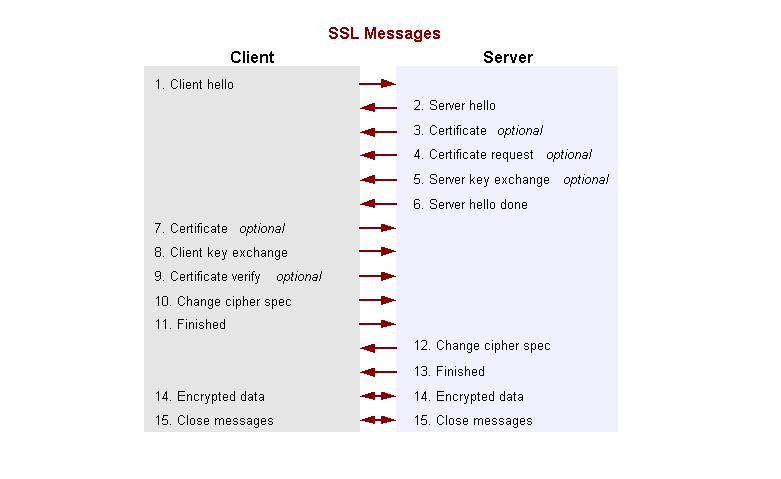
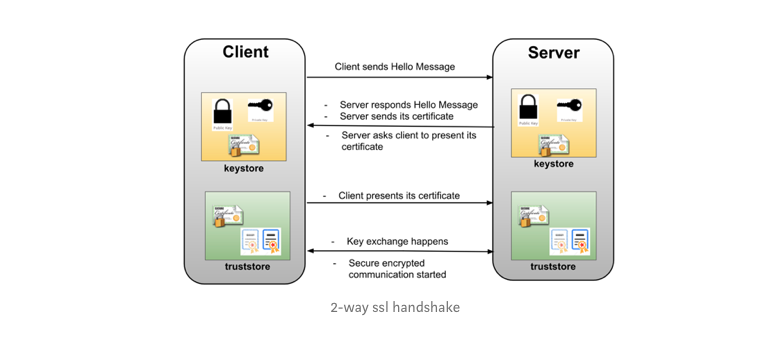
MSSLTraditionally, most of us are familiar with SSL. In this form, the server presents its certificate to the client and the client adds it to its list of trusted certificate. And so, the client can talk to the server.2 way SSL(Mutual SSL) is the same principle but both ways. i.e. both the client and the server has to establish trust between themselves using a trusted certificate. In this way of a digital handshake, the server needs to present a certificate to authenticate itself to client and client has to present its certificate to server.

Couple of example diagrams below:



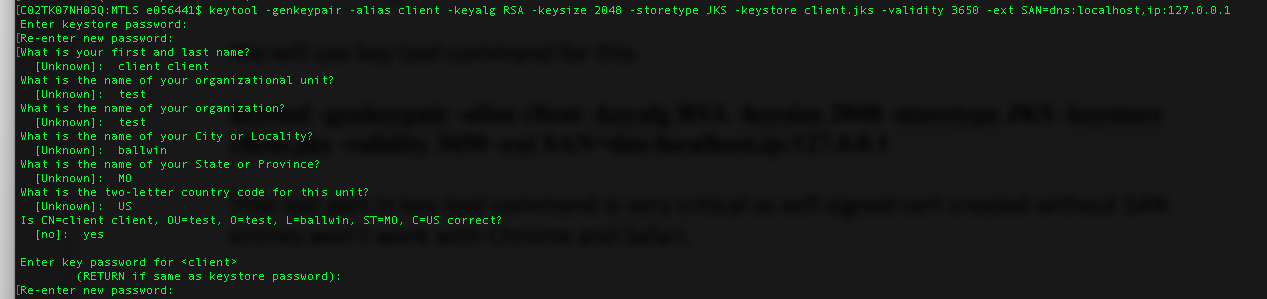


What we are using:Java 1.8  
Spring Boot 2.1.2  
keytool — this comes already with jdk installation.  
  
  
We will create 2 Spring Boot applications. We can call it client and server.  
  
Create A Self Signed Client Cert:

We will use key tool command for this.

**keytool -genkeypair -alias client -keyalg RSA -keysize 2048 -storetype JKS -keystore client.jks -validity 3650 -ext SAN=dns:localhost,ip:127.0.0.1**

That last part in key tool command is very critical as self-signed cert created without SAN entries won’t work with Chrome and Safari.



# Create Self Signed Server Cert:

**keytool -genkeypair -alias server -keyalg RSA -keysize 2048 -storetype JKS -keystore server.jks -validity 3650 -ext SAN=dns:localhost,ip:127.0.0.1**



# Create public certificate file from client cert:

Now that we’ve client and server certs created, we need to set up trust between both. To do that, we’ll import client cert in to the server’s trusted certificates and vice versa. But before we can do that, we need to extract public certificate of each jks file.

**keytool -export -alias client -file client.crt -keystore client.jks**



# **Create Public Certificate File From Server Cert:**

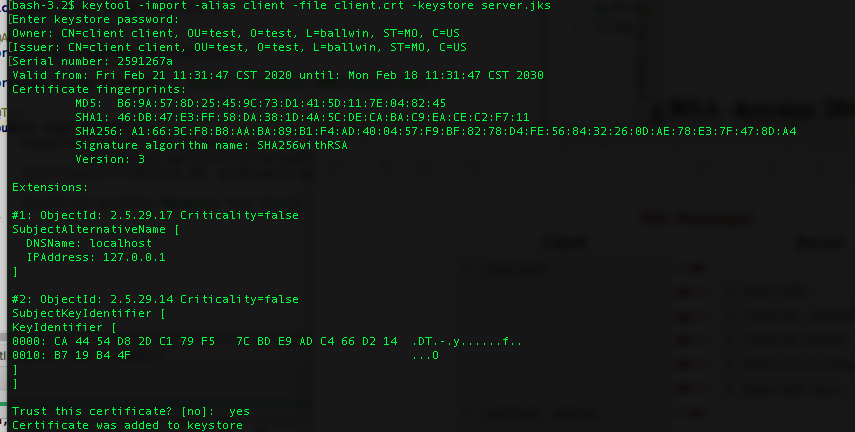
**keytool -export -alias server -file server.crt -keystore server.jks**

****

Now, we will have to import client’s cert to server’s keystore and server’s cert to client’s keystore file.

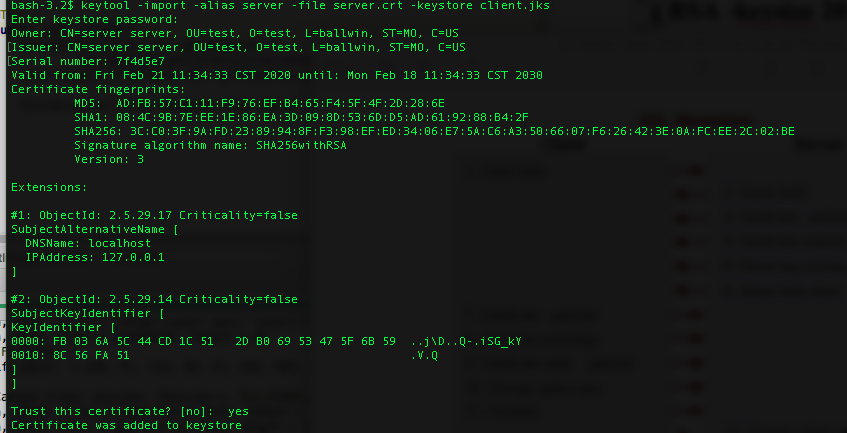
# **Import Client Cert to Server jks File:**

**keytool -import -alias client -file client.crt -keystore server.jks**



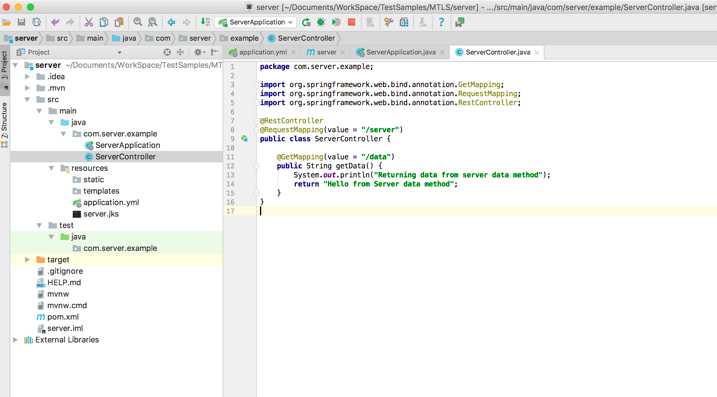
# **Import Server Cert to Client jks File:**

