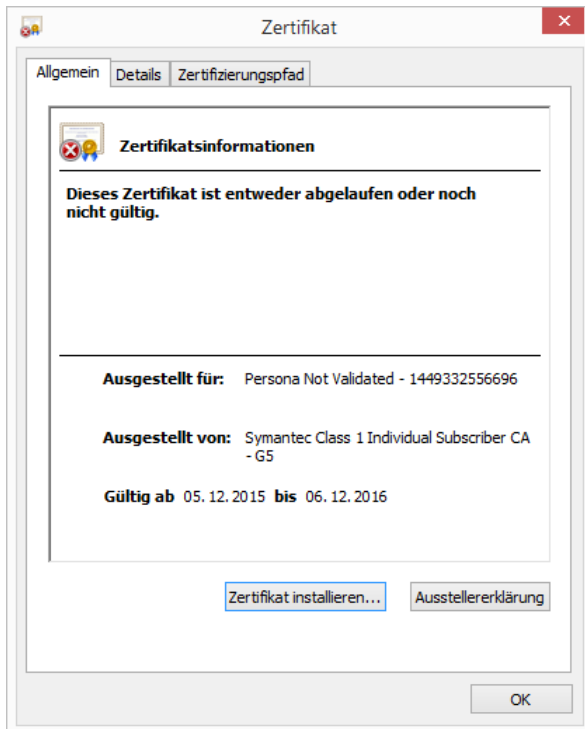
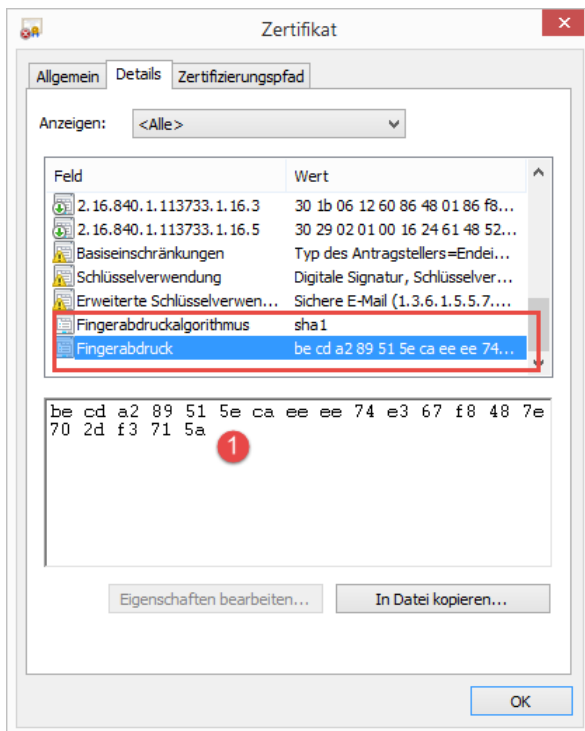


Zertifikat Fingerabdruck SHA256

Zertifikate haben einen Fingerabdruck. Wenn wir die Details des Zertifikates öffnen fällt uns immer wieder auf, dass der Fingerabdruckalgorithmus SHA1 ist. Hierbei scheint es sich noch immer um ein Anzeigeproblem zu handeln, obwohl der Fingerabdruck bereits als SHA256 hinterlegt ist.



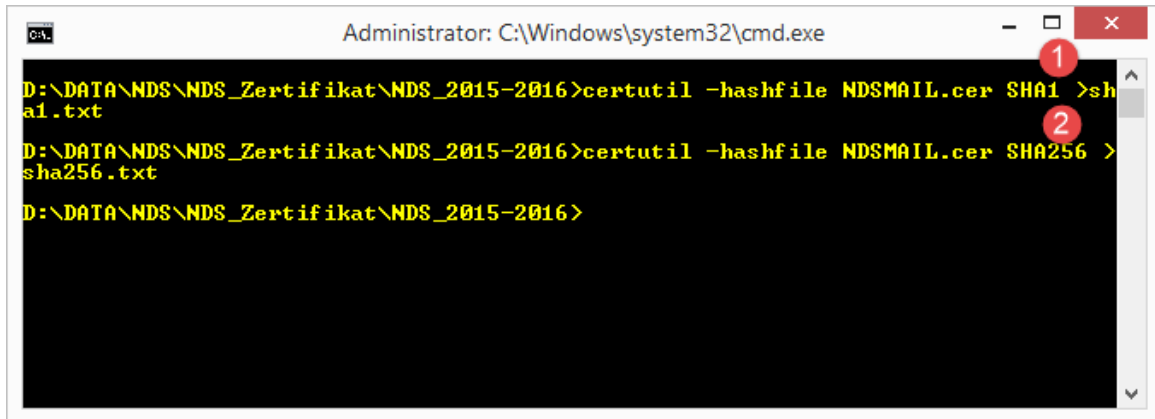
Anzeigefehler?!



