Discovery Disclosure (January 1998)

"jan1998.txt"
Mac line breaks, line break after last line, no trailing spaces

```
MD5 hash:   583646cdf33605d4cdcdd77ed9a78a2c
SHA-1 hash: 9506a242d7d22ff7b0c3b74e3a5c93150767a09f
```

Hashes published to the following internet newsgroups:
1998-01-03: Message ID <34AE8D80.67B1@webshuttle.ch> to "comp.sys.mac.hypercard"
1998-01-04: Message to "comp.lang.java.programmer"

Hashes republished in references of 'Discovery Disclosure (January 2000)'

Discovery Disclosure (January 2000)

"jan2000.txt"
DOS line breaks, no line break after last line, no trailing spaces

```
MD5 hash:   91303789c0ace6ae9f6b2fd013ca871d
SHA-1 hash: e5b5b56dd5eb57dfc1996d85b468a9ec3d928789
```

e-TimeStamp 15.1.2000, ca. 11.30 (am)
[testing phase there, seemingly signing computer not in secure environment yet]

```
SHA-1: 9235885b864b0916e51b350c014bb05bb26ad825
Sign.: 8963b8acf54d394b75c1d6d2eb14c058d517d2e80fdb6befedb56e63f3ce99d0
       834bd01f0abb41ef200b51854adeffa2ebcb5d57f0bb0a4cc55847166265137f
       94e8fac92bd8b59b80b28537596debab5c4eae1e290872ac53c435971c159d5f
       a4f030f075208de201da42cea245343124b5fdbe2f6b75e673a3b4adaa6820c4
       9340e2c2de3a55fc95c77561604f59c7017a8950f1181909623ab1fa7f94d3d8
       caeb5e0f87766a221d8ee56c00154afe6584e13f2745940f15a0a1e5f3502b01
       3c97b91b1043da0208199d09f61dff8a9ef49077bc302398a9c480ef444c236d
       e9e60de9ec581e0eeeeaf8a158f0e9c6552accb1beb8f1211ad977a38882f9c7
```

All 4 hashes concated (binary, in above order, base64 encoded):

```
begin certificate
kTA3icCs5q6fay/QE8qHHeW1tW3V61ffwZlthbRoqew9koeJkjWIW4ZLCRblGzUMAUuwW7Jq
2CWJY7is9U05S3XB1tLrFMBY1RfS6A/ba+/ttW5j886Z0INL0B8Ku0HvIAtRhUre/6Lry11X
8LsKTMVYRxZiZRN/lOj6ySvYtZuAsoU3WW3rq1xOrh4pCHKsU8Q1lxwVnV+k8DDwdSCN4gHa
Qs6iRTQxJLX9vi9rdeZzo7StqmggxJNA4sLeOlX8lcd1YWBPWccBeolQ8RgZCWI6sfp/lNPY
yuteD4d2aiIdjuVsABVK/mWE4T8nRZQPFaCh5fNQKwE8l7kbEEPaAggZnQn2Hf+KnvSQd7ww
I5ipxIDvREwjbenmDensWB4O7ur4oVjw6cZVKsyxvrjxIRrZd6OIgvnH
end certificate
```

Published to the following internet newsgroups:
2000-01-15: alt.test, comp.sys.mac.hypercard, comp.lang.java.programmer, comp.lang.java.help
2000-01-17: comp.sys.mac.hypercard

Swisskey Zertifikat 010200000408
[end of june 2001: certificates will be revoked, swisskey stops for individuals]

e=2^16+1, n =

```
CA7F8873C05070A9284EC0FAF6AB66B703B71CC6782945AB436366FE17CCF552
BA1B9E1543F97748D5D3F8BC247FB07CC0124AA38D0AD9A87CE0305517DCBC7B
D0D992F9546660C7D01F193CA48FFB87A32B1C8A4DB954BDC2DF0B8324FB43B6
B649C68B94DAAAFDBC442F44CE8D7963FADEF76C0881107598F253C4E2E72EBB
```

d =

```
B2364D1379C411727DDBD970C4D811FCAD53610AB643B461C65BDC0F7148DAFA
A4799BC5A15E1281D255CC0960A1D3E3E671F2A83F7FB610D75DC28B91059E06
538B4AF27F5CE00B33E89AD0A4F586E02438CE5020CF6A88D31A1B4252F74029
DE8390DEFFC97A74A8C2FBF6872E9CEA1BA6ED57FAFDDB2D0E4DFADE5E5E37A9
```

base64((md5lsha-1)^d mod n):

```
DZodO12rbj9xAV0UeFWllhq1FMkHjO2qS8rFtBYwcQmkV6ORLMXtBdVONyFUD2tm
fmrZK/Re3tcg76K+ZZG3WiTjv1q1yMTmKmQrkMCIRzS/xBXbkQRTf/iQeqrR5eRH
z0QVAguiGlJMSYX4iSNCathr9nEWBMqCRo4JLLAGi5o=
```

