All data below is presented in hexadecimal format.

Byte dump and explanation of the Target Colliding Certificates
---

% here starts the certificate

% ASN.1 tag[length]: byte length of entire certificate: 0x0629 = 1577
30[82:06:29]

% here starts the to be signed part

%% ihv[0] = 01234567 89ABCDEF FEDCBA98 76543210
%% begin prefix, begin block 1

% ASN.1 tag[length]: byte length of to be signed part: 0x0511 = 1297
30[82:05:11]

% version number: 0x02 stands for version 3
A0[03]
02[01]02

% serial number
% 0x010C0001 = 17563649
% 0x020C0001 = 34340865
02[04]01:0C:00:01 / 02[04]02:0C:00:01

% signature algorithm
30[0D]
06[09]2A:86:48:86:F7:0D:01:01:04
05[00]

% issuer DN starts here
30[3D]

% issuer CN
31[1A]
30[18]
06[03]55:04:03
% H a s h C o l l i s i o n C A
13[11]48:61:73:68:20:43:6F:6C:6C:69:73:69:6F:6E:20:43:41

% issuer L
31[12]
30[10]

%% end block 1
%% ihv[1] = 488FAE30 B8259F77 F81AA107 09F1667D / 8CD14B34 EE2CE093 EE1238A7 0A9449C1
%% begin block 2

06[03]55:04:07
% E i n d h o v e n
13[09]45:69:6E:64:68:6F:76:65:6E

% issuer C
31[0B]
30[09]
06[03]55:04:06
% N L
13[02]4E:4C

% validity period: January 1, 2006, 00h00m01s to December 31, 2007, 23h59m59s
30[1E]
% 0 6 0 1 0 1 0 0 0 0 0 1 Z
17[0D]30:36:30:31:30:31:30:30:30:30:30:31:5A
% 0 7 1 2 3 1 2 3 5 9 5 9 Z
17[0D]30:37:31:32:33:31:32:33:35:39:35:39:5A

% subject DN starts here
30[54]

% subject CN
31

%% end block 2
%% ihv[2] = 3E15562D 935DC895 0E86F877 F650A439 / 7D99D701 71564750 3BDA995E 53F9EB07
%% begin block 3

[19] / [15]
30[17] / 30[13]
06[03]55:04:03
% A r j e n K . L e n s t r a / M a r c S t e v e n s
13[10]41:72:6A:65:6E:20:4B:2E:20:4C:65:6E:73:74:72:61 / 13[0C]4D:61:72:63:20:53:74:65:76:65:6E:73

