```
URL endpoint created successfully!
keyStore is :
keyStore type is : jks
keyStore provider is :
init keystore
init keymanager of type SunX509
trustStore is: /Users/amusarra/.mykeystore
trustStore type is : jks
trustStore provider is :
init truststore
adding as trusted cert:
  Subject: EMAILADDRESS=info@sugarcrm-fe-1.local, CN=sugarcrm-fe-1.local,
OU=Research Development, O=Shirus Labs Ltd, L=Rome, ST=Italy, C=IT
  Issuer:  EMAILADDRESS=info@shiruslabs.com, CN=www.shiruslabs.com, OU=IT
Systems, O=Shirus Labs Ltd, L=Rome, ST=Italy, C=IT
  Algorithm: RSA; Serial number: 0x1
  Valid from Thu Apr 28 02:18:12 CEST 2011 until Sun Apr 25 02:18:12 CEST
2021

trigger seeding of SecureRandom
done seeding SecureRandom
Allow unsafe renegotiation: false
Allow legacy hello messages: true
Is initial handshake: true
Is secure renegotiation: false
%% No cached client session
*** ClientHello, TLSv1
RandomCookie:  GMT: 1287446936 bytes = { 34, 19, 132, 181, 138, 114, 13, 67,
100, 111, 100, 155, 35, 132, 108, 102, 110, 106, 128, 57, 200, 147, 175, 25,
246, 233, 34, 252 }
Session ID:  {}
Cipher Suites: [SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
SSL_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA, SSL_RSA_WITH_DES_CBC_SHA,
SSL_DHE_RSA_WITH_DES_CBC_SHA, SSL_DHE_DSS_WITH_DES_CBC_SHA,
SSL_RSA_EXPORT_WITH_RC4_40_MD5, SSL_RSA_EXPORT_WITH_DES40_CBC_SHA,
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA, SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA,
TLS_EMPTY_RENEGOTIATION_INFO_SCSV]
Compression Methods:  { 0 }
***
Thread-2, WRITE: TLSv1 Handshake, length = 81
Thread-2, WRITE: SSLv2 client hello message, length = 110
```

```
Thread-2, READ: TLSv1 Handshake, length = 81
*** ServerHello, TLSv1
RandomCookie:  GMT: 1287126586 bytes = { 72, 54, 32, 71, 9, 157, 75, 184, 3,
159, 95, 8, 18, 248, 108, 249, 179, 60, 205, 184, 204, 135, 186, 220, 27, 85,
249, 234 }
Session ID:  {116, 147, 251, 240, 232, 125, 76, 210, 112, 151, 13, 181, 7,
214, 55, 176, 224, 217, 109, 201, 161, 74, 143, 121, 131, 243, 108, 67, 131,
234, 146, 232}
Cipher Suite: SSL_RSA_WITH_RC4_128_MD5
Compression Method: 0
Extension renegotiation_info, renegotiated_connection: <empty>
***
%% Created:  [Session-1, SSL_RSA_WITH_RC4_128_MD5]
** SSL_RSA_WITH_RC4_128_MD5
Thread-2, READ: TLSv1 Handshake, length = 1484
*** Certificate chain
chain [0] = [
[
  Version: V1
  Subject: EMAILADDRESS=info@sugarcrm-fe-1.local, CN=sugarcrm-fe-1.local,
OU=Research Development, O=Shirus Labs Ltd, L=Rome, ST=Italy, C=IT
  Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

  Key:  Sun RSA public key, 4096 bits
  modulus:
802714230918458018116584767702942663321475407800375981542687685293215600656121
211977868607386144844062698688246937923298407285153446352018325441288568133143871701098063532336310820216053399715105612622032427407830794723941723963302907273682201967984685272509448411609722527933446350559182345787458566295153377894098258970302729394298817061344127168891166069762683263953403322683456690224707417994747043827762268738254946094023907269354228758821503477154800689910313169868373935038762384493733844944158526594347039867793168886125221637114334394877543471208465369800232976363757896869482959629581072250271478376575112926349445458843882077114445052819463501568952722155045514538734776188445002502857454917694681233621417881857645356541330488841071724528674484910620105215169603673228870668976871932068203075096708042410230906603195931273852438676954873177986440608690339507570744022558159438767928976115306840998902410402320694963995246588971790315533198527647190475209611866384825702078042819354402551004610162199323012226779732141407194344432372383268185097381400232343186482950313649466428536782071581307192341158124421774224993248878094539282273493316490283128955290329155517864737950489642654212817648893242550734840 47
  public exponent: 65537
  Validity: [From: Thu Apr 28 02:18:12 CEST 2011,
               To: Sun Apr 25 02:18:12 CEST 2021]
  Issuer: EMAILADDRESS=info@shiruslabs.com, CN=www.shiruslabs.com, OU=IT
```

```
Systems, O=Shirus Labs Ltd, L=Rome, ST=Italy, C=IT
  SerialNumber: [    01]

]
  Algorithm: [SHA1withRSA]
  Signature:
0000: A7 FC 8F 20 D4 3C 1B BD   1C 46 77 CC 60 6D 1A CA  ... .<...Fw.`m..
0010: 94 6F 69 7A C4 01 92 97   F6 B7 D0 E1 43 A1 76 8D  .oiz........C.v.
