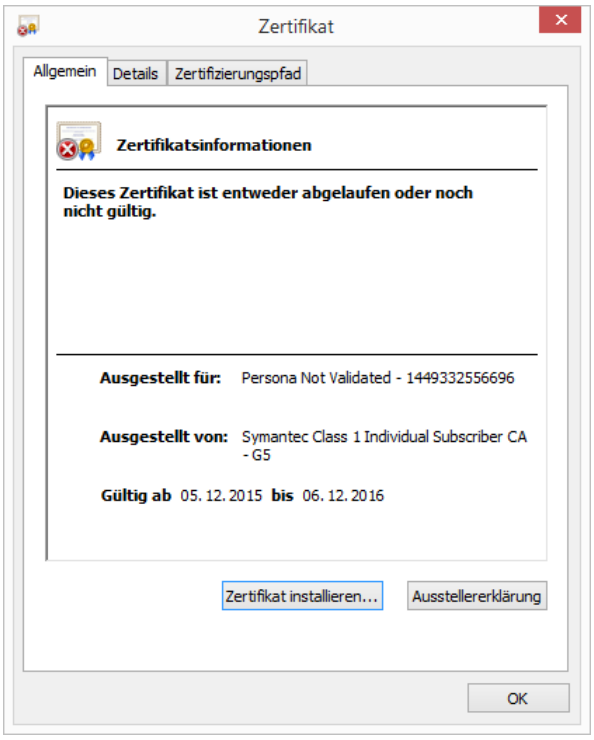
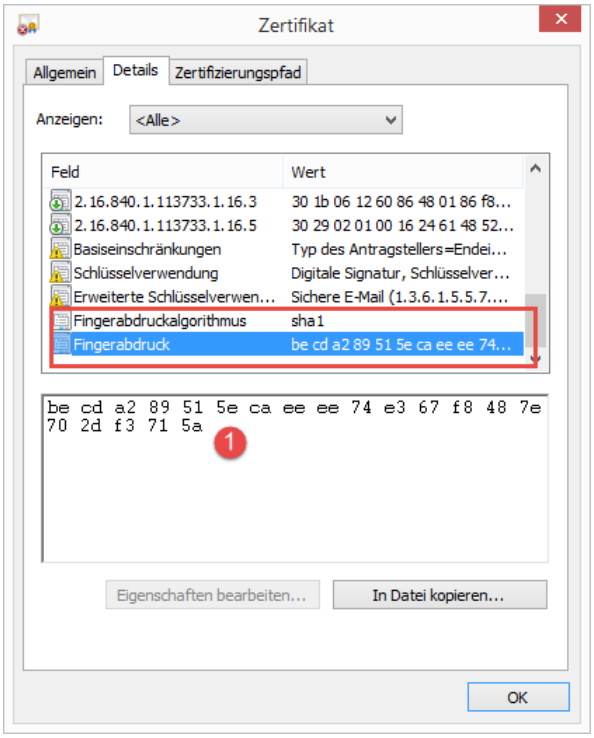
Zertifikat Fingerabdruck SHA256

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.



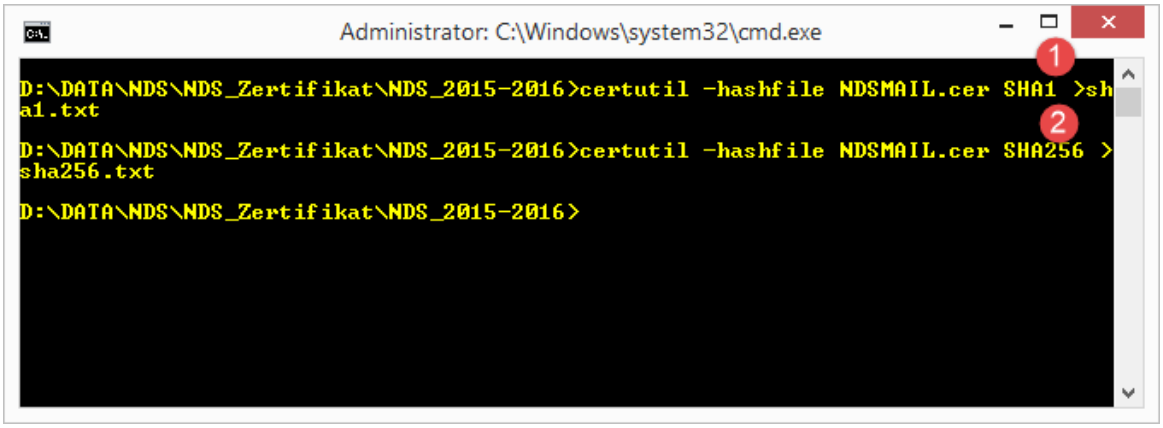
Anzeigefehler?!



