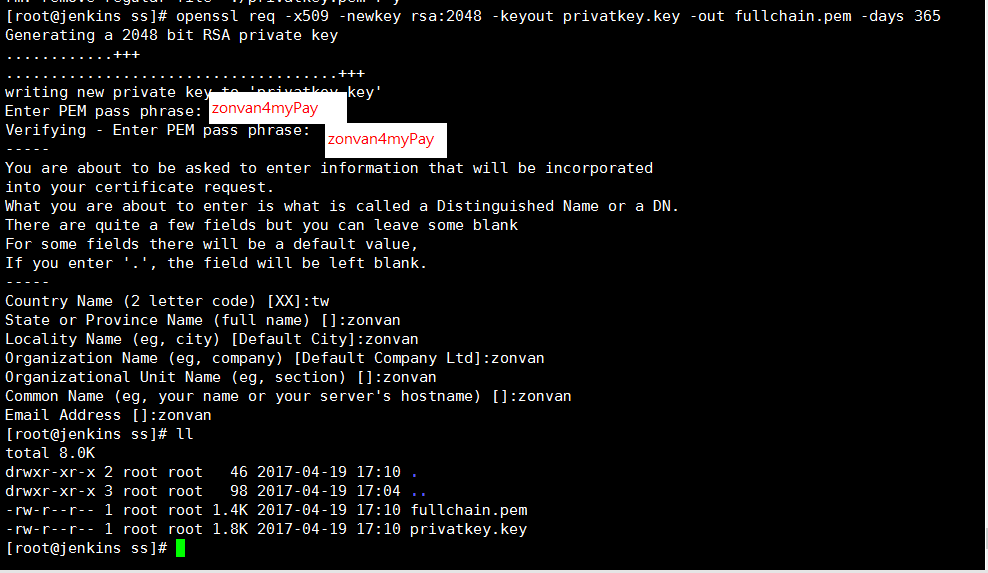
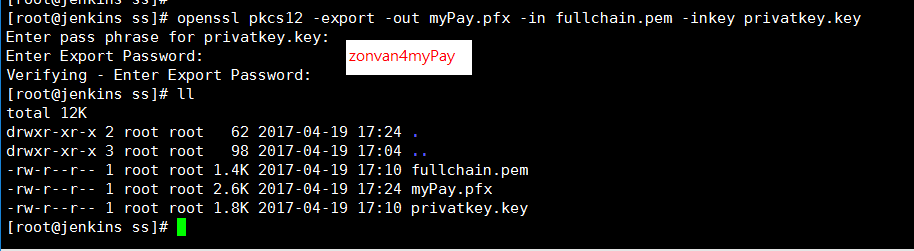
Create ssl => 收费证书 可以拿到 \*\*\*.key 和 \*\*\*.pem (密码)

|  |
| --- |
| openssl req -x509 -newkey rsa:2048 -keyout privatkey.key -out fullchain.pem -days 365 |



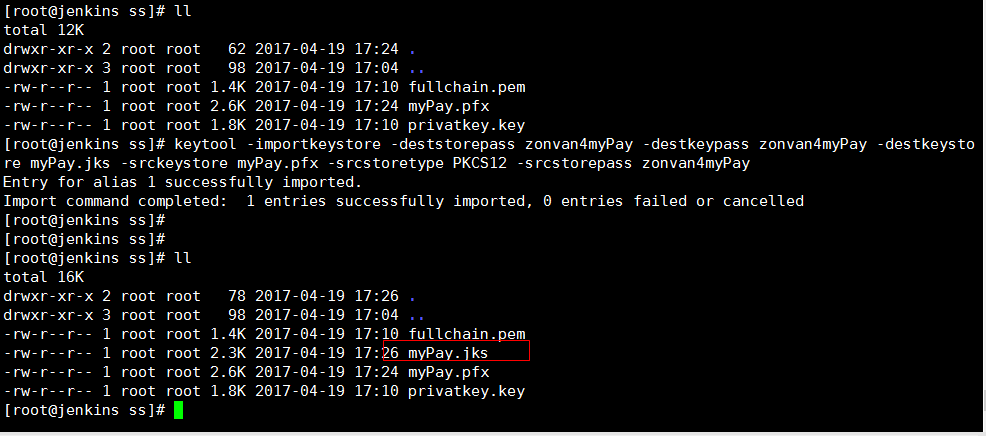
首先将这俩货合并成 \*\*\*.pfx

|  |
| --- |
| openssl pkcs12 -export -out myPay.pfx -in fullchain.pem -inkey privatkey.key |