% subject O

```
31[16] / 31[1A]
30[14] / 30[18]
06[03]55:04:0A
%      C  o  l  l  i  s  i  o  n  a  i  r  s /        C  o  l  l  i  s  i  o  n     F  a  c  t  o  r  y
13[0D]43:6F:6C:6C:69:73:69:6F:6E:61:69:72:73 / 13[11]43:6F:6C:6C:69:73:69:6F:6E:20:46:61:63:74:6F:72:79

% subject L
31[12]
30[10]
06[03]55:04:07
%      E  i  n
13[09]45:69:6E

%% end block 3
%% ihv[3] = A2934A57 268FC8FB 99270DB2 BD42867F / 9756EBE6 6FC92AD6 0256345C 8EC444A8
%% begin block 4

%d  h  o  v  e  n
64:68:6F:76:65:6E

% subject C
31[0B]
30[09]
06[03]55:04:06
%      N  L
13[02]4E:4C

% ASN.1 tag[length]: byte length of public key info structure, 0x0422 = 1058
30[82:04:22]

% public key algorithm
30[0D]
06[09]2A:86:48:86:F7:0D:01:01:01
05[00]

% ASN.1 tag[length]: byte length of structure, 0x040F = 1039
03[82:04:0F]00

% ASN.1 tag[length]: byte length of subject public key info, 0x040A = 1034
30[82:04:0A]

% ASN.1 tag[length]: byte length of modulus field, 8192 bits, 0x0401 = 1025
02[82:04:01]

% public key modulus starts here

% zero byte to make integer positive
00

%% end prefix, block 4 still incomplete
%% begin birthday block

% modulus part 1: 96 birthdaying bits
EE73E7D6 B3B34FBA A1393D02 / 1A09B4CB 40C7267A AF017F9B

%% end birthday block, block 4 now complete
%% ihv[4] = 2D857B4E 0479B725 9F7662D4 7771220B / 2D857B4E A419FB61 3F17A610 17126647
%% begin 8 near collision blocks, blocks 5 to 12

% begin modulus part 2, near collision block 1
A4742581 8DC84F86 736E9072 28BBE877 / A4742581 8DC84F86 736E9072 28BBE877
0203858D 8CF1837A FF5E6C22 13036AF3 / 0203858D 8CF1837A FF5E6C22 13036AF3
D95C77E9 C2237D60 8CC4A9FB 97308BBF / D95C77E9 C2237D60 8CC4A9FB 97307BBF
9828612F 1599E261 5BCCDEDA 5930532F / 9828612F 1599E261 5BCCDEDA 5930532F

%% ihv[5] = E745A147 68C24DF4 F16EF79A 0EE57A77 / E745A147 086391F0 910F3B97 AE85BE73

% near collision block 2
B3DD1172 78E49440 1433630E 7461C1DC / B3DD1172 78E49440 1433630E 7461C1DC
9B801B2E 552015A5 13FF7AE7 973EF44B / 9B801B2E 552015A5 13FF7AE7 973EF44B
8352E4E0 4979B31E B600654D 51F4A381 / 8352E4E0 4979B31E B600654D 51F4A481
CEBE3F0B D099D130 D1456FAB E04A3E98 / CEBE3F0B D099D130 D1456FAB E04A3E98

%% ihv[6] = 6900F0DD 6880AD3B 8A559C5D 95807BC7 / 6900F0DD 0821F13B 2AF6DF5D 3521BFC7

% near collision block 3
85C8C4FB 297B86B5 7752CD64 19809FE3 / 85C8C4FB 297B86B5 7752CD64 19809FE3
7E6286F0 7732D1E0 69A5B4E5 6670B8BB / 7E6286F0 7732D1E0 69A5B4E5 6670B8BB
BAE5C211 742A131D 05711CF1 FE32AF93 / BAE5C211 742A131D 05711CF1 FE22AF93
3F1EEF22 4762E3AA DAC17C40 E448CA41 / 3F1EEF22 4762E3AA DAC17C40 E448CA41

%% ihv[7] = 6F48D9E5 989D51D0 5CA3E94D 800AF3F8 / 6F48D9E5 383E55D0 FC43ED4D 20ABF6F8

% near collision block 4
A879A03D 3CF665F2 39C7F3FE 82B384E8 / A879A03D 3CF665F2 39C7F3FE 82B384E8
35E7C9E8 BDEE30C2 68A21212 84789DF4 / 35E7C9E8 BDEE30C2 68A21212 84789DF4
2F44906F 19B79026 464436E1 DA65FA0C / 2F44906F 19B79026 464436E1 DA64FA0C
```

```
53A377FA 0D2B012B 7DDC2855 DAE5B551 / 53A377FA 0D2B012B 7DDC2855 DAE5B551

%% ihv[8] = 80D9AE06 6685A793 F953E15A 6EDE318F / 80D9AE06 0626A793 99F4E05A 0E7F318F

%% near collision block 5
51E28034 112120B5 E79EC5F2 6A9F69DA / 51E28034 112120B5 E79EC5F2 6A9F69DA
85D74EF6 A97A0B11 64EFA25F B1AE26BA / 85D74EF6 A97A0B11 64EFA25F B1AE26BA
451CCDA7 A2E78433 9C447D56 0549A60B / 451CCDA7 A2E78433 9C447D56 2549A60B
F0676294 BF580C91 9EC45702 5D3C7860 / F0676294 BF580C91 9EC45702 5D3C7860

%% ihv[9] = 73A70AC0 FAA8B223 9EAB7BE4 23EC6388 / 73A70AC0 9AC9B223 3ECC7BE4 C30C6488

% near collision block 6
B98296C0 AB9FE5B1 D353882E 26C1F721 / B98296C0 AB9FE5B1 D353882E 26C1F721
B41899D9 72B5A1D5 050B6845 36448010 / B41899D9 72B5A1D5 050B6845 36448010
AF8C7AFF 7CE8EACC B9B1FBBD D129D4F5 / AF8C7AFF 7CE8EACC B9B1FBBD C929D4F5
D499FB81 2924DF30 2CB3C450 23386297 / D499FB81 2924DF30 2CB3C450 23386297

%% ihv[10] = DE56FC8A 9A091FEB 1E6E537D 16629AC4 / DE56FC8A 3A0A1FEB BE6E537D B6629AC4

% near collision block 7
9396B3A4 6CD0FF7F 1426711C 459297B6 / 9396B3A4 6CD0FF7F 1426711C 459297B6
5D1CEF66 C18751E0 94BF08F3 B2981C5C / 5D1CEF66 C18751E0 94BF08F3 B2981C5C
CE52D963 D5A4259A 64557E4D 1B9EFE2D / CE52D963 D5A4259A 64557E4D 1B9EFE0D
9A516D1E 6EC8BB37 066825AE A6361660 / 9A516D1E 6EC8BB37 066825AE A6361660

%% ihv[11] = DCA82596 635B2D4F 0EDB818B DEE0D521 / DCA82596 835B2D4F 2EDB818B FEE0D521

% near collision block 8
2BD7D116 25A06A90 739B4D0A 06EA872A / 2BD7D116 25A06A90 739B4D0A 06EA872A
3AF9EBA1 2629BED6 7940561B D9374A89 / 3AF9EBA1 2629BED6 7940561B D9374A89
D60F0D72 2C9FEB68 33EC53F0 B0FD76AA / D60F0D72 2C9FEB68 33EC53F0 B0FD76A2
047B66C9 0FCEB1D2 E22CC099 B9A4B93E / 047B66C9 0FCEB1D2 E22CC099 B9A4B93E

%% end 8 near collision blocks, blocks 5 to 12
%% ihv[12] = 505D9746 FAB00B32 8018DBC3 4A87DF11
%% begin remaining modulus blocks, blocks 13 to 20

% begin modulus part 3
0000000F 54A89517 6E4C295A 405FAF54 CEE82D04 3A45CE40 B155BE34 EBDE7847
85A25B7F 894D424F A127B157 A8A120F9 9FE53102 C81FA90E 0B9BDA1B A775DF75

%% ihv[13] = DAC293C4 10FD4B46 5B174166 617DA963

D9152A80 257A1ED3 52DD49E5 7E068FF3 F02CABD4 AC97DBBC 3FA0205A 74302F65
C7F49A41 9E08FD54 BFAFC14D 78ABAAB3 0DDB3FC8 48E3DF02 C5A40EDA 248C9FF4