keytool -import -alias server -file server.crt -keystore client.jks

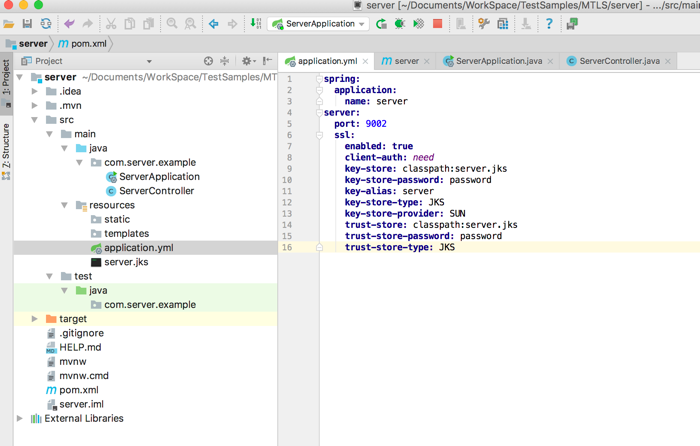


# **Configure Server For Mutual SSL:**

* Create a simple springboot app with a rest controller



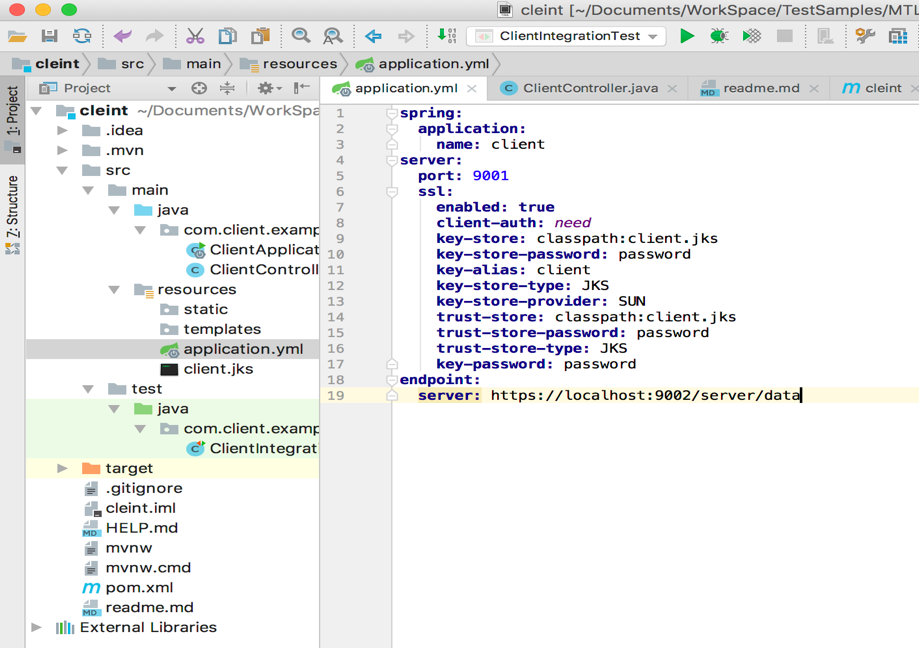
* Copy final server jks file to the src/main/resources/ folder of server application. Add the entries shown below in application.yml



# **Configure Client for Mtutual SSL:**

Now, this requires some more changes than the server side as https communication is going to be initiated from here.

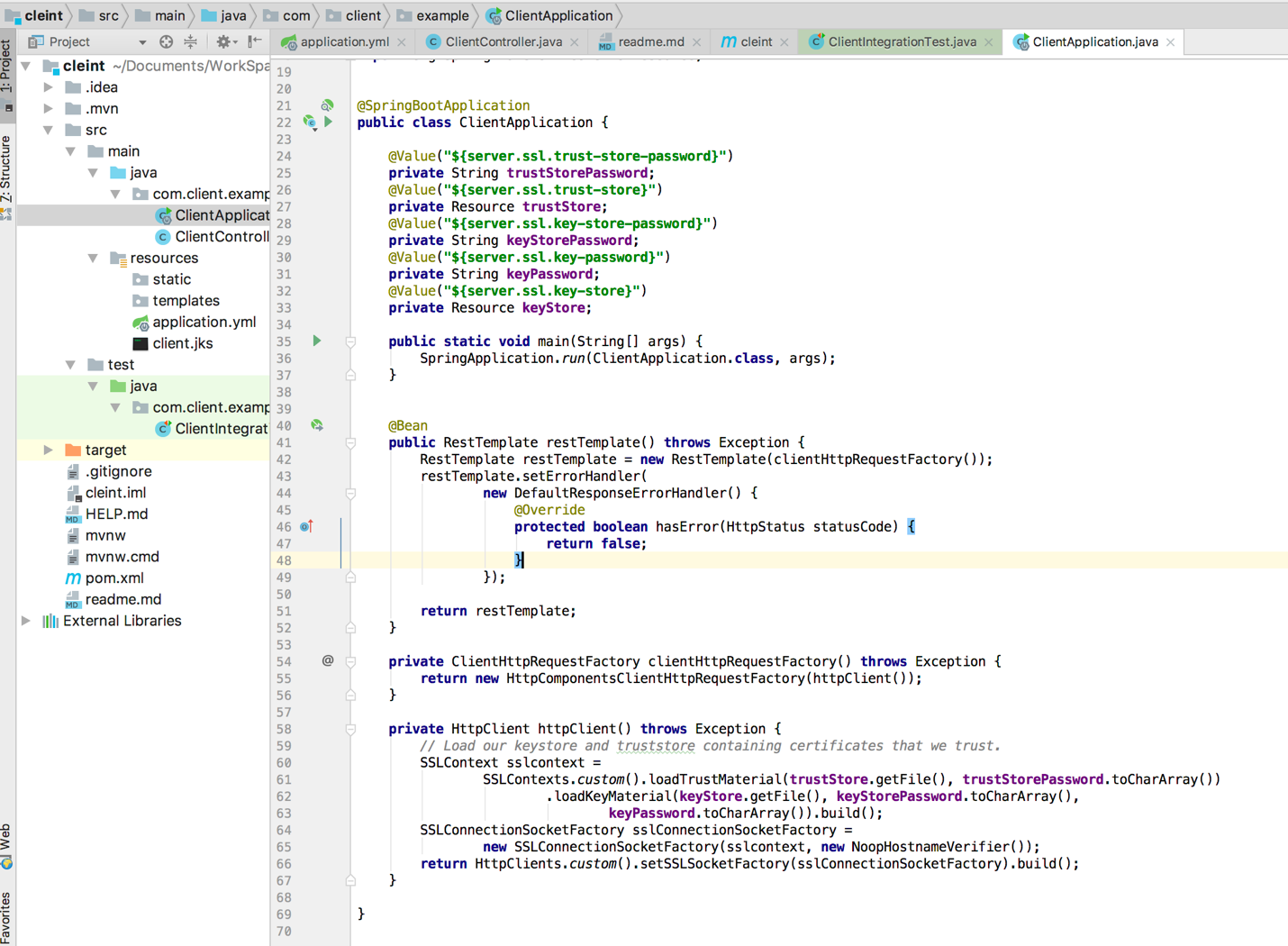
* First, copy final client to src/main/resources/ folder
* Next, add the entries shown below in application.yml



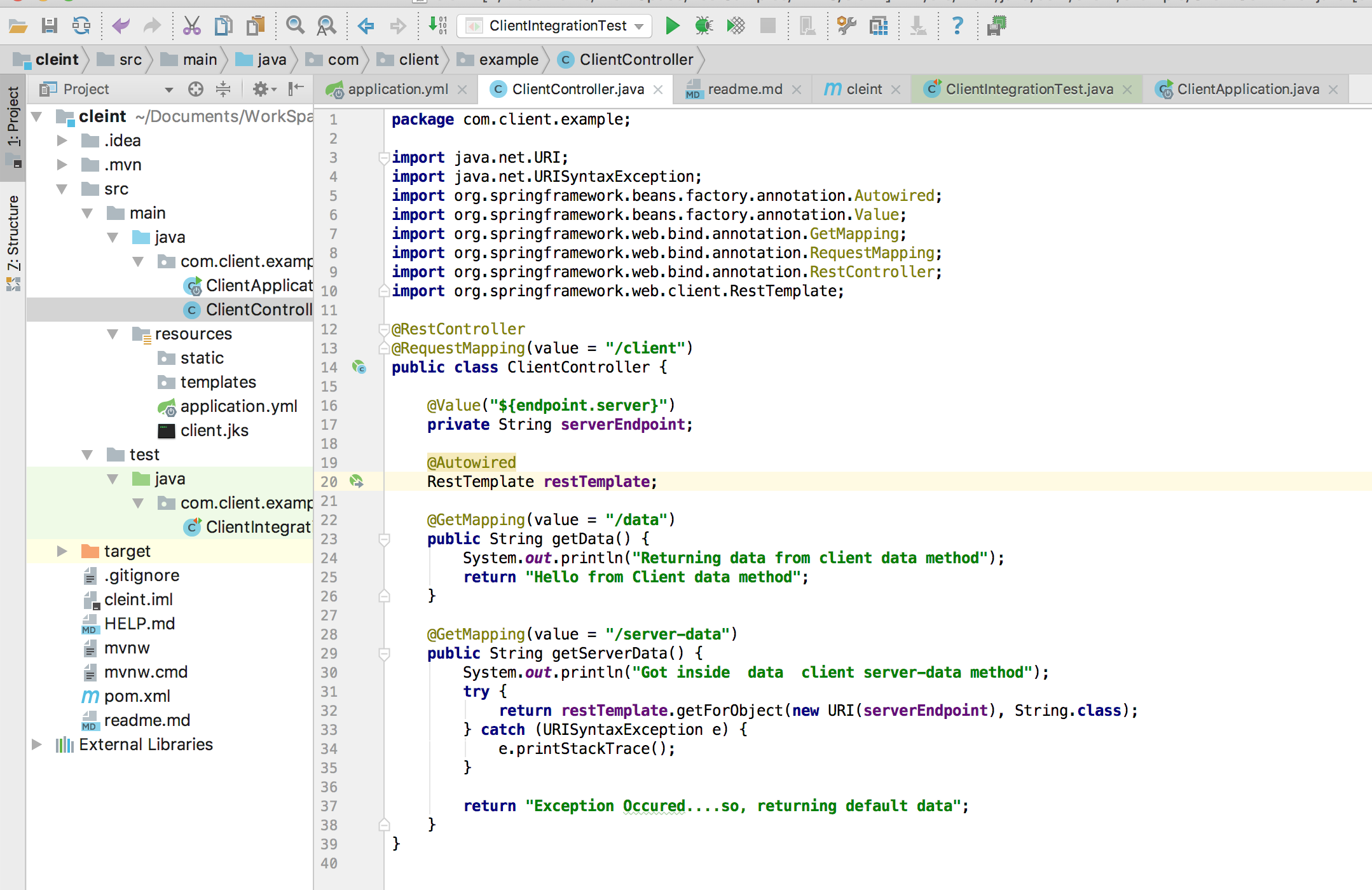
* We will need to add the below dependency in our pom