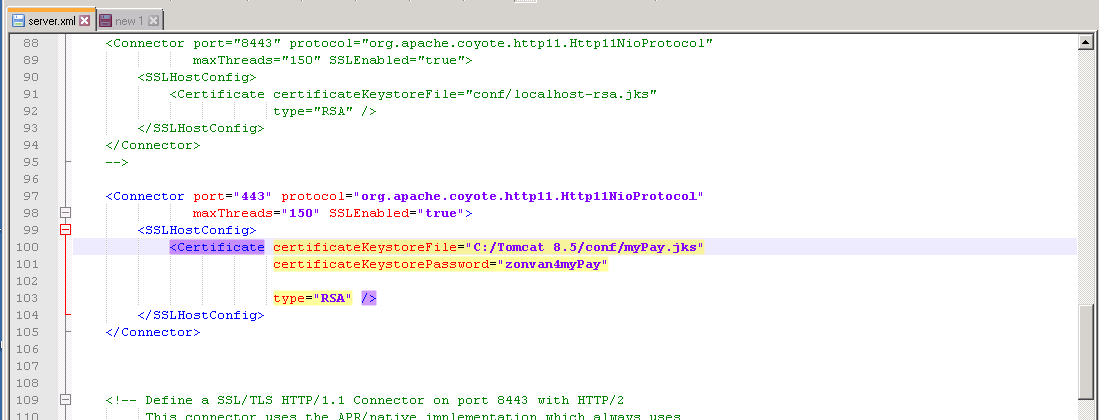
然后再转换成jks证书 运行命令

|  |
| --- |
| keytool -importkeystore -deststorepass zonvan4myPay -destkeypass zonvan4myPay -destkeystore myPay.jks -srckeystore myPay.pfx -srcstoretype PKCS12 -srcstorepass zonvan4myPay |



修改Tomcat 8.5 conf/service.xml

|  |
| --- |
| <Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"  maxThreads="150" SSLEnabled="true">  <SSLHostConfig>  <Certificate certificateKeystoreFile="C:/Tomcat 8.5/conf/myPay.jks"  certificateKeystorePassword="zonvan4myPay"    type="RSA" />  </SSLHostConfig>  </Connector> |



另一种java jks

|  |
| --- |
| keytool -genkey -alias zonvan -keyalg RSA -keypass zonvan -storepass zonvan -keystore keystore.jks |

Service.xml

|  |
| --- |
| <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"  maxThreads="150" SSLEnabled="true">  <SSLHostConfig>  <Certificate certificateKeystoreFile="conf/keystore.jks"  certificateKeystorePassword="zonvan"  certificateKeyAlias="zonvan"  type="RSA" />  </SSLHostConfig>  </Connector> |