signature appended => "jan2000s.txt" (empty line in between, no line break after last line)

```
MD5 hash:   4e18f1e7da8f69f3807765069d6e6e62
SHA-1 hash: 167e7eeff4a3c8bb9ae6f684b7325c364a6b66a9
```

```
-----BEGIN CERTIFICATE-----
MIIEgTCCA2mgAwIBAgIGAQIAAAQIMA0GCSqGSIb3DQEBBAUAMIGZMQswCQYDVQQG
EwJDSDEUMBIGA1UEChMLU3dpc3NrZXkgQUcxHjAcBgNVBAsTFTAwODUxMDAwMDAw
MDUwMDAwMDM5NDEbMBkGA1UECxMSUHVibGljIENBIFNlcnZpY2VzMRAwDgYDVQQH
EwdadWVyaWNoMSUwIwYDVQQDExxTd2lzc2tleSBQZXJzb25hbCBJRCBDQSAxMDI0
MB4XDTAwMDEyMzEzMTYyMloXDTAyMDEyMzEzMTYwMFowgZ4xGzAZBgNVBAoTElBy
aXZhdGUgSW5kaXZpZHVhbDEeMBwGA1UECxMVMDA4NTEwMDAwNTM2OTAwMDAwMTAy
MRMwEQYDVQQLEwowNy4wOC4xOTY2MQswCQYDVQQGEwJDSDEWMBQGA1UEAxMNQWxh
aW4gU3RhbGRlcjElMCMGCSqGSIb3DQEJARYWYXN0YWxkZXJAd2Vic2h1dHRsZS5j
aDCBoDANBgkqhkiG9w0BAQEFAAOBjgAwggCJAoGBAMp/iHPAUHCpKE7A+varZrcD
txzGeClFq0NjZv4XzPVSuhueFUP5d0jV0/i8JH+wfMASSqONCtmofOAwVRfcvHvQ
2ZL5VGZgx9AfGTykj/uHoyscik25VL3C3wuDJPtDtrZJxouU2qr9vEQvRM6NeWP6
3vdsCIEQdZjyU8Ti5y67AgMBAAGjggFJMIIBRTALBgNVHQ8EBAMCBaAwEQYJYIZI
AYb4QgEBBAQDAgWgMIHXBglghkgBhvhCAQ0EgckWgcZUaGlzIGNlcnRpZmljYXRl
IGhhcyBiZWVuIGlzc3VlZCBieSBTd2lzc2tleSBBRyBnb3Zlcm5lZCBieSBpdHMg
Q2VydGlmaWNhdGUgUHJhY3RpY2UgU3RhdGVtZW50IChDUFMpLiBDUFMgYW5kIGZ1
cnRoZXIgaW5mb3JtYXRpb24gYWJvdXQgU3dpc3NrZXkgY2VydGlmaWNhdGVzIGFy
ZSBhdmFpbGFibGUgYXQgaHR0cDovL3d3dy5zd2lzc2tleS5jaC4wCQYDVR0TBAIw
ADA+BglghkgBhvhCAQMEMRYvaHR0cHM6Ly9jcmwuc3dpc3NrZXkuY2gvcHJvZHNz
bC9nZXRfc3RhdHVzP3NpZD0wDQYJKoZIhvcNAQEEBQADggEBACtcsZrgrH1UNCK0
FnV7jyM0znThwKaPysG133xtfTTh3Sk3tZa5HfotbaurwYlGzx6m772z7btT+Brx
qEiHWX1V3BWSFifYQ3PJulocMltdcNBSdCBvqUCu4X7nWpYE+uXNNLGfIgGQbNK2
hgwUcVWHhF8K56jTddS9oEbq8Oe4hZHf6Te1VBs/WElGtPNqJpeZCfB6CrK5UVVx
sjvcy1YpzT2f+GN2NF8OKvettfwqKyn1LgPyrYZs80YWYq9FlbDocBfI/4z/63kx
edDUvcS1eBjsXSIhPuqSq+4gwQlTAFPVCuoe5WvHF7IIeqVgdb3yOsBf4BKJ023W
xH5NLZU=
-----END CERTIFICATE-----
```

```
MD5 hash:   25be3f1299130bbbf8beffba619be69c
SHA-1 hash: dabd936d03d39596da830368fd9c2e0d204048e7
```

e-timestamp of "jan2000s.txt" (2000-07-03)

New format according to RFC 2630, derived from PKCS#7 (RFC 2315):
- SHA-1 of file under id-ct-TSTInfo in octet string
- SHA-1 of timestamp under messageDigest in octet string
- 2048 bit signature of timestamp under rsaEncryption in octet string
[IP-Protector output is serialized java object, includes PKCS#7 file and other data]

```
SHA-1: b7695cbe1067fb21a3c83cb9fe33d296d86cb865
Sign.: 2e8e731e841bef4df29987dd3aa6b7e492b2e72946ae12f69e530273ffeeb712
       07da970d6bb778b592ed7a2f66a18c9838e42b07c9697c94456a481eaf3a358c
       6aa0d88decf826aefde2fc214ceba6c00dc2adcf93f52f536f9573125043fef5
       73fdfc7cdfa309f0ebcb3f3b2d0f9c2045606e3f1e4466f4a91befe3eb1c99f2
       fc890d3ef0ee3b9f309c07fdb7191522c7bc2aed4cbf753818c351efff75ae03
       129e42ab936ad97af9f894169ea1321f6ab12050d96f60e3c06749df45bee226
       1e936e6473757447a8bd0dc577f8097eb7788ebe11ede8495f72c8cbefa5312a
       92384f085c9e3d7945ea055e61596209d1acd402f8ae99c3eea5094b01c19031
```

