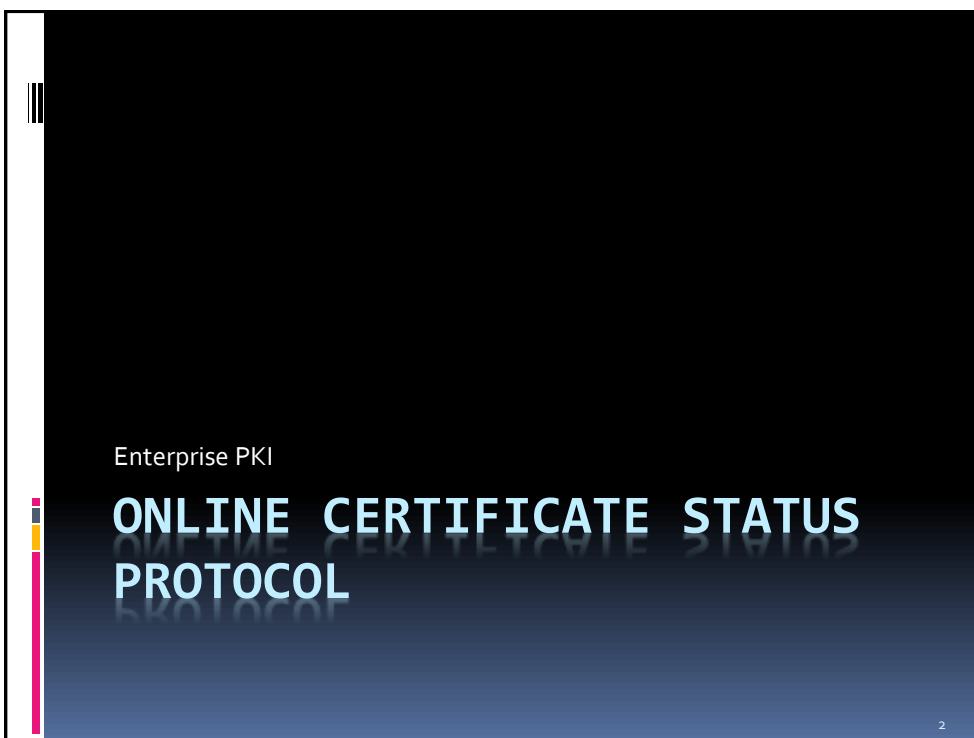


Ondřej Ševeček | PM Windows Server | GOPAS a.s. |  
MCM: Directory Services | MVP: Enterprise Security |  
ondrej@sevecek.com | www.sevecek.com |

# KEY ARCHIVAL, OCSP

Slide 1 features a dark blue gradient background with a vertical white bar on the left containing a barcode and a small colored bar. The text is centered and has a reflection effect.

1



Enterprise PKI

# ONLINE CERTIFICATE STATUS PROTOCOL

Slide 2 features a dark blue gradient background with a vertical white bar on the left containing a barcode and a small colored bar. The text is centered and has a reflection effect.

2

## OCSP vs. CRL scenario (big public CA)

- Verisign CRL
  - 900 kB
  - 10 days expiration
  - ~ 500 000 000 clients?
  - = 4 Gbps constant traffic
- Verisign OCSP
  - 1450 B OCSP response
  - 10 days expiration based on CRL
  - ~ 500 000 000 clients?
  - 5 servers touched by each client
  - =  $900 \text{ kB} / (1450 \text{ B} * 5) = 124 \times$  better = 36 Mbps

3

## OCSP vs. CRL scenario (private CA)

- Private CRL
  - 900 kB
  - 10 days expiration
  - ~ 50 000 clients?
  - = 4 Mbps constant traffic
- Private OCSP
  - 1450 B OCSP response
  - 10 days expiration based on CRL
  - ~ 50 000 clients?
  - 50 services touched by each client
  - mutual certificate validation
  - =  $900 \text{ kB} / (2 * 50 * 1450 \text{ B}) = 6 \times$  better = 650 Kbps

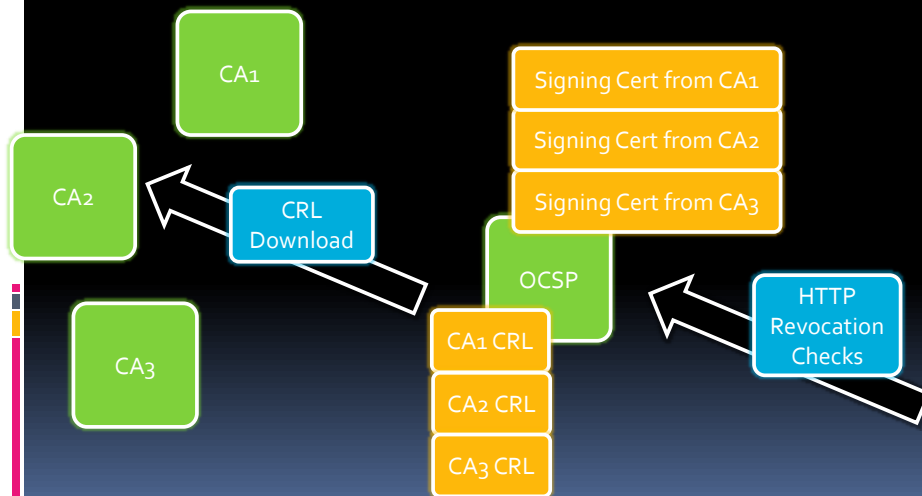
4

## OCSP preference count

- CryptnetCachedOcspswitchToCrlCount
- HKLM\Software\Policies\Microsoft\SystemCertificates\ChainEngine\Config