<**dependency**>  
 <**groupId**>org.apache.httpcomponents</**groupId**>  
 <**artifactId**>httpclient</**artifactId**>  
</**dependency**>

* Spring Boot comes with a RestTemplate class for http communication. We will use this class for our https call from the client application to the server. And because we are going with Mutual SSL, we need to configure this RestTemplate to use the trust store with server certificate.



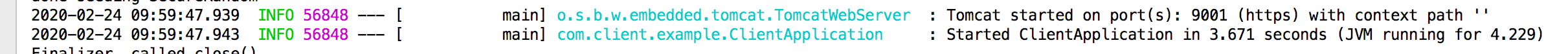
* we will create a controller class with 2 methods :



# **Running the Application:**

Compile both the client and server code and start the application. You will see that both applications will start on defined port in application.yml with https





But, there is still one problem. How do you test this? If you try to access the application with [https://localhost](https://localhost/) url, your browser will complain about the client certificate being needed!!! Why? We’ve accessed all these https applications in the world so far without any problem. So, what’s so special about our application?

Because it’sMutual SSL. When we access gateway url in browser, our browser becomes the client to our client application and so, our client web app will ask the browser to present a cert for authentication.

To overcome this, we will have to import a cert to our browser. But our browser can’t understand a .jks file. Instead, it understands PKCS12 format. So, how do we convert .jks file to PKCS12 format? Again, keytool command to the rescue.

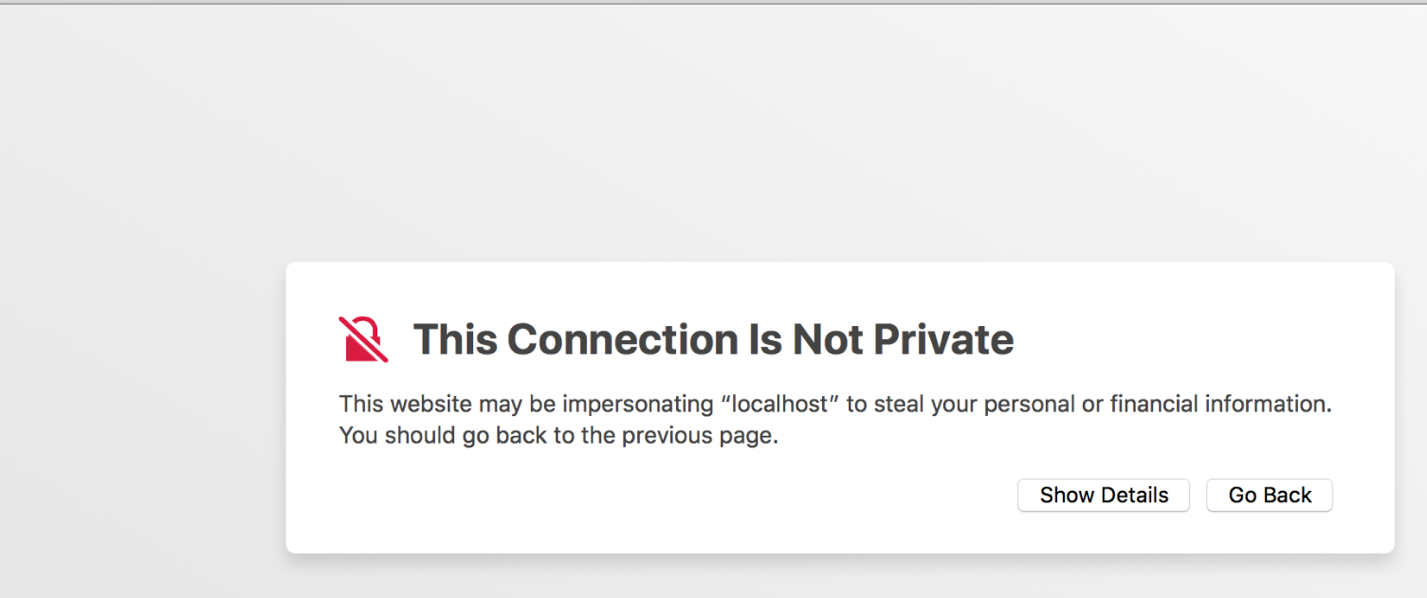
**keytool -importkeystore -srckeystore server.jks -destkeystore server.p12 -srcstoretype JKS -deststoretype PKCS12 -srcstorepass password -deststorepass password -srcalias server -destalias server -srckeypass password -destkeypass password -noprompt**

****

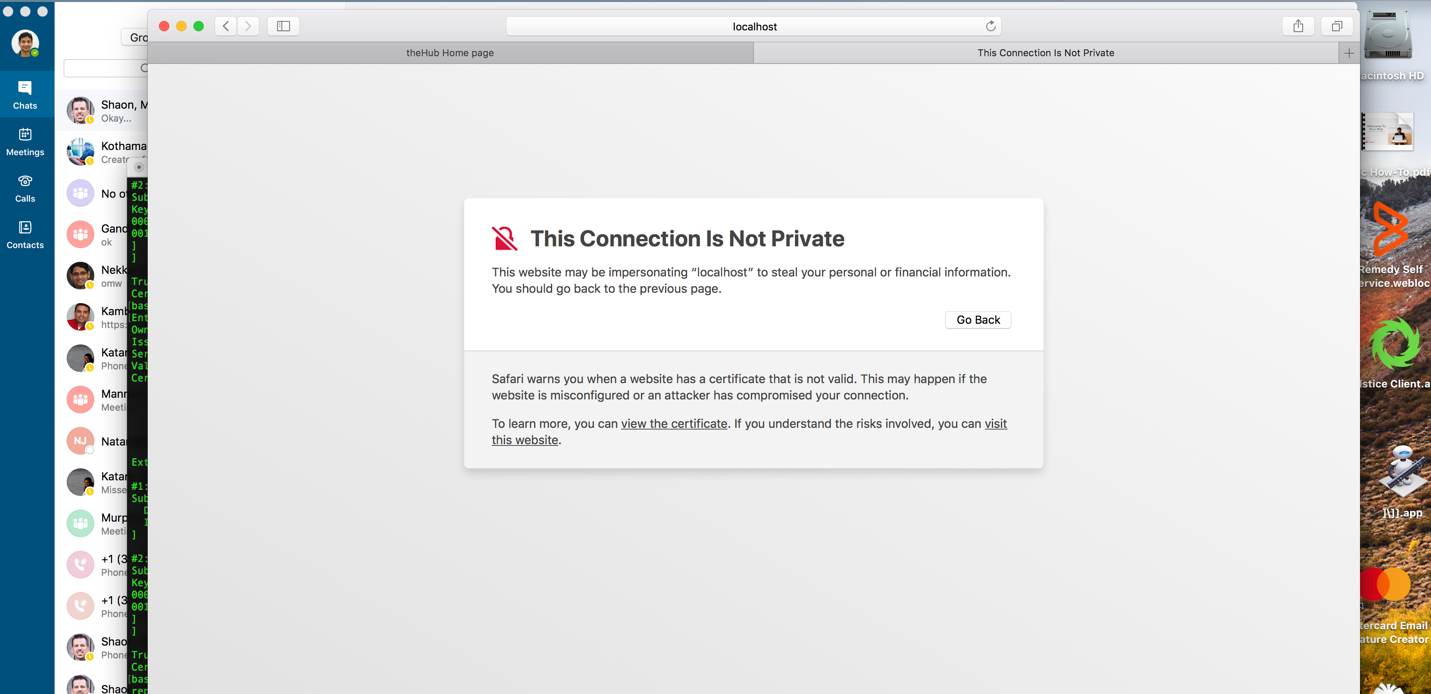
To import this .p12 file on mac, you will need to import this on login keychain.