PKCS#7 file:

```
  0 30  649: SEQUENCE {
  4 06    9:   OBJECT IDENTIFIER signedData (1 2 840 113549 1 7 2)
 15 A0  634:   [0] {
 19 30  630:     SEQUENCE {
 23 02    1:       INTEGER 1
 26 31    9:       SET {
 28 30    7:         SEQUENCE {
 30 06    5:           OBJECT IDENTIFIER sha1 (1 3 14 3 2 26)
          :           }
          :         }
 37 30   85:       SEQUENCE {
 39 06   11:         OBJECT IDENTIFIER
          :           id-ct-TSTInfo (1 2 840 113549 1 9 16 1 4)
 52 A0   70:         [0] {
 54 04   68:           OCTET STRING
          :             304202010005003 01f300706052b0e03
          :             021a0414167e7eeff4a3c8bb9ae6f684
          :             b7325c364a6b66a902020198180f3230
          :             303030373033313633353 1335aa005a1
          :             03020105

          :           }
          :         }
124 31  525:       SET {
128 30  521:         SEQUENCE {
132 02    1:           INTEGER 1
135 30  120:           SEQUENCE {
137 30  115:             SEQUENCE {
139 31   11:               SET {
141 30    9:                 SEQUENCE {
143 06    3:                   OBJECT IDENTIFIER countryName (2 5 4 6)
148 13    2:                   PrintableString 'US'
          :                   }
          :                 }
152 31   11:               SET {
154 30    9:                 SEQUENCE {
156 06    3:                   OBJECT IDENTIFIER stateOrProvinceName (2 5 4 8)
161 13    2:                   PrintableString 'DE'
          :                   }
          :                 }
165 31   24:               SET {
167 30   22:                 SEQUENCE {
```

```
169 06    3:                  OBJECT IDENTIFIER organizationName (2 5 4 10)
174 13   15:                  PrintableString 'DigiStamp, Inc.'
          :                  }
          :                }
191 31   26:              SET {
193 30   24:                SEQUENCE {
195 06    3:                  OBJECT IDENTIFIER commonName (2 5 4 3)
200 13   17:                  PrintableString 'www.digistamp.com'
          :                  }
          :                }
219 31   19:              SET {
221 30   17:                SEQUENCE {
223 06    3:                  OBJECT IDENTIFIER localityName (2 5 4 7)
228 13   10:                  PrintableString 'Wilmington'
          :                  }
          :                }
240 31   12:              SET {
242 30   10:                SEQUENCE {
244 06    3:                  OBJECT IDENTIFIER
          :                    organizationalUnitName (2 5 4 11)
249 13    3:                  PrintableString 'TSA'
          :                  }
          :                }
          :              }
254 02    1:            INTEGER 27
          :            }
257 30    7:          SEQUENCE {
259 06    5:            OBJECT IDENTIFIER sha1 (1 3 14 3 2 26)
          :            }
266 A0  110:          [0] {
268 30   26:            SEQUENCE {
270 06    9:              OBJECT IDENTIFIER
          :                contentType (1 2 840 113549 1 9 3)
281 31   13:              SET {
283 06   11:                OBJECT IDENTIFIER
          :                  id-ct-TSTInfo (1 2 840 113549 1 9 16 1 4)
          :                }
          :              }
296 30   35:            SEQUENCE {
298 06    9:              OBJECT IDENTIFIER
          :                messageDigest (1 2 840 113549 1 9 4)
309 31   22:              SET {
311 04   20:                OCTET STRING
          :                  b7695cbe1067fb21a3c83cb9fe33d296
          :                  d86cb865
          :                }
          :              }
333 30   43:            SEQUENCE {
335 06   11:              OBJECT IDENTIFIER
          :                id-aa-signingCertificate (1 2 840 113549 1 9 16 2 12)
348 31   28:              SET {
350 30   26:                SEQUENCE {
352 30   24:                  SEQUENCE {
354 30   22:                    SEQUENCE {
356 04   20:                      OCTET STRING
          :                    dc6c020bb5aab619dd94199f08291cd4
          :                    39819730
          :                        }
          :                    }
          :                  }
          :                }
          :              }
          :            }
378 30   13:          SEQUENCE {
380 06    9:            OBJECT IDENTIFIER
          :              rsaEncryption (1 2 840 113549 1 1 1)
```

```
 391 05    0:             NULL
           :             }
 393 04  256:           OCTET STRING
           :             2e8e731e841bef4df29987dd3aa6b7e4
           :             92b2e72946ae12f69e530273ffeeb712
           :             07da970d6bb778b592ed7a2f66a18c98
           :             38e42b07c9697c94456a481eaf3a358c
           :             6aa0d88decf826aefde2fc214ceba6c0
           :             0dc2adcf93f52f536f9573125043fef5
           :             73fdfc7cdfa309f0ebcb3f3b2d0f9c20
           :             45606e3f1e4466f4a91befe3eb1c99f2
           :             fc890d3ef0ee3b9f309c07fdb7191522
           :             c7bc2aed4cbf753818c351efff75ae03
           :             129e42ab936ad97af9f894169ea1321f
           :             6ab12050d96f60e3c06749df45bee226
           :             1e936e6473757447a8bd0dc577f8097e
           :             b7788ebe11ede8495f72c8cbefa5312a
           :             92384f085c9e3d7945ea055e61596209
           :             d1acd402f8ae99c3eea5094b01c19031

           :           }
           :         }
           :       }
           :     }
           :   }
```