0020: C6 93 BE 67 38 09 5D 43   F7 A3 98 80 D5 9B 77 A0  ...g8.]C......w.
0030: C9 00 D6 C7 52 98 54 BB   2F 9C 4B D1 5A 20 C7 06  ....R.T./.K.Z ..
0040: FA 2F 49 FA 83 4B 20 E2   83 05 30 2A A5 5A 7E 0E  ./I..K ...0*.Z..
0050: F8 72 2B C6 50 E1 11 CF   12 36 F3 17 53 BB 74 F4  .r+.P....6..S.t.
0060: F2 94 5D C4 52 8C 4F 19   4D C5 B8 D5 73 7B DE A8  ..].R.O.M...s...
0070: 19 1A E5 60 88 A6 BF E7   6F C2 C6 46 30 6D 49 0E  ...`....o..F0mI.
0080: 6E E2 B2 05 1C 59 99 88   7A 98 9F CC 1A 32 49 DB  n....Y..z....2I.
0090: 5F 86 85 B7 44 72 1A E2   F6 FD 3B 0D 9A 05 76 E5  _...Dr....;...v.
00A0: 7A CA BF 99 15 35 E5 25   45 A6 5D 90 66 66 FF DB  z....5.%E.].ff..
00B0: 2F 8C 67 7B 30 49 99 37   C1 3A CE 4C 0E 27 2B 5E  /.g.0I.7.:.L.'+^
00C0: F4 61 4A DE C5 83 58 9E   DE C8 65 93 28 AB FD 7D  .aJ...X...e.(...
00D0: 79 19 E4 E1 EF E5 64 8A   CF DA 71 92 09 C1 E4 DE  y.....d...q.....
00E0: 8C A2 36 02 D6 E9 80 01   6B 89 D3 58 95 76 D6 77  ..6.....k..X.v.w
00F0: 0E FB 73 FA 09 C2 E2 50   D1 7D D7 76 BA 8B FA FD  ..s....P...v....
0100: 8B E8 9F C2 39 28 02 4E   69 E4 EC 7A DE 78 66 92  ....9(.Ni..z.xf.
0110: 9A AB C9 46 21 73 E0 B9   F8 C8 22 22 A2 D0 E6 36  ...F!s....""...6
0120: 1F FF 7D 1D 60 B6 48 41   77 77 48 03 9E B1 73 7F  ....`.HAwwH...s.
0130: 60 95 07 59 17 77 4B BE   C2 33 C8 88 71 7B 03 88  `..Y.wK..3..q...
0140: 2A 45 38 9D 86 83 82 76   16 06 63 C0 5A 44 22 B7  *E8....v..c.ZD".
0150: B6 BC 2A FC D3 49 BD BB   BF 68 AF 8D 73 BC 50 63  ..*..I...h..s.Pc
0160: AC 98 64 15 56 E1 90 69   A0 5A 1B BF 55 04 54 ED  ..d.V..i.Z..U.T.
0170: 84 F9 69 8A 1E 8A 28 F7   4A A0 15 2B 0C 5F 05 8F  ..i...(.J..+._..
0180: 83 4C 0A B3 2B 05 3F 90   A2 B8 12 3D 4E 8F 4B E9  .L..+.?....=N.K.
0190: E1 70 E1 95 A4 B9 49 6C   A3 80 28 C5 53 08 7D 8E  .p....Il..(.S...
01A0: D3 DD 03 76 AD 9F E6 EB   A9 F3 D2 8E 5D 6B DD 49  ...v........]k.I
01B0: 50 B3 16 C3 84 5F D2 14   DF BC EE 40 C5 95 19 62  P...._.....@...b
01C0: F2 35 78 CC 7F E6 FD 6D   5A 42 39 86 B1 44 EA BD  .5x....mZB9..D..
01D0: 02 CA 41 23 08 A3 9B 98   7D 5F 58 B4 51 71 3B 6E  ..A#....._X.Qq;n
01E0: 32 5F 06 BF 64 C1 5A 8A   0B 6F 51 8F B7 21 46 A5  2_..d.Z..oQ..!F.
01F0: F9 A4 17 DB FB 9C E4 D8   CD D4 72 E1 43 AD 61 65  ..........r.C.ae

]
***
Found trusted certificate:
[
[
  Version: V1
```

```
  Subject: EMAILADDRESS=info@sugarcrm-fe-1.local, CN=sugarcrm-fe-1.local,
OU=Research Development, O=Shirus Labs Ltd, L=Rome, ST=Italy, C=IT
  Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

  Key:  Sun RSA public key, 4096 bits
  modulus:
802714230918458018116584767702942663321475407800375981542687685293215600656121
211977868607386144844062698688246937923298407285153446352018325441288568133143871701098063532336310820216053399715105612622032427407830794723941723963302907273682201967984685272509448411609722527933446350559182345787458566295153377894098258970302729394298817061344127168891166069762683263953403322683456690224707417994747043827762268738254946094023907269354228758821503477154800689910313169868373935038762384493733844944158526594347039867793168886125221637114334394877543471208465369800232976363757896869482959629581072250271478376575112926349445458843882077114445052819463501568952722155045514538734776188445002502857459176946812336214178818576453565413304888410717245286744849106201052151696036732288706689768719320682030750967080424102309066031959312738524386769548731779864406086903395075707440225581594387679289761153068409989024104023206949639952465889717903155331985276471904752096118663848257020780428193544025510046101621993230122267797321414071943444323723832681850973814002323431864829503136494664285367820715813071923411581244217742249932488780945392822734933164902831289552903291555178647379504896426542128176488932425507348404 7
  public exponent: 65537
  Validity: [From: Thu Apr 28 02:18:12 CEST 2011,
              To: Sun Apr 25 02:18:12 CEST 2021]
  Issuer: EMAILADDRESS=info@shiruslabs.com, CN=www.shiruslabs.com, OU=IT
Systems, O=Shirus Labs Ltd, L=Rome, ST=Italy, C=IT
  SerialNumber: [    01]

]
  Algorithm: [SHA1withRSA]
  Signature:
0000: A7 FC 8F 20 D4 3C 1B BD   1C 46 77 CC 60 6D 1A CA  ... .<...Fw.`m..
