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

COMPLEX CERTIFICATE POLICIES

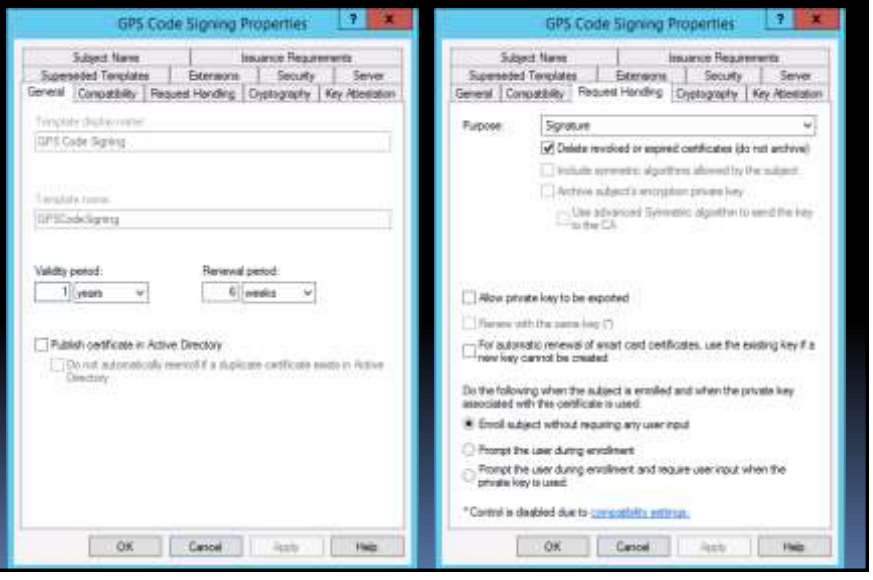
1

Enterprise PKI

CODE SIGNING

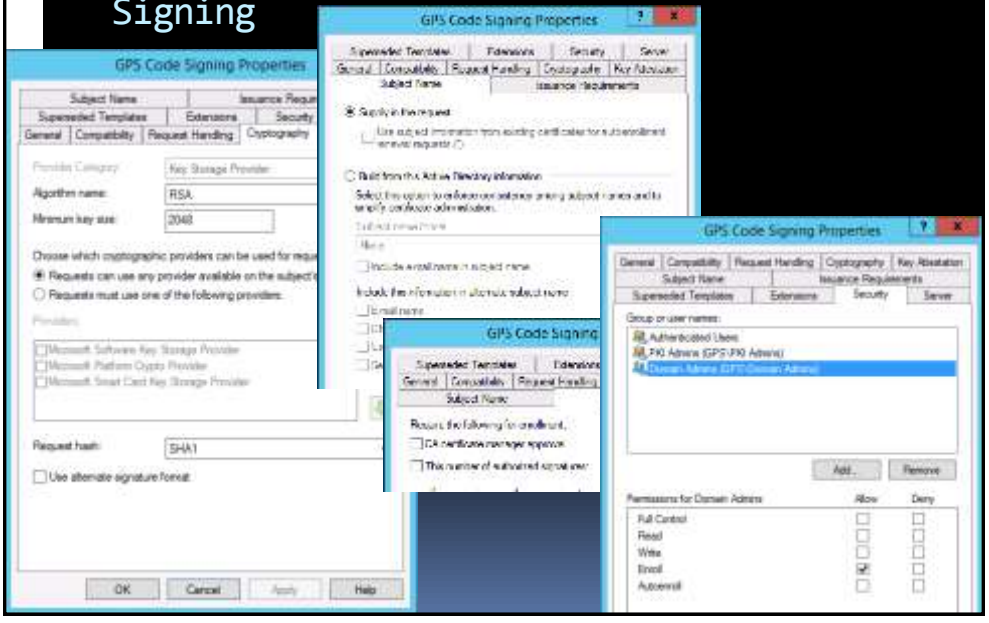
2

Certificate template details for Code Signing



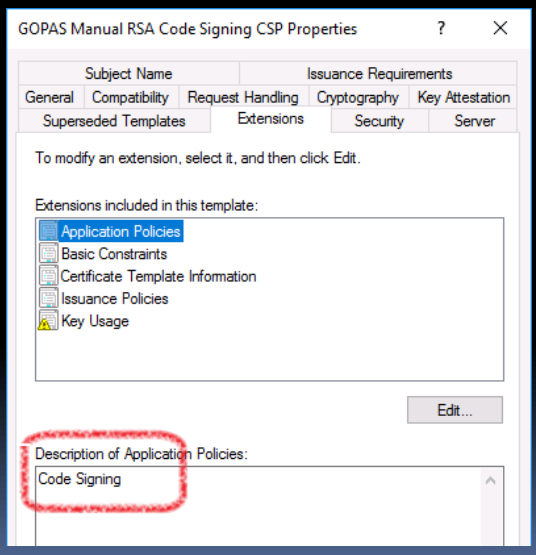
3

Certificate template details for Code Signing



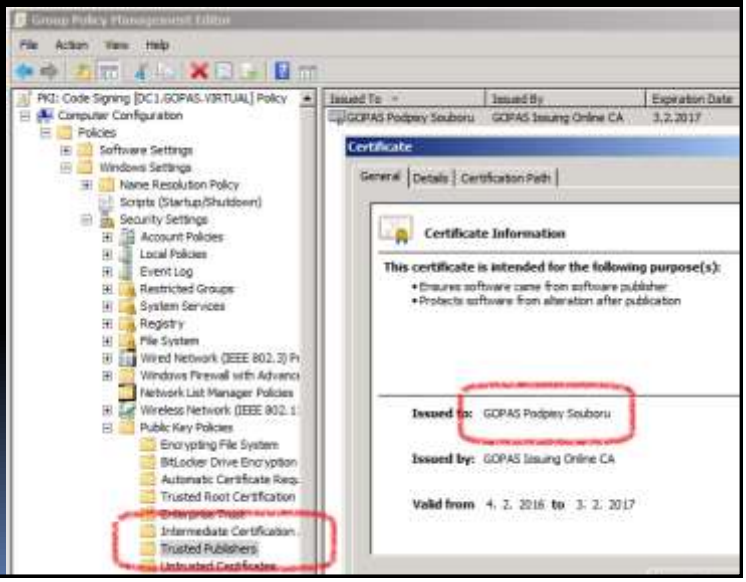
4

Code Signing EKU 1.3.6.1.5.5.7.3.3



5

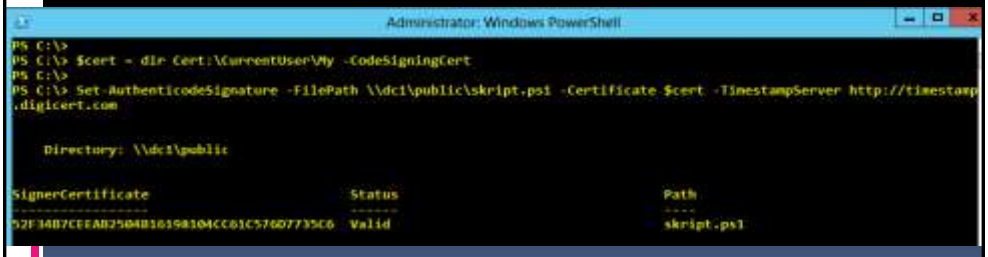
Make the certificate trusted in the Trusted Publishiers list



6

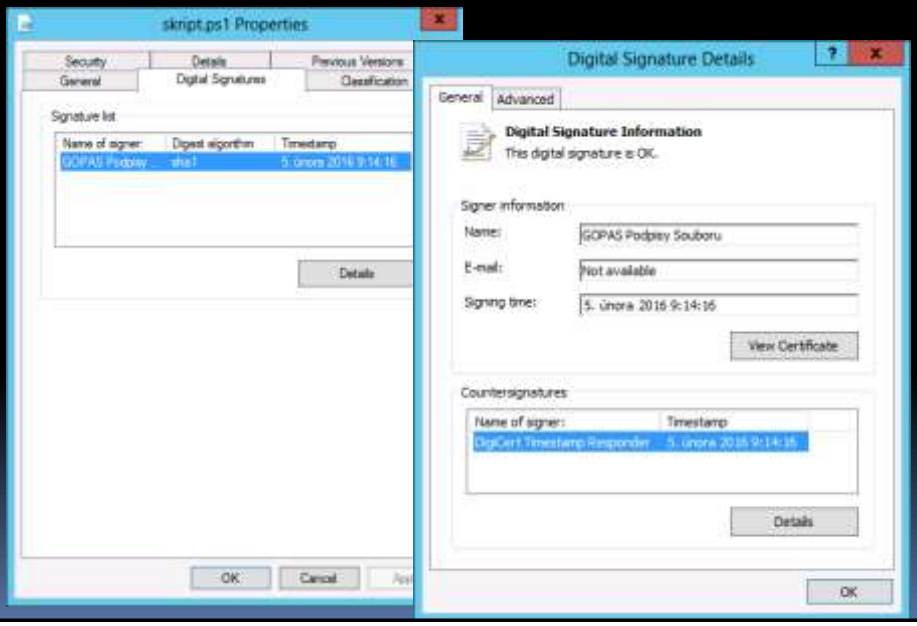
Set-AuthenticodeSignature
must use TimestampServer in order to trust the signature after certificate expiration

http://timestamp.digicert.com
http://www.startssl.com/timestamp
http://timestamp.globalsign.com/scripts/timestamp.dll
http://timestamp.verisign.com/scripts/timestamp.dll