%% ihv[14] = 524312A4 FD34CF77 AF144C43 7EAC0BBF

7482850C FDFBDD9B C55547B7 404F5803 C1BB8163 2173127E 1A93B24A FB6E7A80
450865DB 374676D5 76BA5296 CCC6C130 82D1AB36 521F1A8A D945466B 9EF06AF4

%% ihv[15] = AA6FAC2C FD95D7C2 2F35ACF8 2B55B146

3A02D70B 7FB8B7DC 6D268C3D BA6898F6 552FA3FB B33DCBFA DA7B33FA 75D93AFE
262BD37A FF75995F D0E9774B A5A26A7C 443FF34E 461502A2 CB777E98 2D007375

%% ihv[16] = 065C03F4 E72681A5 4B874ABF 80BC3C3D

14B88ED2 8D61F428 E88387DF 2BF02230 AD17A9D4 4FF36485 0A07DB42 A7826AC2
EE3899CA C3EC2747 21D476D9 6658F537 16676587 F8FF14DB 8DE6741A FA2206DB

%% ihv[17] = D4852EBA A84E005A 8C82A341 46D0AD3A

A3B11828 BA87C6E1 E88A022F 1AA8DDD0 37EAB049 B5C7D305 3D0A63D7 861DEA07
B3D8B720 DE068CF4 7E657BB4 4450B85D 52F749D5 9572DF0C 0E3433B4 7C9AA19A

%% ihv[18] = FCABDB31 44B842CC D7E3DFE8 C94A6729

856F1DC3 CDADBAFB 143035C8 5A53AF57 22038F76 5C0D621B 66B69FFF FD091D4A
661A453B F1DAED1A 3A2341B3 7D7F623B 158F6EC0 2B49A253 64430FCB 5861483E

%% ihv[19] = 80AC53D6 1C9869AE A3208576 1A042D0F

1E9543ED 2EE7E54A 4C108A6E 64194098 0EE60D14 AEE559AF 30037E75 B2309CE0
21FFE310 9BF20538 92AB0AE4 03516E2A B58067F7

%% end remaining modulus blocks, blocks 13 to 20, block 20 still incomplete
%% begin remaining part of block 20

% public key exponent, 0x010001 = 65537
02[03]01:00:01

% version 3 extensions
A3[1A]
30[18]
30[09]
```

```
06

%% end block 20
%% ihv[20] = 0BA61117 33324BB0 9A2227F5 0C4496E2
%% begin block 21

[03]55:1D:13
04[02]30:00
30[0B]
06[03]55:1D:0F
04[04]
03[02]05:E0

% here ends the to be signed part

%% end block 21, still incomplete
%% MD5 padding and Merkle-Damgaard strengthening used to compute final ihv
%% ihv[final] = C6B2FE88 912770FC 6F2DB71F 58C7D251

% here starts the remainder of the certificate

% signature algorithm
30[0D]
06[09]2A:86:48:86:F7:0D:01:01:04
05[00]

% ASN.1 tag[length]: byte length of signature, 0x0101 = 257
03[82:01:01]00

% signature value, 2048 bits = 256 bytes
86C0876D 20682DC8 97443F97 690DDFB2 9074CB25 C358F09F 81234CE2 65A44333
CB6A78B2 32732917 00DCD6BA DF55088A 19A317A5 1D6092AC 3F6FC624 3601367A
6A2FC096 9B4E8913 BFC2315F 5AF35D83 FBD03C95 78392422 17BEB9AD 8873D442
F3A36200 CA198F63 45BCB76C CB27FCF2 DBEA239E 50FDDD3C D69304C9 50E7094A
FF0A9659 02B72206 D04E3759 BAED05AE 05922D8B E93556C8 CACDC360 6C56EE37
89C3775F 767A8909 AB444BC1 D7EE4A41 677302EF DF337B4C EE082D92 18FE44AA
5D68D34E FB796AC4 3219DCF8 DD4C2E6E C458EFA4 82DA7E18 1C086417 7124F0CF
214B0C5A 28EFECA4 0EC532BB 7673FFEA 9B9BD0A0 B1EFE6DB 97C518C4 DB17B9A5

% here ends the certificate

------------------------------
Construction of the RSA moduli
------------------------------

parts 1 and 2, 4192 bits (as bitstrings):

b1 =
EE73E7D6 B3B34FBA A1393D02 A4742581 8DC84F86 736E9072 28BBE877 0203858D\
8CF1837A FF5E6C22 13036AF3 D95C77E9 C2237D60 8CC4A9FB 97308BBF 9828612F\
1599E261 5BCCDEDA 5930532F B3DD1172 78E49440 1433630E 7461C1DC 9B801B2E\
552015A5 13FF7AE7 973EF44B 8352E4E0 4979B31E B600654D 51F4A381 CEBE3F0B\
D099D130 D1456FAB E04A3E98 85C8C4FB 297B86B5 7752CD64 19809FE3 7E6286F0\
7732D1E0 69A5B4E5 6670B8BB BAE5C211 742A131D 05711CF1 FE32AF93 3F1EEF22\
4762E3AA DAC17C40 E448CA41 A879A03D 3CF665F2 39C7F3FE 82B384E8 35E7C9E8\
BDEE30C2 68A21212 84789DF4 2F44906F 19B79026 464436E1 DA65FA0C 53A377FA\
0D2B012B 7DDC2855 DAE5B551 51E28034 112120B5 E79EC5F2 6A9F69DA 85D74EF6\
A97A0B11 64EFA25F B1AE26BA 451CCDA7 A2E78433 9C447D56 0549A60B F0676294\
BF580C91 9EC45702 5D3C7860 B98296C0 AB9FE5B1 D353882E 26C1F721 B41899D9\
72B5A1D5 050B6845 36448010 AF8C7AFF 7CE8EACC B9B1FBBD D129D4F5 D499FB81\
2924DF30 2CB3C450 23386297 9396B3A4 6CD0FF7F 1426711C 459297B6 5D1CEF66\
C18751E0 94BF08F3 B2981C5C CE52D963 D5A4259A 64557E4D 1B9EFE2D 9A516D1E\
6EC8BB37 066825AE A6361660 2BD7D116 25A06A90 739B4D0A 06EA872A 3AF9EBA1\
2629BED6 7940561B D9374A89 D60F0D72 2C9FEB68 33EC53F0 B0FD76AA 047B66C9\
0FCEB1D2 E22CC099 B9A4B93E

b2 =
1A09B4CB 40C7267A AF017F9B A4742581 8DC84F86 736E9072 28BBE877 0203858D\
8CF1837A FF5E6C22 13036AF3 D95C77E9 C2237D60 8CC4A9FB 97307BBF 9828612F\
1599E261 5BCCDEDA 5930532F B3DD1172 78E49440 1433630E 7461C1DC 9B801B2E\
552015A5 13FF7AE7 973EF44B 8352E4E0 4979B31E B600654D 51F4A481 CEBE3F0B\
D099D130 D1456FAB E04A3E98 85C8C4FB 297B86B5 7752CD64 19809FE3 7E6286F0\
7732D1E0 69A5B4E5 6670B8BB BAE5C211 742A131D 05711CF1 FE22AF93 3F1EEF22\
4762E3AA DAC17C40 E448CA41 A879A03D 3CF665F2 39C7F3FE 82B384E8 35E7C9E8\
BDEE30C2 68A21212 84789DF4 2F44906F 19B79026 464436E1 DA64FA0C 53A377FA\
0D2B012B 7DDC2855 DAE5B551 51E28034 112120B5 E79EC5F2 6A9F69DA 85D74EF6\
A97A0B11 64EFA25F B1AE26BA 451CCDA7 A2E78433 9C447D56 2549A60B F0676294\
BF580C91 9EC45702 5D3C7860 B98296C0 AB9FE5B1 D353882E 26C1F721 B41899D9\
72B5A1D5 050B6845 36448010 AF8C7AFF 7CE8EACC B9B1FBBD C929D4F5 D499FB81\
2924DF30 2CB3C450 23386297 9396B3A4 6CD0FF7F 1426711C 459297B6 5D1CEF66\
C18751E0 94BF08F3 B2981C5C CE52D963 D5A4259A 64557E4D 1B9EFE0D 9A516D1E\
6EC8BB37 066825AE A6361660 2BD7D116 25A06A90 739B4D0A 06EA872A 3AF9EBA1\
2629BED6 7940561B D9374A89 D60F0D72 2C9FEB68 33EC53F0 B0FD76A2 047B66C9\
0FCEB1D2 E22CC099 B9A4B93E

part 3, 4000 bits (as bitstring):
```