Open keychain access

* Click on login under “keychains” and “Certificates” under Category
* Drag and drop the .p12 file here. It will prompt for the .p12 file password. Enter it and add.
* Double click the cert you just uploaded and under “Trust” and select the “Always Trust” option. This will ask you for your login keychain password. Enter it and proceed.
* Please close your browser windows, open and clear your cookies/cache and then hit [**https://localhost:9001/client/server-data**](https://localhost:9001/client/server-data) and you will be given a warning for “Connection not private” error.



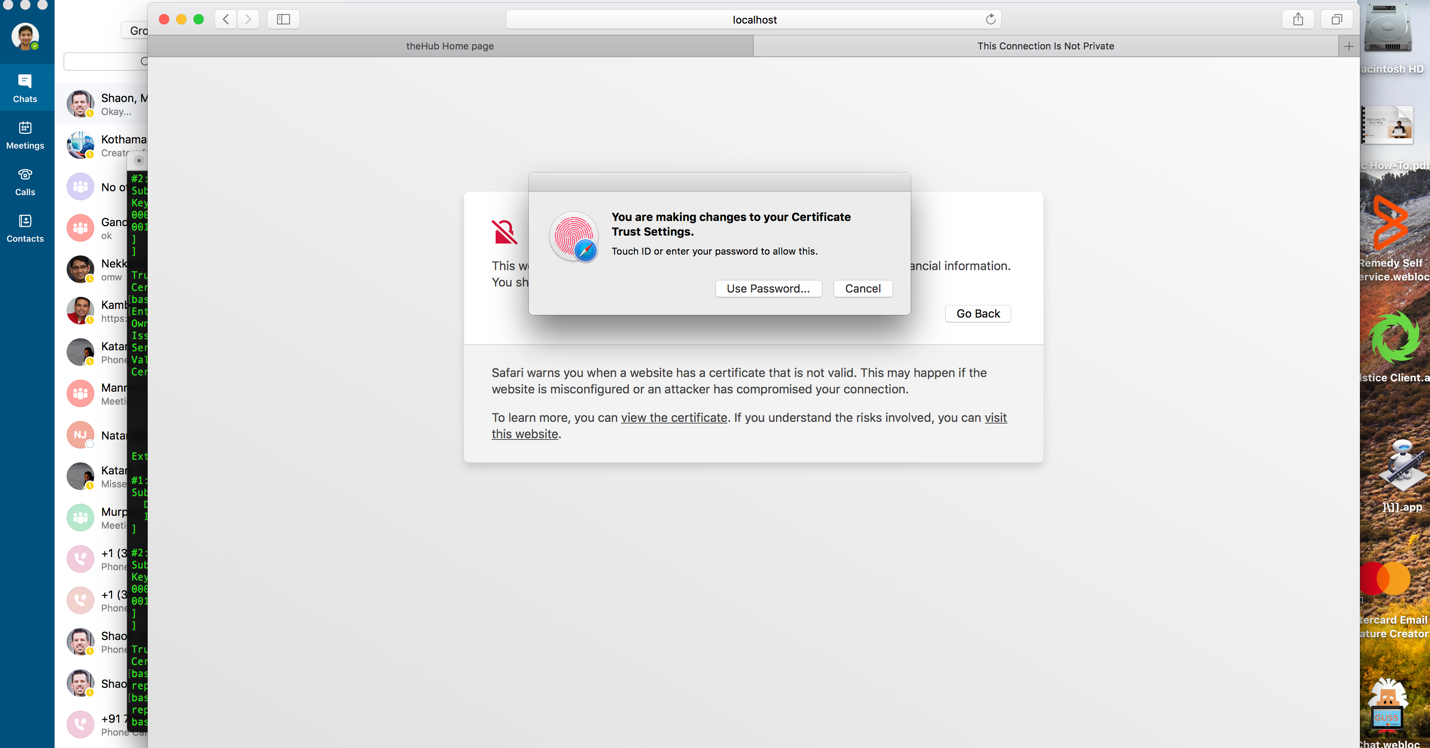
* Click “Show Details”



* Click on “visit this website” and you will get below screen.

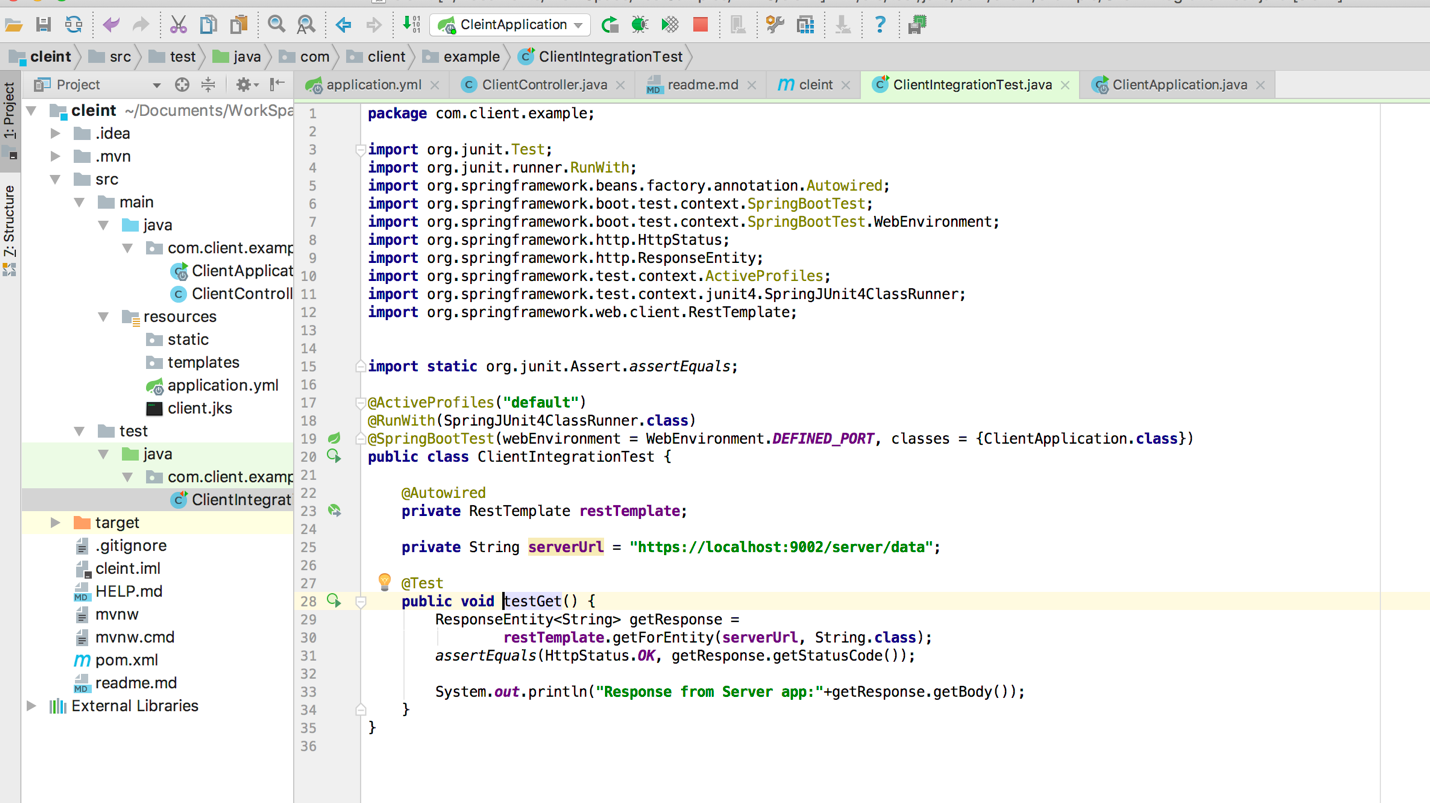


* One final step. You will need to enter your mac login password.



And that’s it. You will be able to load the method. And if you check logs of your gateway and ms application, you will see appropriate debug entries.

The otherway to test the connection is, as client application is a full SpringBoot app however we are just using the integration test support in SpringBoot as an easy way to make a secure connection to the server.