7

Code signature and timestamp in GUI



8

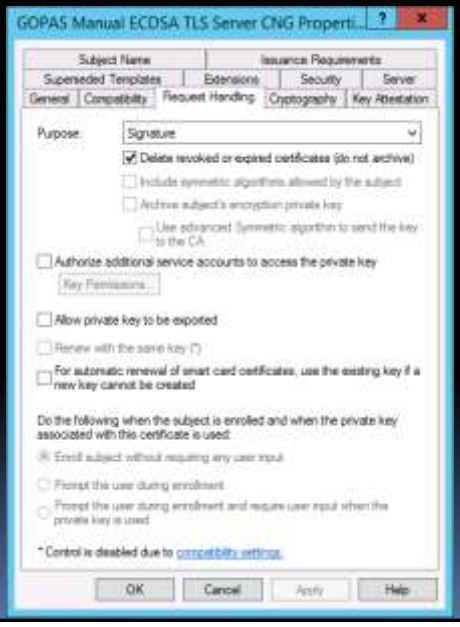
Code signing

- .EXE, .VBS, .PS1
  - Other text files would need to change extension
- You cannot sign .BAT files
- powershell -Command
  - does not follow Execution Policy

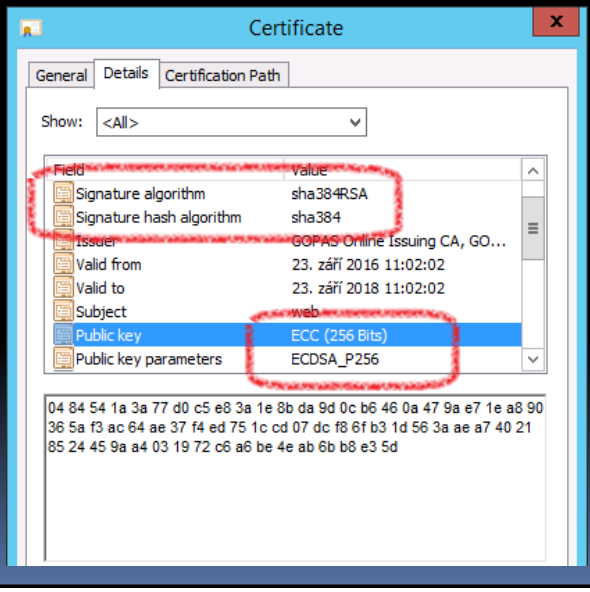
Enterprise PKI

CNG WEB SERVER CERTIFICATES

CNG KSP (Key Storage Provider) template



Issued certificate from an RSA 2048 CA which signes with SHA384



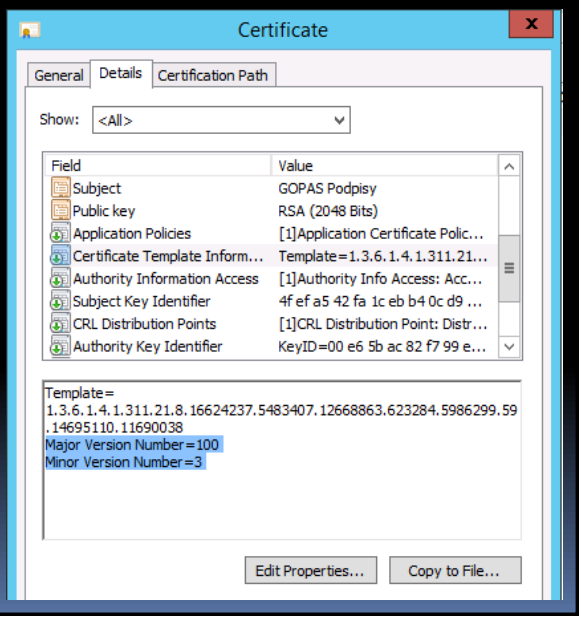
Enterprise PKI

CERTIFICATE TEMPLATE LIFECYCLE

Template versioning

- Major.Minor
- Minor version change
  - stored in issued certificates
  - does not change with Security tab changes (2008 R2-)
- Major version change
  - Reenroll all certificate holders

Template versions in issued certificates



15

Superseded templates

Currently issued certificate are reenrolled with the superseding template

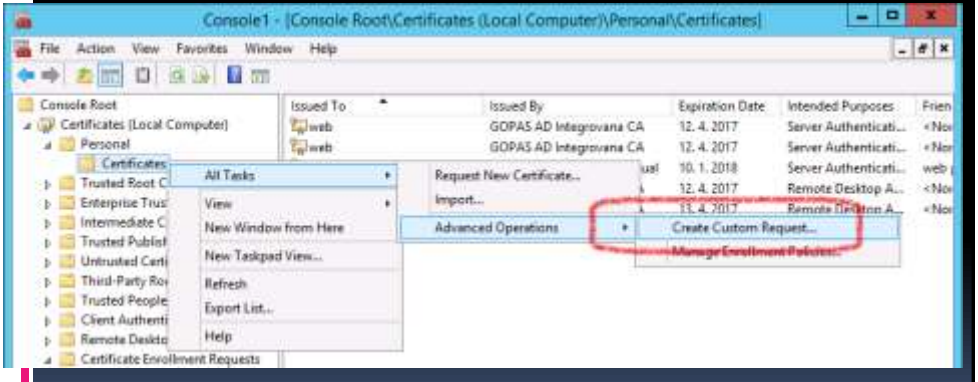
16

Enterprise PKI

MANUAL/OFFLINE CERTIFICATE REQUESTS, SCEP AND WS

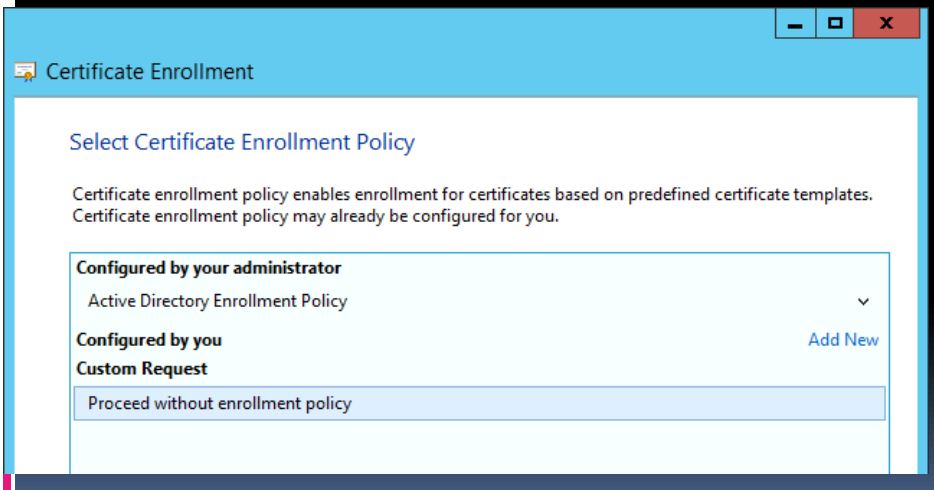
17

Create custom request to produce an offline file-based request (non-domain machines, public CAs)