0010: 94 6F 69 7A C4 01 92 97   F6 B7 D0 E1 43 A1 76 8D  .oiz........C.v.
0020: C6 93 BE 67 38 09 5D 43   F7 A3 98 80 D5 9B 77 A0  ...g8.]C......w.
0030: C9 00 D6 C7 52 98 54 BB   2F 9C 4B D1 5A 20 C7 06  ....R.T./.K.Z ..
0040: FA 2F 49 FA 83 4B 20 E2   83 05 30 2A A5 5A 7E 0E  ./I..K ...0*.Z..
0050: F8 72 2B C6 50 E1 11 CF   12 36 F3 17 53 BB 74 F4  .r+.P....6..S.t.
0060: F2 94 5D C4 52 8C 4F 19   4D C5 B8 D5 73 7B DE A8  ..].R.O.M...s...
0070: 19 1A E5 60 88 A6 BF E7   6F C2 C6 46 30 6D 49 0E  ...`....o..F0mI.
0080: 6E E2 B2 05 1C 59 99 88   7A 98 9F CC 1A 32 49 DB  n....Y..z....2I.
0090: 5F 86 85 B7 44 72 1A E2   F6 FD 3B 0D 9A 05 76 E5  _...Dr....;...v.
00A0: 7A CA BF 99 15 35 E5 25   45 A6 5D 90 66 66 FF DB  z....5.%E.].ff..
00B0: 2F 8C 67 7B 30 49 99 37   C1 3A CE 4C 0E 27 2B 5E  /.g.0I.7.:.L.'+^
00C0: F4 61 4A DE C5 83 58 9E   DE C8 65 93 28 AB FD 7D  .aJ...X...e.(...
```

```
00D0: 79 19 E4 E1 EF E5 64 8A   CF DA 71 92 09 C1 E4 DE  y.....d...q.....
00E0: 8C A2 36 02 D6 E9 80 01   6B 89 D3 58 95 76 D6 77  ..6.....k..X.v.w
00F0: 0E FB 73 FA 09 C2 E2 50   D1 7D D7 76 BA 8B FA FD  ..s....P...v....
0100: 8B E8 9F C2 39 28 02 4E   69 E4 EC 7A DE 78 66 92  ....9(.Ni..z.xf.
0110: 9A AB C9 46 21 73 E0 B9   F8 C8 22 22 A2 D0 E6 36  ...F!s...""...6
0120: 1F FF 7D 1D 60 B6 48 41   77 77 48 03 9E B1 73 7F  ....`.HAwwH...s.
0130: 60 95 07 59 17 77 4B BE   C2 33 C8 88 71 7B 03 88  `..Y.wK..3..q...
0140: 2A 45 38 9D 86 83 82 76   16 06 63 C0 5A 44 22 B7  *E8....v..c.ZD".
0150: B6 BC 2A FC D3 49 BD BB   BF 68 AF 8D 73 BC 50 63  ..*..I...h..s.Pc
0160: AC 98 64 15 56 E1 90 69   A0 5A 1B BF 55 04 54 ED  ..d.V..i.Z..U.T.
0170: 84 F9 69 8A 1E 8A 28 F7   4A A0 15 2B 0C 5F 05 8F  ..i...(.J..+._..
0180: 83 4C 0A B3 2B 05 3F 90   A2 B8 12 3D 4E 8F 4B E9  .L..+.?....=N.K.
0190: E1 70 E1 95 A4 B9 49 6C   A3 80 28 C5 53 08 7D 8E  .p....Il..(.S...
01A0: D3 DD 03 76 AD 9F E6 EB   A9 F3 D2 8E 5D 6B DD 49  ...v........]k.I
01B0: 50 B3 16 C3 84 5F D2 14   DF BC EE 40 C5 95 19 62  P...._.....@...b
01C0: F2 35 78 CC 7F E6 FD 6D   5A 42 39 86 B1 44 EA BD  .5x....mZB9..D..
01D0: 02 CA 41 23 08 A3 9B 98   7D 5F 58 B4 51 71 3B 6E  ..A#....._X.Qq;n
01E0: 32 5F 06 BF 64 C1 5A 8A   0B 6F 51 8F B7 21 46 A5  2_..d.Z..oQ..!F.