# Client SSL logs:

Allow unsafe renegotiation: false

Allow legacy hello messages: true

Is initial handshake: true

Is secure renegotiation: false

Ignoring unsupported cipher suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

Ignoring unsupported cipher suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

Ignoring unsupported cipher suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

Ignoring unsupported cipher suite: TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

Ignoring unsupported cipher suite: TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

Ignoring unsupported cipher suite: TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

Ignoring unsupported cipher suite: TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

%% No cached client session

\*\*\* ClientHello, TLSv1.2

RandomCookie: GMT: 1582496068 bytes = { 152, 83, 221, 91, 127, 6, 213, 183, 125, 147, 244, 157, 199, 161, 32, 100, 123, 141, 189, 225, 26, 84, 167, 9, 250, 186, 146, 251 }

Session ID: {}

Cipher Suites: [TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA, TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDH\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_DHE\_DSS\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA, TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA, SSL\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA, TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA, TLS\_ECDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA, SSL\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA, SSL\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA, TLS\_EMPTY\_RENEGOTIATION\_INFO\_SCSV]

Compression Methods: { 0 }

Extension elliptic\_curves, curve names: {secp256r1, secp384r1, secp521r1, sect283k1, sect283r1, sect409k1, sect409r1, sect571k1, sect571r1, secp256k1}

Extension ec\_point\_formats, formats: [uncompressed]

Extension signature\_algorithms, signature\_algorithms: SHA512withECDSA, SHA512withRSA, SHA384withECDSA, SHA384withRSA, SHA256withECDSA, SHA256withRSA, SHA256withDSA, SHA224withECDSA, SHA224withRSA, SHA224withDSA, SHA1withECDSA, SHA1withRSA, SHA1withDSA

\*\*\*

main, WRITE: TLSv1.2 Handshake, length = 167

main, READ: TLSv1.2 Handshake, length = 1467

\*\*\* ServerHello, TLSv1.2

RandomCookie: GMT: 1582496068 bytes = { 248, 60, 234, 170, 109, 107, 123, 115, 37, 241, 101, 152, 31, 96, 159, 167, 65, 13, 188, 252, 191, 185, 182, 245, 250, 93, 130, 35 }

Session ID: {94, 83, 249, 68, 56, 159, 208, 78, 34, 238, 36, 9, 103, 179, 94, 86, 243, 19, 173, 184, 56, 50, 184, 25, 129, 142, 197, 39, 102, 159, 74, 17}

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256

Compression Method: 0

Extension renegotiation\_info, renegotiated\_connection: <empty>

\*\*\*

%% Initialized: [Session-1, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256]

\*\* TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256

\*\*\* Certificate chain

chain [0] = [

[

Version: V3

Subject: CN=server server, OU=test, O=test, L=ballwin, ST=MO, C=US

Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

Key: Sun RSA public key, 2048 bits

modulus: 17372860922214586275774169236353994346940549609668964581525121631710752835705496804788208017836977999824613531847396919215945952215688526855112218560807043223329607424458114182231509722171749407837021075627649241974637210084546113911557642461477122030825450084980014106473513966491302140050922075768475727576012149290211595375494517113919335195092319115877686720498497447145571720206434546045292560102501923347962897326036761632903320842453781432169299264882193768746101755438193597957361861502156317963738660745374589883482669134596155153298985203999702627609950392462136063414793841457649023747713713840291518891297

public exponent: 65537

Validity: [From: Fri Feb 21 11:34:33 CST 2020,

To: Mon Feb 18 11:34:33 CST 2030]

Issuer: CN=server server, OU=test, O=test, L=ballwin, ST=MO, C=US

SerialNumber: [ 07f4d5e7]

Certificate Extensions: 2

[1]: ObjectId: 2.5.29.17 Criticality=false

SubjectAlternativeName [

DNSName: localhost

IPAddress: 127.0.0.1

]

[2]: ObjectId: 2.5.29.14 Criticality=false

SubjectKeyIdentifier [

KeyIdentifier [

0000: FB 03 6A 5C 44 CD 1C 51 2D B0 69 53 47 5F 6B 59 ..j\D..Q-.iSG\_kY

0010: 8C 56 FA 51 .V.Q

]

]

]

Algorithm: [SHA256withRSA]

Signature:

0000: 35 3F 7E 3A 28 26 AD 43 CA 14 A3 81 6B 8C A6 B3 5?.:(&.C....k...

0010: E2 77 58 A7 69 E4 C5 EC C2 6F 0E F7 82 56 4F CD .wX.i....o...VO.

0020: 8E 22 D0 69 61 5D 1F FB 8D FE D3 7F C2 84 19 8F .".ia]..........

0030: D5 39 29 8D D7 2E FD 97 CF 4F DC D6 AE 61 9B EE .9)......O...a..

0040: 35 78 C3 4B F3 BD 46 91 37 EB FE 42 D1 18 9D B6 5x.K..F.7..B....

0050: C7 BD F4 2E 46 9E 66 30 16 25 83 74 F3 AC CF FC ....F.f0.%.t....

0060: 70 28 76 A1 D5 A6 02 BA 96 67 A6 AA 7C B6 BC 3A p(v......g.....:

0070: E3 27 70 A9 CD 6D 94 19 06 15 98 15 AE 60 82 9F .'p..m.......`..

0080: FC 56 F3 DA AF 5F 24 A9 31 07 C5 09 0E BC 23 02 .V...\_$.1.....#.

0090: BA 65 7D 4F 5A 28 CD 22 EA CC 34 94 60 C6 D5 8C .e.OZ(."..4.`...

00A0: E8 9D CA CE 76 D8 6D 97 9D D8 51 82 51 CB EA 95 ....v.m...Q.Q...

00B0: 4E 1D D6 24 3A 1D E8 DC 1F D6 F8 25 6A B5 6B 98 N..$:......%j.k.

00C0: F8 10 77 0A 75 B7 01 C5 9A 5F 1C BF AF DF 09 B0 ..w.u....\_......

00D0: 97 1D AC 64 C0 62 95 17 42 8E F1 3A 9C 5B 81 D9 ...d.b..B..:.[..

00E0: 46 5F 68 79 CD 21 12 5C 89 F0 99 63 D6 7B BC AF F\_hy.!.\...c....

00F0: 27 44 CC E4 66 95 5D A5 E0 99 C9 60 1E 2C 26 54 'D..f.]....`.,&T

]

\*\*\*

Found trusted certificate:

[

[

Version: V3

Subject: CN=server server, OU=test, O=test, L=ballwin, ST=MO, C=US

Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

Key: Sun RSA public key, 2048 bits

modulus: 17372860922214586275774169236353994346940549609668964581525121631710752835705496804788208017836977999824613531847396919215945952215688526855112218560807043223329607424458114182231509722171749407837021075627649241974637210084546113911557642461477122030825450084980014106473513966491302140050922075768475727576012149290211595375494517113919335195092319115877686720498497447145571720206434546045292560102501923347962897326036761632903320842453781432169299264882193768746101755438193597957361861502156317963738660745374589883482669134596155153298985203999702627609950392462136063414793841457649023747713713840291518891297

public exponent: 65537

Validity: [From: Fri Feb 21 11:34:33 CST 2020,

To: Mon Feb 18 11:34:33 CST 2030]

Issuer: CN=server server, OU=test, O=test, L=ballwin, ST=MO, C=US

SerialNumber: [ 07f4d5e7]

Certificate Extensions: 2

[1]: ObjectId: 2.5.29.17 Criticality=false

SubjectAlternativeName [

DNSName: localhost

IPAddress: 127.0.0.1

]

[2]: ObjectId: 2.5.29.14 Criticality=false

SubjectKeyIdentifier [

KeyIdentifier [

0000: FB 03 6A 5C 44 CD 1C 51 2D B0 69 53 47 5F 6B 59 ..j\D..Q-.iSG\_kY

0010: 8C 56 FA 51 .V.Q

]

]

]

Algorithm: [SHA256withRSA]

Signature:

0000: 35 3F 7E 3A 28 26 AD 43 CA 14 A3 81 6B 8C A6 B3 5?.:(&.C....k...

0010: E2 77 58 A7 69 E4 C5 EC C2 6F 0E F7 82 56 4F CD .wX.i....o...VO.

0020: 8E 22 D0 69 61 5D 1F FB 8D FE D3 7F C2 84 19 8F .".ia]..........

0030: D5 39 29 8D D7 2E FD 97 CF 4F DC D6 AE 61 9B EE .9)......O...a..

0040: 35 78 C3 4B F3 BD 46 91 37 EB FE 42 D1 18 9D B6 5x.K..F.7..B....

0050: C7 BD F4 2E 46 9E 66 30 16 25 83 74 F3 AC CF FC ....F.f0.%.t....

0060: 70 28 76 A1 D5 A6 02 BA 96 67 A6 AA 7C B6 BC 3A p(v......g.....:

0070: E3 27 70 A9 CD 6D 94 19 06 15 98 15 AE 60 82 9F .'p..m.......`..

0080: FC 56 F3 DA AF 5F 24 A9 31 07 C5 09 0E BC 23 02 .V...\_$.1.....#.

0090: BA 65 7D 4F 5A 28 CD 22 EA CC 34 94 60 C6 D5 8C .e.OZ(."..4.`...

00A0: E8 9D CA CE 76 D8 6D 97 9D D8 51 82 51 CB EA 95 ....v.m...Q.Q...

00B0: 4E 1D D6 24 3A 1D E8 DC 1F D6 F8 25 6A B5 6B 98 N..$:......%j.k.

00C0: F8 10 77 0A 75 B7 01 C5 9A 5F 1C BF AF DF 09 B0 ..w.u....\_......

00D0: 97 1D AC 64 C0 62 95 17 42 8E F1 3A 9C 5B 81 D9 ...d.b..B..:.[..

00E0: 46 5F 68 79 CD 21 12 5C 89 F0 99 63 D6 7B BC AF F\_hy.!.\...c....