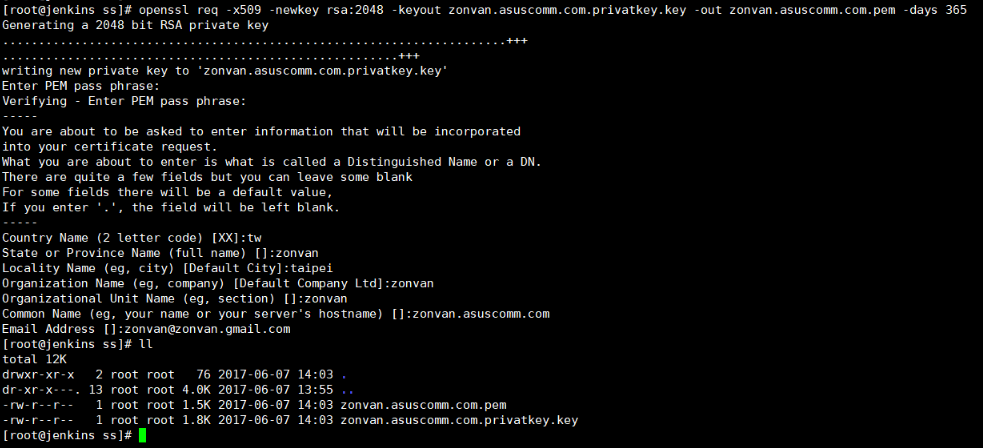
Web.xml

|  |
| --- |
| <security-constraint>  <web-resource-collection>  <web-resource-name>myPay</web-resource-name>  <url-pattern>/\*</url-pattern>  </web-resource-collection>  <user-data-constraint>  <transport-guarantee>CONFIDENTIAL</transport-guarantee>  </user-data-constraint>  </security-constraint> |

openssl req -x509 -newkey rsa:2048 -keyout zonvan.asuscomm.com.privatkey.key -out zonvan.asuscomm.com.pem -days 365

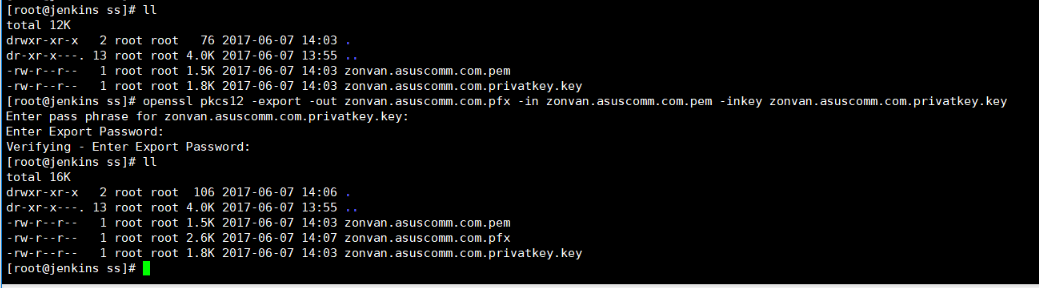
zonvan.asuscomm.com

zonvan4myPay

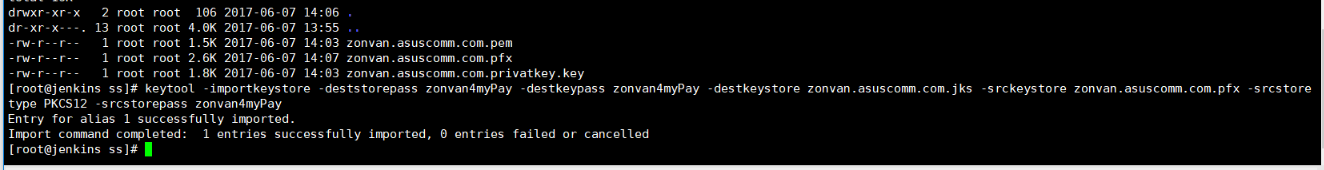


openssl pkcs12 -export -out zonvan.asuscomm.com.pfx -in zonvan.asuscomm.com.pem -inkey zonvan.asuscomm.com.privatkey.key

zonvan4myPay \* 3 times



keytool -importkeystore -deststorepass zonvan4myPay -destkeypass zonvan4myPay -destkeystore zonvan.asuscomm.com.jks -srckeystore zonvan.asuscomm.com.pfx -srcstoretype PKCS12 -srcstorepass zonvan4myPay



合并 ip.jks into zonvan.asuscomm.com.jks

keytool -importkeystore -srckeystore ip.jks -srcstorepass zonvan4myPay -destkeystore zonvan.asuscomm.com.jks -deststorepass zonvan4myPay

no ip

合并 zonvan2.asuscomm.com.jks into zonvan.asuscomm.com.jks

keytool -importkeystore -srckeystore zonvan2.asuscomm.com.jks -srcstorepass zonvan4myPay -destkeystore zonvan.asuscomm.com.jks -deststorepass zonvan4myPay

