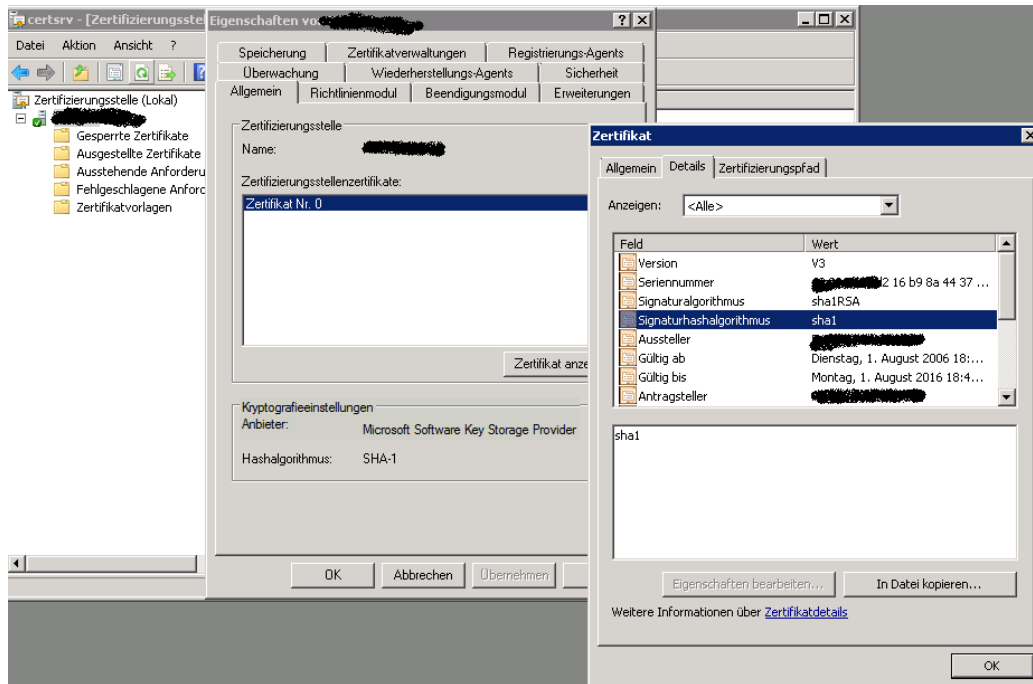


# Windows Server 2008 R2 / 2012 RootCA von SHA1 auf SHA256 hochstufen fuer CNG (Suite B)

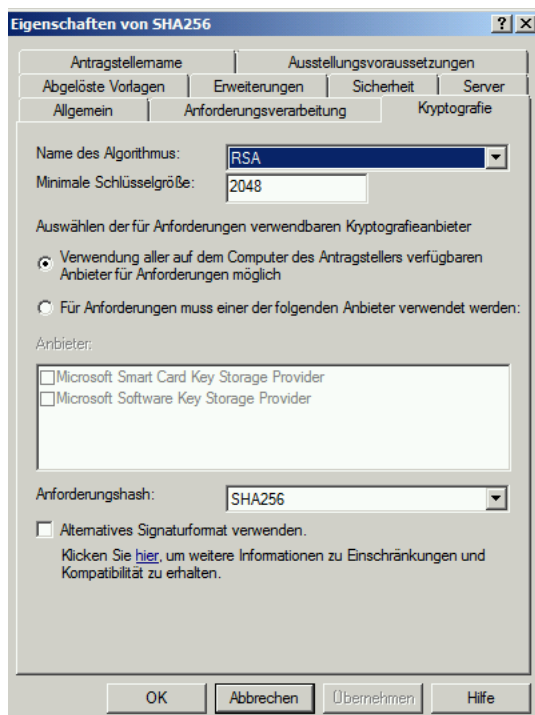
## Root CA Eigenschaften

Hash Algorithmus der Kryptografie Einstellungen ist SHA1. Das Zertifikat verwendet sha1RSA und sha1

