Ing. Ondřej Ševeček | PM Windows Server | GOPAS a.s. |
MCM: Directory Services | MVP: Enterprise Security | CEH |
ondrej@sevecek.com | www.sevecek.com |

CA LIFECYCLE AND BACKUP/RESTORE

1

Renewing Enterprise CAs

- Must update AD configuration under Enterprise Admins member
  - CN=nTAuthCertificates
    - adds new item into cACertificate attribute
  - CN=CDP
    - adds new object cRLRevocationList (name index (1))
  - CN=Certification Authorities
    - adds new item itno cACertificate attribute
- PKI Admins member can update
  - CN=AIA
    - adds new item into cACertificate attribute
  - CN=EnrollmentServices
    - replaces the only item in the cACertificate attribute

2

Renew SubCA #0 c:\windows\capolicy.inf longer key only

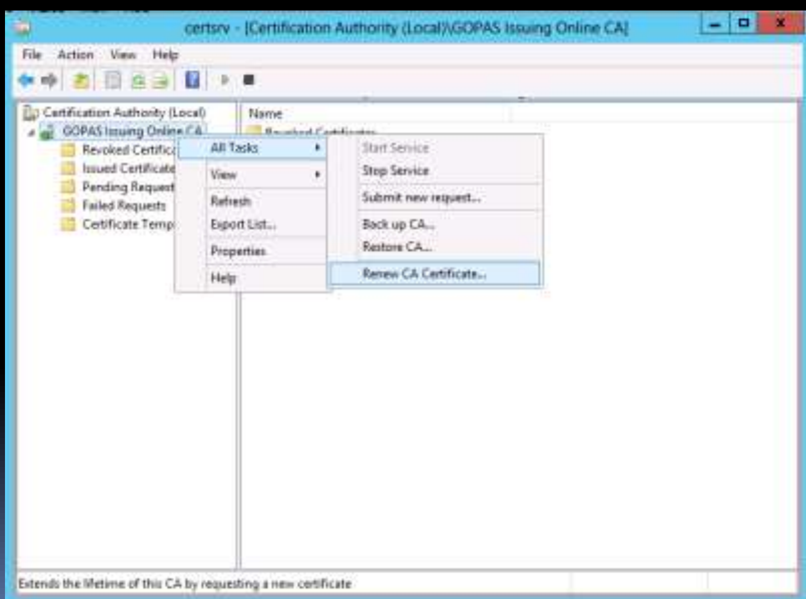
capolicy.inf - Notepad

File Edit Format View Help

```
[Version]
  Signature= "$Windows NT$"

[certsrv_server]
RenewalKeyLength=4096
RenewalValidityPeriod=Years
```

3

Renew SubCA 1#



4

Renew SubCA 2#

5

policy.inf

```
[Version]
Signature = "$Windows NT$"

[PolicyStatementExtension]
Policies = AllIssuancePolicy
Critical = False

[AllIssuancePolicy]
OID = 2.5.29.32.0

[NameConstraintsExtension]
Include = NameConstraintsPermitted
Critical = True

[NameConstraintsPermitted]
DNS = .gopas.cz
UPN = @gopas.cz
```