01F0: F9 A4 17 DB FB 9C E4 D8   CD D4 72 E1 43 AD 61 65  ..........r.C.ae

]
Thread-2, READ: TLSv1 Handshake, length = 4
*** ServerHelloDone
*** ClientKeyExchange, RSA PreMasterSecret, TLSv1
Thread-2, WRITE: TLSv1 Handshake, length = 518
SESSION KEYGEN:
PreMaster Secret:
0000: 03 01 D7 20 9E F9 05 4C   9A 9A 72 DB CF 8F C2 52  ... ...L..r....R
0010: A3 02 DE 33 AD 1E B9 8D   13 28 02 39 80 18 A8 22  ...3.....(.9..."
0020: 80 D6 7D DE 46 78 58 AB   11 44 1B E3 0A 10 E2 1D  ....FxX..D......
CONNECTION KEYGEN:
Client Nonce:
0000: 4D BD E2 98 22 13 84 B5   8A 72 0D 43 64 6F 64 9B  M..."....r.Cdod.
0010: 23 84 6C 66 6E 6A 80 39   C8 93 AF 19 F6 E9 22 FC  #.lfnj.9......".
Server Nonce:
0000: 4D B8 FE 3A 48 36 20 47   09 9D 4B B8 03 9F 5F 08  M..:H6 G..K..._.
0010: 12 F8 6C F9 B3 3C CD B8   CC 87 BA DC 1B 55 F9 EA  ..l..<.......U..
Master Secret:
0000: 26 BF 4D 81 2F 1F 91 DB   A6 3B 77 68 6E 88 18 FF  &.M./....;whn...
0010: 5D 36 6E E5 54 5E 43 C4   77 BF 56 07 58 6F 53 BB  ]6n.T^C.w.V.XoS.
0020: 79 F9 2C 6B BB 6F B0 2F   F2 9A D3 C0 C1 BC EF 12  y.,k.o./........
Client MAC write Secret:
0000: CD EF B9 9D A7 61 A0 83   43 F4 EB 24 89 42 00 4E  .....a..C..$.B.N
Server MAC write Secret:
0000: FB 77 37 EC 24 FE 93 73   6C 65 80 13 73 A1 E8 1D  .w7.$..sle..s...
```

```
Client write key:
0000: 79 88 9E 31 CA DA 31 64   96 CB B9 93 53 20 60 88  y..1..1d....S `.
Server write key:
0000: 0C 1B BB DA E2 40 C1 1E   A4 AA 4E E9 37 35 E3 A7  .....@....N.75..
... no IV used for this cipher
Thread-2, WRITE: TLSv1 Change Cipher Spec, length = 1
*** Finished
verify_data:  { 248, 73, 115, 146, 19, 252, 146, 81, 19, 230, 223, 26 }
***
Thread-2, WRITE: TLSv1 Handshake, length = 32
Thread-2, READ: TLSv1 Change Cipher Spec, length = 1
Thread-2, READ: TLSv1 Handshake, length = 32
*** Finished
verify_data:  { 42, 162, 11, 228, 180, 2, 86, 88, 90, 189, 183, 180 }
***
%% Cached client session: [Session-1, SSL_RSA_WITH_RC4_128_MD5]
Thread-2, WRITE: TLSv1 Application Data, length = 206
Thread-2, READ: TLSv1 Application Data, length = 333
Thread-2, READ: TLSv1 Application Data, length = 22
Thread-2, READ: TLSv1 Application Data, length = 16400
Thread-2, READ: TLSv1 Application Data, length = 14967
Thread-2, READ: TLSv1 Application Data, length = 18
Thread-2, READ: TLSv1 Application Data, length = 21
{http://schemas.xmlsoap.org/soap/encoding/}Struct already exists
Service created successfully
Service Name:{http://www.sugarcrm.com/sugarcrm}sugarsoap
Service WSDL:https://sugarcrm-fe-1.local/crm-6.1/service/v2/soap.php?wsdl
Stub created successfully!