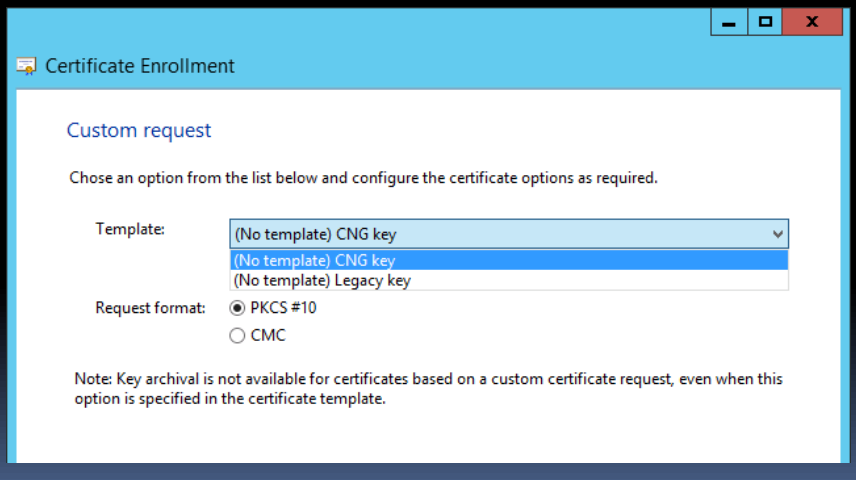
18

No certificate template available on workgroup machines



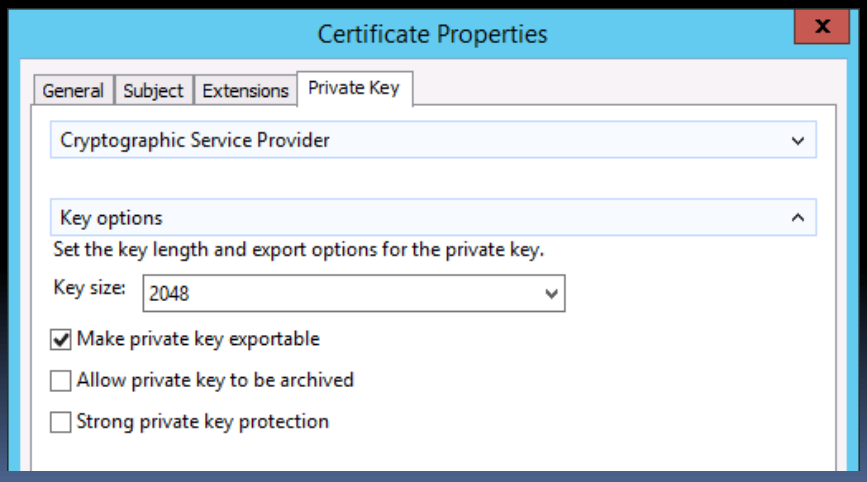
19

Select newer CNG/KSP or the older CSP provider to manage the private key locally



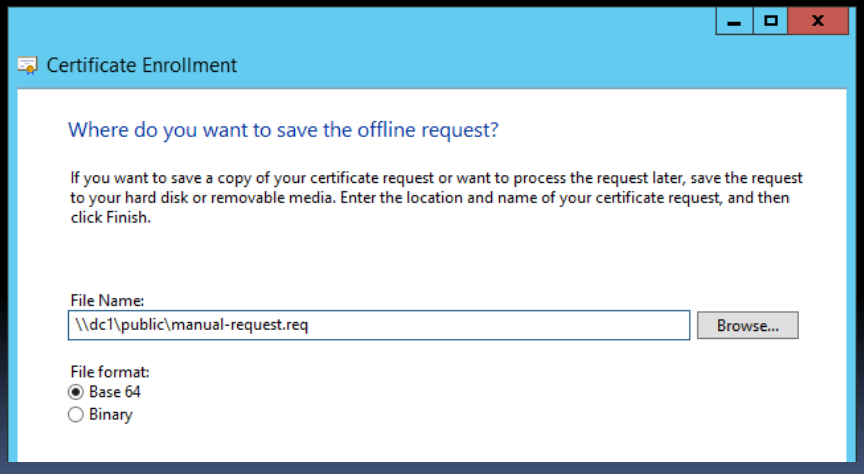
20

Make sure you correctly select the key size and if exportability requested



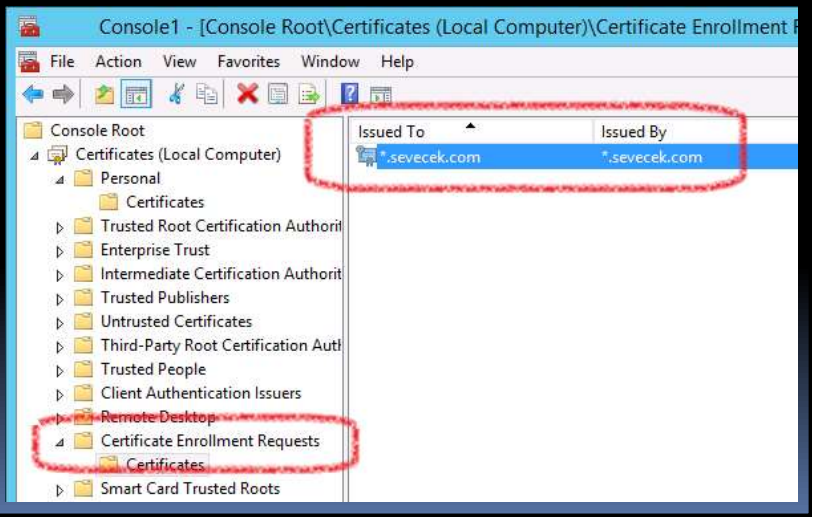
21

You can copy/paste Base64 file contents into web browsers

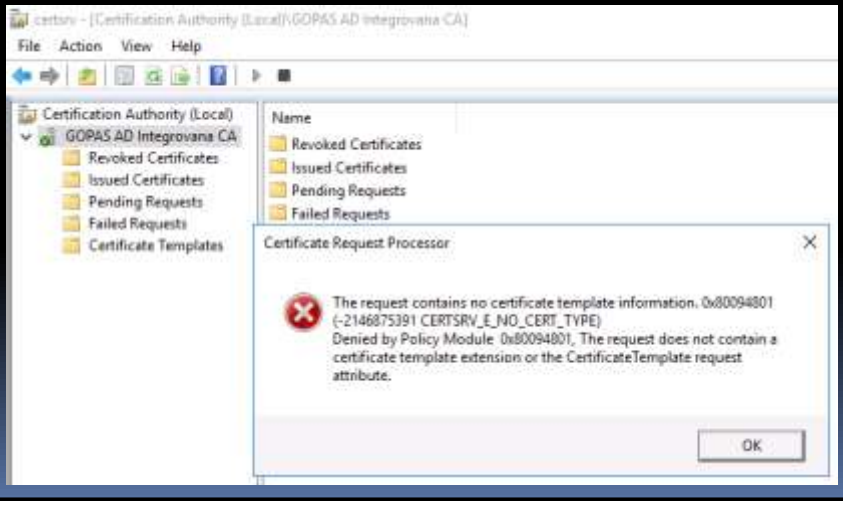


22

The self-signed certificate request is stored locally in order to keep the private key



Importing on an enterprise AD integrated CA requires a request with certificate template extension specified
Error: -2146875391 0x80094801 CERTSRV_E_NO_CERT_TYPE
The request contains no certificate template information



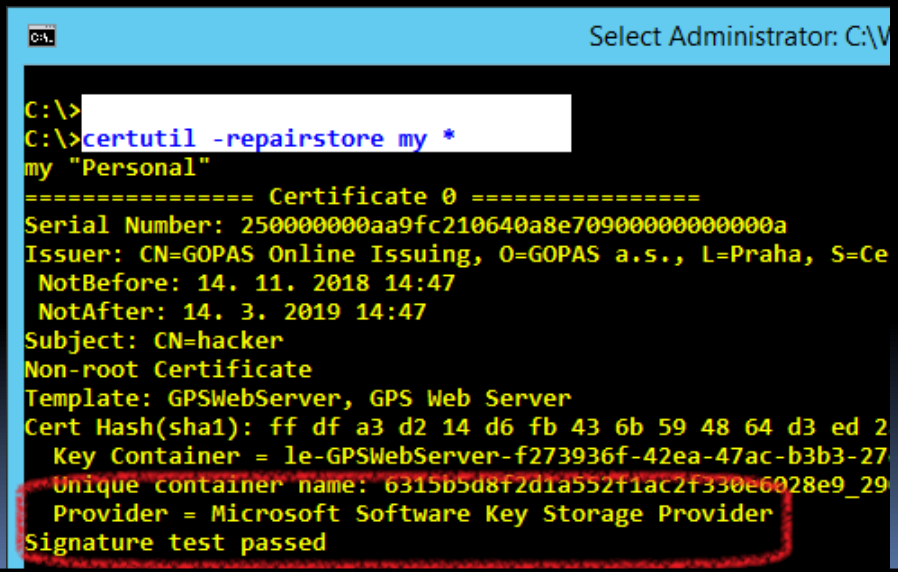
Add the CertificateTemplate extension information and re-sign the request

CERTREQ -attrib "CertificateTemplate:GPSWebServer" -submit

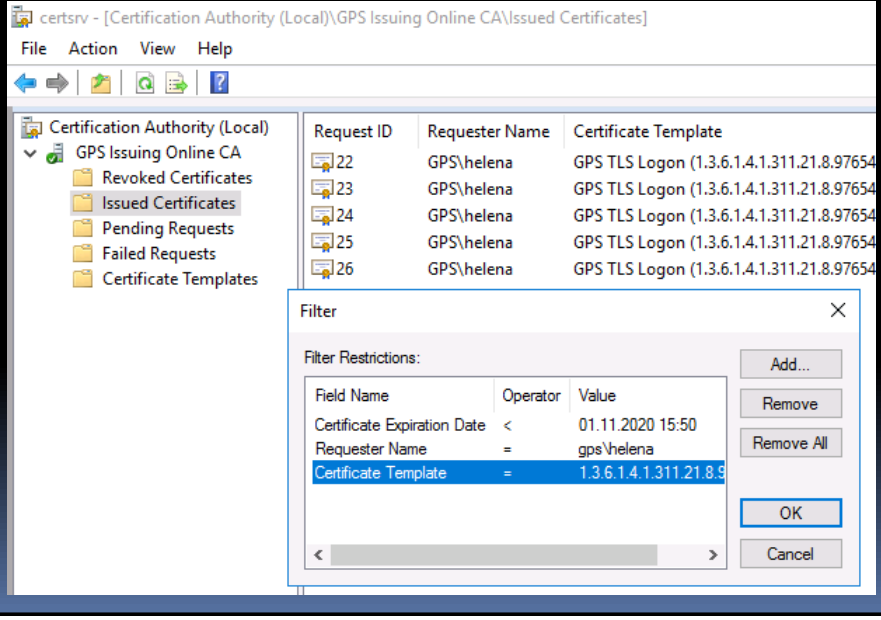
Changing SAN

```
-attrib
"CertificateTemplate:GPSWebServer
\nSAN:DNS=www.sevecek.com&DNS=www
.gopas.cz"
```

