



<u>Тема</u> **Безопасность в JAVA**

Часть Сертификат изнутри

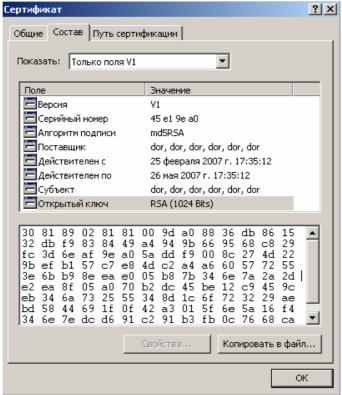
Автор ASKIL (omendba@gmail.com)

26.02.2007

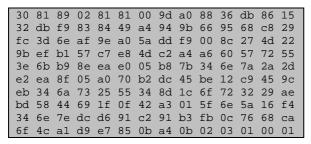
Рассмотрим, каким образом можно получить доступ в внутренности сертификата.

Пусть имеется сертификат c:/DorPubCert.crt. Его свойства можно про-

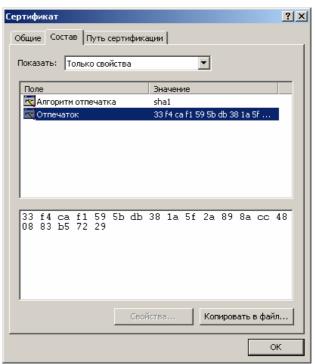
смотреть на рисунке.



Открытый ключ RSA имеет вид:



Свойства сертификата:



В шестнадцатеричном виде сертификат выглядит следующим образом:

```
3082 021A 3082 0183 0204 45E1 9EA0 300D 0609 2A86
4886 F70D 0101 0405 0030 5431 0C30 0A06 0355
1303 646F
          7231 0C30 0A06 0355 0408
                                    1303 646F
OC30 OA06 O355 O407 1303 646F
                              7231
                                    OC30 OA06 0355
               7231 0C30 0A06 0355
040A 1303 646F
                                    040B 1303
7231 0C30 0A06 0355 0403
                         1303 646F
                                    7230
                                         1E17
                         325A
                                    3037 3035
3730 3232
          3531
               3433
                    3531
                              170D
               5A30 5431
                         0030
                                    0355
3134
    3335
          3132
                               DAD6
                                         0406
646F
    7231
          0C30 0A06 0355
                         0408
                              1303
                                    646F
                                         7231
OA06 0355
          0407
               1303 646F
                         7231
                               OC30 OA06 O355
1303
    646F
               OC30 OA06 O355
                               040B
                                    1303
                                         646F
          7231
               0403
                               7230
                                              0609
OC30 OA06 O355
                    1303
                         646F
                                    819F
                                         300D
2A86 4886 F70D 0101 0105 0003 818D 0030 8189
8100
    9DA0 8836
               DB86
                    1532
                         DBF9
                               8384
                                    49A4
                                         949B
                         DDF9 008C
          3D6E AF9E A05A
                                    274D
6808
    29FC
                                         229B
                         553E 6BB9 8EEA E005
57C7 E84D C2A4 A660 5772
346E 7A2A
          2DE2
               EA8F
                    05A0
                         70B2
                               DC45
                                    BE12 C945
346A
    7325
          5534 8D1C 6F72
                         3229 AEBD
                                    5844 691F
A301 5F6E 5A16 F434 6E7E DCD6 91C2
                                    91B3 FB0C
          D9E7
               850B A40B
                         0203
                               0100
                                    0130
                                         0D06
     4CA1
8648 86F7
          ODO1 0104 0500 0381 8100 0E60 73DD
1675 FA05 BBB4 C0B2
                    2CCD F98A
                                    07CE 25E2
                              3717
483A 615C
          5175 BD52 D6DA
                         149C
                               CB20
                                    13D4 6023
          6678
DE9E 056C
               9894 B223 DC31 DD4D
                                    7051 7A52
D7CB 4EF8 E02A DADF 536B 86D5
                              20EC
                                    2457 FF8F
5DF6 131B AB72 B511 7A36 E0B5 C565
                                   FB5E 057A
          79D5 7E5A 87DA 7333 04A3 BC6C B57D
```