Allow unsafe renegotiation: false
Allow legacy hello messages: true
Is initial handshake: true
Is secure renegotiation: false
%% Client cached [Session-1, SSL_RSA_WITH_RC4_128_MD5]
%% Try resuming [Session-1, SSL_RSA_WITH_RC4_128_MD5] from port 51067
*** ClientHello, TLSv1
RandomCookie:  GMT: 1287446941 bytes = { 156, 31, 237, 238, 20, 247, 126, 1,
114, 12, 131, 99, 36, 218, 44, 143, 10, 108, 120, 57, 212, 4, 9, 216, 76, 93,
127, 99 }
Session ID:  {116, 147, 251, 240, 232, 125, 76, 210, 112, 151, 13, 181, 7,
214, 55, 176, 224, 217, 109, 201, 161, 74, 143, 121, 131, 243, 108, 67, 131,
234, 146, 232}
Cipher Suites: [SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
```

```
SSL_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA, SSL_RSA_WITH_DES_CBC_SHA,
SSL_DHE_RSA_WITH_DES_CBC_SHA, SSL_DHE_DSS_WITH_DES_CBC_SHA,
SSL_RSA_EXPORT_WITH_RC4_40_MD5, SSL_RSA_EXPORT_WITH_DES40_CBC_SHA,
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA, SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA,
TLS_EMPTY_RENEGOTIATION_INFO_SCSV]
Compression Methods:  { 0 }
***
main, WRITE: TLSv1 Handshake, length = 113
main, READ: TLSv1 Handshake, length = 81
*** ServerHello, TLSv1
RandomCookie:  GMT: 1287126592 bytes = { 59, 0, 159, 48, 111, 114, 32, 53,
245, 23, 24, 61, 110, 160, 108, 13, 207, 137, 36, 28, 235, 198, 108, 91, 12,
248, 166, 30 }
Session ID:  {116, 147, 251, 240, 232, 125, 76, 210, 112, 151, 13, 181, 7,
214, 55, 176, 224, 217, 109, 201, 161, 74, 143, 121, 131, 243, 108, 67, 131,
234, 146, 232}
Cipher Suite: SSL_RSA_WITH_RC4_128_MD5
Compression Method: 0
Extension renegotiation_info, renegotiated_connection: <empty>
***
CONNECTION KEYGEN:
Client Nonce:
0000: 4D BD E2 9D 9C 1F ED EE   14 F7 7E 01 72 0C 83 63  M...........r..c
0010: 24 DA 2C 8F 0A 6C 78 39   D4 04 09 D8 4C 5D 7F 63  $.,..lx9....L].c
Server Nonce:
0000: 4D B8 FE 40 3B 00 9F 30   6F 72 20 35 F5 17 18 3D  M..@;..0or 5...=
0010: 6E A0 6C 0D CF 89 24 1C   EB C6 6C 5B 0C F8 A6 1E  n.l...$...l[....
Master Secret:
0000: 26 BF 4D 81 2F 1F 91 DB   A6 3B 77 68 6E 88 18 FF  &.M./....;whn...
0010: 5D 36 6E E5 54 5E 43 C4   77 BF 56 07 58 6F 53 BB  ]6n.T^C.w.V.XoS.
0020: 79 F9 2C 6B BB 6F B0 2F   F2 9A D3 C0 C1 BC EF 12  y.,k.o./........
Client MAC write Secret:
0000: 55 F0 D1 29 86 D3 C9 60   5D DE F7 57 DF 84 12 67  U..)...`]..W...g
Server MAC write Secret:
0000: 23 EE 01 E7 4D A4 1C 19   95 FE 9B 73 83 80 A2 50  #...M......s...P
Client write key:
0000: 6E DA 15 8B 76 4A 88 60   29 85 71 66 BB CB B2 8E  n...vJ.`).qf....
Server write key:
0000: 83 45 D6 37 0C 13 53 41   AB 7A 83 2E F5 75 B9 DA  .E.7..SA.z...u..
... no IV used for this cipher
%% Server resumed [Session-1, SSL_RSA_WITH_RC4_128_MD5]
main, READ: TLSv1 Change Cipher Spec, length = 1
main, READ: TLSv1 Handshake, length = 32
*** Finished
```

```
verify_data:  { 78, 93, 50, 140, 190, 127, 121, 19, 29, 90, 155, 186 }
***
main, WRITE: TLSv1 Change Cipher Spec, length = 1
*** Finished
verify_data:  { 131, 61, 150, 52, 81, 123, 75, 64, 140, 1, 204, 200 }
***
main, WRITE: TLSv1 Handshake, length = 32
main, setSoTimeout(6000) called
main, WRITE: TLSv1 Application Data, length = 1292
main, READ: TLSv1 Application Data, length = 516
main, READ: TLSv1 Application Data, length = 1441
main, READ: TLSv1 Alert, length = 18
main, RECV TLSv1 ALERT:  warning, close_notify
main, called closeInternal(false)
main, SEND TLSv1 ALERT:  warning, description = close_notify
main, WRITE: TLSv1 Alert, length = 18
main, called close()
main, called closeInternal(true)
main, called close()
main, called closeInternal(true)
Login Successfully for will
Your session Id: m6k42b59c91ft5aiegop216g62
Allow unsafe renegotiation: false
Allow legacy hello messages: true
Is initial handshake: true
Is secure renegotiation: false
%% Client cached [Session-1, SSL_RSA_WITH_RC4_128_MD5]
%% Try resuming [Session-1, SSL_RSA_WITH_RC4_128_MD5] from port 51068
*** ClientHello, TLSv1
RandomCookie:  GMT: 1287446941 bytes = { 136, 168, 46, 17, 86, 226, 239, 249,
113, 71, 222, 230, 36, 234, 239, 166, 52, 28, 170, 30, 235, 129, 46, 156,
229, 154, 96, 191 }
Session ID:  {116, 147, 251, 240, 232, 125, 76, 210, 112, 151, 13, 181, 7,
214, 55, 176, 224, 217, 109, 201, 161, 74, 143, 121, 131, 243, 108, 67, 131,
234, 146, 232}
Cipher Suites: [SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
SSL_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA, SSL_RSA_WITH_DES_CBC_SHA,
SSL_DHE_RSA_WITH_DES_CBC_SHA, SSL_DHE_DSS_WITH_DES_CBC_SHA,
SSL_RSA_EXPORT_WITH_RC4_40_MD5, SSL_RSA_EXPORT_WITH_DES40_CBC_SHA,
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA, SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA,
TLS_EMPTY_RENEGOTIATION_INFO_SCSV]
```

```
Compression Methods:  { 0 }
***
main, WRITE: TLSv1 Handshake, length = 113
main, READ: TLSv1 Handshake, length = 81
*** ServerHello, TLSv1
RandomCookie:  GMT: 1287126592 bytes = { 238, 227, 49, 131, 54, 23, 69, 103,
216, 48, 144, 58, 81, 157, 29, 241, 0, 70, 43, 66, 186, 113, 57, 122, 142,
136, 92, 218 }
Session ID:  {116, 147, 251, 240, 232, 125, 76, 210, 112, 151, 13, 181, 7,
214, 55, 176, 224, 217, 109, 201, 161, 74, 143, 121, 131, 243, 108, 67, 131,
234, 146, 232}
Cipher Suite: SSL_RSA_WITH_RC4_128_MD5
Compression Method: 0
Extension renegotiation_info, renegotiated_connection: <empty>
***
CONNECTION KEYGEN:
Client Nonce:
0000: 4D BD E2 9D 88 A8 2E 11   56 E2 EF F9 71 47 DE E6  M.......V...qG..
