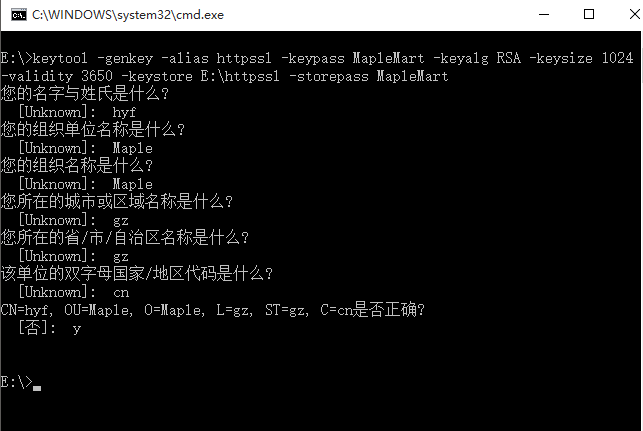
在dubbo-http-service项目中httpssl证书就是这样生成的



在申请Android Map API Key的时候使用到了java中Keytool，下面转一篇介绍java中Keytool的文章：  
<http://blog.csdn.net/tony1130/archive/2010/01/05/5134318.aspx>  
－－－－－－－－－－－－－－－－－－－－－－－－－

Keytool 是一个Java 数据证书的管理工具 ,Keytool 将密钥（key）和证书（certificates）存在一个称为keystore的文件中。

在keystore里，包含两种数据：

(1)密钥实体（Key entity）——密钥（secret key）又或者是私钥和配对公钥（采用非对称加密）   
(2)可信任的证书实体（trusted certificate entries）——只包含公钥

**JDK中keytool常用命令**:

**-genkey**      在用户主目录中创建一个默认文件".keystore",还会产生一个mykey的别名，mykey中包含用户的公钥、私钥和证书(在没有指定生成位置的情况下,keystore会存在用户系统默认目录，如：对于window xp系统，会生成在系统的C:\Documents and Settings\UserName\文件名为“.keystore”)

**-alias**       产生别名,每个keystore都关联这一个独一无二的alias，这个alias通常不区分大小写

**-keystore**    指定密钥库的名称(产生的各类信息将不在.keystore文件中)

**-keyalg**      指定密钥的算法 (如 RSA  DSA（如果不指定默认采用DSA）)

**-validity**    指定创建的证书有效期多少天

**-keysize**     指定密钥长度

**-storepass**   指定密钥库的密码(获取keystore信息所需的密码)

**-keypass**     指定别名条目的密码(私钥的密码)

**-dname**       指定证书拥有者信息

例如：  "CN=名字与姓氏,OU=组织单位名称,O=组织名称,L=城市或区域名称,ST=州或省份名称,C=单位的两字母国家代码"

**-list**        显示密钥库中的证书信息

**-v**           显示密钥库中的证书详细信息

**-export**      将别名指定的证书导出到文件

keytool -export -alias 需要导出的别名 -keystore 指定keystore -file 指定导出的证书位置及证书名称 -storepass 密码

**-file**        参数指定导出到文件的文件名

**-delete**      删除密钥库中某条目

keytool -delete -alias 指定需删除的别名  -keystore 指定keystore  -storepass 密码

**-printcert**   查看导出的证书信息

keytool -printcert -file yushan.crt

**-keypasswd**   修改密钥库中指定条目口令

keytool -keypasswd -alias 需修改的别名 -keypass 旧密码 -new  新密码  -storepass keystore密码  -keystore

**-import**      将已签名数字证书导入密钥库

keytool -import -alias 指定导入条目的别名 -keystore 指定keystore -file 需导入的证书

**下面是各选项的缺省值**。   
-alias "mykey"

-keyalg "DSA"

-keysize 1024

-validity 90

-keystore 用户宿主目录中名为 .keystore 的文件

-file 读时为标准输入，写时为标准输出 

**1、keystore的生成：**

(1)分阶段生成：  
     keytool -genkey -alias yushan(别名) -keypass yushan(别名密码) -keyalg RSA(算法) -keysize 1024(密钥长度) -validity 365(有效期，天单位) -keystore e:\yushan.keystore(指定生成证书的位置和证书名称) -storepass 123456(获取keystore信息的密码)；回车输入相关信息即可；  
       