b =
0000000F 54A89517 6E4C295A 405FAF54 CEE82D04 3A45CE40 B155BE34 EBDE7847\
85A25B7F 894D424F A127B157 A8A120F9 9FE53102 C81FA90E 0B9BDA1B A775DF75\
D9152A80 257A1ED3 52DD49E5 7E068FF3 F02CABD4 AC97DBBC 3FA0205A 74302F65\
C7F49A41 9E08FD54 BFAFC14D 78ABAAB3 0DDB3FC8 48E3DF02 C5A40EDA 248C9FF4\
7482850C FDFBDD9B C55547B7 404F5803 C1BB8163 2173127E 1A93B24A FB6E7A80\
450865DB 374676D5 76BA5296 CCC6C130 82D1AB36 521F1A8A D945466B 9EF06AF4\
3A02D70B 7FB8B7DC 6D268C3D BA6898F6 552FA3FB B33DCBFA DA7B33FA 75D93AFE\
262BD37A FF75995F D0E9774B A5A26A7C 443FF34E 461502A2 CB777E98 2D007375\
14B88ED2 8D61F428 E88387DF 2BF02230 AD17A9D4 4FF36485 0A07DB42 A7826AC2\
EE3899CA C3EC2747 21D476D9 6658F537 16676587 F8FF14DB 8DE6741A FA2206DB\
A3B11828 BA87C6E1 E88A022F 1AA8DDD0 37EAB049 B5C7D305 3D0A63D7 861DEA07\
B3D8B720 DE068CF4 7E657BB4 4450B85D 52F749D5 9572DF0C 0E3433B4 7C9AA19A\
856F1DC3 CDADBAFB 143035C8 5A53AF57 22038F76 5C0D621B 66B69FFF FD091D4A\
661A453B F1DAED1A 3A2341B3 7D7F623B 158F6EC0 2B49A253 64430FCB 5861483E\
1E9543ED 2EE7E54A 4C108A6E 64194098 0EE60D14 AEE559AF 30037E75 B2309CE0\
21FFE310 9BF20538 92AB0AE4 03516E2A B58067F7