6

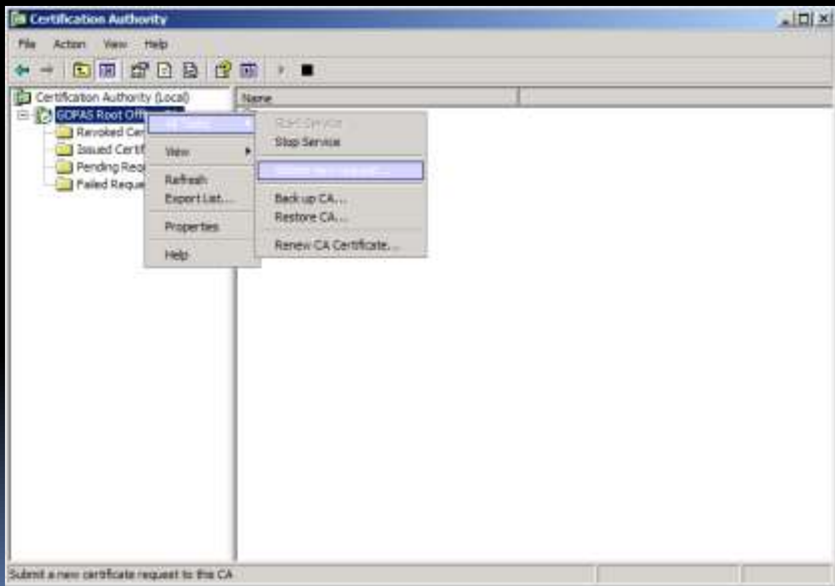
policy.inf

```
[ApplicationPolicyStatementExtension]
Policies = AppSCPolicy, AppClAuthPolicy, AppSrvAuthPolicy
Critical = False

[AppClAuthPolicy]
OID = 1.3.6.1.5.5.7.3.2 ; Client Authentication

[AppSrvAuthPolicy]
OID = 1.3.6.1.5.5.7.3.1 ; Server Authentication

[AppSCPolicy]
OID = 1.3.6.1.4.1.311.20.2.2 ; Smart Card Logon

[ApplicationPolicyConstraintsExtension]
RequireExplicitPolicy = 1
InhibitPolicyMapping = 1
Critical = True
```


Renew SubCA 3#

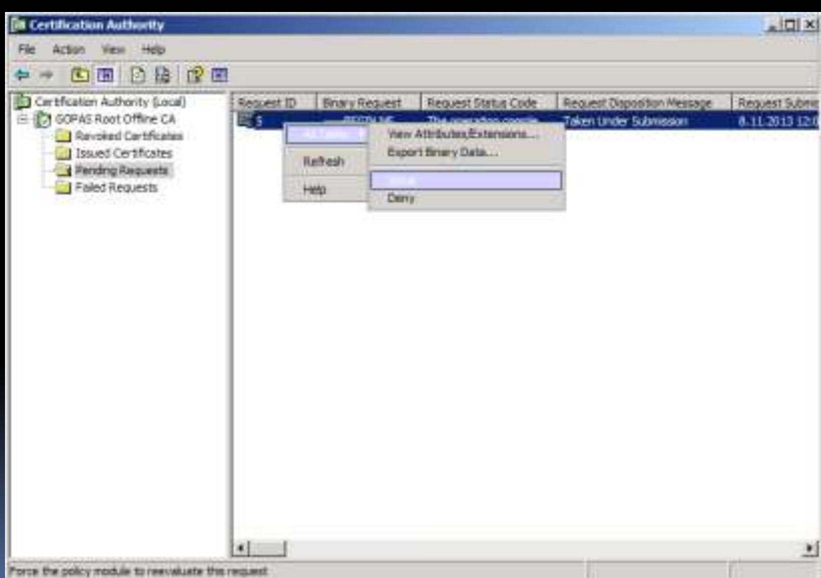
- Apply qualified subCA restrictions on RootCA
- CERTREQ -policy -q -f -cert "GOPAS Offline Root CA" entCAoriginal.req capolicy-qualifiedSubordinateCA.inf qualifiedEntCA.req