hexdump:

```
3082028906092a864886f70d010702a082027a308202760201013109300706052b0e03021a3055060b2a864886f70d0109100104a046044430420201000500301f300706052b0e03021a0414167e7eeff4a3c8bb9ae6f684b7325c364a6b66a902020198180f32303030303037303331363335313335aa005a1030201053182020d308202090201013078307307331 0b300906035504061302555331 0b300906035504081302444531183016060355040a130f446967695374616d702c20496e632e311a3018060355040313117777772e646967697374616d702e636f6d3113301106035504071 30a57696c6d696e67746f6e310c300a060355040b13035453410201 1b300706052b0e03021aa06e301a06092a864886f70d010903310d060b2a864886f70d01091001043023060 92a864886f70d01090431160414b7695cbe1067fb21a3c83cb9fe33d296d86cb865302b060b2a864886f70d010910020c311c301a301830160414dc6c020bb5aab619dd94199f08291cd439819730300d06092a864886f70d01010105000482010 02e8e731e841bef4df29987dd3aa6b7e492b2e72946ae12f69e530273ffeeb71207da970d6bb778b592ed7a2f66a18c9838e42b07c9697c94456a481eaf3a358c6aa0d88decf826aefde2fc214ceba6c00dc2adcf93f52f536f9573125043fef573fdfc7cdfa309f0ebcb3f3b2d0f9c2045606e3f1e4466f4a91befe3eb1c99f2fc890d3ef0ee3b9f309c07fdb7191522c7bc2aed4cbf753818c351efff75ae03129e42ab936ad97af9f894169ea1321f6ab12050d96f60e3c06749df45bee2261e936e6473757447a8bd0dc577f8097eb7788ebe11ede8495f72c8cbefa5312a92384f085c9e3d7945ea055e61596209d1acd402f8ae99c3eea5094b01c19031
```

To be published:
- swisskey signature of "jan2000.txt", i.e. (md5lsha-1)^d mod n
- sha1 hash of swisskey certificate [proofs that certificate existed at that time, not just the key]
- md5+sha1 hash of "jan2000s.txt"
- sha1 hash and signature of timestamp of 2000-07-03 for "jan2000s.txt"
460 bytes

```
begin certificate
DZodO12rbj9xAV0UeFWllhq1FMkHjO2qS8rFtBYwcQmkV6ORLMXtBdVONyFUD2tmfmrZK/Re
3tcg76K+ZZG3WiTjv1q1yMTmKmQrkMCIRzS/xBXbkQRTf/iQeqrR5eRHz0QVAguiGlJMSYX4
iSNCathr9nEWBMqCRo4JLLAGi5ravZNtA9OVltqDA2j9nC4NIEBI504Y8efaj2nzgHdlBp1u
bmIWfn7v9KPIu5rm9oS3Mlw2SmtmqbdpXL4QZ/sho8g8uf4z0pbYbLhlLo5zHoQb703ymYfd
```

```
Oqa35JKy5ylGrhL2nlMCc//utxIH2pcNa7d4tZLtei9moYyYOOQrB8lpfJRFakgerzo1jGqg
2I3s+Cau/eL8IUzrpsANwq3Pk/UvU2+VcxJQQ/71c/38fN+jCfDryz87LQ+cIEVgbj8eRGb0
qRvv4+scmfL8iQ0+8O47nzCcB/23GRUix7wq7Uy/dTgYw1Hv/3WuAxKeQquTatl6+fiUFp6h
Mh9qsSBQ2W9g48BnSd9FvuImHpNuZHN1dEeovQ3Fd/gJfrd4jr4R7ehJX3LIy++lMSqSOE8I
XJ49eUXqBV5hWWIJ0azUAviumcPupQlLAcGQMQ==
end certificate
```

Published to the following internet newsgroups:
2000-07-10: comp.lang.java.programmer, comp.lang.java.misc, alt.test

Published in delphi about box:
2000-10-07: version 1.0 (ca. 450 downloads)
2000-10-09: version 1.01
2000-10-19: version 1.02

Discovery Disclosure (March 2001)

"mar2001.txt"
DOS line breaks, no line break after last line, no trailing spaces

```
MD5 hash:   c52af9527e3c645f87ec0d430ea366e2
SHA-1 hash: b0f4be90f7bdd3c40cc4cb376700aaee790b32aa
```

base64((md5|sha-1)^d mod n):

```
AJqYm0MxxfJElKUoJ45cNpjEaDM1m0WVZZdJEQ3gzKjeepvqtiD1mpvJTuXR1MeL
02JknvecVqt7F+PPfjeqObNbG9YtBLB+WuQ97lMlnqMUmUrQAlUXfnOrUVQAxAfM
wfsCRD1AR2skJbgMmcu1ykwo088KSujJXe3620GNw2Ts
```

signature appended => "mar2001s.txt" (empty line in between, no line break after last line)
caution: if decoded 129 bytes long (leading 0 byte)

```
MD5 hash:   e83b2ce3ec033fa9724be4bab66d879f
SHA-1 hash: 928076849e465dd3988ab37f836da53c770f7c8f
```

e-timestamp of "mar2001s.txt" (2001-03-29???)

```
SHA-1: 13618e41ad8826f4745fa9f582a92e905d3fde83
Sign.: ab98ce9f83f6207dfeb5b8255337658e9bd571d7d4a799bfae1752b74fd1da93
       ff1890eadb2c1d077b6b7884b09e380e8969f085ff1a0381e0228cd57d373f75
       328a98ee8419d2671e31960d80cedefd014f200fb54a5cffaffa1f5471f3ef9f
       de4697bdf70401c28f8b8a0581288dfb12d25538fc4232264dbd55688de26615
       ab5cf0bab8fcf9b5896ae8617cb9de2c65a13bd52de1c806ae879cf5b7ba17c7
       d2e104c8c90ad61e80d744c10efca54b203f0432962efe429a491720e51dd098
       a76b3cc73493d0cc472cee3ff89ce7dfc49dd4f7f756b5c0a78d6c5ae171c23a
       923ccc42f3f37ddaf6f2ff64e300298b2c3734645aa702329ab0e6205f021bee
```