The RSA moduli in the two certificates are n1 = b1 || b and n2 = b2 || b.
Note that in fact n2, seen as integer instead of as bitstring, has only
8189 bits rather than 8192.
These moduli have the factorization into primes n1 = p1 * q1 and n2 = p2 * q2, where

p1 (1976 bits) =
FF6E89C1 C29EC1B6 DCAC6227 EAD2226C E7E07D35 3F2296F7 940E6154 17A8363C\
482171DE ECC75091 E5934F7E 7C1D6EAC 90B3A8D7 AD7C39CD A6364D79 CE8D9063\
906933C9 64EAACF5 003B5D3A 1DF30C83 74C3CE80 4E54B4A8 DB6AEF33 166E282F\
8425B5A9 9E640BC0 F87C3507 C888119E 2479DCF4 4E88538B CE9E7BC3 A7D7A454\
78F69937 9FA845DB 43636513 FB3C2468 D32AB56F FD4A49C4 D73EB135 6C6FFEAA\
921B8A27 6DF4CA34 512835C4 CCC3E6B2 77A689F5 73009A2B 90E985FD E63CE7F3\
59D30AC1 92A2C97F 05C9DCEC 46B17355 0F926164 9F4613E8 B349B5C4 CB090692\
8278DBFF 534B02E8 5A305B93 069BA793 5893BE68 F9C197

q1 (6216 bits) =
EEFBB2C9 1643AA22 781B125D 90AD9902 042ED052 014C6850 75CEA8D9 DFB1D536\
62BD8F25 591F997C EA8858A7 5AE94F6D 44C72F78 20531F3B 76557D32 F76AA193\
1394BED3 58F05230 3C9D7BA4 2BD36096 56413726 06518755 FF242A65 162E22C5\
52A6A93B 9A1A534B 542985A5 799BC125 12B81601 72A3934A 36EA6D56 A42D4AA9\
38BF9A34 8337A180 A2EDC533 F6FCE2C0 5E434E5D 94E6112B 775059D5 B1F5C7F8\
287B90E3 20A47EFD DBA228FE 9FFF8CC5 9DB27028 1AE4E90E 4E03C910 06DD5796\
E4C49AB6 F848EC4B 771A8195 058563EE 4528B15A 059D5FCC 8F3939FA 85984875\
B5F39D75 AA0DA66E D8B98D99 6C72EFDD 975FE67D 825D57C4 AB30442C A6747292\
4B1E6880 754B3B0A 46E3EFFD A2F23D1B 7CE849E4 0CCDBBF7 9DA76994 6B73627C\
32BE54E1 3FE041FA 8FBA9E09 266ED779 E99F38D3 E246D6E9 40CB02D1 F1F2A431\
53193A7E 83C387D2 A5D1CD25 D553A43A 528F3274 5F3CA462 3300A2CD 62E7A8EA\
73317CD3 6E0C755F 74F71683 979362EF 54217090 FEC5DDD7 498EEF4F AC394418\
7FDDA2C2 565B67E5 44811F29 D81DFF84 8B2A7365 1775F731 0E1869AD 05E98A51\
1E864DE8 D95F0F7A 1A6091A8 A59BB1F9 22EA8D09 CBE26A04 00ECFC5C BC6C7066\
90E9D1CC EE596AE7 F11B78B3 39330FEE 5F8E5C3A 0ADE07D0 A477F948 D06EB446\
E0023D60 1B7B55A5 6C898F14 64BAA6A1 EC4A71D1 4E8EA3B0 7197FF6B 8EF9CD2F\
94866D85 2ACD066E 2B25ABE3 96D7C271 329B8A2A C75AACA4 555A0B4B E6AF1D92\
52C6F5BE 27D37E3D 4BB1E034 FAB8C70C 841AB59D FFA27261 969FFFF6 28A05179\
D21710CF 592D83D0 CCC109B1 271A5DB2 BD75DB3A 000097D1 6B8CEC14 297FA12D\
106E06A3 76B3006E 8DA72E63 F77B0230 68C8A01C D6845E96 5238C34D 52E8B1D8\
EF0400AC 1C70AD19 96DB608C 16D41D92 29D2E890 5C4554C0 FBB173B3 6427218B\
65344D06 B4863B32 3A7FAF5F B7CD0E95 0AD91A7E 533227B8 E0D9E3EA 7478302A\
2F754192 FB2E635E C9A42AAB 5ECFA80F F32AED07 DD0DAB62 78AD814E E4652611\
DB25A22B 759D69D8 92518FE1 9ECA67AF F5D31D53 D1FF354F 18C3D801 FB907C5B\
F47FD09F 433DE498 A1

p2 (1976 bits) =
F134344B 72A468C3 EA7A5B2F 97CDFE2F DB9194CE 47B03C85 9A4E8A0F BE2B1B1B\
55CE1E96 5409BB5F 0F07F2CF B67C3FE3 27853D37 8D0038A6 94A16AAD 84038E18\
D69746A4 C1126D21 D5839065 F0885C60 BB174114 B76B003F 368AB2EF 6FF46A59\
34DBCBE1 1517FD9E 6F418A06 F4F3BE6A ABB77B2F 999B4FE9 76C8096E C0133761\
AFD0149B 4816EAC9 2C06E1AF 60C05F19 FDA2A23A B4A5CA4A 05403033 EB65FB3C\
648B0536 09C5C43A 4EE308CA BA8E639C EB7C297D 56A398DD C35E42B7 31AFC9C0\
22414B8F 6A94A280 E4D9EF28 F995553B 3FA3E308 19911F98 43276163 91336C18\
85EC8062 A1D2CA68 990C0174 561DAE3F 6B3C7378 2D53BD