Renew SubCA 4#



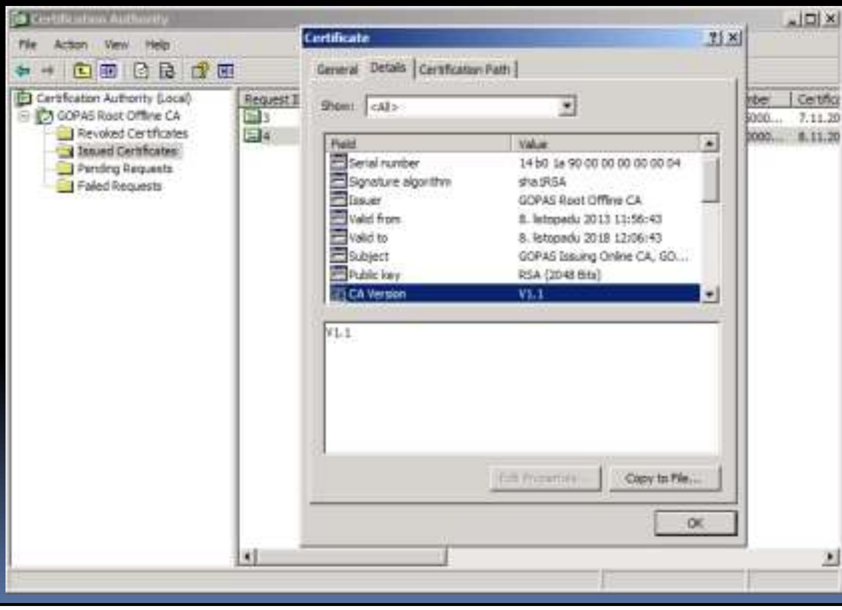
9

Renew SubCA 5#



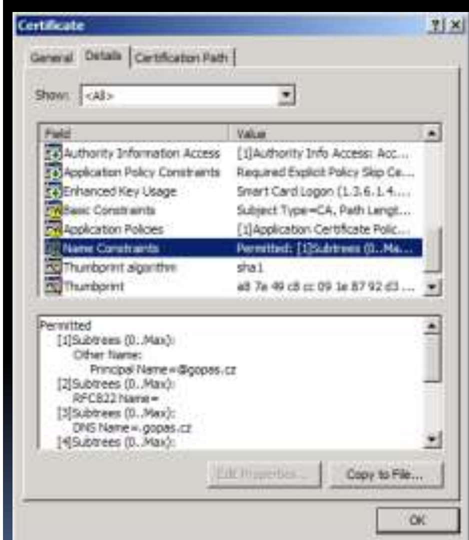
10

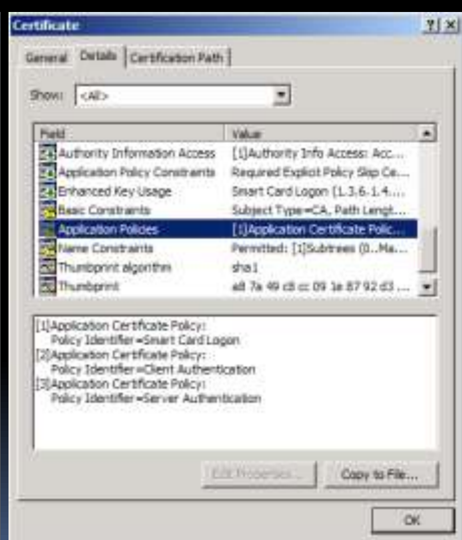
Renew SubCA 6#



11

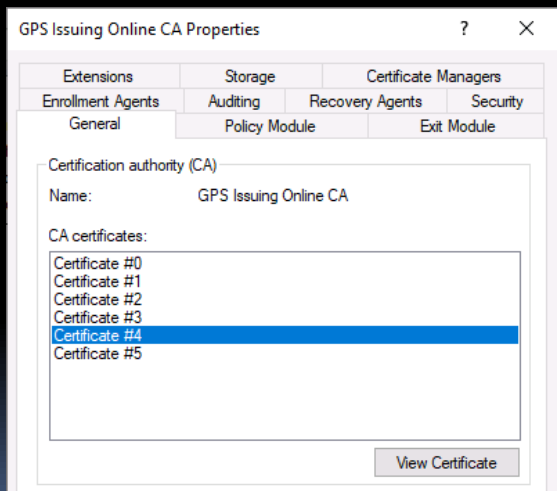
Renew SubCA 7#





12

Renew SubCA 8#



13

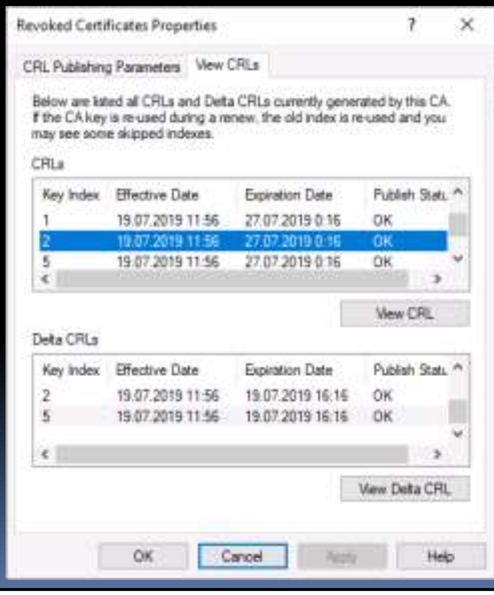
CaVersion extension (Issuer Name ID)