PKCS#7 file:

```
   0 30  650: SEQUENCE {
```

```
  4 06    9:   OBJECT IDENTIFIER signedData (1 2 840 113549 1 7 2)
 15 A0  635:   [0] {
 19 30  631:     SEQUENCE {
 23 02    1:       INTEGER 1
 26 31    9:       SET {
 28 30    7:         SEQUENCE {
 30 06    5:           OBJECT IDENTIFIER sha1 (1 3 14 3 2 26)
          :           }
          :         }
 37 30   83:       SEQUENCE {
 39 06   11:         OBJECT IDENTIFIER
          :           id-ct-TSTInfo (1 2 840 113549 1 9 16 1 4)
 52 A0   68:         [0] {
 54 04   66:           OCTET STRING
          :             3040020100050030 1f300706052b0e03
          :             021a0414928076849e465dd3988ab37f
          :             836da53c770f7c8f02020293180f3230
          :             3031303332393138353133385a300302
          :             0104

          :           }
          :         }
122 31  528:       SET {
126 30  524:         SEQUENCE {
130 02    1:           INTEGER 1
133 30  123:           SEQUENCE {
135 30  118:             SEQUENCE {
137 31   11:               SET {
139 30    9:                 SEQUENCE {
141 06    3:                   OBJECT IDENTIFIER countryName (2 5 4 6)
146 13    2:                   PrintableString 'US'
          :                   }
          :                 }
150 31   11:               SET {
152 30    9:                 SEQUENCE {
154 06    3:                   OBJECT IDENTIFIER stateOrProvinceName (2 5 4 8)
159 13    2:                   PrintableString 'TX'
          :                   }
          :                 }
163 31   24:               SET {
165 30   22:                 SEQUENCE {
167 06    3:                   OBJECT IDENTIFIER organizationName (2 5 4 10)
172 13   15:                   PrintableString 'DigiStamp, Inc.'
          :                   }
          :                 }
189 31   22:               SET {
191 30   20:                 SEQUENCE {
193 06    3:                   OBJECT IDENTIFIER commonName (2 5 4 3)
198 13   13:                   PrintableString 'DigiStamp TSA'
          :                   }
          :                 }
213 31   12:               SET {
215 30   10:                 SEQUENCE {
217 06    3:                   OBJECT IDENTIFIER
          :                     organizationalUnitName (2 5 4 11)
222 13    3:                   PrintableString 'TSA'
          :                   }
          :                 }
227 31   26:               SET {
229 30   24:                 SEQUENCE {
231 06    3:                   OBJECT IDENTIFIER
          :                     organizationalUnitName (2 5 4 11)
236 13   17:                   PrintableString 'www.DigiStamp.com'
          :                   }
          :                 }
          :               }
```

```
255 02    1:            INTEGER 45
          :            }
258 30    7:          SEQUENCE {
260 06    5:            OBJECT IDENTIFIER sha1 (1 3 14 3 2 26)
          :            }
267 A0  110:          [0] {
269 30   26:            SEQUENCE {
271 06    9:              OBJECT IDENTIFIER
          :                contentType (1 2 840 113549 1 9 3)
282 31   13:              SET {
284 06   11:                OBJECT IDENTIFIER
          :                  id-ct-TSTInfo (1 2 840 113549 1 9 16 1 4)
          :                }
          :              }
297 30   35:            SEQUENCE {
299 06    9:              OBJECT IDENTIFIER
          :                messageDigest (1 2 840 113549 1 9 4)
310 31   22:              SET {
312 04   20:                OCTET STRING
          :                  13618e41ad8826f4745fa9f582a92e90
          :                  5d3fde83

          :                }
          :              }
334 30   43:            SEQUENCE {
336 06   11:              OBJECT IDENTIFIER
          :                id-aa-signingCertificate (1 2 840 113549 1 9 16 2 12)
349 31   28:              SET {
351 30   26:                SEQUENCE {
353 30   24:                  SEQUENCE {
355 30   22:                    SEQUENCE {
357 04   20:                      OCTET STRING
          :                    857880442a56f7f5ee349c41bd203972
          :                    39c1281f

          :                      }
          :                    }
          :                  }
          :                }
          :              }
          :            }
379 30   13:          SEQUENCE {
381 06    9:            OBJECT IDENTIFIER
          :              rsaEncryption (1 2 840 113549 1 1 1)
392 05    0:            NULL
          :            }
394 04  256:          OCTET STRING
          :            ab98ce9f83f6207dfeb5b8255337658e
          :            9bd571d7d4a799bfae1752b74fd1da93
          :            ff1890eadb2c1d077b6b7884b09e380e
          :            8969f085ff1a0381e0228cd57d373f75
          :            328a98ee8419d2671e31960d80cedefd
          :            014f200fb54a5cffaffa1f5471f3ef9f
          :            de4697bdf70401c28f8b8a0581288dfb
          :            12d25538fc4232264dbd55688de26615
          :            ab5cf0bab8fcf9b5896ae8617cb9de2c
          :            65a13bd52de1c806ae879cf5b7ba17c7
          :            d2e104c8c90ad61e80d744c10efca54b
          :            203f0432962efe429a491720e51dd098
          :            a76b3cc73493d0cc472cee3ff89ce7df
          :            c49dd4f7f756b5c0a78d6c5ae171c23a
          :            923ccc42f3f37ddaf6f2ff64e300298b
          :            2c3734645aa702329ab0e6205f021bee

          :          }
          :        }
```

```
:       }
:     }
:   }
```