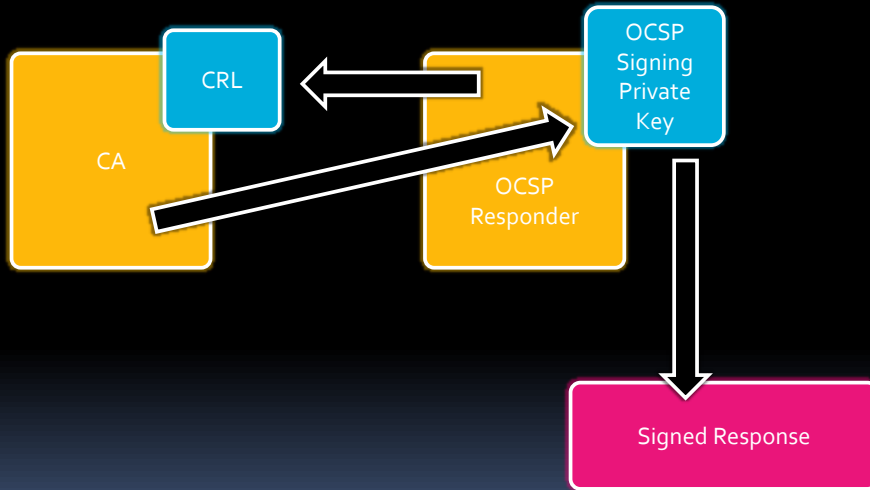
5

## OCSP Responder Certificates and CRLs



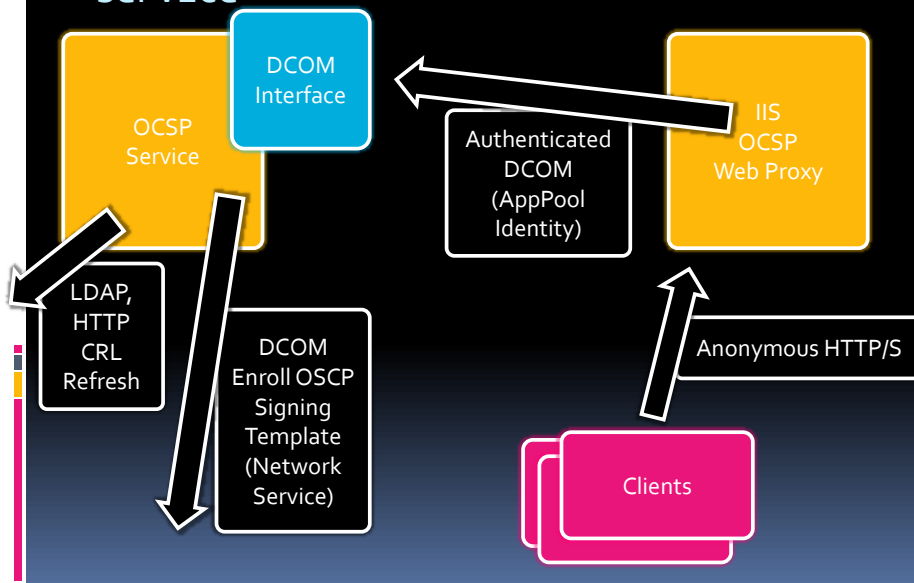
6

# OCSP Response Signing

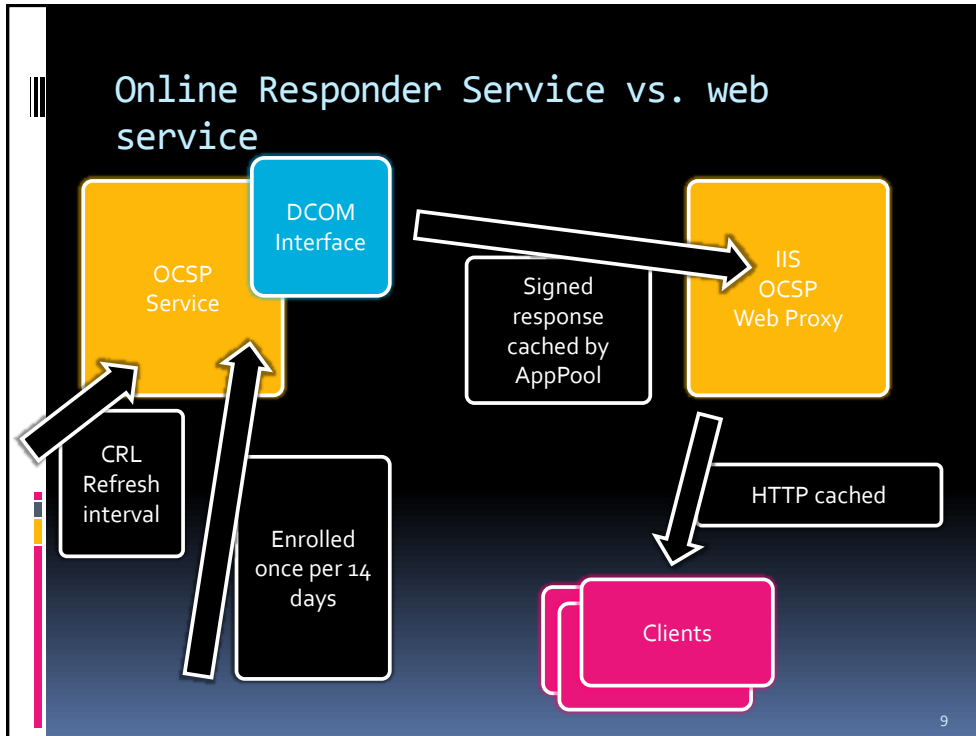


7

# Online Responder Service vs. web service



8



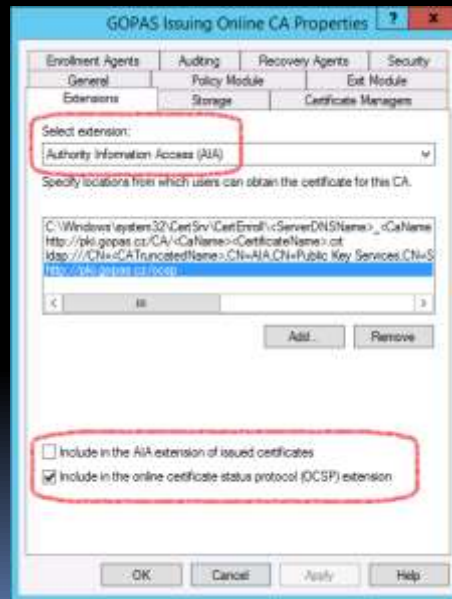
9

## OCSP client

- Windows **Vista/2008** and newer
- Caches responses in **CryptNetUrlCache** similarly as CRL