00F0: 27 44 CC E4 66 95 5D A5 E0 99 C9 60 1E 2C 26 54 'D..f.]....`.,&T

]

\*\*\* ECDH ServerKeyExchange

Signature Algorithm SHA512withRSA

Server key: Sun EC public key, 256 bits

public x coord: 111496265063758734745760006262779800076489613022363788663517540013931959696275

public y coord: 67116944108481046059025115215397962333632126341138744134767596050084957309108

parameters: secp256r1 [NIST P-256, X9.62 prime256v1] (1.2.840.10045.3.1.7)

\*\*\* CertificateRequest

Cert Types: RSA, DSS, ECDSA

Supported Signature Algorithms: SHA512withECDSA, SHA512withRSA, SHA384withECDSA, SHA384withRSA, SHA256withECDSA, SHA256withRSA, SHA256withDSA, SHA224withECDSA, SHA224withRSA, SHA224withDSA, SHA1withECDSA, SHA1withRSA, SHA1withDSA

Cert Authorities:

<CN=client client, OU=test, O=test, L=ballwin, ST=MO, C=US>

\*\*\* ServerHelloDone

matching alias: client

\*\*\* Certificate chain

chain [0] = [

[

Version: V3

Subject: CN=client client, OU=test, O=test, L=ballwin, ST=MO, C=US

Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

Key: Sun RSA public key, 2048 bits

modulus: 24287528907801981421324572601676670441258200916949275385048340252273955078887552993479094437188280282938777977496566293029552888700281387937196347787194756621718957257844049297154505071502910472431570405546473071595495086906654531498589374667664957338721495578199009409488608250531346518321651722148905945712521910426240160055361824574369063162002167383934917381756949756560308316988941651268123933884724048116139061360531693953832650387309035331777905672796932845549029509677315792770881974724127805697425999783110611857279202129936460222872801768326080894940426094606830863368827376316900422950901591434333075992363

public exponent: 65537

Validity: [From: Fri Feb 21 11:31:47 CST 2020,

To: Mon Feb 18 11:31:47 CST 2030]

Issuer: CN=client client, OU=test, O=test, L=ballwin, ST=MO, C=US

SerialNumber: [ 2591267a]

Certificate Extensions: 2

[1]: ObjectId: 2.5.29.17 Criticality=false

SubjectAlternativeName [

DNSName: localhost

IPAddress: 127.0.0.1

]

[2]: ObjectId: 2.5.29.14 Criticality=false

SubjectKeyIdentifier [

KeyIdentifier [

0000: CA 44 54 D8 2D C1 79 F5 7C BD E9 AD C4 66 D2 14 .DT.-.y......f..

0010: B7 19 B4 4F ...O

]

]

]

Algorithm: [SHA256withRSA]

Signature:

0000: 76 86 DB CC 9E BD 70 DF 35 AB A2 D3 32 57 1F EB v.....p.5...2W..

0010: 38 CC 8F 1B 3A A7 F2 B2 21 8D 24 1F 06 98 C9 C9 8...:...!.$.....

0020: D7 85 B6 B7 53 36 1C D2 C3 30 35 A4 BF BD 94 5C ....S6...05....\

0030: 13 D0 62 C9 D2 E9 CE 58 DB A3 40 03 C3 9A 23 DF ..b....X..@...#.

0040: C9 D3 22 12 7D 7D E8 0B 33 F6 17 CB 47 B7 1F 7F ..".....3...G...

0050: 2D 7F D5 B3 06 38 81 87 39 8D EB 0C B7 A8 26 26 -....8..9.....&&

0060: 9D 02 81 0A 5C 5D 39 B4 B5 06 25 00 04 A9 6A F5 ....\]9...%...j.

0070: 50 DD 55 27 BB E3 26 B9 35 4D 5B 90 56 A9 66 9E P.U'..&.5M[.V.f.

0080: 0F E3 11 FF C8 01 C2 2D E6 EB 0C DC 6F 22 E1 3B .......-....o".;

0090: FE 4E 59 39 9F D1 1E 21 3B 20 85 1F E2 8D 63 74 .NY9...!; ....ct

00A0: C4 D9 F0 FF 3A D5 9E 04 46 7F 35 8C C4 63 DF B9 ....:...F.5..c..

00B0: E2 3C DD DE E4 60 23 FE 70 58 EF 84 03 3D 07 05 .<...`#.pX...=..

00C0: 4C E0 5D 0C 6A EE CD 21 43 D7 D9 F8 4D F6 6F E7 L.].j..!C...M.o.

00D0: D3 97 F5 48 C6 2A 3A 53 90 B9 BD 27 3F 60 18 8B ...H.\*:S...'?`..

00E0: 2D 2B 17 29 4E F1 A0 9A D8 05 CC CB 4D 8B F3 37 -+.)N.......M..7

00F0: DD 45 C0 8F BE CF 21 E9 77 78 E5 D5 8E 68 3B D7 .E....!.wx...h;.

]

\*\*\*

\*\*\* ECDHClientKeyExchange

ECDH Public value: { 4, 233, 102, 78, 117, 128, 225, 16, 186, 206, 51, 136, 92, 167, 230, 122, 61, 180, 184, 227, 148, 148, 203, 254, 147, 28, 1, 65, 181, 84, 250, 151, 34, 180, 158, 200, 128, 50, 77, 97, 27, 170, 163, 195, 28, 168, 107, 221, 229, 88, 169, 181, 74, 146, 247, 187, 86, 54, 149, 154, 184, 40, 64, 34, 128 }

main, WRITE: TLSv1.2 Handshake, length = 979

SESSION KEYGEN:

PreMaster Secret:

0000: F9 11 D2 BD D5 70 EB 3B 04 58 39 12 8A 11 BE 71 .....p.;.X9....q

0010: 59 65 72 75 A4 78 A3 F3 19 46 78 21 8F DA 6B B2 Yeru.x...Fx!..k.

CONNECTION KEYGEN:

Client Nonce:

0000: 5E 53 F9 44 98 53 DD 5B 7F 06 D5 B7 7D 93 F4 9D ^S.D.S.[........

0010: C7 A1 20 64 7B 8D BD E1 1A 54 A7 09 FA BA 92 FB .. d.....T......

Server Nonce:

0000: 5E 53 F9 44 F8 3C EA AA 6D 6B 7B 73 25 F1 65 98 ^S.D.<..mk.s%.e.

0010: 1F 60 9F A7 41 0D BC FC BF B9 B6 F5 FA 5D 82 23 .`..A........].#

Master Secret:

0000: 42 BE 8E DD F5 2C 10 6A 3F 02 0D 0A 70 92 AC 4E B....,.j?...p..N

0010: 71 E5 34 9E 6B C6 FD E7 62 01 1C 8B 9F 3F E1 D6 q.4.k...b....?..

0020: 9F 99 28 3F EA 0A 9E 6A 0A B4 90 06 6C C4 88 11 ..(?...j....l...

Client MAC write Secret:

0000: 6A 25 99 8B 63 57 4F B3 6E 74 D0 F2 D8 7F EC 83 j%..cWO.nt......

0010: 25 2B B4 B0 63 06 D4 BD 73 B2 E0 A2 B4 51 8E 5A %+..c...s....Q.Z

Server MAC write Secret:

0000: 4A 60 1E 27 93 63 68 39 75 CF F6 45 39 63 FD D0 J`.'.ch9u..E9c..

0010: A4 A7 40 35 4E 68 80 F7 1E 04 63 37 7E BA DA BD ..@5Nh....c7....

Client write key:

0000: 84 33 D8 22 E6 4F 08 A1 12 47 75 89 E6 C4 CC E8 .3.".O...Gu.....

Server write key:

0000: D9 FE 96 7A 16 E7 73 36 88 93 EE 00 E1 84 0D FC ...z..s6........

... no IV derived for this protocol

\*\*\* CertificateVerify

Signature Algorithm SHA512withRSA

main, WRITE: TLSv1.2 Handshake, length = 264

main, WRITE: TLSv1.2 Change Cipher Spec, length = 1

\*\*\* Finished

verify\_data: { 29, 2, 184, 194, 1, 241, 6, 201, 79, 130, 85, 119 }

\*\*\*

main, WRITE: TLSv1.2 Handshake, length = 80

main, READ: TLSv1.2 Change Cipher Spec, length = 1

main, READ: TLSv1.2 Handshake, length = 80

\*\*\* Finished

verify\_data: { 47, 219, 78, 79, 74, 45, 156, 163, 95, 213, 255, 156 }

\*\*\*

%% Cached client session: [Session-1, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256]

main, WRITE: TLSv1.2 Application Data, length = 272

main, READ: TLSv1.2 Application Data, length = 192

main, setSoTimeout(0) called

Response from Server app:Hello from Server data method

2020-02-24 10:26:44.526 INFO 58836 --- [ Thread-5] o.s.s.concurrent.ThreadPoolTaskExecutor : Shutting down ExecutorService 'applicationTaskExecutor'

Process finished with exit code 0

# Server SSL Logs:

Using SSLEngineImpl.