q2 (6213 bits) =
1BA29917 5A36417B 7D97B956 83424A92 BA57330B 65059FE1 B8C6C851 AC35CB95\
1D8F4FD3 0944C356 6F92597A D8D4519A BB71045F 7B61A1A7 AEF2AEC4 8AD107B9\
7724604D 14754534 4121848C 6E80263B 5BD9CD43 F94222DE CCDCBA6E 9A03BF36\
FF54C9BC B6E5CC95 8994F401 FB815CF7 F91895BF D7CFF28D A45D5A03 AFD310A4\
0A8BDAD5 98788687 6200AEC9 4F67B27A 82675E9C 3BBAD1C1 7CCEF5D9 369743C7\
2D295656 08BC22B1 D96834F2 C94AF09E 2C784485 A48CDA49 8433E583 1CB519EE\
D3539DA2 155BF840 DE5F20A3 2C3D7382 939B1242 E1109A47 E06B651A 3A798E6D\
62A00CF5 A1C74DC1 E21D8D07 C3015468 A8DADF90 7AD5084F FF1ACABE F8D3F552\
CCBD8632 ADC35F57 4EFEEF42 AA6BA84D 994106EB 8E582B71 A983D924 756A948A\
161B9CBB 9E234355 3D213D65 2E8D8CCC 9133ED6D 8FC22E06 DA5A35DE 2AE38B1A\
3D859695 21C2C1EE B0605B0A 3382A34A 3D1EBA3E 83CFE6C0 8EDD83D0 538DFDEE\
8316DDB0 74061320 EE26F11C 43E2E0B9 02DC4FEF 0871F130 A3DA2946 7E1867C8\
795B581C 01E66EB5 625BAE28 37375FAA EA6653CC FF15651B B305B66D 93CCC8EA\
092FF2D0 3B191B4D E083208A E56D0F76 C2F6C9B6 E8CC8A7F 23AD678D 2ABFEF52\
301F0940 68475A41 AEED7E6A 9D8F1FAE FCBB0E18 2B8A0AF3 910BC7F1 AFDA9A63\
553B3393 6FF4D95F 540D8BA7 B898275D 1EB75ED1 11900FA0 50C6B9F9 27F3A06C\

3016CBA0 2DB94B12 1F21828C 8547D8A6 6C995FE7 6B114642 67BAB44D 7C7C2DC9\
A5944CCC 720777CF 2B9DDCF1 DF731D58 FC74A430 A44A22BE 24135CC2 2E6DF762\
49ACBC96 948E89E9 CFFCD00A C80DEF90 868D3BDC 8BAFE546 C4611DCA 49782A3A\
08FCCFD1 9A84EEA1 480F49AB 6F22A17D 63D56141 ED8613ED 2227DEE7 3D57811B\
E05A847B 965C30AB 6120C732 8E5E969B 881DAB4B 8EC9CA63 2AC8F190 1EE91621\
5F930A8A D3FDC065 EDF8D536 08D7860F 5D9CA14A 9B546B98 E2F6943F 00064173\
D652BFC4 0701F794 210E0594 C8F5D78D B698FB98 E2B3608A A1881E4F 13B90C3A\
08E86918 8C47C8E7 D9AD2D0F E57527E1 994AF6C0 CDA91FB4 EC336A73 F06DD12C\
53AE7787 116FAA8B C3