Wie kommen wir denn nun an den Wert des SHA256 Fingerabdruckalgorithmus?

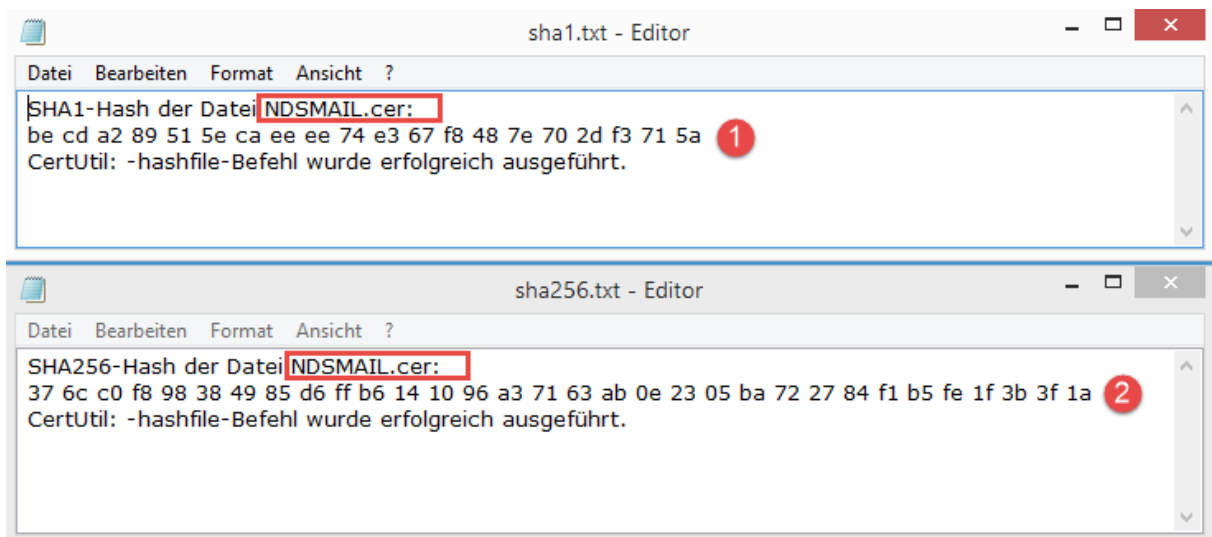
Zertifikat Fingerabdruck SHA256

Unter Windows 7 aufwärts können wir uns den Wert mit dem Parameter hashfile exportieren. Ab Windows 8 ist auch die Hilfe dokumentiert.

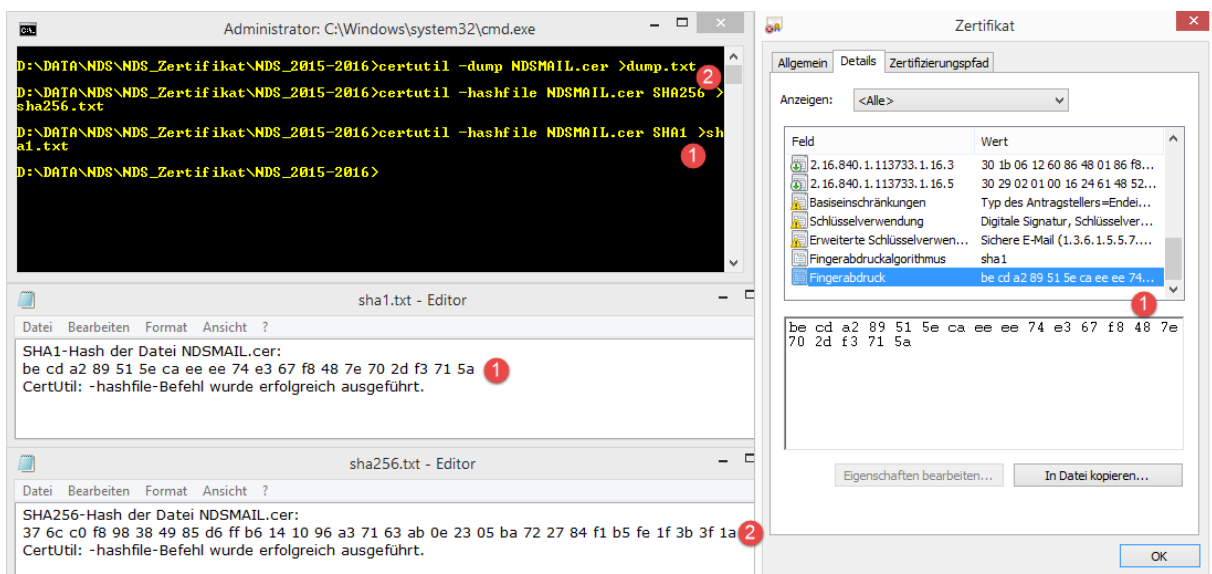


```
Administrator: C:\Windows\system32\cmd.exe
D:\DATA\NDS\NDS_Zertifikat\NDS_2015-2016>certutil -hashfile NDSMAIL.cer SHA1 >sha1.txt
D:\DATA\NDS\NDS_Zertifikat\NDS_2015-2016>certutil -hashfile NDSMAIL.cer SHA256 >sha256.txt
D:\DATA\NDS\NDS_Zertifikat\NDS_2015-2016>
```