Pairing orphaned certificates with their private key



Filtering in ADCS console



CERTREQ .INF file sample (continues …)

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

[NewRequest]
KeySpec = 1
KeyUsage = 0xA0
KeyLength = 2048
RequestType = "CMC"
Subject = "CN=*.gopas.cz"
Exportable = FALSE
MachineKeySet = TRUE
PrivateKeyArchive = FALSE
Silent = TRUE
SMIME = FALSE
UseExistingKeySet = FALSE
HashAlgorithm = SHA1
AlternateSignatureAlgorithm = FALSE
FriendlyName = Cert Web Services
SuppressDefaults = FALSE
```

29

CERTREQ .INF file sample (continues …)

```
[RequestAttributes]
CertificateTemplate =
"GOPASManualRSATLSServerCompatiblenoApproval"
SAN = "DNS=*.gopas.cz&DNS=*.sevecek.com"

[Strings]
OID_EXT_BASIC_CONSTRAINTS = "2.5.29.19"
OID_EXT_NAME_CONSTRAINTS = "2.5.29.30"
OID_EXT_AUTHORITY_INFORMATION_ACCESS = "1.3.6.1.5.5.7.1.1"
OID_EXT_SUBJECT_ALTERNATIVE_NAME = "2.5.29.17"
OID_EXT_SMIME_CAPABILITIES = "1.2.840.113549.1.9.15"
OID_EXT_CERTIFICATE_POLICIES = "2.5.29.32"
OID_EXT_CRL_DISTRIBUTION_POINTS = "2.5.29.31"
OID_EXT_AP_APPLICATION_POLICIES = "1.3.6.1.4.1.311.21.10"
OID_EXT_ENHANCED_KEY_USAGE = "2.5.29.37"
OID_EXT_KEY_USAGE = "2.5.29.15"
OID_EKU_IPSEC_IKE_INTERMEDIATE = "1.3.6.1.5.5.8.2.2"
OID_EKU_CERTIFICATE_REQUEST_AGENT = "1.3.6.1.4.1.311.20.2.1"
OID_EKU_SERVER_AUTHENTICATION = "1.3.6.1.5.5.7.3.1"
OID_EKU_REMOTE_DESKTOP_AUTHENTICATION = "1.3.6.1.4.1.311.54.1.2"
```

30

CERTREQ .INF file sample (... continued)

```
OID_EKU_ENCRYPTING_FILE_SYSTEM = "1.3.6.1.4.1.311.10.3.4"
OID_EKU_CLIENT_AUTHENTICATION = "1.3.6.1.5.5.7.3.2"
OID_EKU_CODE_SIGNING = "1.3.6.1.5.5.7.3.3"
OID_EKU_SMART_CARD_LOGON = "1.3.6.1.4.1.311.20.2.2"
OID_EKU_DOCUMENT_SIGNING = "1.3.6.1.4.1.311.10.3.12"
KEY_SPEC_AT_KEYEXCHANGE = "1"
KEY_SPEC_AT_NONE = "0"
KEY_SPEC_SIGNATURE = "2"
CERT_KEY_USAGE_ENCIPHER_ONLY = "1"
CERT_KEY_USAGE_NON_REPUDIATION = "64"
CERT_KEY_USAGE_KEY_CERT_SIGN = "4"
CERT_KEY_USAGE_DATA_ENCIPHERMENT = "16"
CERT_KEY_USAGE_DIGITAL_SIGNATURE = "128"
CERT_KEY_USAGE_DECIPHER_ONLY = "32768"
CERT_KEY_USAGE_CRL_SIGN = "2"
CERT_KEY_USAGE_OFFLINE_CRL_SIGN = "2"
CERT_KEY_USAGE_KEY_ENCIPHERMENT = "32"
CERT_KEY_USAGE_KEY_AGREEMENT = "8"

[EnhancedKeyUsageExtension]
OID = %OID_EKU_SERVER_AUTHENTICATION%
```


Deprecated: Web Enrollment pages

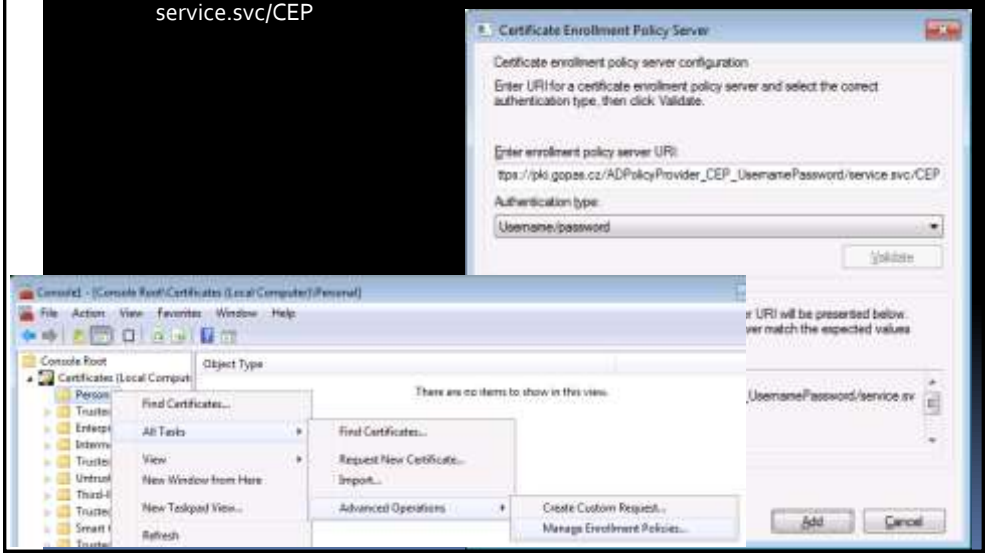
- schema version 1/2 (2000/2003)
- no CNG/KSP
- request signature SHA-1 or MD5 only

- create request wizard
  - IE must allow Unsafe ActiveX
    - Local Intranet zone ONLY
    - IE Enhanced Security Configuration DISABLED
    - ActiveX enabled
  - private key goes into user's profile
    - => must be exportable (or Mimikatz)

- Attributes
  - SAN:DNS=*.gopas.cz&DNS=gopas.cz&DNS=*.gopas.virtual&UPN=kamil@gopas.virtual&Email=ondrej@sevecek.com

Certificate Enrollment Web Services

- https://pki.gopas.cz/ADPolicyProvider_CEP_UsernamePassword/service.svc/CEP



33

CEP and CES bug

- template compatibility must be
  - CA 2012 R2 maximum
- fails to display templates requiring CA 2016+

34

NDES and SCEP

- Simple Certificate Enrollment Protocol
  - HTTP POST
- Network Device Enrollment Service

- https://pki.gopas.cz/certsrv/mscep_admin
- https://pki.gopas.cz/certsrv/mscep

- debug logging:
  - certutil -setreg Enroll\Debug 0xfffffffe3
  - C:\Users\appPoolAccount\mscep.log

NDES and SCEP bug

- must be Windows Authentication in order for CERTREQ to work

- move the ExtensionlessUrlHandler module bellow Static File module

SCEP notes

- https://pki.gopas.cz/certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=default
  - returns .P7B (PKCS#7) envelope with CA and both RA certificates

37

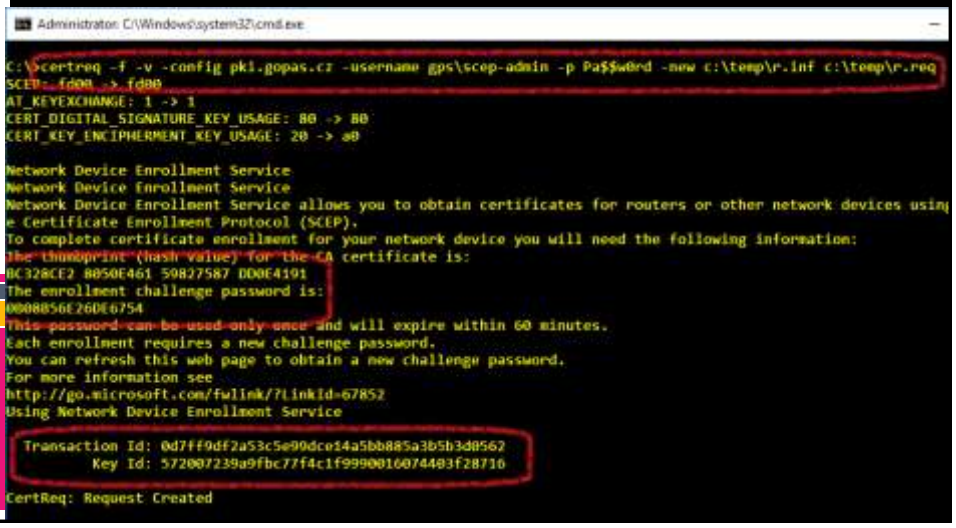
CERTREQ and SCEP .INF