no zonvan2

keytool -list -v -keystore zonvan.asuscomm.com.jks -storepass zonvan4myPay

|  |
| --- |
| [root@jenkins kk]# keytool -list -v -keystore zonvan.asuscomm.com.jks -storepass zonvan4myPay  Keystore type: JKS  Keystore provider: SUN  Your keystore contains 3 entries  Alias name: zonvan2  Creation date: Jun 7, 2017  Entry type: PrivateKeyEntry  Certificate chain length: 1  Certificate[1]:  Owner: EMAILADDRESS=zonvan@zonvan.com, CN=zonvan2.asuscomm.com, OU=zonvan2, O=zonvan2, L=taipei, ST=zonvan2, C=tw  Issuer: EMAILADDRESS=zonvan@zonvan.com, CN=zonvan2.asuscomm.com, OU=zonvan2, O=zonvan2, L=taipei, ST=zonvan2, C=tw  Serial number: f87f3cdc638fd392  Valid from: Wed Jun 07 14:19:16 CST 2017 until: Thu Jun 07 14:19:16 CST 2018  Certificate fingerprints:  MD5: 94:D5:8E:40:19:59:02:DD:34:A4:86:69:DA:55:19:F1  SHA1: 6E:A4:86:F2:FB:52:28:5F:B6:42:11:DC:25:2E:B1:CD:D2:29:B8:45  SHA256: 20:C2:91:96:F7:B1:54:2A:B6:0B:4F:D5:0B:A6:08:F3:09:2C:F5:E0:CE:05:24:25:62:DC:26:23:A2:71:8F:BD  Signature algorithm name: SHA256withRSA  Version: 3  Extensions:  #1: ObjectId: 2.5.29.35 Criticality=false  AuthorityKeyIdentifier [  KeyIdentifier [  0000: F9 BD 9F 0A DE FD AC 39 B7 78 16 08 11 A3 17 E8 .......9.x......  0010: 0E F3 B2 C6 ....  ]  ]  #2: ObjectId: 2.5.29.19 Criticality=false  BasicConstraints:[  CA:true  PathLen:2147483647  ]  #3: ObjectId: 2.5.29.14 Criticality=false  SubjectKeyIdentifier [  KeyIdentifier [  0000: F9 BD 9F 0A DE FD AC 39 B7 78 16 08 11 A3 17 E8 .......9.x......  0010: 0E F3 B2 C6 ....  ]  ]  \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  Alias name: 1  Creation date: Jun 7, 2017  Entry type: PrivateKeyEntry  Certificate chain length: 1  Certificate[1]:  Owner: EMAILADDRESS=zonvan@zonvan.gmail.com, CN=zonvan.asuscomm.com, OU=zonvan, O=zonvan, L=taipei, ST=zonvan, C=tw  Issuer: EMAILADDRESS=zonvan@zonvan.gmail.com, CN=zonvan.asuscomm.com, OU=zonvan, O=zonvan, L=taipei, ST=zonvan, C=tw  Serial number: d7ba68ffd6b0256c  Valid from: Wed Jun 07 14:03:32 CST 2017 until: Thu Jun 07 14:03:32 CST 2018  Certificate fingerprints:  MD5: 51:E1:60:B8:7C:5C:52:3C:45:6B:85:66:27:B4:3D:F0  SHA1: D1:1D:0B:5B:57:F0:EE:D9:1E:F0:9A:66:63:7F:17:97:3B:FF:76:19  SHA256: 38:9A:3D:C6:17:97:A9:F3:67:89:5D:2F:E6:48:B7:E9:40:16:88:98:9E:97:0F:5F:82:74:CA:29:38:43:D9:F6  Signature algorithm name: SHA256withRSA  Version: 3  Extensions:  #1: ObjectId: 2.5.29.35 Criticality=false  AuthorityKeyIdentifier [  KeyIdentifier [  0000: 68 78 28 75 EE 6E E3 8D 74 16 AA 73 0E 8E DB CB hx(u.n..t..s....  0010: 86 0D 2D F3 ..-.  ]  ]  #2: ObjectId: 2.5.29.19 Criticality=false  BasicConstraints:[  CA:true  PathLen:2147483647  ]  #3: ObjectId: 2.5.29.14 Criticality=false  SubjectKeyIdentifier [  KeyIdentifier [  0000: 68 78 28 75 EE 6E E3 8D 74 16 AA 73 0E 8E DB CB hx(u.n..t..s....  0010: 86 0D 2D F3 ..-.  ]  ]  \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  Alias name: ip  Creation date: Jun 7, 2017  Entry type: PrivateKeyEntry  Certificate chain length: 1  Certificate[1]:  Owner: EMAILADDRESS=zonvan@zonvan, CN=61.216.133.169, OU=zonvan, O=zonvan, L=taipei, ST=zonvan, C=tw  Issuer: EMAILADDRESS=zonvan@zonvan, CN=61.216.133.169, OU=zonvan, O=zonvan, L=taipei, ST=zonvan, C=tw  Serial number: 8007b6a45456ca0b  Valid from: Wed Jun 07 14:30:18 CST 2017 until: Thu Jun 07 14:30:18 CST 2018  Certificate fingerprints:  MD5: E7:B6:C0:16:E3:63:4A:A1:02:09:0C:B1:72:91:01:A2  SHA1: 3F:C8:45:36:1F:50:F5:78:48:99:02:1F:F8:A7:94:9D:C8:EE:96:61  SHA256: 50:45:1D:BF:9B:99:54:3F:95:EC:AF:82:0C:CA:96:0D:7C:AC:21:B0:C4:D4:0B:BA:2A:1D:B6:81:1C:FF:65:40  Signature algorithm name: SHA256withRSA  Version: 3  Extensions:  #1: ObjectId: 2.5.29.35 Criticality=false  AuthorityKeyIdentifier [  KeyIdentifier [  0000: AE 06 0D A9 B0 E7 D8 28 FB AC 79 31 59 19 EE BF .......(..y1Y...  0010: 08 18 7F BA ....  ]  ]  #2: ObjectId: 2.5.29.19 Criticality=false  BasicConstraints:[  CA:true  PathLen:2147483647  ]  #3: ObjectId: 2.5.29.14 Criticality=false  SubjectKeyIdentifier [  KeyIdentifier [  0000: AE 06 0D A9 B0 E7 D8 28 FB AC 79 31 59 19 EE BF .......(..y1Y...  0010: 08 18 7F BA ....  ]  ]  \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* |