0010: 24 EA EF A6 34 1C AA 1E   EB 81 2E 9C E5 9A 60 BF  $...4.........`.
Server Nonce:
0000: 4D B8 FE 40 EE E3 31 83   36 17 45 67 D8 30 90 3A  M..@..1.6.Eg.0.:
0010: 51 9D 1D F1 00 46 2B 42   BA 71 39 7A 8E 88 5C DA  Q....F+B.q9z..\.
Master Secret:
0000: 26 BF 4D 81 2F 1F 91 DB   A6 3B 77 68 6E 88 18 FF  &.M./....;whn...
0010: 5D 36 6E E5 54 5E 43 C4   77 BF 56 07 58 6F 53 BB  ]6n.T^C.w.V.XoS.
0020: 79 F9 2C 6B BB 6F B0 2F   F2 9A D3 C0 C1 BC EF 12  y.,k.o./........
Client MAC write Secret:
0000: 08 EB 15 23 69 D1 CC F9   F9 29 6E 12 E7 68 93 14  ...#i....)n..h..
Server MAC write Secret:
0000: EB AC 2A 3A 0E 1B 92 02   79 8E B2 67 98 C8 E9 34  ..*:....y..g...4
Client write key:
0000: 9C D2 67 2F 93 B4 10 79   5A 7D 67 AA 8D E2 5A 41  ..g/...yZ.g...ZA
Server write key:
0000: BF 2D F2 7C 9E F8 3F B2   64 F1 D8 1B DE 54 03 2A  .-....?.d....T.*
... no IV used for this cipher
%% Server resumed [Session-1, SSL_RSA_WITH_RC4_128_MD5]
main, READ: TLSv1 Change Cipher Spec, length = 1
main, READ: TLSv1 Handshake, length = 32
*** Finished
verify_data:  { 88, 212, 157, 254, 6, 206, 207, 7, 233, 181, 185, 89 }
***
main, WRITE: TLSv1 Change Cipher Spec, length = 1
*** Finished
verify_data:  { 205, 0, 191, 132, 179, 165, 106, 119, 49, 94, 0, 154 }
***
```

```
main, WRITE: TLSv1 Handshake, length = 32
main, setSoTimeout(6000) called
main, WRITE: TLSv1 Application Data, length = 2914
main, READ: TLSv1 Application Data, length = 515
main, READ: TLSv1 Application Data, length = 665
main, READ: TLSv1 Alert, length = 18
main, RECV TLSv1 ALERT:  warning, close_notify
main, called closeInternal(false)
main, SEND TLSv1 ALERT:  warning, description = close_notify
main, WRITE: TLSv1 Alert, length = 18
main, called close()
main, called closeInternal(true)
main, called close()
main, called closeInternal(true)
Set entry was successful! Contacts Id: 9fb6aa6c-139f-9bdc-98ec-4db8fe9de9f8
Allow unsafe renegotiation: false
Allow legacy hello messages: true
Is initial handshake: true
Is secure renegotiation: false
%% Client cached [Session-1, SSL_RSA_WITH_RC4_128_MD5]
%% Try resuming [Session-1, SSL_RSA_WITH_RC4_128_MD5] from port 51069
*** ClientHello, TLSv1
RandomCookie:  GMT: 1287446941 bytes = { 187, 6, 29, 52, 50, 215, 202, 72,
184, 99, 32, 195, 207, 80, 55, 15, 237, 133, 72, 185, 60, 211, 194, 155, 182,
145, 76, 165 }
Session ID:  {116, 147, 251, 240, 232, 125, 76, 210, 112, 151, 13, 181, 7,
214, 55, 176, 224, 217, 109, 201, 161, 74, 143, 121, 131, 243, 108, 67, 131,
234, 146, 232}
Cipher Suites: [SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
SSL_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA, SSL_RSA_WITH_DES_CBC_SHA,
SSL_DHE_RSA_WITH_DES_CBC_SHA, SSL_DHE_DSS_WITH_DES_CBC_SHA,
SSL_RSA_EXPORT_WITH_RC4_40_MD5, SSL_RSA_EXPORT_WITH_DES40_CBC_SHA,
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA, SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA,
TLS_EMPTY_RENEGOTIATION_INFO_SCSV]
Compression Methods:  { 0 }
***
main, WRITE: TLSv1 Handshake, length = 113
main, READ: TLSv1 Handshake, length = 81
*** ServerHello, TLSv1
RandomCookie:  GMT: 1287126592 bytes = { 120, 81, 44, 153, 69, 184, 42, 156,
17, 40, 36, 194, 89, 129, 249, 56, 34, 158, 85, 49, 112, 28, 147, 140, 210,
```

```
80, 171, 110 }
Session ID:  {116, 147, 251, 240, 232, 125, 76, 210, 112, 151, 13, 181, 7,
214, 55, 176, 224, 217, 109, 201, 161, 74, 143, 121, 131, 243, 108, 67, 131,
234, 146, 232}
Cipher Suite: SSL_RSA_WITH_RC4_128_MD5
Compression Method: 0
Extension renegotiation_info, renegotiated_connection: <empty>
***
CONNECTION KEYGEN:
Client Nonce:
0000: 4D BD E2 9D BB 06 1D 34   32 D7 CA 48 B8 63 20 C3  M......42..H.c .