hexdump:

```
3082028a06092a864886f70d010702a082027b30820277020101310930070605
2b0e03021a3053060b2a864886f70d0109100104a044044230400201000500030
1f300706052b0e03021a0414928076849e465dd3988ab37f836da53c770f7c8f
02020293180f323030313033323931383531333385a3003020104318202103082
020c020101307b3076310b3009060355040613025553310b3009060355040813
025458311830160603550405a130f4469676953746l6d702c20496e632e311630
140603550403130d446967695374616d7020545341310c300a060355040b1303
545341311a3018060355040b13117777772e446967695374616d702e636f6d02
012d300706052b0e03021aa06e301a06092a864886f70d010903310d060b2a86
4886f70d01091001043023060 92a864886f70d0109043116041413618e41ad88
26f4745fa9f582a92e905d3fde83302b060b2a864886f70d010910020c311c30
1a3018301604148578804 42a56f7f5ee349c41bd20397239c1281f300d06092a
864886f70d01010105000 4820100ab98ce9f83f6207dfeb5b8255337658e9bd5
71d7d4a799bfae1752b74fd1da93ff1890eadb2c1d077b6b7884b09e380e8969
f085ff1a0381e0228cd57d373f75328a98ee8419d2671e31960d80cedefd014f
200fb54a5cffaffa1f5471f3ef9fde4697bdf70401c28f8b8a0581288dfb12d2
5538fc4232264dbd55688de26615ab5cf0bab8fcf9b5896ae8617cb9de2c65a1
3bd52de1c806ae879cf5b7ba17c7d2e104c8c90ad61e80d744c10efca54b203f
0432962efe429a491720e51dd098a76b3cc73493d0cc472cee3ff89ce7dfc49d
d4f7f756b5c0a78d6c5ae171c23a923ccc42f3f37ddaf6f2ff64e300298b2c37
34645aa702329ab0e6205f021bee
```

To be published:
- swisskey signature of "mar2001.txt", i.e. (md5lsha-1)^d mod n
- sha1 hash of swisskey certificate [proofs that certificate existed at that time, not just the key]
- md5+sha1 hash of "mar2001s.txt"
- sha1 hash and signature of timestamp of 2001-03-29 for "mar2001s.txt"
460 bytes

```
begin certificate
AJqYm0MxxfJElKUoJ45cNpjEaDM1m0WVZZdJEQ3gzKjeepvqtiD1mpvJTuXR1MeL
02JknvecVqt7F+PPfjeqObNbG9YtBLB+WuQ97lMlnqMUmUrQAlUXfnOrUVQAxAfM
wfsCRD1AR2skJbgMmcu1ykwo088KSujJXe3620GNw2Ts2r2TbQPTlZbagwNo/Zwu
DSBASOfoOyzj7AM/qXJL5Lq2bYefkoB2hJ5GXdOYirN/g22lPHcPfI8TYY5BrYgm
9HRfqfWCqS6QXT/eg6uYzp+D9iB9/rW4JVM3ZY6b1XHX1KeZv64XUrdP0dqT/xiQ
6tssHQd7a3iEsJ44Dolp8IX/GgOB4CKM1X03P3UyipjuhBnSZx4xlg2Azt79AU8g
D7VKXP+v+h9UcfPvn95Gl733BAHCj4uKBYEojfsS0lU4/EIyJk29VWiN4mYVq1zw
urj8+bWJauhhfLneLGWhO9Ut4cgGroec9be6F8fS4QTIyQrWHoDXRMEO/KVLID8E
MpYu/kKaSRcg5R3QmKdrPMc0k9DMRyzuP/ic59/EndT391a1wKeNbFrhccI6kjzM
QvPzfdr28v9k4wApiyw3NGRapwIymrDmIF8CG+4=
end certificate
```

Published to the following internet newsgroups:
2001-03-29: comp.lang.java.misc, comp.lang.java.help, alt.test

Published in delphi about box:
2001-04-19: version 1.20
2001-05-03: version 1.21
2001-xx-xx: CD that comes with:
PalmPilot™ and Palm™ Organizers! I Didn't Know You Could Do That…™, Second Edition, by Neil J. Salkind, ISBN 0-7821-2936-6, published ca. June 2001

Collation of Discovery Disclosures (May 2001)

"may2001.txt"
DOS line breaks, line break after last line, no trailing spaces

```
MD5 hash:   41855aa8a5848d7292264d6589e5251a
SHA-1 hash: 67b737effb1ebed2eed33f34eb80aa2d7c645c49
```

base64((md5lsha-1)^d mod n):

```
nQaakjjUrzkD+juqpbEPbYLuJJBV9+xCMZiIjg8WVHqofWALH/0pChUu20+wDXwx
Ye5NgZeTBgZXfLM6nH7Dpe7uAOVlb66fLYANdmrm8ftn/47lhNfCqfEeuzfxAsXH
pYdrkFKgDjpnuj7lIVp7+u7T8TfzaoFX19cht2/YUoE=
```

signature appended => "may2001s.txt" (empty line in between, no line break after last line)

```
MD5 hash:   d114b72e5b3e0f3404b3dff2d6a5490b
SHA-1 hash: 7251f4f5d16ad44ca537c2b468588982230e6c02
```