Nach dem Export der beiden Hashwerte öffne ich die Textdateien und lege diese mal neben (unter) einander.



Das Ganze mal etwas komprimierter:



Zertifikat Fingerabdruck SHA256

Der DUMP des Zertifikats zeigt uns die gleichen Werte an:

Kein Stammzertifikat

Schlüssel-ID-Hash(rfc-sha1): 12 25 5b 60 69 99 f8 0c c2 82 60 cf 26 05 34 18 73 5a 23 bc

Schlüssel-ID-Hash(sha1): b9 0a f3 5c e2 ed 3a 1b 36 46 9e 75 97 d1 bc 89 b6 02 58 b9

Schlüssel-ID-Hash(md5): 18ea971f355ec8accd4b56496da72f5f

Schlüssel-ID-Hash(sha256): df1c64d884f63b4c02a948db1b6c1ccbaddee862d2b07ef4052f1b30bb5f8d8c

Zertifikathash(md5): 0b a4 8c 74 25 8d 4e d6 d0 73 40 8f b8 1d c3 bd

Zertifikathash(sha1): be cd a2 89 51 5e ca ee ee 74 e3 67 f8 48 7e 70 2d f3 71 5a

Zertifikathash(sha256): 376cc0f898384985d6ffb6141096a37163ab0e2305ba722784f1b5fe1f3b3f1a