0010: CF 50 37 0F ED 85 48 B9   3C D3 C2 9B B6 91 4C A5  .P7...H.<.....L.
Server Nonce:
0000: 4D B8 FE 40 78 51 2C 99   45 B8 2A 9C 11 28 24 C2  M..@xQ,.E.*..($.
0010: 59 81 F9 38 22 9E 55 31   70 1C 93 8C D2 50 AB 6E  Y..8".U1p....P.n
Master Secret:
0000: 26 BF 4D 81 2F 1F 91 DB   A6 3B 77 68 6E 88 18 FF  &.M./....;whn...
0010: 5D 36 6E E5 54 5E 43 C4   77 BF 56 07 58 6F 53 BB  ]6n.T^C.w.V.XoS.
0020: 79 F9 2C 6B BB 6F B0 2F   F2 9A D3 C0 C1 BC EF 12  y.,k.o./........
Client MAC write Secret:
0000: 25 96 59 72 3C 9C 86 F7   D1 AE 0E 81 FC 1A 1A 1D  %.Yr<...........
Server MAC write Secret:
0000: 1F 4C 22 DD 34 7F FC AF   84 43 54 F4 47 CF 64 B9  .L".4....CT.G.d.
Client write key:
0000: 8D 0E C1 7A A3 BC 55 03   DD 66 58 95 EC D0 78 93  ...z..U..fX...x.
Server write key:
0000: 7B E1 D9 DF 9A 14 CF 8F   1E 1F E8 A9 94 5E 67 30  .............^g0
... no IV used for this cipher
Finalizer, called close()
%% Server resumed [Session-1, SSL_RSA_WITH_RC4_128_MD5]
Finalizer, called closeInternal(true)
main, READ: TLSv1 Change Cipher Spec, length = 1
Finalizer, called close()
Finalizer, called closeInternal(true)
main, READ: TLSv1 Handshake, length = 32
*** Finished
verify_data:  { 131, 224, 84, 17, 208, 74, 154, 188, 26, 181, 88, 40 }
***
main, WRITE: TLSv1 Change Cipher Spec, length = 1
*** Finished
verify_data:  { 81, 46, 153, 83, 211, 240, 217, 109, 79, 243, 191, 30 }
***
main, WRITE: TLSv1 Handshake, length = 32
main, setSoTimeout(6000) called
main, WRITE: TLSv1 Application Data, length = 1113
```

```
main, READ: TLSv1 Application Data, length = 516
main, READ: TLSv1 Application Data, length = 6895
main, READ: TLSv1 Alert, length = 18
main, RECV TLSv1 ALERT:  warning, close_notify
main, called closeInternal(false)
main, SEND TLSv1 ALERT:  warning, description = close_notify
main, WRITE: TLSv1 Alert, length = 18
main, called close()
main, called closeInternal(true)
main, called close()
main, called closeInternal(true)
Get entry was successful! Response:
Attribute Name: 'modified_by_name' Attribute Value: 'Will Westin'
Attribute Name: 'created_by_name' Attribute Value: 'Will Westin'
Attribute Name: 'id' Attribute Value: '9fb6aa6c-139f-9bdc-98ec-4db8fe9de9f8'
Attribute Name: 'date_entered' Attribute Value: '2011-04-28 05:42:24'
Attribute Name: 'date_modified' Attribute Value: '2011-04-28 05:42:24'
Attribute Name: 'modified_user_id' Attribute Value: 'seed_will_id'
Attribute Name: 'created_by' Attribute Value: 'seed_will_id'
Attribute Name: 'description' Attribute Value: 'Contatto creato dal Client
SOAP Java'
Attribute Name: 'deleted' Attribute Value: '0'
Attribute Name: 'first_name' Attribute Value: 'Antonio'
Attribute Name: 'last_name' Attribute Value: 'Musarra'
Attribute Name: 'title' Attribute Value: 'IT Senior Consultant'
Attribute Name: 'do_not_call' Attribute Value: '0'
Attribute Name: 'email1' Attribute Value: 'antonio.musarra@gmail.com'
Allow unsafe renegotiation: false
Allow legacy hello messages: true
Is initial handshake: true
Is secure renegotiation: false
%% Client cached [Session-1, SSL_RSA_WITH_RC4_128_MD5]
%% Try resuming [Session-1, SSL_RSA_WITH_RC4_128_MD5] from port 51070
*** ClientHello, TLSv1
RandomCookie:  GMT: 1287446941 bytes = { 118, 63, 47, 44, 122, 185, 21, 112,
240, 73, 193, 20, 53, 67, 94, 219, 110, 230, 218, 67, 25, 84, 84, 214, 199,