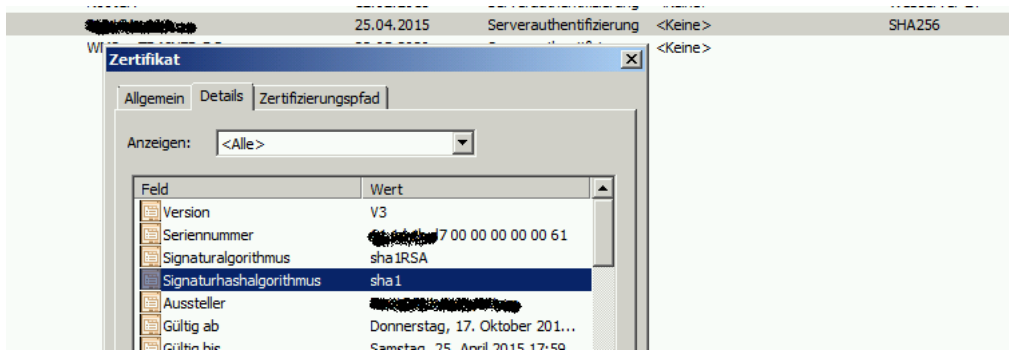


## CA Templates

Wenn man ein Certificate Template dupliziert kann man natuerlich die neuen CNG / SuiteB Algorithmen auswaehlen (SHA 256 ist der Name des Templates in diesem Beispiel).



Es wird trotzdem ein Zertifikat basierend auf SHA1 ausgestellt.

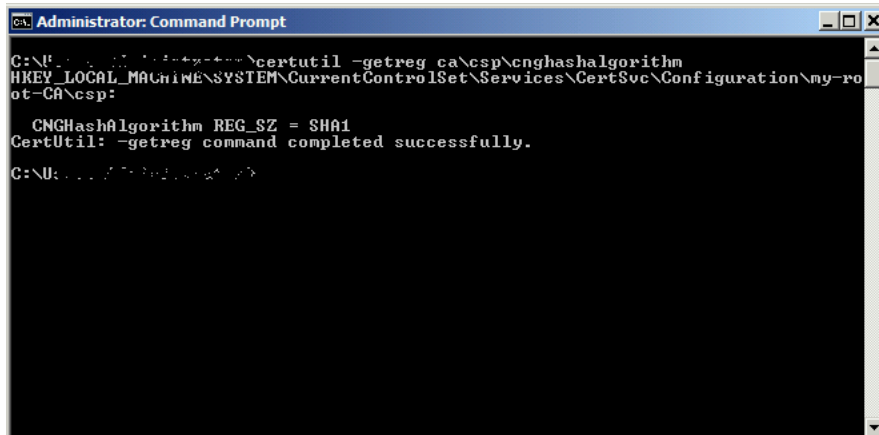


### CSP Provider an der CA anzeigen

```
certutil -getreg ca\csp\Provider
```

Hash Algorithm anzeigen

```
certutil -getreg ca\csp\cnghashalgorithm
```



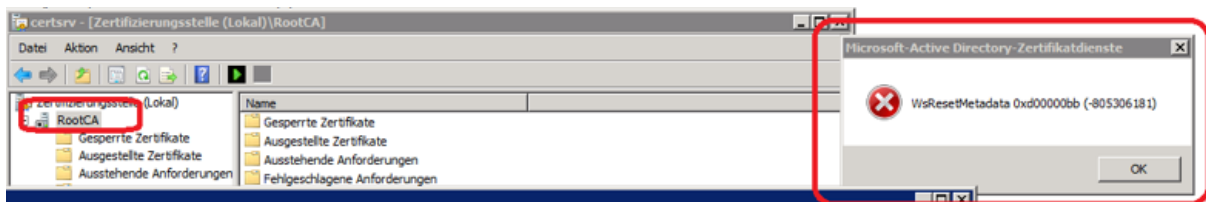
Wie zu sehen ist, wird als CNG Algorithmus SHA1 verwendet.