```
[NewRequest]
RequestType = SCEP
Subject = "CN=*.gopas.cz"
Exportable = true
MachineKeySet = true
HashAlgorithm = SHA1
KeyAlgorithm = RSA
KeyLength = 2048
KeySpec = AT_KEYEXCHANGE
KeyUsage = "CERT_DIGITAL_SIGNATURE_KEY_USAGE |
CERT_KEY_ENCIPHERMENT_KEY_USAGE"
SuppressDefaults = true
ProviderName = "Microsoft Enhanced RSA and AES
Cryptographic Provider"
```

38

CERTREQ and SCEP -new goes into /mscep_admin
Request encrypted with RA Encryption

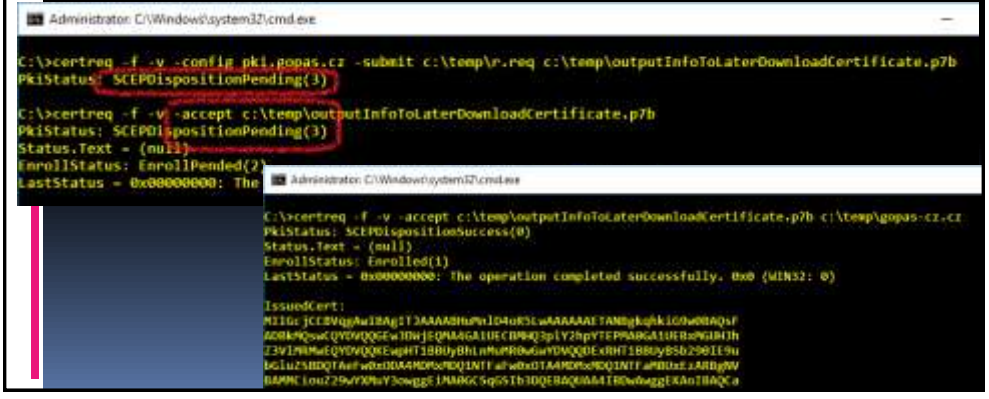
```
certreq -f -v -config pki.gopas.cz -username gps\srv-admin -p
Pa$$w0rd -new c:\temp\r.inf c:\temp\r.req
```



CERTREQ and SCEP -submit and -accept go into /mscep anonymously

```
certreq -f -v -config pki.gopas.cz -submit c:\temp\r.req
c:\temp\outputInfoToLaterDownloadCertificate.p7b