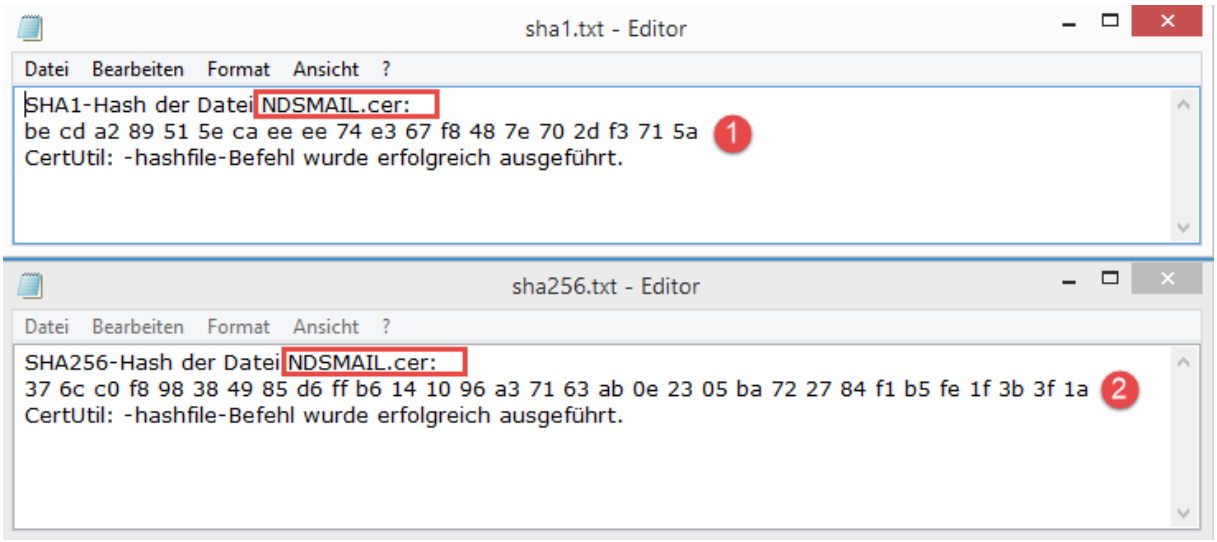
Wie kommen wir denn nun an den Wert des SHA256 Fingerabdruckalgorithmus?

Zertifikat Fingerabdruck SHA256

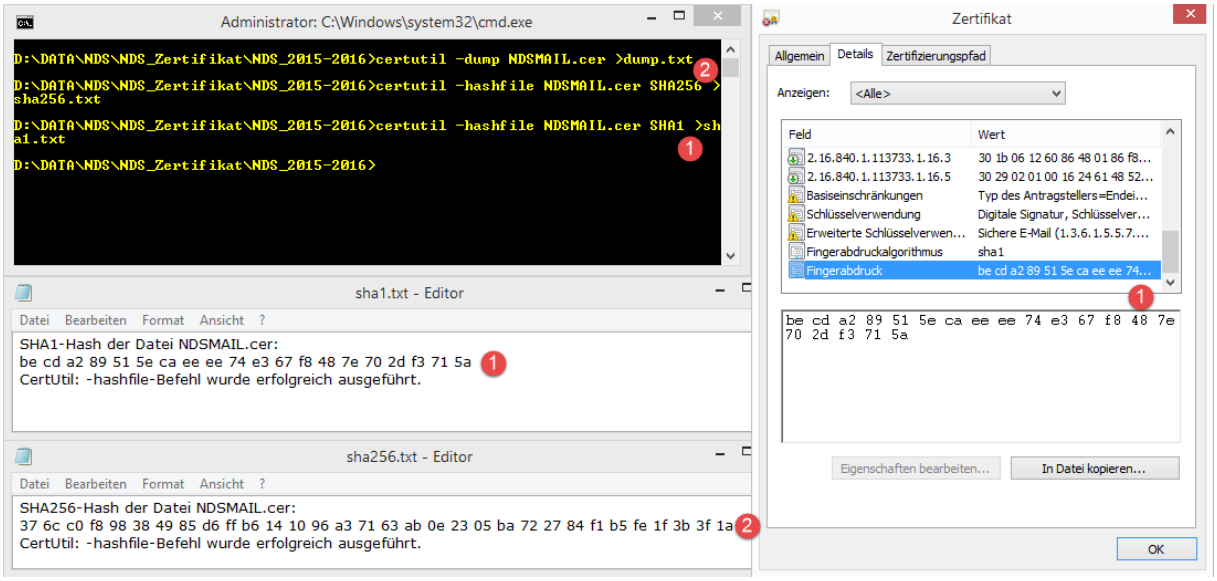
Unter Windows 7 aufwärts können wir uns den Wert mit dem Parameter hashfile exportieren. Ab Windows 8 ist auch die Hilfe dokumentiert.



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.