Both RSA key pairs have public exponent

e = 010001

but their private exponents are of course different

d1 =
0A4752C2 0D82F837 DA45465C FBCBC9E6 18BF7EB6 13F9BB1E 40A540F3 0852308A\
967DBEA6 29A5DF51 64B26C04 D0E4CC82 760CE395 AADBBB5C 0DFB58BA CC8B490D\
2788379A ECC31B04 1C7E19C7 DF9FF2E5 95527D15 7A097106 A97BA148 AA274E84\
A3C4BB4A 1F5F8EE3 B6C04EF5 8656A769 07A1C857 D58E94CF 4D6E1732 3C403525\
843B6D2A 068B50B1 FEFC1450 ACCBA7BA 0FE2B43E D442EC79 9923D340 922D1B15\
F87D6750 9E1D377B FFFB71EB 1DB653B4 3EE6A566 45DAC75D A3107A43 05A086BC\
5A8967B8 F0AF1075 17A20F9D DEEE473A FC8ABE80 3F7F6004 238C2B79 7B015FD1\
B9862FF1 E162C316 AB412BC5 DFD7BBC6 1E3CAC69 09F45CC2 F8588F0E BC478A29\
0CCF8515 E24E52B3 88906F74 7E97F2C0 E7CA997B 185C74E4 C39804EB F3054D2D\
9AABFEC9 59F0E0F9 250C8AE8 35E7314B 10C43976 37C98701 902A5BC4 BD872C61\
622C470F C441AB87 7FB9B700 10A562F8 34A79B00 9A914C84 FBB39539 D6260C29\
70AB31DC 9AE0499F 3E933080 0D921349 420F33A6 BFCEA05E FE0FCBE1 C4E46D1F\
713DC17A B895F0EE 9731563F F44CE23E D790476C 01181F6C 9AD391FE 363410BA\
6782C061 F34C745C 9BAB1D3B 4E1D7254 A174292C EFCFB80E E65957DC 7382C17D\
9E036721 1127A65F D4BA4908 3A45F024 04C2B1A7 B6268F03 9FC55DB0 C1C36C88\
932DF3EA EB14C2ED 2AF191B4 F5BE28D3 F302DD69 2AA0CBF9 20256DAB 7E24C918\
0F5E0D34 57CA63BA A7479C12 FFD0B0F0 7D804EBE 1B15C192 076801D4 232964D9\
62BB4FA2 BF25043A 9EB6312C F01502FA B367300A C9BFFF5F B2F2C0A4 05F8BC5D\
937CA10D 6BD8AFB9 92632D95 8EEEC9A3 91A7FA69 B7254DCB F682A56E BC0F25AA\
A67F49D6 62DA4C67 B25F722B 8C8A80A3 02BB9FA1 B911A0F8 23EBB160 758CC565\
12D266E0 CCD329E7 179EC8CB C7E92798 C03A99FF 8BB6E704 5458457B 753F671C\
FABB7CBD 89529F91 9B90AC34 0A603B65 96783541 C910C0AC CC48B4D2 B94825B8\
B10F613A C2C85FE0 3D42B60D 091AFBFE AAF5D48A 96D0442F 330621F0 451DC17C\
5856A0B1 46F3F9CB C491339C 0F131E37 848F3290 6305640D FFB95EFD 30FF78BE\
B7E1F025 AABEAE32 279507F8 2EF6B1DE 06129809 E3970442 C81FBC2D E3CAC48F\
371719CD D383D796 5EAA295C 5C2DCF50 EFF57B0D F65A707E FADC9F7E AC1C41D8\
2A45F976 0BE3BBE1 E6BC15F5 A14BC600 29008297 9A9FC238 F82F6E81 B5942716\
7F8B3E50 36E73312 C481F377 3EA0E735 1B742192 6757B011 F8369A9B D62157EE\
AA52DECF B18C3B05 C3BCAF6A 57C03A51 B70D2AAC BF67B803 DA5202E6 9B51A8A2\
68E33542 5651BF6F 4A71F374 5AEAC841 C59E5B99 223769B9 497E3E39 018F719B\
109341FE F75E195D 13941A0C 7365165D 76BFC771 4C248D2B D1FAD547 0F0FE2F3\
3DF1D3BF B258ED7A 3A13AFF5 C9539600 80E92AE4 EECEB26E 126B1989 BE88BBC1

d2 =
04B2E9B8 A069102D A5B57C84 E709BAD7 057237BF C8C71434 35DBAB59 06B901FA\
088C7130 DA32FD0A AD29B9BC 65E68511 5F62AE36 A550BC68 55E17F03 957EFC02\
D6401E15 79CEA00D 01797219 B2B8DB74 3012F81A 144B2DBE 270C9942 A9A155C6\
67C05187 A7F33C07 DD489427 A87C6627 7FBB01B3 321F2228 F0F85853 C0AE9E8C\
104A21F1 5062DA83 4707BF02 216A98F9 C683AF4C C24AE41C 036A2DF0 8D1754C8\
C28A1E4C 0464CE1F 73FC35AA 53513153 9B0618CA ECF77BC4 C41B185A 5752CACF\
01D8FBC3 1295464A 23A86B2F AC2ABEDB 2E4C3D1B 9887D825 7F0ACC9A 6757FC1D\
0F6193D5 11B2E5D6 07A808C1 4F626D3A 4F86CBF1 CC4E7520 1263ADF6 7CCCF916\
B0CF2180 18B7EE2A D17A85A5 CA215F9E 5A4D6A97 924ACD8E 2C41D1B2 D3AEB9F4\
0F1D6649 7EF7B5E3 5374102B EE3B841F BC1591A8 F17C76D0 A0C67BB2 B5BAF667\
4A9D278B AEF3D383 9A46904B 77C4835A F16481B8 7F5281D0 143E5AB4 79A44846\
ED7B0AD0 E32DB0C0 5BBEF49B 8EE6A56A 0368F396 489CA74A 066F6230 43F492C9\
28B11EC3 A069DA1A D1A2BC64 48DB49E4 125DC12B E5B5B5FB 1BBA5813 F0701879\
90BC07C3 1923B22B 600043BB DEBCD622 027B77B1 7CD51FD0 5762BF69 2E3F4378\
101B42B3 778E867C D3E6D43D 24FA56EF A63B1C05 5809C8B6 DA1E742C 0ECBEC00\
B89A2783 D0E977C1 7FDAEF0D D41E9643 D4DD0696 D6D7A992 0656E8A1 84BA7EA4\
85B4FCC7 6D93FB79 034B5F1A 2B0C75E2 33EBABA4 E14CDAE6 1E483C59 23E2ACBA\
166F691E C7EC7487 1A23DACE 4CEC8A76 00E894BE F8A4F0B3 DBCD046D A14FC2A1\
426EBE48 2BDDC780 DE6615E6 77F7B350 C2AED57D C3569794 4B8F99BD E8CE513D\
C6B2CFEC F5B7E8FB 6AC2227B 75914A17 19891EE2 DFEF621D 4D698DDF B480A6FD\
3BF0AC9B 51825012 ACDE6E5B AF9D8C2C 9B5C549A 6BA55126 9F77435D D7E88943\
32352C99 45FF0E0B 3EE34914 E5BEBACB 368B4ED9 EB00F982 8E2A1BBA 86D8C6E7\
93265879 571F2F93 E8762880 65193429 1E113E82 3EB42291 CA9B13F3 2B218664\
46C7BE39 62E4E46A 65968BD5 1145E789 E0112419 D0CA64C1 C56647BE 22DF8C5F\
C896D1D0 03B7BFC5 25449572 513146ED 902272B5 FA63409E 47DD4A2E 4ED96F56\
7434B703 6CC278BC A3139081 F5F99B5B 7F2ACE24 8F66D3A7 DCC8DB8E A80ECE2A\
AD951EFC 107680AD 43B047D5 AF38FE3B 79014752 4727CA78 2AB3E447 DCE40040\
EC9584DF 8E1ABCFB 289BAE28 1738C1C3 E6B6F505 1BB54669 1EB70CB7 1F2BA55C\
8BEEB0A7 B62903DC 7E735F46 B8C55F18 8B5138DC F444FEC0 7C509B10 AEB5745A\
F30B387C 72022A6F 5D556632 661BFD2C AD224AB8 4AA4B594 C71E9842 16D99007\
85A04081 8DB4569A 0834F000 D6A64535 6D4C391A 1E2DEF92 403ECDEA D885D9CD\
949B79E9 208FA235 8D4E7596 84831E53 409797DF A8ED2DFA DEE948CC 812FBFE9