Allow unsafe renegotiation: false

Allow legacy hello messages: true

Is initial handshake: true

Is secure renegotiation: false

Ignoring unsupported cipher suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 for TLSv1.1

Ignoring unsupported cipher suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 for TLSv1.1

Ignoring unsupported cipher suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

Ignoring unsupported cipher suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

https-jsse-nio-9002-exec-1, READ: TLSv1.2 Handshake, length = 167

\*\*\* ClientHello, TLSv1.2

RandomCookie: GMT: 1582496068 bytes = { 152, 83, 221, 91, 127, 6, 213, 183, 125, 147, 244, 157, 199, 161, 32, 100, 123, 141, 189, 225, 26, 84, 167, 9, 250, 186, 146, 251 }

Session ID: {}

Cipher Suites: [TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA, TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDH\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_DHE\_DSS\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA, TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA, SSL\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA, TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA, TLS\_ECDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA, SSL\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA, SSL\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA, TLS\_EMPTY\_RENEGOTIATION\_INFO\_SCSV]

Compression Methods: { 0 }

Extension elliptic\_curves, curve names: {secp256r1, secp384r1, secp521r1, sect283k1, sect283r1, sect409k1, sect409r1, sect571k1, sect571r1, secp256k1}

Extension ec\_point\_formats, formats: [uncompressed]

Extension signature\_algorithms, signature\_algorithms: SHA512withECDSA, SHA512withRSA, SHA384withECDSA, SHA384withRSA, SHA256withECDSA, SHA256withRSA, SHA256withDSA, SHA224withECDSA, SHA224withRSA, SHA224withDSA, SHA1withECDSA, SHA1withRSA, SHA1withDSA

\*\*\*

%% Initialized: [Session-1, SSL\_NULL\_WITH\_NULL\_NULL]

matching alias: server

Standard ciphersuite chosen: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256

%% Negotiating: [Session-1, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256]

\*\*\* ServerHello, TLSv1.2

RandomCookie: GMT: 1582496068 bytes = { 248, 60, 234, 170, 109, 107, 123, 115, 37, 241, 101, 152, 31, 96, 159, 167, 65, 13, 188, 252, 191, 185, 182, 245, 250, 93, 130, 35 }

Session ID: {94, 83, 249, 68, 56, 159, 208, 78, 34, 238, 36, 9, 103, 179, 94, 86, 243, 19, 173, 184, 56, 50, 184, 25, 129, 142, 197, 39, 102, 159, 74, 17}

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256

Compression Method: 0

Extension renegotiation\_info, renegotiated\_connection: <empty>

\*\*\*

Cipher suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256

\*\*\* Certificate chain

chain [0] = [

[

Version: V3

Subject: CN=server server, OU=test, O=test, L=ballwin, ST=MO, C=US

Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

Key: Sun RSA public key, 2048 bits

modulus: 17372860922214586275774169236353994346940549609668964581525121631710752835705496804788208017836977999824613531847396919215945952215688526855112218560807043223329607424458114182231509722171749407837021075627649241974637210084546113911557642461477122030825450084980014106473513966491302140050922075768475727576012149290211595375494517113919335195092319115877686720498497447145571720206434546045292560102501923347962897326036761632903320842453781432169299264882193768746101755438193597957361861502156317963738660745374589883482669134596155153298985203999702627609950392462136063414793841457649023747713713840291518891297

public exponent: 65537

Validity: [From: Fri Feb 21 11:34:33 CST 2020,

To: Mon Feb 18 11:34:33 CST 2030]

Issuer: CN=server server, OU=test, O=test, L=ballwin, ST=MO, C=US

SerialNumber: [ 07f4d5e7]

Certificate Extensions: 2

[1]: ObjectId: 2.5.29.17 Criticality=false

SubjectAlternativeName [

DNSName: localhost

IPAddress: 127.0.0.1

]

[2]: ObjectId: 2.5.29.14 Criticality=false

SubjectKeyIdentifier [

KeyIdentifier [

0000: FB 03 6A 5C 44 CD 1C 51 2D B0 69 53 47 5F 6B 59 ..j\D..Q-.iSG\_kY

0010: 8C 56 FA 51 .V.Q

]

]

]

Algorithm: [SHA256withRSA]

Signature:

0000: 35 3F 7E 3A 28 26 AD 43 CA 14 A3 81 6B 8C A6 B3 5?.:(&.C....k...

0010: E2 77 58 A7 69 E4 C5 EC C2 6F 0E F7 82 56 4F CD .wX.i....o...VO.

0020: 8E 22 D0 69 61 5D 1F FB 8D FE D3 7F C2 84 19 8F .".ia]..........

0030: D5 39 29 8D D7 2E FD 97 CF 4F DC D6 AE 61 9B EE .9)......O...a..

0040: 35 78 C3 4B F3 BD 46 91 37 EB FE 42 D1 18 9D B6 5x.K..F.7..B....

0050: C7 BD F4 2E 46 9E 66 30 16 25 83 74 F3 AC CF FC ....F.f0.%.t....

0060: 70 28 76 A1 D5 A6 02 BA 96 67 A6 AA 7C B6 BC 3A p(v......g.....:

0070: E3 27 70 A9 CD 6D 94 19 06 15 98 15 AE 60 82 9F .'p..m.......`..

0080: FC 56 F3 DA AF 5F 24 A9 31 07 C5 09 0E BC 23 02 .V...\_$.1.....#.

0090: BA 65 7D 4F 5A 28 CD 22 EA CC 34 94 60 C6 D5 8C .e.OZ(."..4.`...

00A0: E8 9D CA CE 76 D8 6D 97 9D D8 51 82 51 CB EA 95 ....v.m...Q.Q...

00B0: 4E 1D D6 24 3A 1D E8 DC 1F D6 F8 25 6A B5 6B 98 N..$:......%j.k.

00C0: F8 10 77 0A 75 B7 01 C5 9A 5F 1C BF AF DF 09 B0 ..w.u....\_......

00D0: 97 1D AC 64 C0 62 95 17 42 8E F1 3A 9C 5B 81 D9 ...d.b..B..:.[..

00E0: 46 5F 68 79 CD 21 12 5C 89 F0 99 63 D6 7B BC AF F\_hy.!.\...c....

00F0: 27 44 CC E4 66 95 5D A5 E0 99 C9 60 1E 2C 26 54 'D..f.]....`.,&T

]

\*\*\*

\*\*\* ECDH ServerKeyExchange

Signature Algorithm SHA512withRSA

Server key: Sun EC public key, 256 bits

public x coord: 111496265063758734745760006262779800076489613022363788663517540013931959696275

public y coord: 67116944108481046059025115215397962333632126341138744134767596050084957309108

parameters: secp256r1 [NIST P-256, X9.62 prime256v1] (1.2.840.10045.3.1.7)

\*\*\* CertificateRequest

Cert Types: RSA, DSS, ECDSA

Supported Signature Algorithms: SHA512withECDSA, SHA512withRSA, SHA384withECDSA, SHA384withRSA, SHA256withECDSA, SHA256withRSA, SHA256withDSA, SHA224withECDSA, SHA224withRSA, SHA224withDSA, SHA1withECDSA, SHA1withRSA, SHA1withDSA

Cert Authorities:

<CN=client client, OU=test, O=test, L=ballwin, ST=MO, C=US>

\*\*\* ServerHelloDone

https-jsse-nio-9002-exec-1, WRITE: TLSv1.2 Handshake, length = 1467

https-jsse-nio-9002-exec-2, READ: TLSv1.2 Handshake, length = 979

\*\*\* Certificate chain

chain [0] = [

[

Version: V3

Subject: CN=client client, OU=test, O=test, L=ballwin, ST=MO, C=US

Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

Key: Sun RSA public key, 2048 bits

modulus: 24287528907801981421324572601676670441258200916949275385048340252273955078887552993479094437188280282938777977496566293029552888700281387937196347787194756621718957257844049297154505071502910472431570405546473071595495086906654531498589374667664957338721495578199009409488608250531346518321651722148905945712521910426240160055361824574369063162002167383934917381756949756560308316988941651268123933884724048116139061360531693953832650387309035331777905672796932845549029509677315792770881974724127805697425999783110611857279202129936460222872801768326080894940426094606830863368827376316900422950901591434333075992363

public exponent: 65537

Validity: [From: Fri Feb 21 11:31:47 CST 2020,

To: Mon Feb 18 11:31:47 CST 2030]

Issuer: CN=client client, OU=test, O=test, L=ballwin, ST=MO, C=US

SerialNumber: [ 2591267a]

Certificate Extensions: 2

[1]: ObjectId: 2.5.29.17 Criticality=false

SubjectAlternativeName [

DNSName: localhost

IPAddress: 127.0.0.1

]

[2]: ObjectId: 2.5.29.14 Criticality=false

SubjectKeyIdentifier [

KeyIdentifier [

0000: CA 44 54 D8 2D C1 79 F5 7C BD E9 AD C4 66 D2 14 .DT.-.y......f..

0010: B7 19 B4 4F ...O

]

]

]

Algorithm: [SHA256withRSA]

Signature:

0000: 76 86 DB CC 9E BD 70 DF 35 AB A2 D3 32 57 1F EB v.....p.5...2W..

0010: 38 CC 8F 1B 3A A7 F2 B2 21 8D 24 1F 06 98 C9 C9 8...:...!.$.....

0020: D7 85 B6 B7 53 36 1C D2 C3 30 35 A4 BF BD 94 5C ....S6...05....\

0030: 13 D0 62 C9 D2 E9 CE 58 DB A3 40 03 C3 9A 23 DF ..b....X..@...#.

0040: C9 D3 22 12 7D 7D E8 0B 33 F6 17 CB 47 B7 1F 7F ..".....3...G...

0050: 2D 7F D5 B3 06 38 81 87 39 8D EB 0C B7 A8 26 26 -....8..9.....&&

0060: 9D 02 81 0A 5C 5D 39 B4 B5 06 25 00 04 A9 6A F5 ....\]9...%...j.

