATE ISSUED TO ===

Common Name (CN): 127.0.0.1

Organization (O): TLS Zhijie Li Certificate Authority

Organizational Unit (OU): <Not Part Of Certificate>

=== CERTIFICATE ISSUED BY ===

Common Name (CN): 127.0.0.1

Organization (O): TLS Zhijie Li Certificate Authority

Organizational Unit (OU): <Not Part Of Certificate>

Not Before: Wed Nov 18 00:00:00 2015

Not After: Fri Jul 27 00:00:00 2029

RSA bitsize: 1024

Sig Type: SHA1

Socket is 100

# Handshaking

## State: sending Client Hello (1)

sending 56 bytes

16 03 02 00 33 01 00 00 : 2f 03 02 56 4d 2d 43 c5

19 fb 0a 66 46 d4 b7 d6 : 13 9b 1c 91 60 5a c0 d8

9e 9b 46 4f d2 91 23 0d : 9d 1f 01 00 00 08 00 35

00 2f 00 05 00 04 01 00 :

received 5 bytes

16 03 01 00 4a

received 74 bytes

02 00 00 46 03 01 56 4d : 2d 44 47 11 b6 4b 55 f7

59 98 40 b8 40 58 d0 05 : 02 7d 52 ed c6 da a2 0f

9f 2d 52 8d 46 ac 20 db : b5 ac 29 b3 ec b9 07 2a

10 71 2e 5c 07 f2 c8 f5 : 0f 50 18 a7 7d b7 40 65

46 2f b4 f7 af ad 98 00 : 35 00

ssl\tlsProtocol.c.do\_handshake()--Line 223

## State: receiving Server Hello (2)

ssl\tlsProtocol.c.do\_handshake()--Line 225

received 5 bytes

16 03 01 02 6b

received 619 bytes

0b 00 02 67 00 02 64 00 : 02 61 30 82 02 5d 30 82

01 c6 02 09 00 d9 4c cc : b5 0b b3 28 61 30 0d 06

09 2a 86 48 86 f7 0d 01 : 01 05 05 00 30 73 31 2c

30 2a 06 03 55 04 0a 13 : 23 54 4c 53 20 5a 68 69

6a 69 65 20 4c 69 20 43 : 65 72 74 69 66 69 63 61

74 65 20 41 75 74 68 6f : 72 69 74 79 31 0b 30 09

06 03 55 04 06 13 02 63 : 6e 31 10 30 0e 06 03 55

04 08 13 07 53 69 63 68 : 75 61 6e 31 10 30 0e 06

03 55 04 07 13 07 43 68 : 65 6e 67 64 75 31 12 30

10 06 03 55 04 03 13 09 : 31 32 37 2e 30 2e 30 2e

31 30 1e 17 0d 31 35 31 : 31 31 38 30 38 34 33 34

32 5a 17 0d 32 39 30 37 : 32 37 30 38 34 33 34 32

5a 30 73 31 2c 30 2a 06 : 03 55 04 0a 13 23 54 4c

53 20 5a 68 69 6a 69 65 : 20 4c 69 20 43 65 72 74

69 66 69 63 61 74 65 20 : 41 75 74 68 6f 72 69 74

79 31 0b 30 09 06 03 55 : 04 06 13 02 63 6e 31 10

30 0e 06 03 55 04 08 13 : 07 53 69 63 68 75 61 6e

31 10 30 0e 06 03 55 04 : 07 13 07 43 68 65 6e 67

64 75 31 12 30 10 06 03 : 55 04 03 13 09 31 32 37

2e 30 2e 30 2e 31 30 81 : 9f 30 0d 06 09 2a 86 48

86 f7 0d 01 01 01 05 00 : 03 81 8d 00 30 81 89 02

81 81 00 cd d8 ce 74 ea : b2 ae 6a 13 c3 48 be e9

a1 25 4d 75 8f ef 6a 17 : 4b de 69 b1 ec 6e c6 ed

ea 64 fc 61 d7 c3 09 09 : 0d 18 37 69 b5 7c 41 e8

49 40 19 63 f9 ac 78 07 : 33 db 95 4f 6a 88 24 85

c4 59 f9 b6 f0 0d 5a 3a : 9b 4d a9 ea c7 ad 77 78

c4 bf ef 68 3e 33 79 46 : 0d ab 63 96 02 f4 4c ce

e3 04 89 df f8 e2 6d 3b : 9c fb 45 2d 95 ad 51 4f

7a b2 4d dc a1 61 18 07 : b5 f4 18 4b 9f 58 79 7f

19 8e 0d 02 03 01 00 01 : 30 0d 06 09 2a 86 48 86

f7 0d 01 01 05 05 00 03 : 81 81 00 cd 55 61 a1 1a

f5 bd 29 14 78 83 e9 65 : fd 27 33 31 58 68 fc c3

9c fc 58 59 e6 14 62 e5 : 7a 88 be 23 28 96 99 00

a1 08 be b6 6a b8 98 5f : f0 a0 b8 40 41 a8 72 11

b2 29 18 39 d9 7a f3 97 : 82 28 13 a4 d5 b3 b3 b6

f1 63 83 a2 3e 54 a2 31 : a4 99 76 b1 33 4f d7 0c

8b 3b 44 cd 08 f2 98 59 : 07 82 19 83 4f 63 8d 4f