Signaturhash: 314e93ce51206799fd491b11a9e9c98f7a34b8cb359e0b38a7d5daa77778bf99

CertUtil: -dump-Befehl wurde erfolgreich ausgeführt.

```
X.509-Zertifikat:
Version: 3
Seriennummer: 706c4794cc2fa260eb57250e84cee14
Signaturalgorithmus:
Algorithmus Objekt-ID: 1.2.840.113549.1.1.11 sha256RSA
Algorithmusparameter:
05 00
Aussteller:
CN=Symantec Class 1 Individual Subscriber CA - G5
OU=Persona Not Validated
OU=Symantec Trust Network
O=Symantec Corporation
C=US
Namenshash (sha1): a3817c5942801108d79e05470e2b48bc7810dc
Namenshash (md5): 578a7c238a5d848fc718a5c0b1c93
Nicht vor: 05.12.2015 01:00
Nicht nach: 06.12.2016 00:59
Antragsteller:
OU=Symantec Trust Network
OU=Persona Not Validated
OU=NMME
E=team@ndr-edv.de
CN=Persona Not Validated - 144931256696
Namenshash (sha1): 94380b7533119a48d93df296bdf7c7c579ce
Namenshash (md5): fa720e75d2e7469a522bf81b2f5e9a1
Öffentlicher Schlüssel-Algorithmus:
Algorithmus Objekt-ID: 1.2.840.113549.1.1.1 RSA (RSA_SIGN)
Algorithmusparameter:
05 00
Länge des öffentlichen Schlüssels: 2048 Bits
Öffentlicher Schlüssel: Nicht verwendete Bits = 0
0000 30 82 01 0a 02 02 01 01 00 a8 98 eb 53 ad ca 12
0010 2e de cb 3c 2a 76 cb cb da d0 a4 6b 8e bc 5f 30
0020 bc 51 75 ee 02 21 5a 99 71 f8 be b8 07 17 2a 48
0030 00 c3 83 15 f1 c1 01 11 c8 be b6 73 98 47 20
0040 7c ca 35 b5 e8 7f 30 b6 1a 26 25 02 bb 18 04 07
0050 8b ea c2 51 05 e1 07 77 1b 29 25 66 53 c4 c0 0e
0060 ca 0a 49 6a 11 56 71 73 9f f0 8b eb fe 03 0c
0070 38 30 82 c7 1d ca c6 28 0d 79 8e ad 2d c0 0e
0080 84 b1 43 05 a5 90 a0 d3 1f 52 3f e6 86 47 cd 9c
0090 8b 2f be 85 77 2d ba 0f 81 04 ca 04 c7 92 7a 31
00a0 bf 74 4d 83 c6 98 03 64 8f f8 78 3d 7a 42 63 bd
00b0 90 73 3a 0b fa 13 87 c1 63 51 42 18 39 cb 18 d2
00c0 63 9e 24 54 d8 eb 08 0c c4 c2 73 13 a4 49 77
00d0 00 85 eb 62 ca ca 2d 0b b9 76 77 9b ba a7 85 3d
00e0 a5 a2 72 e4 c2 cd c2 3c 23 4b 71 ce e7 ad
00f0 a3 46 ec 8d 3a 2c 69 8f c1 b6 73 39 99 d0 95
0100 28 76 43 19 48 d2 9f 23 02 03 01 00 01
Zertifikatserweiterungen: 11
2.5.29.19: Kennzeichen = 1(Kritisch), Länge = 2
Basisbeschränkungen
Typ des Antragstellers-Eindeutigkeit
Einschränkung der Fälschungskriterien
2.5.29.15: Kennzeichen = 1(Kritisch), Länge = 4
Schlüsselverwendung
Digitale Signatur, Schlüsselverschlüsselung (s0)
2.5.29.17: Kennzeichen = 1(Kritisch), Länge = 16
Erweiterte Schlüsselverwendung
Sichere E-Mail (1.3.6.1.5.5.7.3.4)
Clientauthentifizierung (1.3.6.1.5.5.7.3.2)
2.5.29.14: Kennzeichen = 0, Länge = 16
Schlüsselkennung des Antragstellers
12 25 5b 60 69 99 f8 0c c2 82 60 cf 26 05 34 18 73 5a 23 bc
2.5.29.17: Kennzeichen = 0, Länge = 13
Alternativer Antragstellername
RFC822-Name=team@ndr-edv.de
2.5.29.32: Kennzeichen = 0, Länge = 65
Zertifikatskriterien
1(Zertifikatskriterien):
Richtlinienbezeichner=2.16.840.1.113733.1.7.23.1
1(Zertifikatskriterien):
Richtlinienqualifizierungs-Informationen:
Kennung des Richtliniengenerators=CP5
Qualifizierer:
http://www.symantec.com/cps
1(Zertifikatskriterien):
Richtlinienqualifizierungs-Informationen:
Kennung des Richtliniengenerators=Benutzerbenachrichtigung
Qualifizierer:
Benachrichtigungstext=http://www.symantec.com/tpa
2.5.29.31: Kennzeichen = 0, Länge = 56
Spezialisten-Verteilungspunkte
1(Spezialisten-Verteilungspunkt):