### Certificate Authority CNG Algorithmus auf SHA256 umstellen

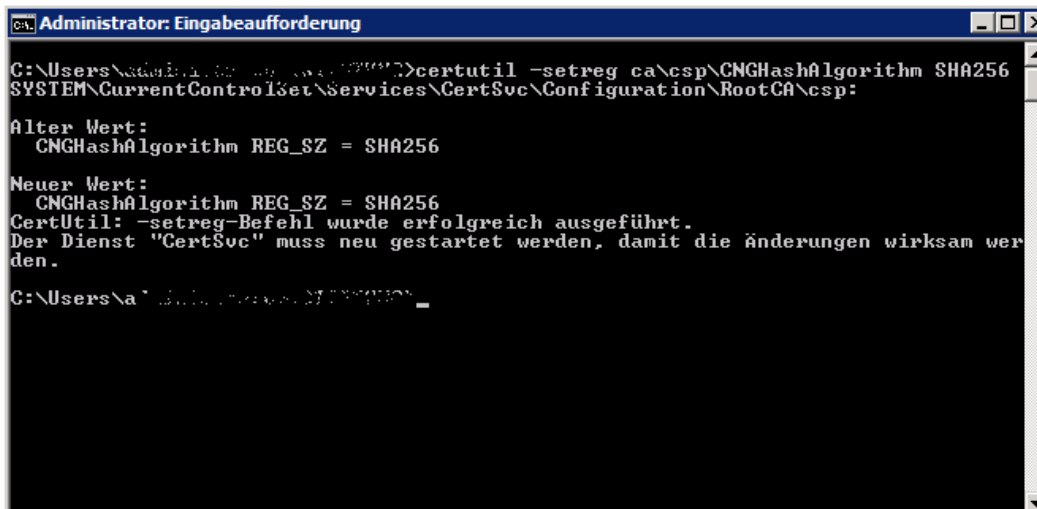
**ACHTUNG:** Wenn der CSP z. B. Microsoft Strong Cryptographic Provider ist, kann SHA256 NICHT verwendet werden

[http://msdn.microsoft.com/en-us/library/bb931357\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/bb931357(VS.85).aspx)

**ACHTUNG:** Der angegebene CNG Algorithmus muss mit Grossbuchstaben geschrieben werden, sonst starten die CA Dienste nicht mehr. Fehlermeldung:



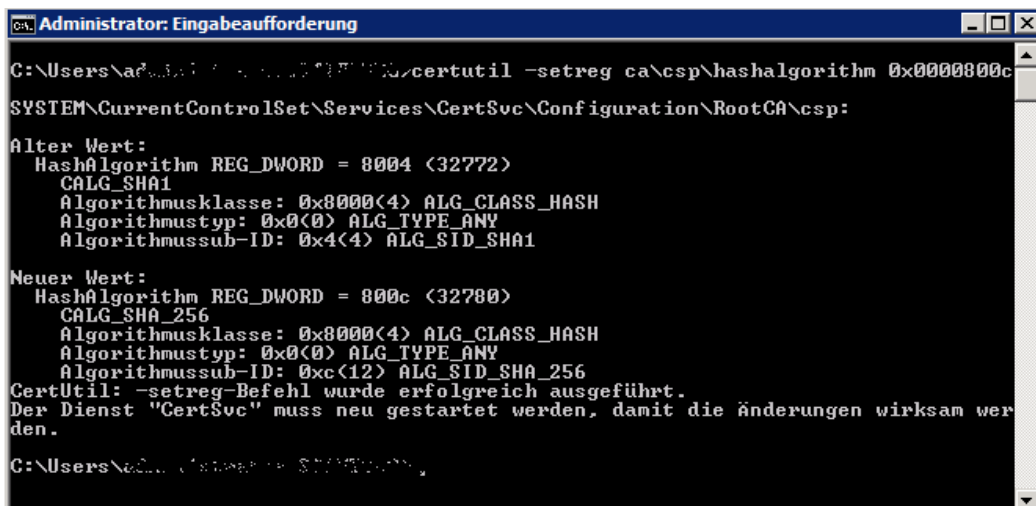
*certutil -setreg ca\csp\CNGHashAlgorithm SHA256*



```
Administrator: Eingabeaufforderung
C:\Users\ad...>certutil -setreg ca\csp\CNGHashAlgorithm SHA256
SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\RootCA\csp:
Alter Wert:
  CNGHashAlgorithm REG_SZ = SHA256
Neuer Wert:
  CNGHashAlgorithm REG_SZ = SHA256
CertUtil: -setreg-Befehl wurde erfolgreich ausgefuehrt.
Der Dienst "CertSvc" muss neu gestartet werden, damit die Aenderungen wirksam werden.
C:\Users\ad...>
```