83 ac 51 4f d6 e8 10 60 : ed eb a0 86 0e 44 6b 4f

13 18 23 90 07 88 66 85 : 68 dd 4c

ssl\tlsProtocol.c.do\_handshake()--Line 223

## State: receiving Certificate (11)

ssl\tlsProtocol.c.do\_handshake()--Line 225

received 5 bytes

16 03 01 00 04

received 4 bytes

0e 00 00 00

ssl\tlsProtocol.c.do\_handshake()--Line 223

## State: receiving Server Hello Done (14)

ssl\tlsProtocol.c.do\_handshake()--Line 225

----------------- RSA DEBUG ----------------

Size: 128

Modulus: (size 32)

CDD8CE74EAB2AE6A13C348BEE9A1254D758FEF6A174BDE69B1EC6EC6EDEA64FC61D7C309090D183769B57C41E849401963F9AC780733DB954F6A882485C459F9B6F00D5A3A9B4DA9EAC7AD7778C4BFEF683E3379460DAB639602F44CCEE30489DFF8E26D3B9CFB452D95AD514F7AB24DDCA1611807B5F4184B9F58797F198E0D

Public Key: (size 1)

00010001

Private Key: (null)

## State: sending Client Key Exchange (16)

sending 139 bytes

16 03 01 00 86 10 00 00 : 82 00 80 5a ad 27 87 73

14 41 1f 34 ea bd 8a 9e : a6 9e 89 21 3d de e6 a7

b3 b0 2d 75 50 6a 24 ca : 5b 2d 69 fb 6d fc 50 9e

2f 1c 6d 73 29 b4 50 e3 : b0 10 ac 98 f6 41 29 6f

bc 24 66 d4 e5 14 89 0e : 1a 52 2d 77 c7 d8 f6 b8

20 58 e3 04 c7 6f 05 2f : ea 61 67 6e 42 e2 28 40

98 30 4c 96 6b 5c d4 af : 5a 1e 4a 51 d1 36 68 fc

e9 d1 32 30 61 1e 4a d5 : 8c 59 e7 3f 91 d0 e6 01

54 a9 cd b2 e4 6d 4b 99 : fe 5d a4

### sending 6 bytes: cipher changed

14 03 01 00 01 01

## State: sending Finished (20)

unencrypted write

14 00 00 0c 6b e8 a1 ff : cd cd 04 06 54 90 4d 70

e5 2b 72 40 f3 0c ba 3c : ee 88 0a a6 d4 c8 50 1f

0f 05 c2 73 0b 0b 0b 0b : 0b 0b 0b 0b 0b 0b 0b 0b

sending 53 bytes

16 03 01 00 30 f4 a9 ae : d0 61 3b b5 44 46 36 e3

7b a3 49 97 71 61 4d 7c : 72 70 18 b6 97 c8 a7 e0

ff 45 e4 fb 35 35 0b b5 : a4 c6 de b8 ce 6e 09 cd

ba 1e 78 ed 29

### received 5 bytes: cipher changed

14 03 01 00 01

received 1 bytes

01

received 5 bytes

16 03 01 00 30

received 48 bytes

87 bd 21 34 c6 92 04 7d : 43 6a 1a 22 f5 c5 e6 86

7e 22 d6 0c 8f 54 1b 02 : 73 40 9d fd 5d c9 61 d2

52 90 3f 2c f3 47 fb 6c : 99 95 7c 93 d2 e2 0a 05

decrypted

14 00 00 0c 61 36 52 9f : a3 02 df c1 92 fc 60 54

ssl\tlsProtocol.c.do\_handshake()--Line 223

## State: receiving Finished (20)

ssl\tlsProtocol.c.do\_handshake()--Line 225

SSL initialized successfully!

# App Data

unencrypted write

47 45 54 20 2f 20 48 54 : 54 50 2f 31 2e 31 0d 0a

95 ce 86 f7 2b 36 6e 96 : b7 57 6f 95 de bc 05 57

4d 2c 0b a3 0b 0b 0b 0b : 0b 0b 0b 0b 0b 0b 0b 0b

sending 53 bytes

17 03 01 00 30 c8 4b 8c : d0 79 dc 8b 6f 7f 4a 50

96 c7 c5 01 bf a4 86 47 : 78 ab b4 63 c2 f4 2f a0

c9 13 46 15 d3 fc 11 f8 : 69 ab 69 6d 2f aa 4c 1a

14 0a 28 fb 50

SSL write "GET / HTTP/1.1

" OK!

received 5 bytes

17 03 01 00 20

the handshaking stage is successful (but not yet complete)

No Error in SSL

unencrypted write

01 00 48 48 22 90 23 cd : 8f f6 42 fd 41 96 87 80

1e 87 e3 d1 89 7e 09 09 : 09 09 09 09 09 09 09 09

sending 37 bytes

15 03 01 00 20 56 ad e7 : bb 86 62 11 84 04 5c 2e

c3 2b 1c 30 6e 2a 25 f6 : c9 b8 07 b2 25 30 b1 77

01 19 e9 4d 91

Alert: close notify