4	2
5. certificate	key same as the 3. certificate

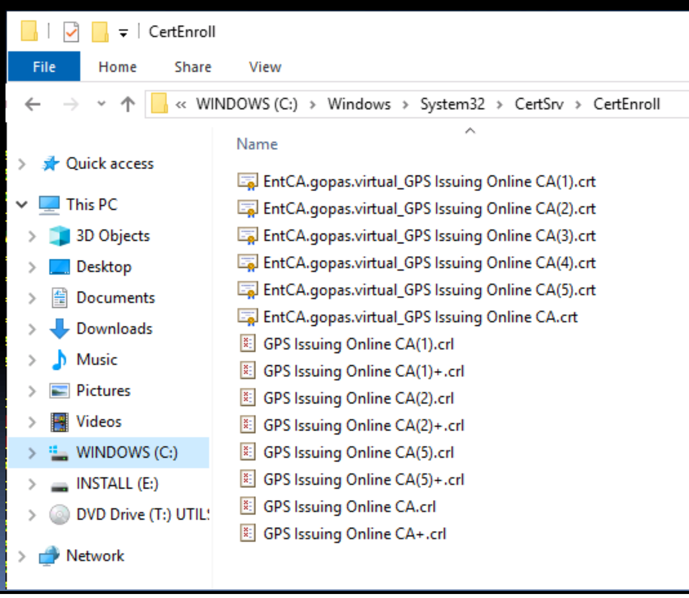
0.0	1.1	2.2	3.2	4.2	5.5
initial key	new key	new key	same key	same key	new key

14

Renew SubCA 9#

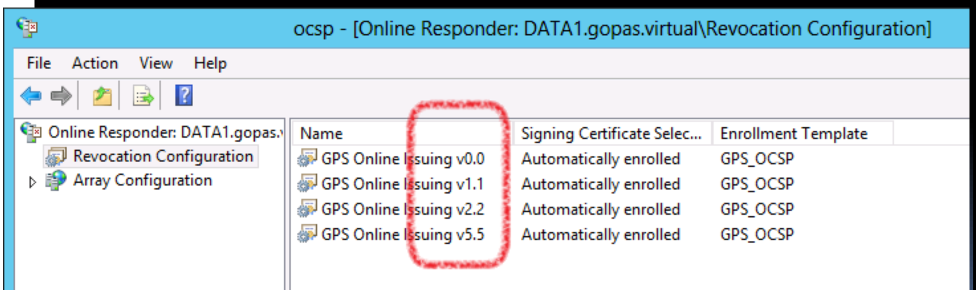


Renew SubCA 10#



Renew SubCA 11#

```
certutil -setreg CA\UseDefinedCACertInRequest 1

# Note: requests contain just the Authority Key Id
#       v2.2 issued by v4.2 CA certificate in fact
```



CA Lifecycle

BACKUP AND RESTORE

Components and disaster recovery

- Certificate(s) + private key(s)
- Registry configuration
  - HKLM\system\CCS\Services\CertSvc\Configuration
- List of active templates
  - LDAP config CN=Entrollment Services
- Template definitions
  - CN=Certificate Templates,...,CN=Configuration
  - + DSACLS permission
- Publishing scripts
- TPM inventory
- publish new CRLs
- Database
  - last issued certificates missing?
  - last revocations missing?

Restore

- Clean OS install
  - different name
  - different domain
- Import CA certificate(s) + private key(s)
  - install HSM drivers
- Install CA
- Import registry backup
- Restore DB
- Reconfigure CDP and AIA
  - correct LDAP permissions
- Restore certificate template list

After restore

- Failure
  - import lost issued certificates into DB
  - re-revoke lost revocations
- Name change
  - correct CA names in registry and AD LDAP
  - permissions

21

Ing. Ondřej Ševeček | PM Windows Server | GOPAS a.s. |
MCM: Directory Services | MVP: Enterprise Security | CEH |
ondrej@sevecek.com | www.sevecek.com |

THANK YOU!

22