Computation of the signature

Hash values of the to be signed parts of the certificates

```
MD5(tbs1)  = C6B2FE88 912770FC 6F2DB71F 58C7D251
MD5(tbs2)  = C6B2FE88 912770FC 6F2DB71F 58C7D251
SHA1(tbs1) = 676FC132 2C50B8C4 34B0D2FA AD58BDDD 0B56C6EF
SHA1(tbs2) = B3CEAD04 9C577264 F450563F 68ACEB8C 6BD925B4
```

The input to raw RSA signing are PKCS#1-padded hashes

```
PKCS#1-padded MD5(tbs1) = PKCS#1-padded MD5(tbs2) =
   1FFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF\
FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF\
FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF\
FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF\
FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF\
FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF\
FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FF003020\
300C0608 2A864886 F70D0205 05000410 C6B2FE88 912770FC 6F2DB71F 58C7D251
```

The signature, computed using the CA private key on the PKCS#1-padded hash

```
sig(tbs1) = sig(tbs2) =
86C0876D 20682DC8 97443F97 690DDFB2 9074CB25 C358F09F 81234CE2 65A44333\
CB6A78B2 32732917 00DCD6BA DF55088A 19A317A5 1D6092AC 3F6FC624 3601367A\
6A2FC096 9B4E8913 BFC2315F 5AF35D83 FBD03C95 78392422 17BEB9AD 8873D442\
F3A36200 CA198F63 45BCB76C CB27FCF2 DBEA239E 50FDDD3C D69304C9 50E7094A\
FF0A9659 02B72206 D04E3759 BAED05AE 05922D8B E93556C8 CACDC360 6C56EE37\
89C3775F 767A8909 AB444BC1 D7EE4A41 677302EF DF337B4C EE082D92 18FE44AA\
5D68D34E FB796AC4 3219DCF8 DD4C2E6E C458EFA4 82DA7E18 1C086417 7124F0CF\
214B0C5A 28EFECA4 0EC532BB 7673FFEA 9B9BD0A0 B1EFE6DB 97C518C4 DB17B9A5
```

Hash values of the entire certificates (plain hash values with standard ihv and padding)

```
MD5(cert1)  = AC23F42A 0DE8D86B F2FCED29 2E4A87B4
MD5(cert2)  = 78FEA03E 587FAC03 5C381529 FAE94E1F
SHA1(cert1) = BC7510B2 71456CFF D765D0C9 CE7A8154 215B7B37
SHA1(cert2) = 6FEA1157 B6EDC59D 28BF9659 0CEAB3CC 32366A51
```

Note that the MD5 hashes of the entire certificates are different. This is due to the fact that the "to be signed" part of the certificate is preceded by a 4 byte ASN.1 header. The SHA1 hashes are shown by Microsoft's Certificate Viewer.

The CA public key:

```
n =
CA70FAC4 4006FBB4 1A8EE419 5AA9771F 75917459 D268B930 46035BA1 DCB54A28\
2A1E2848 B778BAE0 67700ACD 642CB08D 570DBB0F 8956DF23 A0A3C6E5 DFAEEF53\
D8BDC164 F4CBE52E 47AA586E FFF3B29F 0CBD4239 4C646377 EF3DE2F7 BE9B6299\
37451268 B9516A32 F17BD4A4 EA3BA472 3D2FA1A0 F234420A F95040D3 CE0CED5F\
60DB0A26 469F0717 9D2BC29F 623A6180 33969FF7 AC6B92A4 94C127A6 1379B317\
ABB72148 6437542D C6D05DA7 14B6D059 CE470CB3 90841349 37485995 A1E8F334\
9DCFCA31 D618A4FC A487573C 9A426A50 836F9559 BA4DB76A 686095B9 B864DED6\
BDED5345 DBEC3840 DBAC4B0C BACCA014 C5753C28 0585F453 FD520F27 4043A051

e = 010001
```

The CA certificate is self-signed.

We do not provide the CA private key, as all signatures can be checked by the public key.

Marc Stevens
Arjen Lenstra
Benne de Weger

October 21, 2006