Certificates

D. Weber

Generation of a Key

```
$ keytool -genkey
Enter keystore password:  *kstore
What is your first and last name?
  [Unknown]:  Damian Weber
What is the name of your organizational unit?
  [Unknown]:  GIS
What is the name of your organization?
  [Unknown]:  HTW
What is the name of your City or Locality?
  [Unknown]:  SB
What is the name of your State or Province?
  [Unknown]:  Saar
What is the two-letter country code for this unit?
  [Unknown]:  DE
Is
```

```
   CN=Damian Weber, OU=GIS, O=HTW, L=SB, ST=Saar, C=DE
correct?  [no]:  yes

Enter key password for <mykey>
        (RETURN if same as keystore password):

$ ls -l ~/.keystore
-rw-r--r--  1 dw  users  1222 Jun 27 14:47 .keystore
```

List the Keystore

```
$ keytool -list
Enter keystore password:  *kstore

Keystore type: jks
Keystore provider: SUN

Your keystore contains 1 entry

mykey, Jun 27, 2004, keyEntry,
Certificate fingerprint (MD5):
        3A:13:67:EF:BD:83:D3:E9:B0:22:51:91:8F:44:7A:E9
```

Export the X.509v1 Certificate

```
$ keytool -export -file mykey.cert
Enter keystore password:  *kstore
Certificate stored in file <mykey.cert>

$ keytool -printcert -file mykey.cert
Owner: CN=Damian Weber, OU=GIS, O=HTW, L=SB, ST=Saar, C=DE
Issuer: CN=Damian Weber, OU=GIS, O=HTW, L=SB, ST=Saar, C=DE
Serial number: 40dec1f4
Valid from: Sun Jun 27 14:47:48 CEST 2004
     until: Sat Sep 25 14:47:48 CEST 2004
Certificate fingerprints:
MD5:  3A:13:67:EF:BD:83:D3:E9:B0:22:51:91:8F:44:7A:E9
SHA1:
C2:12:B0:17:00:C8:DC:7B:36:75:63:94:77:EB:68:BF:D4:23:25:1C
```

Generate Certificate Signing Request

```
$ keytool -certreq  -file mykey.csr
Enter keystore password:  *kstore
$ cat mykey.csr
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICYTCCAh8CAQAwXDELMAkGA1UEBhMCREUxDTALBgNVBAgTBF...
CgYDVQQKEwNIVFcxDDAKBgNVBAsTA0dJUzEVMBMGA1UEAxMMRG...
ByqGSM44BAEwggEfAoGBAP1/U4EddRIpUt9KnC7s5Of2EbdSPO...
WPq/xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7...
O8UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjx...
9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOut...
zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx+2J6AS...
Zl6Ae1UlZAFMO/7PSSoDgYUAAoGBAPdqJ5DmvkrFc1jsc1Bqek...
ZBezPKbHlujHGFy40SC8/FA02ift/uWV0vDyQVjjsu/QBNqwIV...
-----END NEW CERTIFICATE REQUEST-----
```

SSL Certificate (Serial Number+SigAlg)

On connection establishment, the server sends its certificate.

```
==========================================================
connecting to host
www.bankline.deutsche-bank.com IP 193.150.167.18
==========================================================
SSL connection using DES-CBC3-MD5
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
    64:3d:dd:b6:f1:10:c5:23:cc:f9:db:6e:69:45:2d:09
Signature Algorithm: sha1WithRSAEncryption
```

SSL Certificate (CA+Subject)

```
Issuer: O=VeriSign Trust Network, OU=VeriSign, Inc.,
OU=VeriSign International Server CA - Class 3,
OU=www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97
Validity
    Not Before: Mar  3 00:00:00 2004 GMT
    Not After : Mar  3 23:59:59 2005 GMT
Subject: C=DE, ST=Hessen, L=Eschborn, O=Deutsche Bank AG,
         OU=CIB/GTO Access Systems,
         OU=Terms of use at www.verisign.com/rpa (c)00,
         CN=www.bankline.deutsche-bank.com
```

SSL Certificate (Public Key)

```
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
        Modulus (1024 bit):
            00:e6:11:3b:72:1f:77:98:33:96:2f:1d:9f:44:4b:
            17:17:a0:3f:e6:02:c2:4e:51:5d:ed:5b:ce:b1:ca:
            75:da:d5:3d:7f:65:a6:e1:33:ea:68:f8:fc:f8:c2:
            f2:09:32:f5:cf:c0:3f:ed:10:d3:09:24:63:c7:ab:
            55:52:bf:4e:14:e2:0f:6e:24:49:a3:bf:f8:95:83:
            88:f0:87:be:86:fb:d4:52:c2:6b:f1:6a:27:25:e0:
            ec:c7:39:6c:31:d3:d5:13:03:8b:96:2b:92:52:4b:
            45:f4:5b:a5:70:f3:0f:a5:a2:aa:4b:7d:fc:e0:f2:
            26:c1:3f:fe:21:fe:d2:6c:1d
        Exponent: 65537 (0x10001)
```

SSL Certificate (Additional Info)

```
X509v3 extensions:
 X509v3 Basic Constraints:
     CA:FALSE
 X509v3 Key Usage:
     Digital Signature, Key Encipherment
 X509v3 CRL Distribution Points:
 URI:http://crl.verisign.com/Class3InternationalServer.crl
 X509v3 Certificate Policies:
     Policy: 2.16.840.1.113733.1.7.23.3
       CPS: https://www.verisign.com/rpa
```

OpenSSL Code

```
#include <openssl/ssl.h>
/*...*/
struct sockaddr_in sa;
X509*  server_cert;
/*...*/
sd = socket (AF_INET, SOCK_STREAM, 0);
/*...*/
sa.sin_port= htons(port);
err = connect(sd, (struct sockaddr*) &sa, sizeof(sa));
SSL_set_fd (ssl, sd);
err = SSL_connect (ssl);
printf ("SSL connection using %s\n", SSL_get_cipher (ssl));
server_cert = SSL_get_peer_certificate (ssl);
X509_print_fp(stdout,server_cert);
/*...*/
```

```
SSL_shutdown (ssl);
close (sd);
```