0070: 50 DD 55 27 BB E3 26 B9 35 4D 5B 90 56 A9 66 9E P.U'..&.5M[.V.f.

0080: 0F E3 11 FF C8 01 C2 2D E6 EB 0C DC 6F 22 E1 3B .......-....o".;

0090: FE 4E 59 39 9F D1 1E 21 3B 20 85 1F E2 8D 63 74 .NY9...!; ....ct

00A0: C4 D9 F0 FF 3A D5 9E 04 46 7F 35 8C C4 63 DF B9 ....:...F.5..c..

00B0: E2 3C DD DE E4 60 23 FE 70 58 EF 84 03 3D 07 05 .<...`#.pX...=..

00C0: 4C E0 5D 0C 6A EE CD 21 43 D7 D9 F8 4D F6 6F E7 L.].j..!C...M.o.

00D0: D3 97 F5 48 C6 2A 3A 53 90 B9 BD 27 3F 60 18 8B ...H.\*:S...'?`..

00E0: 2D 2B 17 29 4E F1 A0 9A D8 05 CC CB 4D 8B F3 37 -+.)N.......M..7

00F0: DD 45 C0 8F BE CF 21 E9 77 78 E5 D5 8E 68 3B D7 .E....!.wx...h;.

]

\*\*\*

Found trusted certificate:

[

[

Version: V3

Subject: CN=client client, OU=test, O=test, L=ballwin, ST=MO, C=US

Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

Key: Sun RSA public key, 2048 bits

modulus: 24287528907801981421324572601676670441258200916949275385048340252273955078887552993479094437188280282938777977496566293029552888700281387937196347787194756621718957257844049297154505071502910472431570405546473071595495086906654531498589374667664957338721495578199009409488608250531346518321651722148905945712521910426240160055361824574369063162002167383934917381756949756560308316988941651268123933884724048116139061360531693953832650387309035331777905672796932845549029509677315792770881974724127805697425999783110611857279202129936460222872801768326080894940426094606830863368827376316900422950901591434333075992363

public exponent: 65537

Validity: [From: Fri Feb 21 11:31:47 CST 2020,

To: Mon Feb 18 11:31:47 CST 2030]

Issuer: CN=client client, OU=test, O=test, L=ballwin, ST=MO, C=US

SerialNumber: [ 2591267a]

Certificate Extensions: 2

[1]: ObjectId: 2.5.29.17 Criticality=false

SubjectAlternativeName [

DNSName: localhost

IPAddress: 127.0.0.1

]

[2]: ObjectId: 2.5.29.14 Criticality=false

SubjectKeyIdentifier [

KeyIdentifier [

0000: CA 44 54 D8 2D C1 79 F5 7C BD E9 AD C4 66 D2 14 .DT.-.y......f..

0010: B7 19 B4 4F ...O

]

]

]

Algorithm: [SHA256withRSA]

Signature:

0000: 76 86 DB CC 9E BD 70 DF 35 AB A2 D3 32 57 1F EB v.....p.5...2W..

0010: 38 CC 8F 1B 3A A7 F2 B2 21 8D 24 1F 06 98 C9 C9 8...:...!.$.....

0020: D7 85 B6 B7 53 36 1C D2 C3 30 35 A4 BF BD 94 5C ....S6...05....\

0030: 13 D0 62 C9 D2 E9 CE 58 DB A3 40 03 C3 9A 23 DF ..b....X..@...#.

0040: C9 D3 22 12 7D 7D E8 0B 33 F6 17 CB 47 B7 1F 7F ..".....3...G...

0050: 2D 7F D5 B3 06 38 81 87 39 8D EB 0C B7 A8 26 26 -....8..9.....&&

0060: 9D 02 81 0A 5C 5D 39 B4 B5 06 25 00 04 A9 6A F5 ....\]9...%...j.

0070: 50 DD 55 27 BB E3 26 B9 35 4D 5B 90 56 A9 66 9E P.U'..&.5M[.V.f.

0080: 0F E3 11 FF C8 01 C2 2D E6 EB 0C DC 6F 22 E1 3B .......-....o".;

0090: FE 4E 59 39 9F D1 1E 21 3B 20 85 1F E2 8D 63 74 .NY9...!; ....ct

00A0: C4 D9 F0 FF 3A D5 9E 04 46 7F 35 8C C4 63 DF B9 ....:...F.5..c..

00B0: E2 3C DD DE E4 60 23 FE 70 58 EF 84 03 3D 07 05 .<...`#.pX...=..

00C0: 4C E0 5D 0C 6A EE CD 21 43 D7 D9 F8 4D F6 6F E7 L.].j..!C...M.o.

00D0: D3 97 F5 48 C6 2A 3A 53 90 B9 BD 27 3F 60 18 8B ...H.\*:S...'?`..

00E0: 2D 2B 17 29 4E F1 A0 9A D8 05 CC CB 4D 8B F3 37 -+.)N.......M..7

00F0: DD 45 C0 8F BE CF 21 E9 77 78 E5 D5 8E 68 3B D7 .E....!.wx...h;.

]

\*\*\* ECDHClientKeyExchange

ECDH Public value: { 4, 233, 102, 78, 117, 128, 225, 16, 186, 206, 51, 136, 92, 167, 230, 122, 61, 180, 184, 227, 148, 148, 203, 254, 147, 28, 1, 65, 181, 84, 250, 151, 34, 180, 158, 200, 128, 50, 77, 97, 27, 170, 163, 195, 28, 168, 107, 221, 229, 88, 169, 181, 74, 146, 247, 187, 86, 54, 149, 154, 184, 40, 64, 34, 128 }

SESSION KEYGEN:

PreMaster Secret:

0000: F9 11 D2 BD D5 70 EB 3B 04 58 39 12 8A 11 BE 71 .....p.;.X9....q

0010: 59 65 72 75 A4 78 A3 F3 19 46 78 21 8F DA 6B B2 Yeru.x...Fx!..k.

CONNECTION KEYGEN:

Client Nonce:

0000: 5E 53 F9 44 98 53 DD 5B 7F 06 D5 B7 7D 93 F4 9D ^S.D.S.[........

0010: C7 A1 20 64 7B 8D BD E1 1A 54 A7 09 FA BA 92 FB .. d.....T......

Server Nonce:

0000: 5E 53 F9 44 F8 3C EA AA 6D 6B 7B 73 25 F1 65 98 ^S.D.<..mk.s%.e.

0010: 1F 60 9F A7 41 0D BC FC BF B9 B6 F5 FA 5D 82 23 .`..A........].#

Master Secret:

0000: 42 BE 8E DD F5 2C 10 6A 3F 02 0D 0A 70 92 AC 4E B....,.j?...p..N

0010: 71 E5 34 9E 6B C6 FD E7 62 01 1C 8B 9F 3F E1 D6 q.4.k...b....?..

0020: 9F 99 28 3F EA 0A 9E 6A 0A B4 90 06 6C C4 88 11 ..(?...j....l...

Client MAC write Secret:

0000: 6A 25 99 8B 63 57 4F B3 6E 74 D0 F2 D8 7F EC 83 j%..cWO.nt......

0010: 25 2B B4 B0 63 06 D4 BD 73 B2 E0 A2 B4 51 8E 5A %+..c...s....Q.Z

Server MAC write Secret:

0000: 4A 60 1E 27 93 63 68 39 75 CF F6 45 39 63 FD D0 J`.'.ch9u..E9c..

0010: A4 A7 40 35 4E 68 80 F7 1E 04 63 37 7E BA DA BD ..@5Nh....c7....

Client write key:

0000: 84 33 D8 22 E6 4F 08 A1 12 47 75 89 E6 C4 CC E8 .3.".O...Gu.....

Server write key:

0000: D9 FE 96 7A 16 E7 73 36 88 93 EE 00 E1 84 0D FC ...z..s6........

... no IV derived for this protocol

https-jsse-nio-9002-exec-3, READ: TLSv1.2 Handshake, length = 264

\*\*\* CertificateVerify

Signature Algorithm SHA512withRSA

https-jsse-nio-9002-exec-3, READ: TLSv1.2 Change Cipher Spec, length = 1

https-jsse-nio-9002-exec-4, READ: TLSv1.2 Handshake, length = 80

\*\*\* Finished

verify\_data: { 29, 2, 184, 194, 1, 241, 6, 201, 79, 130, 85, 119 }

\*\*\*

https-jsse-nio-9002-exec-4, WRITE: TLSv1.2 Change Cipher Spec, length = 1

\*\*\* Finished

verify\_data: { 47, 219, 78, 79, 74, 45, 156, 163, 95, 213, 255, 156 }

\*\*\*

https-jsse-nio-9002-exec-4, WRITE: TLSv1.2 Handshake, length = 80

%% Cached server session: [Session-1, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256]

Returning data from server data method

https-jsse-nio-9002-exec-6, WRITE: TLSv1.2 Application Data, length = 143

https-jsse-nio-9002-exec-7, called closeOutbound()

https-jsse-nio-9002-exec-7, closeOutboundInternal()

https-jsse-nio-9002-exec-7, SEND TLSv1.2 ALERT: warning, description = close\_notify

https-jsse-nio-9002-exec-7, WRITE: TLSv1.2 Alert, length = 64