certreq -f -v -accept
c:\temp\outputInfoToLaterDownloadCertificate.p7b
```



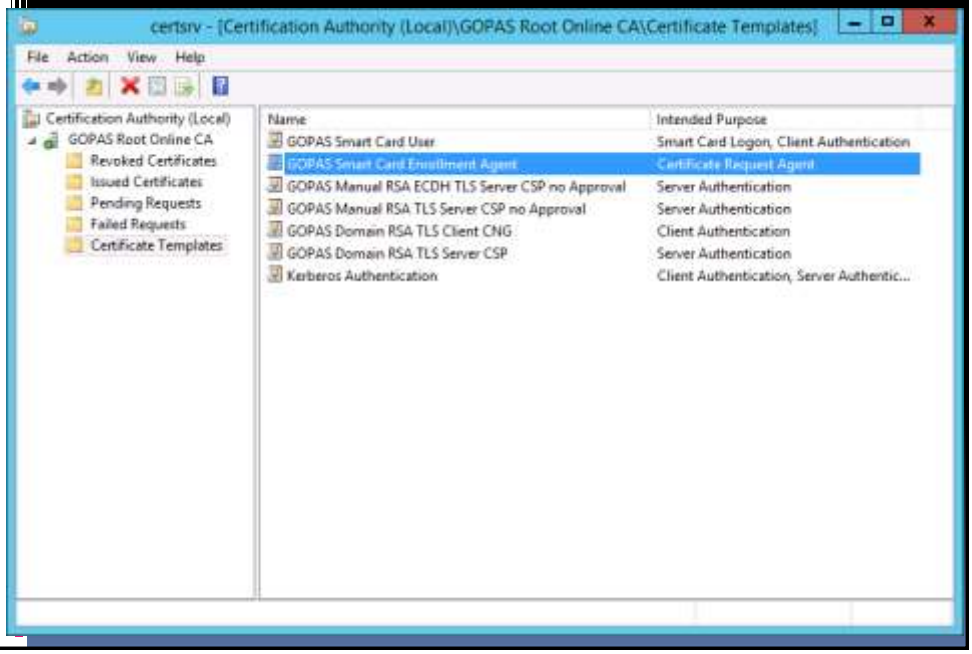
Enterprise PKI

ENROLLMENT AGENTS AKA REGISTRATION AUTHORITIES

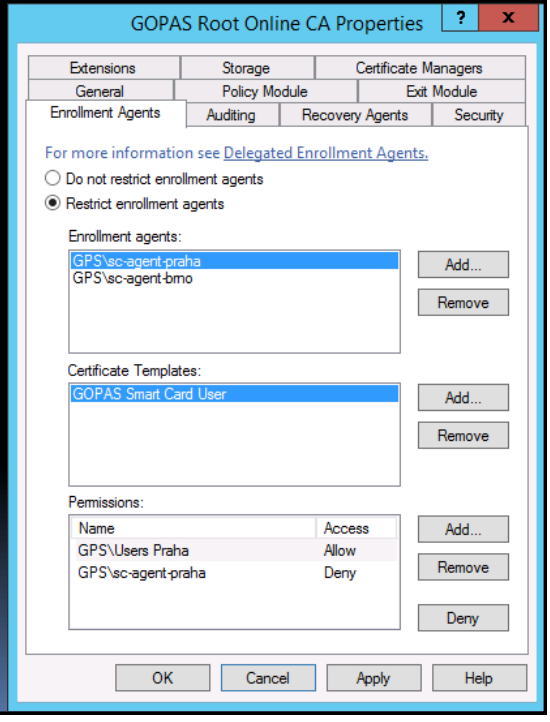
Enrollment agent = registration authority

- Request validation at the requester side instead of at the CA authority
  - user smart card certificate (HR, manager, …)
  - computer certificates (support, CISO, …)
- Limits certificate manager role
  - limit access to CA console
- Store RA certificate on smart card

Enable the two certificate templates in CA



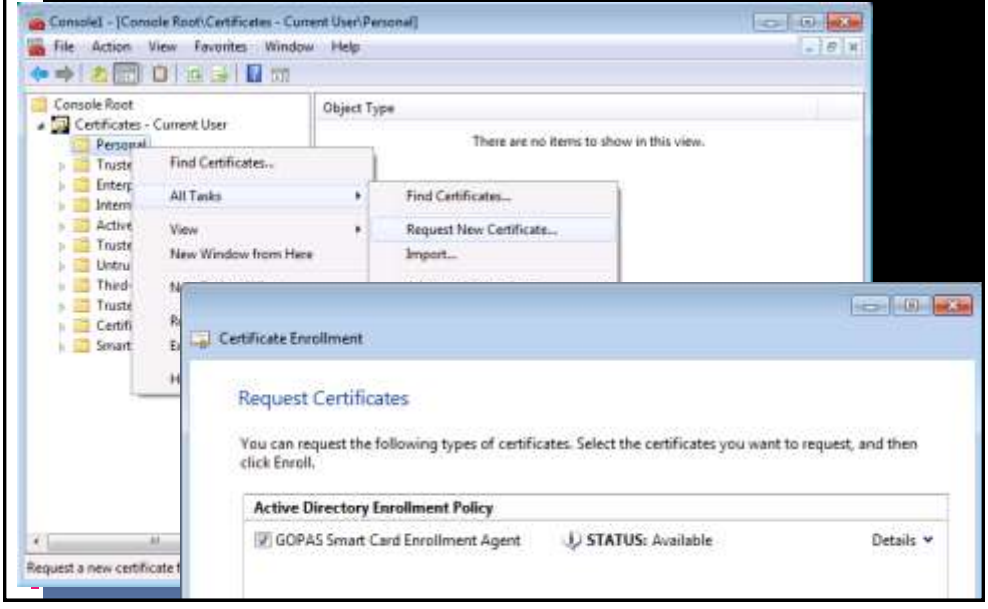
Limit the Enrollment Agents' (Registration Authorities) target end-users and/or groups



Log RA on a client computer

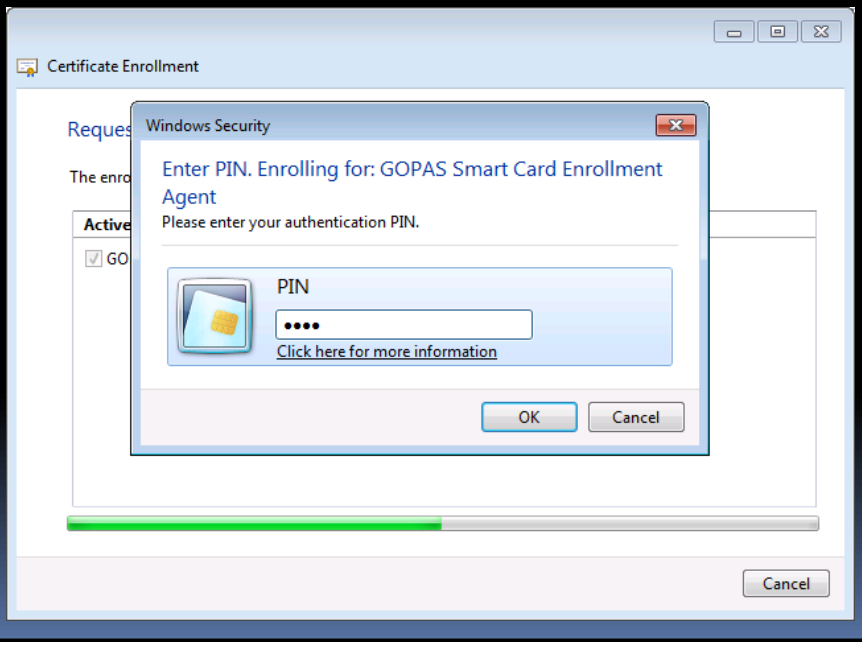
45

Request new RA (Enrollment Agent) certificate



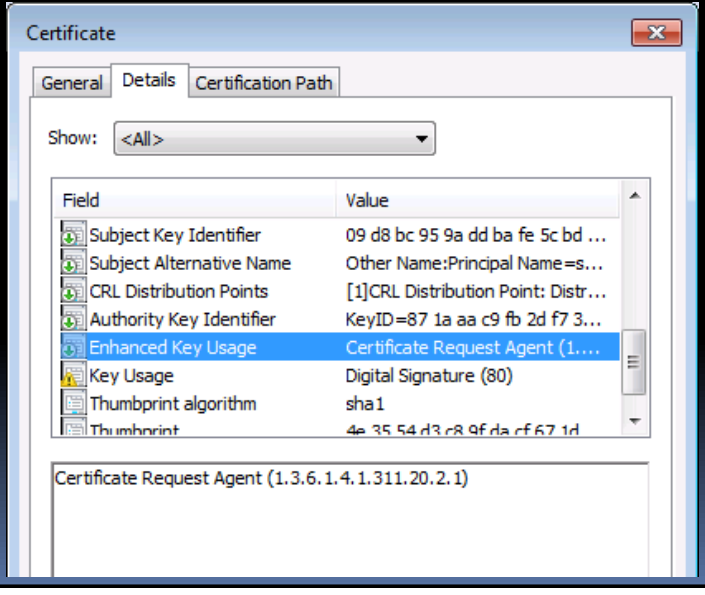
46

Enter PIN for the RA smart card



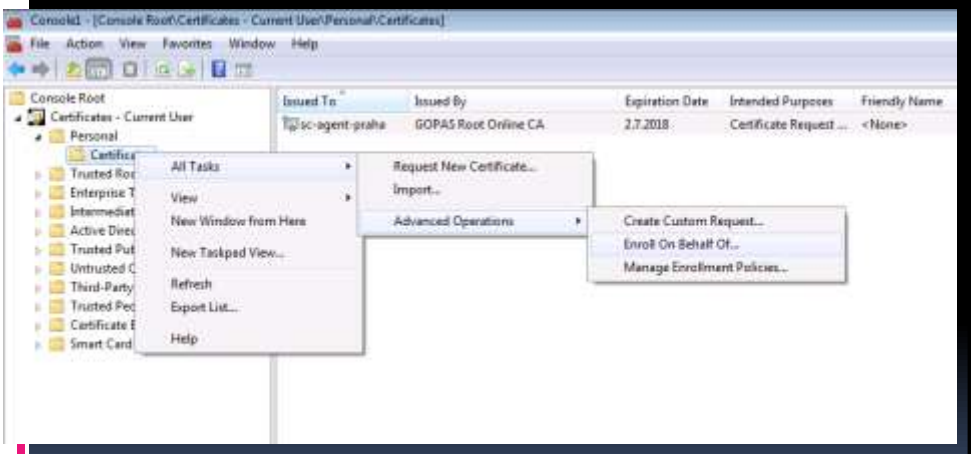
47

Verify EKU of the RA certificate (Certificate Request Agent)

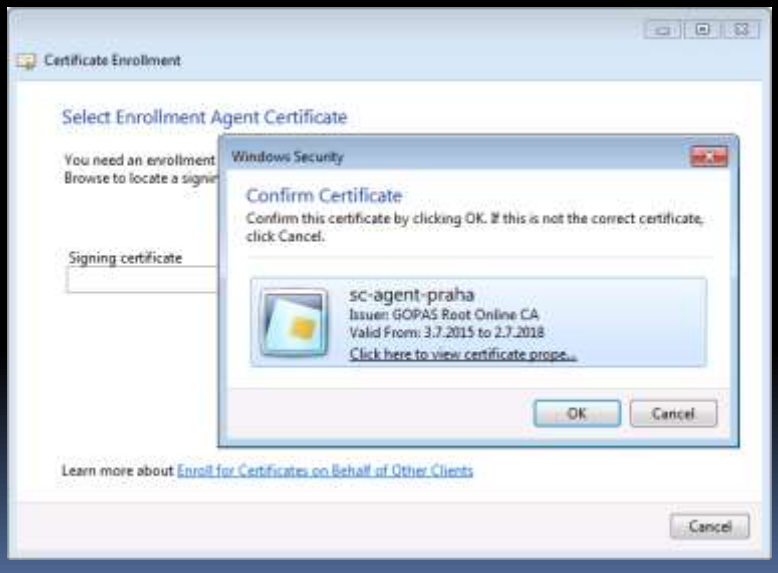


48

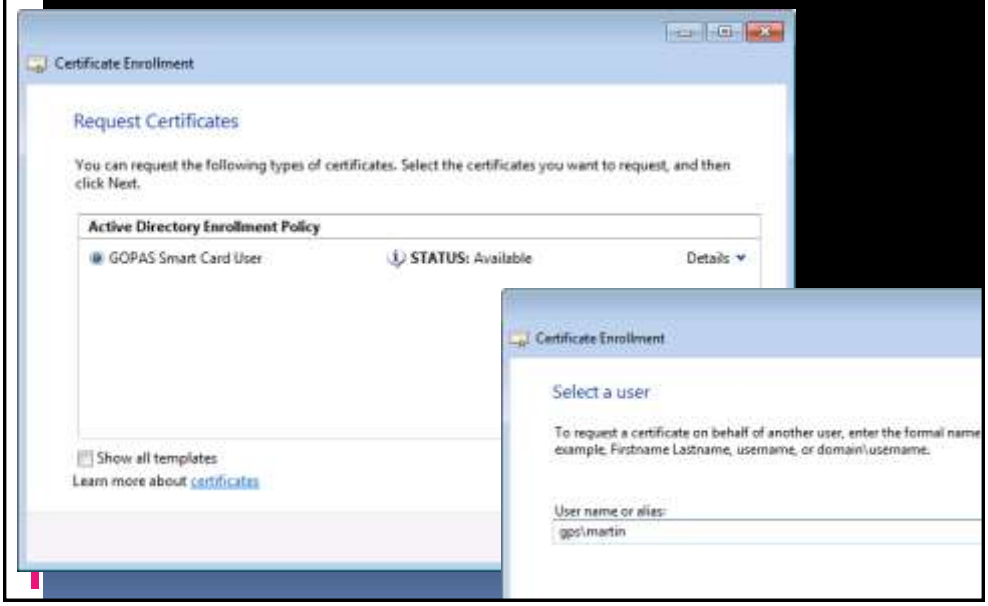
Once we have RA certificate, we can Enroll on Behalf of other users



Select the RA signing certificate which will sign the user's request



Select the template for the end-user certificate and his/her AD login



51

Specify which card the end-user certificate should be enrolled into and let the end-user to provide PIN

52

Enterprise PKI

OTHER CERTIFICATE APPLICATIONS AND NOTES

Key usages

- AT_SIGNATURE
  - used only to sign a message
- AT_KEYEXCHANGE
  - used both to sign a message or export encrypted session key
  - session key can be generated by a smart card (more secure than AT_SIGNATURE which means that the session key must be generated in software)
- Example
  - Windows 7 can use AT_SIGNATURE for S/C logon

CA certificate

Extension	Value	Notes
Subject	CN=GOPAS Root CA OU=Brno Employees O=GOPAS a.s. L=Brno S=Czechia C=CZ	on RootCA the same as Issuer
Exporatable Key	yes in software CSP yes/no in hardware CSP	
Key Type	Signature	
Key Usage	Digital Signature (might be removed) Certificate Signing CRL Signing Offline CRL Signing	might not be present, use CAPOLICY for RootCA and SubCA template
CSP	CNG on Windows 2008+ CSP on Windows 2003-	RSA, DSA (CSP only), ECDSA RSA, DSA
Publish in AD	Certification Authorities Enrollment Services NTAuth Store	AIA if required

CA certificate

Extension	Value	Notes
Basic Constraints	CA Path Length	 x = number of CAs in the chain
Name Constraints	*.praha.gopas.local *@gopas.cz	must be understood by clients
Validity	on RootCA unlimited 5, 6, ...	cannot be revoked anyway cannot issue certificates with longer validity than is its own
Exporatable Key	yes in software CSP yes/no in hardware CSP	
Key Type	Signature	
Key Usage	Digital Signature (might be removed) Certificate Signing CRL Signing Offline CRL Signing	might not be present, use CAPOLICY for RootCA and SubCA template

CA certificate

Extension	Value
Validity	unlimited – RootCA cannot be revoked 5 years – SubCA cannot issue longer certificates than is its own validity
Exporatable Key	yes in software CSP yes/no in hardware CSP
Key Type	Signature
Key Usage	Digital Signature (might be removed) Certificate Signing CRL Signing Offline CRL Signing

57

DC certificate

Template	Issued Certificates	Availability and Enrollment
Domain Controller v1	Subject = dc1.idtt.local SAN = GUID&dns=dc1.idtt.local EKU = client / server	Windows 2000 CA Windows 2000+ DCs manually
Domain Controller Authentictaion v2	Subject = SAN = dns=dc1.idtt.local EKU = client / server / sc	Windows 2003 CA Windows 2003+ DCs autoenrollment
Kerberos Authentication v2	Subject = SAN = dns=idtt.local&dns=IDTT EKU = client / server / sc / kdc	Windows 2008 CA Windows 2003+ DCs autoenrollment