Name des Verteilungspunktes:
Volle: Name:
URL=http://pkc-crl.symantec.com/ca_57de7a238045d848fc718a5c0b1c93/LatestCRL.crl
1.3.6.1.5.5.7.1.1: Kennzeichen = 0, Länge = 42
Zugriff auf Stelleninformationen
1(Stelleninformationszugriff):
Zugriffsmethode=Zertifizierungstellenaussteller (1.3.6.1.5.5.7.48.2)
Alternativer Name:
URL=http://cacert.symantec.com/mpki/symccindsubcag5.crt
2.5.29.35: Kennzeichen = 0, Länge = 18
Stellenklassifizierung
Schlüssel=07 15 95 3d a5 79 b0 33 60 d8 2d 53 dc 09 3d 07 ac 18 70
2.16.840.1.113733.1.16.3: Kennzeichen = 0, Länge = 1d
Unbekannter Erweiterungstyp
0000 30 1b 06 12 60 86 48 01 86 f8 45 01 01 02 02 0...X...E.....
0010 04 01 ad ee 92 13 16 05 31 30 39 32 32 .....10922
0002: 30 1b ; SEQUENCE (1b Bytes)
0004: 60 86 48 01 86 f8 45 01 30 01 02 04 01 ad ee ; OBJECT_ID (12 Bytes)
0014: | 92 13 | 2.16.840.1.113733.1.16.2.2.4.1.96176403 ; IAS_STRING (5 Bytes)
0018: 16 05 ; 10922
001b: 31 30 39 32 32 ; 10922
2.16.840.1.113733.1.16.5: Kennzeichen = 0, Länge = 2b
Unbekannter Erweiterungstyp
0000 30 29 02 01 00 16 24 61 48 52 30 63 48 4d 36 4c 0...saR0cHML
0010 79 39 77 61 12 40 7a 63 6d 43 75 63 33 6c 74 58 ;vWvAC5B20=
0020 58 56 30 61 43 35 6a 62 32 30 3d ;XVvAC5B20=
0002: 30 29 ; SEQUENCE (2b Bytes)
0004: 02 01 ; INTEGER (1 Bytes)
0006: 00 ;
0008: 16 24 ; IAS_STRING (24 Bytes)
000f: 61 48 52 30 63 48 4d 36 4c 79 39 77 61 32 6b 74 ;aR0cHMLyWvAC5
0017: 63 6d 43 75 63 33 6c 74 58 56 30 61 43 35 6a ;cndUC3RYVvAC5
0027: 62 32 30 3d ; b20=
; aR0cHMLyWvAC5B20=3RYVvAC5B20=
Signaturalgorithmus:
Algorithmus Objekt-ID: 1.2.840.113549.1.1.11 sha256RSA
Algorithmusparameter:
05 00
Signatur: Nicht verwendete Bits=0
0000 43 ae 1f 4e 6a 45 0a 90 43 02 39 55 d3 09 a0 a2
0010 3c 6d 4e 7f 0b 45 3c 7a 83 18 80 53 40 bc da 8a
0020 07 6d 13 9d 5a 5e 09 89 b5 09 40 32 5a 0b 0e 89
0030 43 b4 91 c4 cd 3a 9d 06 35 99 4b 5a 50 e7 85 c9
0040 33 55 70 1d ca 32 31 54 53 1d 9e 5a f2 3e 6d
0050 e4 e6 7a bf 6f de e2 9a b5 85 c5 33 e4 76 6e 02
0060 db c0 33 73 c8 30 9f bc 35 9a 30 a9 64 b4 83
0070 ed 6a f8 db 89 83 b0 bd 7c cf ab 34 d1 0a 33
0080 24 00 69 c8 1b 7a 82 72 93 20 a7 e2 0f d5 a0
0090 1d 79 7f c4 d2 67 54 f2 98 ea 31 de 0e a1 c3
00a0 09 09 10 00 e6 4d 5a ce 92 49 49 d7 ca c5 17 f5
00b0 2c 04 84 51 41 67 47 49 25 0f 46 6d 5a 69 2d d2
00c0 a9 a8 f7 d1 aa b0 70 f2 e2 ab b9 11 36 d0 8c 1b
00d0 25 c0 8f 5f 85 43 85 e5 8e 9a 1a bd 04 82 4a
00e0 f0 cc 0b 24 c6 68 41 7a 70 6d 43 63 74 80
00f0 c1 0a 85 48 a1 18 25 43 f0 b3 35 ff aa a0 63 21
Kein Stammzertifikat
Schlüssel-ID-Hash(rfc-sha1): 12 25 5b 60 69 99 f8 0c c2 82 60 cf 26 05 34 18 73 5a 23 bc
Schlüssel-ID-Hash(sha1): b9 0a f3 5c e2 ed 3a 1b 36 46 9e 75 97 d1 bc 89 b6 02 58 b9
Schlüssel-ID-Hash(md5): 18ea971f355ec8accd4b56496da72f5f
Schlüssel-ID-Hash(sha256): df1c64d884f63b4c02a948db1b6c1ccbaddee862d2b07ef4052f1b30bb5f8d8c
Zertifikathash(md5): 0b a4 8c 74 25 8d 4e d6 d0 73 40 8f b8 1d c3 bd
Zertifikathash(sha1): be cd a2 89 51 5e ca ee ee 74 e3 67 f8 48 7e 70 2d f3 71 5a
Zertifikathash(sha256): 376cc0f898384985d6ffb6141096a37163ab0e2305ba722784f1b5fe1f3b3f1a
Signaturhash: 314e93ce51206799fd491b11a9e9c98f7a34b8cb359e0b38a7d5daa77778bf99
CertUtil: -dump-Befehl wurde erfolgreich ausgeführt.
```