Получить сырые байты подписи сертификата можно с помощью метода getSignature(). Эти байты используются для того, чтобы явно проверить подпись вместо использования метода verify():

```
X509Certificate x509 = GetCert("c:/DorPubCert.crt");
System.out.println(GetHexString(x509.getSignature()));
```

При выполнении кода будет выведено следующее:

```
OE 60 73 DD 25 D5 16 75 FA 05 BB B4 C0 B2
2C CD F9 8A 37
               17
                  07
                     CE 25 F2 2F
                                 38
                                    48 3A
61 5C 51 75 BD 52 D6 DA 14 9C
                              CB
                                 20
60 23 CA CE 0E 9E 05 6C 66 78 98 94 B2 23
DC 31 DD 4D 70 51 7A 52 87 1C D7 CB 4E F8
  2A DA DF 53
               6B 86
                     D5
                        20
                           EC
                              24
                                 57
2F 65 5D F6 13 1B AB 72 B5 11 7A 36 E0 B5
C5 65 FB 5E 05 7A 5D 49 A0 C2 C1 BF 79 D5
7E 5A 87 DA 73 33 04 A3 BC 6C B5 7D 81 DD
  48
```

```
3082 021A 3082 0183 0204 45E1 9EA0 300D 0609 2A86
4886 F70D 0101 0405 0030 5431 0C30 0A06 0355 0406
                                 0408
1303 646F
           7231 0C30 0A06 0355
                                       1303 646F
                                                  7231
                                       OC30 OA06 0355
OC30 0A06 0355 0407
                      1303
                           646F
                                 7231
040A 1303 646F
                7231
                      OC30 OA06 0355
                                       040B 1303
     OC30 OA06 0355
                      0403
                            1303
                                 646F
                                       7230
7231
                                            1E17
3730
     3232
          3531 3433
                      3531
                            325A
                                 170D
                                       3037
                                            3035
3134
     3335
           3132
                5A30
                      5431
                           0030
                                 OA06 0355
                                            0406
                                                  1303
     7231
          0030
                DAD6 0355
                           0408
                                            7231
646F
                                 1303 646F
                                                  0030
0A06 0355
           0407
                1303
                      646F
                            7231
                                 DC30 0A06 0355
                                                  040A
1303
     646F
           7231
                0030
                      0A06
                           0355
                                 040B
                                       1303
                                            646F
                                                  7231
OC30 OA06 O355 O403
                      1303 646F
                                 7230 819F
                                            300D 0609
     4886 F70D
                0101
                      0105
                           0003
                                 818D
                                       0030
                                            8189
8100
     9DAO 8836 DB86
                      1532
                           DBF9
                                 8384
                                       49A4
                                            949B
           3D6E AF9E
                      A05A
                           DDF9
                                       274D
6808
     29FC
                                 0080
                                            229B
     E84D C2A4
57C7
                A660
                      5772
                            553E
                                 6BB9
                                       SEEA.
                                            E005 B87B
                      05A0
346E 7A2A
          2DE2
                EA8F
                           70B2
                                 DC45
                                       BE12
                                            C945
                                                  9CEB
     7325
           5534
                8D1C
                      6F72
                            3229 AEBD
                                       5844 691F
A301
     5F6E 5A16 F434 6E7E
                           DCD6 91C2
                                       91B3 FB0C
                                                  7668
     4CA1 D9E7 850B A40B 0203 0100
                                       0130 OD06
                                                  1192A
CA6F
          0001 0104 0500
                           0381
                                 8100
     86F7
                COB2
BD52
                                                  2F38
CACE
                                       D7CE
                BD52 D6DA
9894 B223
DADF 536B
B511 7A36
          5175
6678
E02A
     615C
056C
                                       13D4
7051
                            149C
                           DC31
                                 DD4D
                                                  8710
                           86D5
                                       2457
     4EF8
                            EOB5
                                       FB5E
     131B
     C1BF
```