	can be duplicated	Encryption Key Encipherment RSA and AES CSP on Windows 2008+ RSA Schannel on Windows 2003

58

58

DC certificate

- Issuing CA certificate must be in NTAuth store

59

TLS Server with RSA

Extension	Value
Subject	DNS
SAN	DNS
Exporatable Key	no if enrolling from an internal CA yes if enrolling from a public CA and will copy the certificate (NLB, reverse proxies)
Archive Key	no, transport encryption only
Key Type	Encryption = RSA key exchange Signature = EC/DH key agreement Enable-ExchnageCertificate requires Signature + Encryption SQL configuration manager requires at least Encryption to display the certificate
Key Usage	Key Encipherment LDAPS, Enable-ExchnageCertificate needs Digital Signature as well
CSP/CNG	all Strong, Enhanced, RSA Schannel, AES providers support TLS 1.2 with SHA256 on Windows 2008 IIS can use Microsoft Software Key Storage Provider on Windows 2008 only RSA Schannel on Windows 2003
EKU	Server Authentication 1.3.6.1.5.5.7.3.1
Autoenrollment	no renewall yes? – must replace in the service anyway
Publish in AD	no

60

TLS Server with (EC)DSA

Extension	Value
Subject	DNS
SAN	DNS
Exporatable Key	yes?
Archive Key	no, transport encryption only
Key Type	Signature = ECDH key agreement
Key Usage	Digital Signature
CSP/CNG	Microsoft DH SChannel Cryptographic Provider Microsoft Software Key Storage Provider
EKU	Server Authentication 1.3.6.1.5.5.7.3.1
Autoenrollment	no renewall yes? – must replace in the service anyway
Publish in AD	no

61

Remote desktop authentication

Extension	Value
Subject	DNS
SAN	DNS or manual if necessary for aliases
Exporatable Key	no
Archive Key	no, transport encryption only
Key Type	Encryption = RSA key encipherment (TLS 1.0 only on 2008 R2) Signature = ECDH key agreement with 8/2012 TLS 1.1+
Key Usage	Key Encipherment = RSA key encipherment Digital Signature = EC/DH key agreement
CSP	Microsoft RSA SChannel Cryptographic Provider for 2003 since Vista/2008 can use CNG
EKU	Remote Desktop Authentication 1.3.6.1.4.1.311.54.1.2
Autoenrollment	no GPO defines server authentication template managed automatically by Remote Desktop Configuration service
Publish in AD	no
Renewal	0 days (Remote Desktop Configuration takes care of it itself)
Applies to	Windows 2008/Vista+ RDP servers

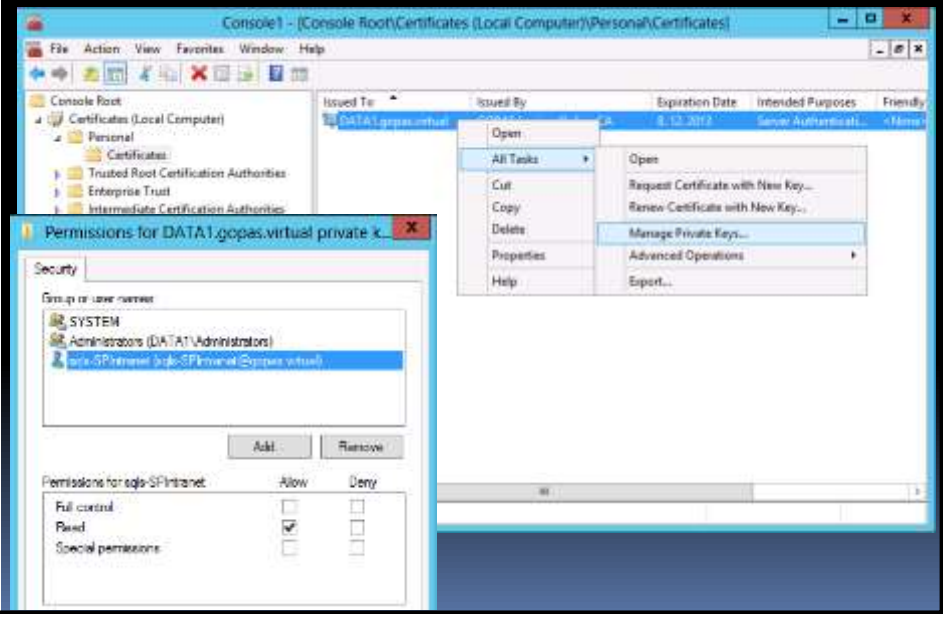
62

SQL TLS Server with RSA

Extension	Value
Subject	DNS or cluster's FQDN
SAN	DNS or cluster's FQDN
Exporatable Key	no
Archive Key	no, transport encryption only
Key Type	Encryption
Key Usage	Key Encipherment
CSP/CNG	Any CSP SQL Server 2012- does not support CNG
EKU	Server Authentication 1.3.6.1.5.5.7.3.1
Autoenrollment	SQL server picks a certificate automatically if one is found private key security must allow SQL server's service account READ or the certificate must be in the instance's own store If you need to enforce encryption on the server side, you must select the certificate (thumbprint) manually
Publish in AD	no

63

SQL TLS Server with RSA



64

IPSec transport with IKEv1

Extension	Value
Subject	not mandatory
SAN	DNS (checks against what the other side claims as its Peer ID)
Exporatable Key	no
Archive Key	no, transport authentication/encryption only
Key Type	Signature
Key Usage	Digital Signature
CSP	Microsoft Enhanced RSA and AES Provider
EKU	a) IPSec IKE Intermediate (IPSec Protection) 1.3.6.1.5.5.8.2.2 + Server Authentication + Client Authentication b) IPSec IKE Intermediate c) Client Authentication
Autoenrollment	yes
Publish in AD	no

65

IPSec transport with AuthIP(TLS)

Extension	Value
Subject	not mandatory if SAN present
SAN	DNS (checks against what the other side claims as its Peer ID)
Exporatable Key	no
Archive Key	no, transport authentication/encryption only
Key Type	Signature and Encryption (on Responder) Signature (on Initiator)