e-timestamp of "may2001s.txt" (2001-05-03)

```
SHA-1: 74d00eeced45e1e4e9521e7ec74a905fe5555c93
Sign.: 5932068630b7b94511a092831235e1a3a9f701d2201d4e18abd830db9d0ae48b
       0f6c70eb8923280f5a8b88774c6dc16feca5a671277f870ee97de47020c1d383
       def425ad9fcea9cd5cbf1848831fbdfa6433879878fc5cd0a29c63da4fcb1548
       ce2345c433d6e443e1ddd5bd079d0bb8e765ca32e8606fbf51fbf6546e085044
       bab56af2c24093bc72926e5971f335209141a2bf5ba57f62f44784feb414ea61
       048252147d4c7df481dfac0b685761d2ed13dde135a45f4280698b64a549facd
       d2f9b271eb28eb7cb46faf56081888f854b130a1a6f8bd4298ac8da7b6fc77a6
       9065cbb2a342c0088c642a035eca7216e1d21429cf5e502c272fd95b05eb8a68
```

PKCS#7 file:

```
  0 30  650: SEQUENCE {
  4 06    9:   OBJECT IDENTIFIER signedData (1 2 840 113549 1 7 2)
 15 A0  635:   [0] {
 19 30  631:     SEQUENCE {
 23 02    1:       INTEGER 1
 26 31    9:       SET {
 28 30    7:         SEQUENCE {
 30 06    5:           OBJECT IDENTIFIER sha1 (1 3 14 3 2 26)
          :           }
          :         }
 37 30   83:       SEQUENCE {
 39 06   11:         OBJECT IDENTIFIER
          :           id-ct-TSTInfo (1 2 840 113549 1 9 16 1 4)
 52 A0   68:         [0] {
 54 04   66:           OCTET STRING
          :             3040020100050030 1f300706052b0e03
          :             021a0414 7251f4f5d16ad44ca537c2b4
          :             68588982230e6c02 02020349180f3230
          :             3031303530333230303434385a300302
          :             0104
```

```
          :           }
          :         }
122 31  528:       SET {
126 30  524:         SEQUENCE {
130 02    1:           INTEGER 1
133 30  123:           SEQUENCE {
135 30  118:             SEQUENCE {
137 31   11:               SET {
139 30    9:                 SEQUENCE {
141 06    3:                   OBJECT IDENTIFIER countryName (2 5 4 6)
146 13    2:                   PrintableString 'US'
          :                   }
          :                 }
150 31   11:               SET {
152 30    9:                 SEQUENCE {
154 06    3:                   OBJECT IDENTIFIER stateOrProvinceName (2 5 4 8)
159 13    2:                   PrintableString 'TX'
          :                   }
          :                 }
163 31   24:               SET {
165 30   22:                 SEQUENCE {
167 06    3:                   OBJECT IDENTIFIER organizationName (2 5 4 10)
172 13   15:                   PrintableString 'DigiStamp, Inc.'
          :                   }
          :                 }
189 31   22:               SET {
191 30   20:                 SEQUENCE {
193 06    3:                   OBJECT IDENTIFIER commonName (2 5 4 3)
198 13   13:                   PrintableString 'DigiStamp TSA'
          :                   }
          :                 }
213 31   12:               SET {
215 30   10:                 SEQUENCE {
217 06    3:                   OBJECT IDENTIFIER
          :                     organizationalUnitName (2 5 4 11)
222 13    3:                   PrintableString 'TSA'
          :                   }
          :                 }
227 31   26:               SET {
229 30   24:                 SEQUENCE {
231 06    3:                   OBJECT IDENTIFIER
          :                     organizationalUnitName (2 5 4 11)
236 13   17:                   PrintableString 'www.DigiStamp.com'
          :                   }
          :                 }
          :               }
255 02    1:             INTEGER 45
          :             }
258 30    7:           SEQUENCE {
260 06    5:             OBJECT IDENTIFIER sha1 (1 3 14 3 2 26)
          :             }
267 A0  110:           [0] {
269 30   26:             SEQUENCE {
271 06    9:               OBJECT IDENTIFIER
          :                 contentType (1 2 840 113549 1 9 3)
282 31   13:               SET {
284 06   11:                 OBJECT IDENTIFIER
          :                   id-ct-TSTInfo (1 2 840 113549 1 9 16 1 4)
          :                 }
          :               }
297 30   35:             SEQUENCE {
299 06    9:               OBJECT IDENTIFIER
          :                 messageDigest (1 2 840 113549 1 9 4)
310 31   22:               SET {
312 04   20:                 OCTET STRING
```

```
          :                   74d00eeced45e1e4e9521e7ec74a905f
          :                   e5555c93

          :                 }
          :               }
 334 30   43:             SEQUENCE {
 336 06   11:               OBJECT IDENTIFIER
          :                 id-aa-signingCertificate (1 2 840 113549 1 9 16 2 12)
 349 31   28:               SET {
 351 30   26:                 SEQUENCE {
 353 30   24:                   SEQUENCE {
 355 30   22:                     SEQUENCE {
 357 04   20:                       OCTET STRING
          :                     857880442a56f7f5ee349c41bd203972
          :                     39c1281f

          :                       }
          :                     }
          :                   }
          :                 }
          :               }
          :             }
 379 30   13:           SEQUENCE {
 381 06    9:             OBJECT IDENTIFIER
          :               rsaEncryption (1 2 840 113549 1 1 1)
 392 05    0:             NULL
          :             }
 394 04  256:           OCTET STRING
          :             5932068630b7b94511a092831235e1a3
          :             a9f701d2201d4e18abd830db9d0ae48b
          :             0f6c70eb8923280f5a8b88774c6dc16f
          :             eca5a671277f870ee97de47020c1d383
          :             def425ad9fcea9cd5cbf1848831fbdfa
          :             6433879878fc5cd0a29c63da4fcb1548
          :             ce2345c433d6e443e1ddd5bd079d0bb8
          :             e765ca32e8606fbf51fbf6546e085044
          :             bab56af2c24093bc72926e5971f33520
          :             9141a2bf5ba57f62f44784feb414ea61
          :             048252147d4c7df481dfac0b685761d2
          :             ed13dde135a45f4280698b64a549facd
          :             d2f9b271eb28eb7cb46faf56081888f8
          :             54b130a1a6f8bd4298ac8da7b6fc77a6
          :             9065cbb2a342c0088c642a035eca7216
          :             e1d21429cf5e502c272fd95b05eb8a68

          :           }
          :         }
          :       }
          :     }
          :   }
```