(2)一次性生成：  
     keytool -genkey -alias yushan -keypass yushan -keyalg RSA -keysize 1024 -validity 365 -keystore e:\yushan.keystore -storepass 123456 -dname "CN=(名字与姓氏), OU=(组织单位名称), O=(组织名称), L=(城市或区域名称), ST=(州或省份名称), C=(单位的两字母国家代码)";(中英文即可)

**2、keystore信息的查看：**   
   keytool -list  -v -keystore e:\keytool\yushan.keystore -storepass 123456  
显示内容：  
---------------------------------------------------Keystore 类型： JKS  
Keystore 提供者： SUN

您的 keystore 包含 1 输入

别名名称： yushan  
创建日期： 2009-7-29  
项类型: PrivateKeyEntry  
认证链长度： 1  
认证 [1]:  
所有者:CN=yushan, OU=xx公司, O=xx协会, L=湘潭, ST=湖南, C=中国签发人:CN=yushan, OU=xx公司, O=xx协会, L=湘潭, ST=湖南, C=中国  
序列号:4a6f29ed  
有效期: Wed Jul 29 00:40:13 CST 2009 至Thu Jul 29 00:40:13 CST 2010  
证书指纹:

MD5:A3:D7:D9:74:C3:50:7D:10:C9:C2:47:B0:33:90:45:C3  
SHA1:2B:FC:9E:3A:DF:C6:C4:FB:87:B8:A0:C6:99:43:E9:4C:4A:E1:18:E8  
         签名算法名称:SHA1withRSA  
         版本: 3  
---------------------------------------------------

缺省情况下，-list 命令打印证书的 MD5 指纹。而如果指定了 -v 选项，将以可读格式打印证书，如果指定了 -rfc 选项，将以可打印的编码格式输出证书。

keytool -list  -rfc -keystore e:\yushan.keystore -

storepass 123456

显示：

---------------------------------------------------

Keystore 类型： JKS  
Keystore 提供者： SUN

您的 keystore 包含 1 输入

别名名称： yushan  
创建日期： 2009-7-29  
项类型: PrivateKeyEntry  
认证链长度： 1  
认证 [1]:  
-----BEGIN CERTIFICATE-----  
MIICSzCCAbSgAwIBAgIESm8p7TANBgkqhkiG9w0BAQUFADBqMQ8

wDQYDVQQGDAbkuK3lm70xDzAN  
BgNVBAgMBua5luWNlzEPMA0GA1UEBwwG5rmY5r2tMREwDwYDVQQ

KDAh4eOWNj+S8mjERMA8GA1UE  
CwwIeHjlhazlj7gxDzANBgNVBAMTBnl1c2hhbjAeFw0wOTA3Mjg

xNjQwMTNaFw0xMDA3MjgxNjQw  
MTNaMGoxDzANBgNVBAYMBuS4reWbvTEPMA0GA1UECAwG5rmW5Y2

XMQ8wDQYDVQQHDAbmuZjmva0x  
ETAPBgNVBAoMCHh45Y2P5LyaMREwDwYDVQQLDAh4eOWFrOWPuDE

PMA0GA1UEAxMGeXVzaGFuMIGf  
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCJoru1RQczRzTnBWx

efVNspQBykS220rS8Y/oX3mZa  
hjL4wLfOURzUuxxuVQR2jx7QI+XKME

+DHQj9r6aAcLBCi/T1jwF8mVYxtpRuTzE/6KEZdhowEe70  
liWLVE

+hytLBHZ03Zhwcd6q5HUMu27du3MPQvqiwzTY7MrwIvQQ8iQIDA

QABMA0GCSqGSIb3DQEB  
BQUAA4GBAGoQQ1/FnTfkpQh

+Ni6h3fZdn3sR8ZzDMbOAIYVLAhBb85XDJ8QZTarHbZMJcIdHxA

l1  
i08ct3E8U87V9t8GZFWVC4BFg/

+zeFEv76SFpVE56iX7P1jpsu78z0m69hHlds77VJTdyfMSvtXv  
sYHP3fxfzx9WyhipBwd8VPK/NgEP  
-----END CERTIFICATE-----

---------------------------------------------------

**3、证书的导出：**

keytool -export -alias yushan -keystore e:\yushan.keystore -file e:\yushan.crt(指定导出的证书位置及证书名称) -storepass 123456