Получить DER-кодировку TBS сертификата. *TBS сертификат* — основа сертификата; он содержит все обозначения и ключевую информацию. Единственная информация, которая не содержится в TBS — название алгоритма подписи. Байты TBS сертификата используются как входные данные для алгоритма подписи сертификата.

```
X509Certificate x509 = GetCert("c:/DorPubCert.crt");
System.out.println(GetHexString(x509.getTBSCertificate()));
```

При выполнении кода будет выведено следующее:

```
30 82 01 83 02 04 45 E1 9E A0 30 0D 06 09
                                                  3082 021A 3082 0183 0204 45E1 9EA0 300D 0609 2A86
                                                  4886 F70D 0101 0405 0030 5431 0C30 0A06 0355 0406 1303 646F 7231 0C30 0A06 0355 0408 1303 646F 7231
2A 86 48 86 F7 0D 01 01 04 05 00 30 54 31
OC 30 0A 06 03 55 04 06 13 03 64 6F 72 31
OC 30 0A 06 03 55 04 08 13 03 64 6F 72 31
                                                  OC30 OA06 O355 O407 1303 646F 7231 OC30 OA06 O355
OC 30 0A 06 03 55 04 07 13 03 64 6F
                                                  040A 1303 646F
                                                                  7231 0C30 0A06 0355 040B 1303 646F
OC 30 0A 06 03 55 04 0A 13 03 64 6F 72 31
                                                  7231 0C30 0A06 0355 0403 1303 646F 7230 1E17 0D30
                                                  3730 3232 3531
                                                                  3433
                                                                       3531
                                                                             325A 170D 3037
                                                                                             3035 3236
OC 30 0A 06 03 55 04 0B 13 03 64 6F 72 31
                                                  3134 3335 3132 5A30 5431 0C30 0A06 0355 0406 1303
OC 30 0A 06 03 55 04 03 13 03 64 6F 72 30
                                                  646F 7231 0C30 0A06 0355 0408 1303 646F 7231 0C30
1E 17 0D 30 37 30 32 32 35 31 34 33 35 31
                                                  OAO6 0355 0407 1303 646F
                                                                            7231 0C30 0A06 0355 040A
32 5A 17 0D 30 37 30 35 32 36 31 34 33 35
                                                  1303 646F 7231 0C30 0A06 0355 040B 1303 646F 7231
31 32 5A 30 54 31 0C 30 0A 06 03 55 04 06
                                                  OC30 OA06 O355 O403 1303 646F
                                                                                  7230 819F
                                                                                            300D 0609
13 03 64 6F 72 31 0C
                       30 0A 06 03 55 04 08
                                                  2A86 4886 F70D 0101 0105 0003 818D 0030 8189 0281
13 03 64 6F 72 31 0C 30 0A 06 03 55 04 07
                                                  8100 9DA0 8836 DB86 1532 DBF9 8384 49A4 949B 6695
13 03 64 6F 72 31 0C 30 0A 06 03 55 04 0A
                                                  68C8 29FC 3D6E AF9E A05A DDF9 008C 274D 229B EFB1
                                                  57C7 E84D C2A4 A660
                                                                            553E 6BB9 8EEA E005 B87B
13 03 64 6F 72 31 0C 30 0A 06 03 55 04 0B
                                                  346E 7A2A 2DE2 EA8F 05A0 70B2 DC45 BE12 C945 9CEB
13 03 64 6F 72 31 0C 30 0A 06 03 55 04 03
                                                  346A 7325 5534 8D1C 6F72
                                                                            3229 AEBD 5844 691F 0F42
13 03 64 6F 72 30 81 9F 30 0D 06 09 2A 86
                                                  A301 5F6E 5A16 F434 6E7E DCD6 91C2 91B3 FB0C
48 86 F7 0D 01 01 01 05 00 03 81 8D 00 30
                                                  CA6F 4CA1 D9E7 850B A40B 0203 0100 0130
81 89 02 81 81 00 9D A0 88 36 DB 86
                                       15
                                                       86F7 0D01 0104
FA05 BBB4 C0B2
615C 5175 BD52
                                                                            0381
F98A
DB F9 83 84 49 A4 94 9B 66 95 68 C8 29 FC
3D 6E AF 9E AO 5A DD F9 00 8C 27 4D 22 9B
                                                       615C 5175
056C 6678
4EF8 E02A
131B AB72
                                                                 BD52 D6DA 149C
9894 B223 DC31
DADF 536B 86D5
B511 7A36 E0B5
                                                                                       13D4
7051
EF B1 57 C7 E8 4D C2 A4 A6 60 57 72 55 3E
                                                                                        2457
FB5E
                                                                                                  2F65
6B B9 8E EA EO 05 B8 7B 34 6E 7A 2A 2D E2
                                                                             E0B5
EA 8F 05 A0 70 B2 DC 45 BE 12 C9 45 9C EB
                                                       C1BF
34 6A 73 25 55 34 8D 1C 6F 72 32 29 AE BD
58 44 69 1F 0F 42 A3 01 5F 6E 5A 16 F4 34
6E 7E DC D6 91 C2 91 B3 FB OC 76 68 CA 6F
4C A1 D9 E7 85 OB A4 OB 02 03 01 00 01
```