hexdump:

```
3082028a06092a864886f70d010702a082027b308202770201013109300706052b0e03021a3053060b2a864886f70d0109100104a044044230400201000500301f300706052b0e03021a04147251f4f5d16ad44ca537c2b468588982230e6c0202020349180f32303031303530333230303434385a3003020104318202103082020c020101307b3076310b300906035504061302555310b3009060355040813025458311830160603550406a130f446967695374616d702c20496e632e311630140603550403130d446967695374616d7020545341310c300a060355040b1303545341311a3018060355040b13117777772e446967695374616d702e636f6d02012d300706052b0e03021aa06e301a06092a864886f70d010903310d060b2a864886f70d010910014302306092a864886f70d010904311604147 4d00eeced45e1e4e9521e7ec74a905fe5555c93302b060b2a864886f70d010910020c311c301a3018301604148578804 42a56f7f5ee349c41bd20397239c1281f300d06092a
```

```
864886f70d010101050004820100593206863 0b7b94511a092831235e1a3a9f7
01d2201d4e18abd830db9d0ae48b0f6c70eb8923280f5a8b88774c6dc16feca5
a671277f870ee97de47020c1d383def425ad9fcea9cd5cbf1848831fbdfa6433
879878fc5cd0a29c63da4fcb1548ce2345c433d6e443e1ddd5bd079d0bb8e765
ca32e8606fbf51fbf6546e085044bab56af2c24093bc72926e5971f335209141
a2bf5ba57f62f44784feb414ea61048252147d4c7df481dfac0b685761d2ed13
dde135a45f4280698b64a549facdd2f9b271eb28eb7cb46faf56081888f854b1
30a1a6f8bd4298ac8da7b6fc77a69065cbb2a342c0088c642a035eca7216e1d2
1429cf5e502c272fd95b05eb8a68
```

To be published:
- swisskey signature of "may2001.txt", i.e. (md5lsha-1)^d mod n
- sha1 hash of swisskey certificate [proofs that certificate existed at that time, not just the key]
- md5+sha1 hash of "may2001s.txt"
- sha1 hash and signature of timestamp of 2001-05-03 for "may2001s.txt"
460 bytes

```
begin certificate
nQaakjjUrzkD+juqpbEPbYLuJJBV9+xCMZiIjg8WVHqofWALH/0pChUu20+wDXwx
Ye5NgZeTBgZXfLM6nH7Dpe7uAOVlb66fLYANdmrm8ftn/47lhNfCqfEeuzfxAsXH
pYdrkFKgDjpnuj7lIVp7+u7T8TfzaoFX19cht2/YUoHavZNtA9OVltqDA2j9nC4N
IEBI59EUty5bPg80BLPf8talSQtyUfT10WrUTKU3wrRoWImCIw5sAnTQDuztReHk
6VIefsdKkF/lVVyTWTIGhjC3uUURoJKDEjXho6n3AdIgHU4Yq9gw250K5IsPbHDr
iSMoD1qLiHdMbcFv7KWmcSd/hw7pfeRwIMHTg970Ja2fzqnNXL8YSIMfvfpkM4eY
ePxc0KKcY9pPyxVIziNFxDPW5EPh3dW9B50LuOdlyjLoYG+/Ufv2VG4IUES6tWry
wkCTvHKSbllx8zUgkUGiv1ulf2L0R4T+tBTqYQSCUhR9TH30gd+sC2hXYdLtE93h
NaRfQoBpi2SlSfrN0vmyceso63y0b69WCBiI+FSxMKGm+L1CmKyNp7b8d6aQZcuy
o0LACIxkKgNeynIW4dIUKc9eUCwnL9lbBeuKaA==
end certificate
```

Published to the following internet newsgroups:
2001-05-04: alt.test.ignore, alt.test.group (Alain Stalder, 'certificate')

Published in delphi about box:
2001-05-07: published in version 2.00

discoveries.pdf (finished 5.3.2002 0:05)

```
MD5 hash:   74cc12a8b0c0f7412f77ce06cfba8817
SHA-1 hash: 3188fd502a8d42799753f076b7bb1c3147a768a3
```

review.pdf

```
MD5 hash:   cfd8de45d11bef6ec06ea4aa8f597aed
SHA-1 hash: 7c50a0b08844862db0242f2f95bd11eb87d4b0c7
```

Hashes for both documents are in code of Delphi 2.01, released 2 April 2002