**4、查看导出的证书信息**

keytool -printcert -file yushan.crt  
显示：（在windows下可以双击yushan.crt查看）  
---------------------------------------------------

所有者:CN=yushan, OU=xx公司, O=xx协会, L=湘潭, ST=湖南, C=中国签发人:CN=yushan, OU=xx公司, O=xx协会, L=湘潭, ST=湖南, C=中国  
序列号:4a6f29ed  
有效期: Wed Jul 29 00:40:13 CST 2009 至Thu Jul 29 00:40:13 CST 2010  
证书指纹:

MD5:A3:D7:D9:74:C3:50:7D:10:C9:C2:47:B0:33:90:45:C3  
SHA1:2B:FC:9E:3A:DF:C6:C4:FB:87:B8:A0:C6:99:43:E9:4C:4A:E1:18:E8  
签名算法名称:SHA1withRSA  
版本: 3  
---------------------------------------------------

**5、证书的导入：**准备一个导入的证书：  
keytool -genkey -alias shuany -keypass shuany -keyalg RSA -keysize 1024 -validity 365 -keystore  e:\shuany.keystore -storepass 123456 -dname "CN=shuany, OU=xx, O=xx, L=xx, ST=xx, C=xx";  
keytool -export -alias shuany -keystore e:\shuany.keystore -file e:\shuany.crt -storepass 123456  
 现在将shuany.crt 加入到yushan.keystore中：keytool -import -alias shuany(指定导入证书的别名，如果不指定默认为mykey,别名唯一，否则导入出错) -file e:\shuany.crt -keystore e:\yushan.keystore -storepass 123456 keytool -list  -v -keystore e:\keytool\yushan.keystore -storepass 123456  
显示：  
---------------------------------------------------

Keystore 类型： JKS  
Keystore 提供者： SUN

您的 keystore 包含 2 输入

别名名称： yushan  
创建日期： 2009-7-29  
项类型: PrivateKeyEntry  
认证链长度： 1  
认证 [1]:  
所有者:CN=yushan, OU=xx公司, O=xx协会, L=湘潭, ST=湖南, C=中国签发人:CN=yushan, OU=xx公司, O=xx协会, L=湘潭, ST=湖南, C=中国  
序列号:4a6f29ed  
有效期: Wed Jul 29 00:40:13 CST 2009 至Thu Jul 29 00:40:13 CST 2010  
证书指纹:

MD5:A3:D7:D9:74:C3:50:7D:10:C9:C2:47:B0:33:90:45:C3 SHA1:2B:FC:9E:3A:DF:C6:C4:FB:87:B8:A0:C6:99:43:E9:4C:4A:E1:18:E8  
签名算法名称:SHA1withRSA  
版本: 3  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

别名名称： shuany  
创建日期： 2009-7-29  
输入类型： trustedCertEntry

所有者:CN=shuany, OU=xx, O=xx, L=xx, ST=xx, C=xx  
签发人:CN=shuany, OU=xx, O=xx, L=xx, ST=xx, C=xx  
序列号:4a6f2cd9  
有效期: Wed Jul 29 00:52:41 CST 2009 至Thu Jul 29

00:52:41 CST 2010  
证书指纹:  
MD5:15:03:57:9B:14:BD:C5:50:21:15:47:1E:29:87:A4:E6  
SHA1:C1:4F:8B:CD:5E:C2:94:77:B7:42:29:35:5C:BB:BB:2E:9E:F0:89:F5  
签名算法名称:SHA1withRSA  
版本: 3  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
---------------------------------------------------

**6、证书条目的删除：**keytool -delete -alias shuany(指定需删除的别名) -keystore yushan.keystore -storepass 123456  
    
**7、证书条目口令的修改：**keytool -keypasswd -alias yushan(需要修改密码的别名) -keypass yushan(原始密码) -new 123456(别名的新密码)  -keystore e:\yushan.keystore -storepass 123456

**8、keystore口令的修改：**   
keytool -storepasswd -keystore e:\yushan.keystore(需修改口令的keystore) -storepass 123456(原始密码) -new yushan(新密码)

**9、修改keystore中别名为yushan的信息**

keytool -selfcert -alias yushan -keypass yushan -keystore e:\yushan.keystore -storepass 123456 -dname "cn=yushan,ou=yushan,o=yushan,c=us"