Key Usage	Digital Signature, Key Encipherment (on Responder) Digital Signature (on Initiator)
CSP	Microsoft Enhanced RSA and AES Provider
EKU	on both Initiator and Responder: a) IPSec IKE Intermediate (IPSec Protection) 1.3.6.1.5.5.8.2.2 + Server Authentication + **Client Authentication** b) IPSec IKE Intermediate + **Client Authentication** **c) Client Authentication**
Autoenrollment	yes
Publish in AD	no

Disable AuthIP: HKLM\System\CCS\Services\IKEEXT\Parameters
IKEFlags = DWORD = + 0x40

66

Domain TLS User with RSA

Extension	Value
Subject	Common Name or Distinguished Name
SAN	UPN
Exporatable Key	no?
Archive Key	no, transport encryption only
Key Type	Signature
Key Usage	Digital Signature
CSP	all Base, Enhanced, AES providers IE can use CNG since Vista/2008 VPN EAP-TLS client can use CNG since Windows 8/2012
EKU	Client Authentication 1.3.6.1.5.5.7.3.2
Autoenrollment	yes
Publish in AD	no

67

Domain SC User with RSA

Extension	Value
Subject	Common Name or Distinguished Name
SAN	UPN or AD mapped subject (Windows 6.0+)
Exporatable Key	no?
Archive Key	no, transport encryption only
Key Type	Signature (AllowSignatureOnlyKeys GPO on Windows 6.0+) Encryption (required on 2000+, more secure)
Key Usage	Digital Signature
CSP	Smart Card compatible provider
EKU	Smart Card Logon 1.3.6.1.4.1.311.20.2.2 can be empty on Windows 6.0+, but if present, must contain Smart Card Logon EKU
Autoenrollment	no?
Publish in AD	no

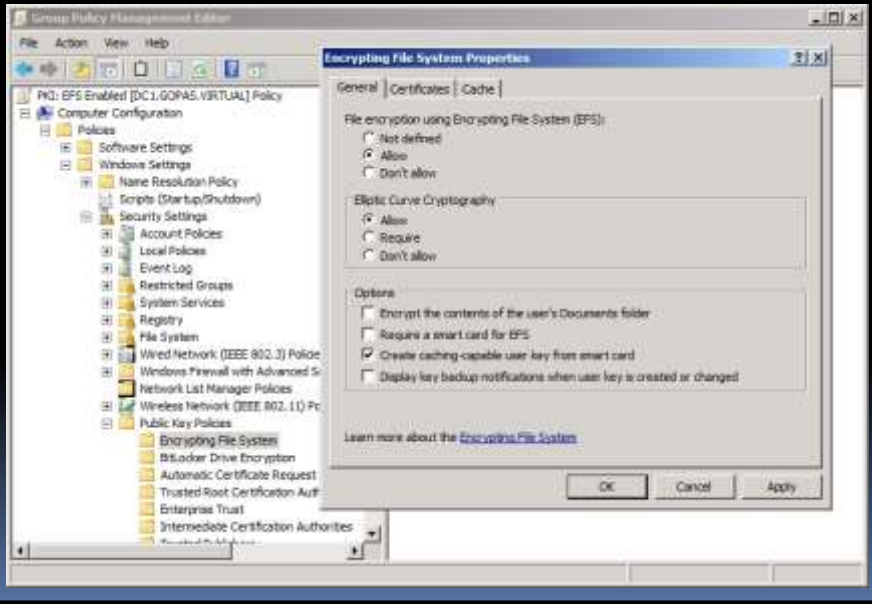
68

Domain EFS User with RSA

Extension	Value
Subject	Common Name or Distinguished Name
SAN	UPN
Exporatable Key	no?
Archive Key	yes
Key Type	Encryption
Key Usage	Key Encipherment
CSP	Microsoft Enhanced Cryptographic Provider v1.0 (does not work with Enhanced RSA and AES CSP) can use CNG on Windows 7/2008 R2 and newer
EKU	Encrypting File System 1.3.6.1.4.1.311.10.3.4
Autoenrollment	no
Publish in AD	yes

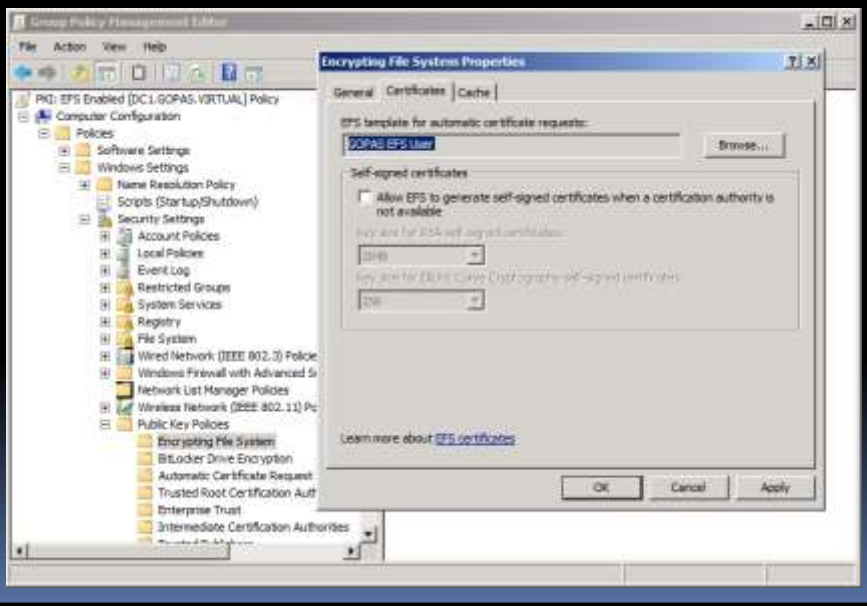
69

Enabling EFS



70

Enabling EFS



71

Cisco AnyConnect Server

Extension	Value
Subject	DNS Unstructured Name = 1.2.840.113549.1.9.2 = DNS Unstructured Address = 1.2.840.113549.1.9.8 = IP
SAN	not mandatory, DNS if present
Exporatable Key	yes or SCEP
Archive Key	no, transport encryption only
Key Type	Signature, Encryption
Key Usage	Digital Signature, Key Encipherment
CSP	any
EKU	Server Authentication Client Authentication
Autoenrollment	no
Publish in AD	no

Note: client uses normal Windows Trusted Root CAs to validate the server certificate

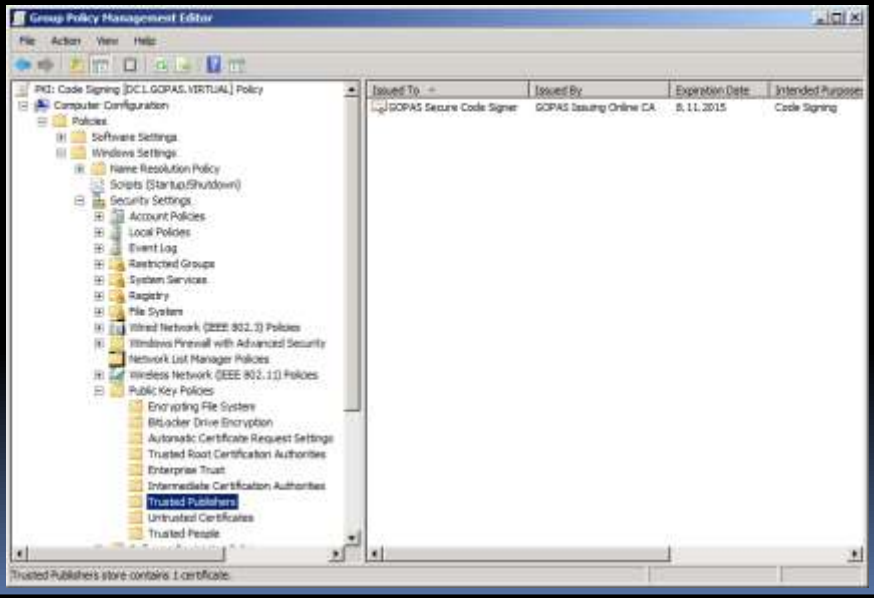
72

Code Signing

Extension	Value
Subject	supply in the request?
SAN	supply in the request?
Exporatable Key	no?
Archive Key	no, signature only
Key Type	Signature
Key Usage	Digital Signature
CSP	any
EKU	Code Signing 1.3.6.1.5.5.7.3.2
Autoenrollment	no
Publish in AD	no
Additional trust	Trusted Publishers store

73

Code Signing



74

CA Exchange

- Generated automatically even if no template defined (not even just in directory)
- Subject – IDTT Root CA-Xchng
  - to distinguish it from CA's certificate
- Valid for a week
- EKU – Private Key Archival

Certificate mapping with user TLS and Smart Card PKINIT certificates

- altSecurityIdentities
- all reverted

- Subject and Issuer fields
  - X509:<I>DC=virtual,DC=gopas,CN=GOPAS Root CA<S>CN=kamil
- Subject DN
  - X509:<S>CN=kamil
- Subject Key Identifier
  - X509:<SKI>ddde2ca4b86db8a908b95c6cbcc8bb1ac7a09a41
- Issuer, and Serial Number
  - X509:<I>DC=gopas,DC=virtual,CN=GOPAS Root CA<SR>320000000000003bde810
- SHA1 Hash
  - X509:<SHA1-PUKEY>ed913fa41377dbfb8eac2bc6fcae71ecd4a974fd
- RFC822 name
  - X509:<RFC822>kamil@gopas.cz

BitLocker

- BitLocker
  - 1.3.6.1.4.1.311.67.1.1
- BitLocker Recovery
  - 1.3.6.1.4.1.311.67.1.2

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

THANK YOU!