(Gegebenenfalls) Hash Algorithmus umstellen

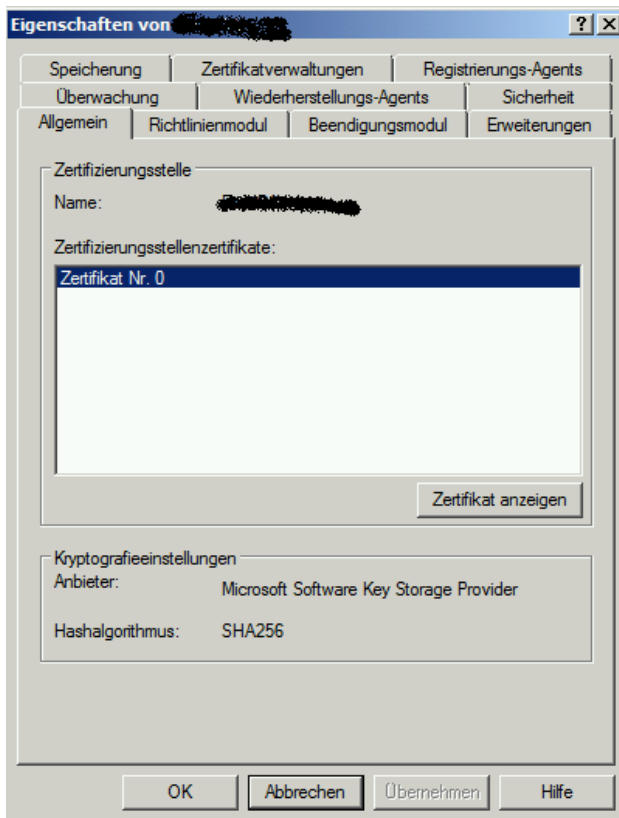
[http://msdn.microsoft.com/en-us/library/windows/desktop/aa375549\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa375549(v=vs.85).aspx)



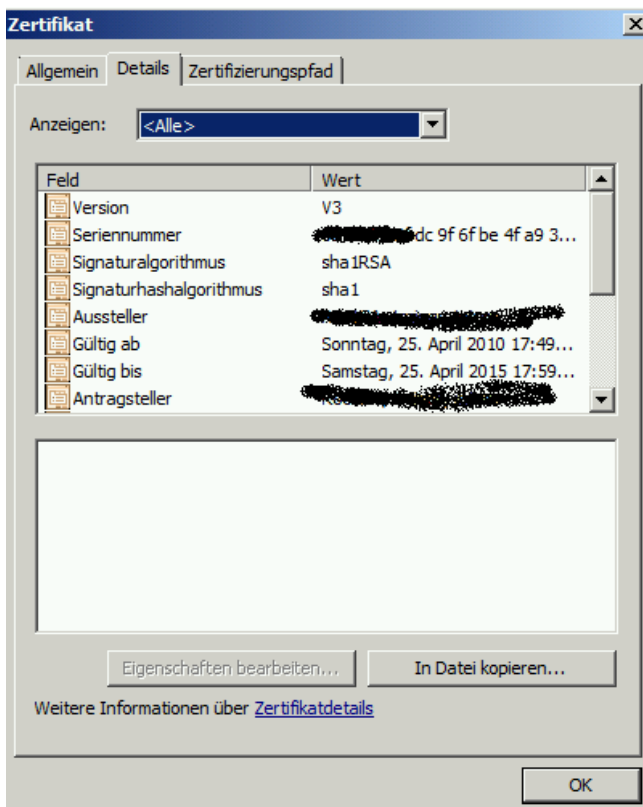
```
Administrator: Eingabeaufforderung
C:\Users\ad...>certutil -setreg ca\csp\hashalgorithm 0x0000800c
SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\RootCA\csp:
Alter Wert:
  HashAlgorithm REG_DWORD = 8004 (32772)
  CALG_SHA1
  Algorithmusklasse: 0x8000(4) ALG_CLASS_HASH
  Algorithmustyp: 0x0(0) ALG_TYPE_ANY
  Algorithmussub-ID: 0x4(4) ALG_SID_SHA1
Neuer Wert:
  HashAlgorithm REG_DWORD = 800c (32780)
  CALG_SHA_256
  Algorithmusklasse: 0x8000(4) ALG_CLASS_HASH
  Algorithmustyp: 0x0(0) ALG_TYPE_ANY
  Algorithmussub-ID: 0xc(12) ALG_SID_SHA_256
CertUtil: -setreg-Befehl wurde erfolgreich ausgefuehrt.
Der Dienst "CertSvc" muss neu gestartet werden, damit die Aenderungen wirksam werden.
C:\Users\ad...>
```

Certificate Authority Dienst neu starten

Anschliessend ist der Hash Algorithmus SHA256



Das ausgestellte Root CA Zertifikat ist noch auf SHA-1 basierend. Das stellt kein Problem dar fuer neu auszustellende Zertifikate.



Anschliessend kann jetzt von einem Client/Server ein neues Zertifikat, basierend auf dem V3 Template und dem SHA-256 Algorithmus, angefordert werden.

