UMSTELLUNG DER INTERNEN PKI VON SHA1 NACH SHA256

EINLEITUNG

In diesem Dokument werden in Stichpunkten die notwendigen Schritte für eine Inplace-Umstellung einer PKI von SHA1 nach SHA2 (speziell SHA256) genannt und kurz beschrieben. Wir gehen von einer zweistufigen PKI aus.

VORAUSSETZUNGEN

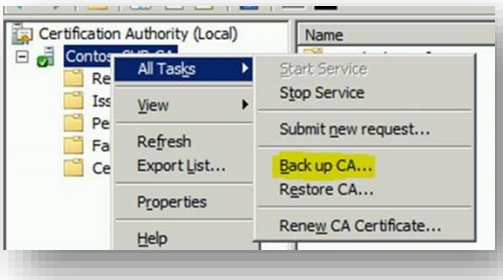
Gilt für Root, als auch für die Issuing-CA.

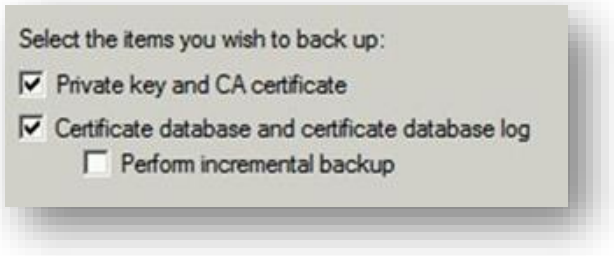
- Mindestens Windows Server 2008
- Temporäre Maschine mit Windows 8.1 / Windows Server 2012 R2 für die Umstellung (certutil)
- Kontrolle der aktuell verwendeten Konfiguration:

```
certutil -getreg CA\CSP\CNGHashAlgorithm
certutil –store my “Name der CA”
```

- CSP-Provider (gelb markiert) müssen auf KSP umgestellt werden

- Backup der CA
  - C:\CA-Backup\
  - MMC + Registry



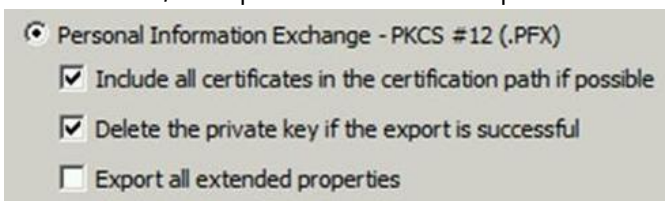



```
reg export HKLM\SYSTEM\CurrentControlSet\services\CertSvc c:\CA-Backup\CAregistry.reg
```

UMSETZUNG

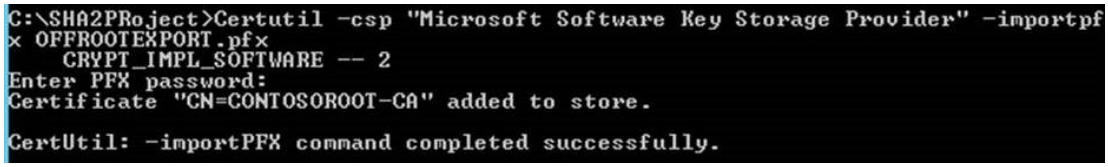
ROOT-CA

1. Von CSP auf KSP umstellen, vor Windows Server 2012:
   a. CA-Service beenden
   b. CA-Zertifikat/e mit privatem Schlüssel exportieren



   c. CA-Zertifikat/e temporär auf Windows 8 / Server 2012 importieren:
   Dieser Schritt ist notwendig, um das Zertifikat selbst auf KSP umzustellen. Der Import-Befehl über certutil kennt die Erweiterung „-csp" erst bei Windows 8 / Server 2012.

```
Certutil –csp “Microsoft Software Key Storage Provider” -importpfx ca-cert.pfx
```



   d. CA-Zertifikat/e wieder mit priv. Schlüssel exportieren
   Sollte bei diesem Schritt in der MMC die Möglich „Mit privatem Schlüsel" zu exportieren ausgegraut sein, so muss das Zertifikat erneut über die MMC-Konsole importiere und die Option, exportieren d. priv. Schlüssels erlauben, gesetzt werden. Dies hat keinen Einfluss auf den Punkt 1.c.
   e. CA-Zertifikat/e wieder in die CA importieren: **Als exportierbar markieren!**
   f. Wurde das Zertifikat der CA bereits mehrmals mit demselben Schlüssel erneuert, bricht diese Prozedur die Assoziierung der Zertifikate. Für jedes erneuerte Zertifikat muss folgender Befehl abgesetzt werden:

```
certutil –repairstore MY serialnumber
```

   g. CSP.reg-Datei mit folgenden Werten importieren:

```
Windows Registry Editor Version 5.00
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\<Your CA Common Name>\CSP]
"ProviderType"=dword:00000000
"Provider"="Microsoft Software Key Storage Provider"
"CNGPublicKeyAlgorithm"="RSA"
"CNGHashAlgorithm"="SHA1"
```

h. EncryptionCsp.reg-Datei mit folgenden Werten importieren:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\<Your CA Common Name>\EncryptionCSP]
"ProviderType"=dword:00000000
"Provider"="Microsoft Software Key Storage Provider"
"CNGPublicKeyAlgorithm"="RSA"
"CNGEncryptionAlgorithm"="3DES"
"MachineKeyset"=dword:00000001
"SymmetricKeySize"=dword:000000a8
```

2. Hash Algorithmus auf SHA2 umstellen
   a. Certutil auf der CA ausführen:

```
certutil -setreg ca\csp\CNGHashAlgorithm SHA256
```

   b. CA-Dienst wieder starten
   c. CA-Zertifikat erneuern
   d. CA-Zertifikat überprüfen
   e. CA-CRL erneuern

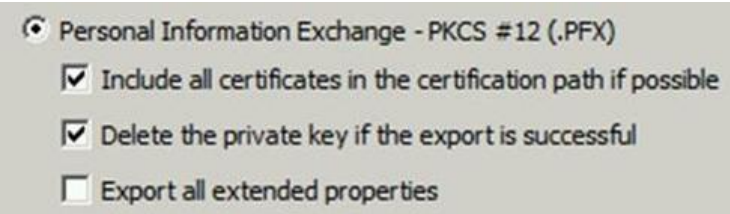
```
Certutil -crl
```

   f. CA-Zertifikat und CRL im Active Directory veröffentlichen

```
certutil -f -dspublish <.CRT file> RootCA
certutil -f -dspublish <.CRL file>
```

ISSUING-CA

1. Von CSP auf KSP umstellen, vor Windows Server 2012:
   a. CA-Service beenden
   b. CA-Zertifikat/e mit privatem Schlüssel exportieren



   c. CA-Zertifikat/e temporär auf Windows 8 / Server 2012 importieren:

Dieser Schritt ist notwendig, um das Zertifikat selbst auf KSP umzustellen. Der Import-Befehl über certutil kennt die Erweiterung „-csp" erst bei Windows 8 / Server 2012.

```
Certutil -csp "Microsoft Software Key Storage Provider" -importpfx ca-cert.pfx
```

```
C:\SHA2PRoject>Certutil -csp "Microsoft Software Key Storage Provider" -importpf
x OFFROOTEXPORT.pfx
    CRYPT_IMPL_SOFTWARE -- 2
Enter PFX password:
Certificate "CN=CONTOSOROOT-CA" added to store.

CertUtil: -importPFX command completed successfully.
```

d. CA-Zertifikat/e wieder mit priv. Schlüssel exportieren
Sollte bei diesem Schritt in der MMC die Möglich „Mit privatem Schlüsel" zu exportieren ausgegraut sein, so muss das Zertifikat erneut über die MMC-Konsole importiere und die Option, exportieren d. priv. Schlüssels erlauben, gesetzt werden. Dies hat keinen Einfluss auf den Punkt 1.c.

e. CA-Zertifikat/e wieder in die CA importieren: **Als exportierbar markieren!**

f. Wurde das Zertifikat der CA bereits mehrmals mit demselben Schlüssel erneuert, bricht diese Prozedur die Assoziierung der Zertifikate. Für jedes erneuerte Zertifikat muss folgender Befehl abgesetzt werden:

```
certutil -repairstore MY serialnumber
```

g. CSP.reg-Datei mit folgenden Werten importieren:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\<Your
CA Common Name>\CSP]
"ProviderType"=dword:00000000
"Provider"="Microsoft Software Key Storage Provider"
"CNGPublicKeyAlgorithm"="RSA"
"CNGHashAlgorithm"="SHA1"
```

h. EncryptionCsp.reg-Datei mit folgenden Werten importieren:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\<Your
CA Common Name>\EncryptionCSP]
"ProviderType"=dword:00000000
"Provider"="Microsoft Software Key Storage Provider"
"CNGPublicKeyAlgorithm"="RSA"
"CNGEncryptionAlgorithm"="3DES"
"MachineKeyset"=dword:00000001
"SymmetricKeySize"=dword:000000a8
```

2. Hash Algorithmus auf SHA2 umstellen
   a. Certutil auf der CA ausführen:

```
certutil -setreg ca\csp\CNGHashAlgorithm SHA256
```

   b. CA-Dienst wieder starten

c. CA-Zertifikat erneuern
   i. Request erstellen und durch Root-CA signieren lassen
   ii. .cer importieren
d. CA-Zertifikat überprüfen
e. CA-CRL erneuern

```
Certutil -crl
```

QUELLEN/REFENZEN

Beispielmigration einer zweistufigen PKI mit Windows Server 2008 R2 (offline- und issuing-CA)	http://blogs.technet.com/b/askds/archive/2015/10/26/sha1-key-migration-to-sha256-for-a-two-tier-pki-hierarchy.aspx
TechNet-Beschreibung zur Umstellung KSP und SHa256	https://technet.microsoft.com/en-us/library/dn771627.aspx
Microsoft-Policy zu SHA1	http://social.technet.microsoft.com/wiki/contents/articles/32288.windows-enforcement-of-authenticode-code-signing-and-timestamping.aspx