Получаем дополнительную информацию о сертификате.

При выполнении кода будет выведено следующее:

```
Чтение сертификата:
Выписан для: CN=dor, OU=dor, O=dor, L=dor, ST=dor, C=dor
Подписано: CN=dor, OU=dor, O=dor, L=dor, ST=dor, C=dor
Сертификат имеет силу от Sun Feb 25 17:35:12 MSK 2007 до Sat May 26 18:35:12 MSD 2007
Номер сертификата SN# 1172414112
Алгоритм MD5withRSA
```

Если распечатать весь сертификат, то можно увидеть следующее при выполнении кода:

```
X509Certificate x509 = GetCert("c:/DorPubCert.crt");
System.out.println(x509);
```

```
Version: V1
 Subject: CN=dor, OU=dor, O=dor, L=dor, ST=dor, C=dor
 Signature Algorithm: MD5withRSA, OID = 1.2.840.113549.1.1.4
 Key: Sun RSA public key, 1024 bits
 modulus:
110689498759792672155782929226463744525925956518953088894220071981615059438556349315190\\
653779344085280701741510145939389039693407771597720310375610371057199112160617730261663
748999795979026063747825278238160648697218311179
 public exponent: 65537
 Validity: [From: Sun Feb 25 17:35:12 MSK 2007,
              To: Sat May 26 18:35:12 MSD 2007]
 Issuer: CN=dor, OU=dor, O=dor, L=dor, ST=dor, C=dor
SerialNumber: [45e19ea0]
 Algorithm: [MD5withRSA]
 Signature:
0000: 0E 60 73 DD 25 D5 16 75
                             FA 05 BB B4 C0 B2 2C CD
                                                      .`s.%..u....,.
                              2F 38 48 3A 61 5C 51 75
                                                      ..7...%./8H:a\Qu
.R.....`#....
0010: F9 8A 37 17 07 CE 25 F2
0020: BD 52 D6 DA 14 9C CB 20
                              13 D4 60 23 CA CE 0E 9E
                                                      .lfx...#.1.MpQzR
0030: 05 6C 66 78 98 94 B2 23
                              DC 31 DD 4D 70 51 7A 52
0040: 87 1C D7 CB 4E F8 E0 2A
                              DA DF 53 6B 86 D5 20 EC
                                                      ....N...*..Sk... .
0050: 24 57 FF 8F 2F 65 5D F6
                              13 1B AB 72 B5 11 7A 36
                                                      $W../e]....z6
                              5D 49 A0 C2 C1 BF 79 D5
0060: E0 B5 C5 65 FB 5E 05 7A
                                                      ...e.^.z]I....y.
0070: 7E 5A 87 DA 73 33 04 A3
                              BC 6C B5 7D 81 DD 79 48
                                                      .Z..s3...l...yH
```