97, 137, 247 }
Session ID:  {116, 147, 251, 240, 232, 125, 76, 210, 112, 151, 13, 181, 7,
214, 55, 176, 224, 217, 109, 201, 161, 74, 143, 121, 131, 243, 108, 67, 131,
234, 146, 232}
Cipher Suites: [SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
SSL_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,
```

```
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA, SSL_RSA_WITH_DES_CBC_SHA,
SSL_DHE_RSA_WITH_DES_CBC_SHA, SSL_DHE_DSS_WITH_DES_CBC_SHA,
SSL_RSA_EXPORT_WITH_RC4_40_MD5, SSL_RSA_EXPORT_WITH_DES40_CBC_SHA,
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA, SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA,
TLS_EMPTY_RENEGOTIATION_INFO_SCSV]
Compression Methods:  { 0 }
***
main, WRITE: TLSv1 Handshake, length = 113
main, READ: TLSv1 Handshake, length = 81
*** ServerHello, TLSv1
RandomCookie:  GMT: 1287126592 bytes = { 24, 50, 169, 209, 155, 125, 235, 99,
69, 134, 81, 138, 222, 193, 203, 56, 150, 103, 176, 46, 13, 67, 241, 220, 49,
207, 195, 210 }
Session ID:  {116, 147, 251, 240, 232, 125, 76, 210, 112, 151, 13, 181, 7,
214, 55, 176, 224, 217, 109, 201, 161, 74, 143, 121, 131, 243, 108, 67, 131,
234, 146, 232}
Cipher Suite: SSL_RSA_WITH_RC4_128_MD5
Compression Method: 0
Extension renegotiation_info, renegotiated_connection: <empty>
***
CONNECTION KEYGEN:
Client Nonce:
0000: 4D BD E2 9D 76 3F 2F 2C   7A B9 15 70 F0 49 C1 14  M...v?/,z..p.I..
0010: 35 43 5E DB 6E E6 DA 43   19 54 54 D6 C7 61 89 F7  5C^.n..C.TT..a..
Server Nonce:
0000: 4D B8 FE 40 18 32 A9 D1   9B 7D EB 63 45 86 51 8A  M..@.2.....cE.Q.
0010: DE C1 CB 38 96 67 B0 2E   0D 43 F1 DC 31 CF C3 D2  ...8.g...C..1...
Master Secret:
0000: 26 BF 4D 81 2F 1F 91 DB   A6 3B 77 68 6E 88 18 FF  &.M./....;whn...
0010: 5D 36 6E E5 54 5E 43 C4   77 BF 56 07 58 6F 53 BB  ]6n.T^C.w.V.XoS.
0020: 79 F9 2C 6B BB 6F B0 2F   F2 9A D3 C0 C1 BC EF 12  y.,k.o./........
Client MAC write Secret:
0000: AB 4B DF 03 BD 9D 36 99   88 C4 CC F5 30 F7 3E C5  .K....6.....0.>.
Server MAC write Secret:
0000: 0E 27 5F 14 8F 6F 14 79   E1 70 E0 23 94 70 AE A3  .'_..o.y.p.#.p..
Client write key:
0000: 3B 11 15 8C A7 B5 85 61   B9 44 F2 FA D8 9A 06 BF  ;......a.D......
Server write key:
0000: 09 75 A2 8B C0 D6 B7 BE   4A 20 63 B5 F7 A5 54 F2  .u......J c...T.
... no IV used for this cipher
%% Server resumed [Session-1, SSL_RSA_WITH_RC4_128_MD5]
main, READ: TLSv1 Change Cipher Spec, length = 1
main, READ: TLSv1 Handshake, length = 32
*** Finished
verify_data:  { 118, 98, 192, 246, 14, 44, 31, 60, 243, 216, 79, 47 }
```

```
***
main, WRITE: TLSv1 Change Cipher Spec, length = 1
*** Finished
verify_data:  { 225, 248, 27, 214, 230, 245, 244, 145, 99, 173, 205, 88 }
***
main, WRITE: TLSv1 Handshake, length = 32
main, setSoTimeout(6000) called
main, WRITE: TLSv1 Application Data, length = 835
main, READ: TLSv1 Application Data, length = 515
main, READ: TLSv1 Application Data, length = 494
main, READ: TLSv1 Alert, length = 18
main, RECV TLSv1 ALERT:  warning, close_notify
main, called closeInternal(false)
main, SEND TLSv1 ALERT:  warning, description = close_notify
main, WRITE: TLSv1 Alert, length = 18
main, called close()
main, called closeInternal(true)
main, called close()
main, called closeInternal(true)
Logout Successfully for will
```