|  |
| --- |
| <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"  maxThreads="150"  SSLEnabled="true"  Address = "192.168.0.189"  keystoreFile="C:/zonvan/java.tools/tomcat/tomcat-test-ssl/ssk.key/zonvan.asuscomm.com.jks"  keyAlias="1"  keystorePass="zonvan4myPay"  >  </Connector>  <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"  maxThreads="150"  SSLEnabled="true"  Address = "127.0.0.1"  keystoreFile="C:/zonvan/java.tools/tomcat/tomcat-test-ssl/ssk.key/zonvan2.asuscomm.com.jks"  keyAlias="1"  keystorePass="zonvan4myPay"  >  </Connector>  <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"  maxThreads="150"  SSLEnabled="true"  Address = "192.168.88.1"  keystoreFile="C:/zonvan/java.tools/tomcat/tomcat-test-ssl/ssk.key/ip.jks"  keyAlias="1"  keystorePass="zonvan4myPay"  >  </Connector> |

|  |
| --- |
| <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"  maxThreads="150" SSLEnabled="true" >  <SSLHostConfig>  <Certificate certificateKeystoreFile="C:/zonvan/java.tools/tomcat/tomcat-test-ssl/ssk.key/zonvan.asuscomm.com.jks"  certificateKeystorePassword="zonvan4myPay"  certificateKeyAlias="1"  type="RSA" />  <Certificate certificateKeystoreFile="C:/zonvan/java.tools/tomcat/tomcat-test-ssl/ssk.key/zonvan2.asuscomm.com.jks"  certificateKeystorePassword="zonvan4myPay"  certificateKeyAlias="1"  type="RSA" />  <Certificate certificateKeystoreFile="C:/zonvan/java.tools/tomcat/tomcat-test-ssl/ssk.key/ip.jks"  certificateKeystorePassword="zonvan4myPay"  certificateKeyAlias="1"  type="RSA" />  </SSLHostConfig>  </Connector> |