  - **CERTUTIL -urlcache OCSP**
- Checks response signature
  - checks revocation status of the signing certificate!
  - if not disabled in the signing certificate by 1.3.6.1.5.5.7.48.1.5

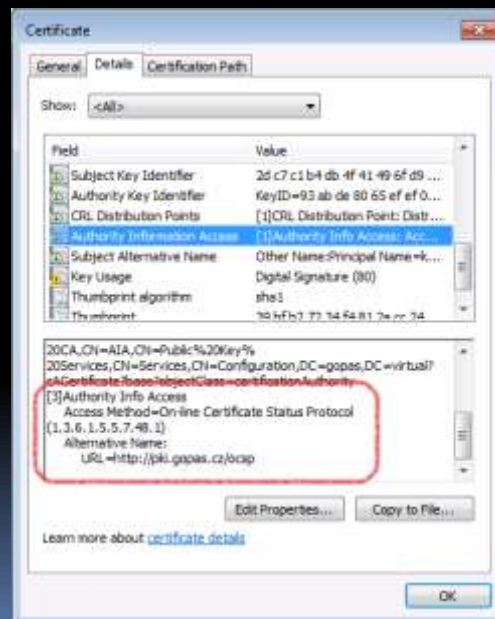
10

## Configuring AIA OSCP path in CA settings



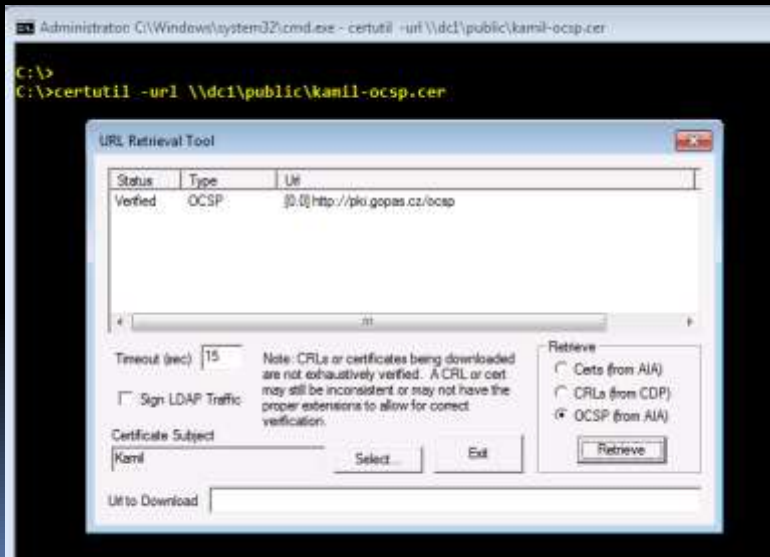
11

## OCSP url included in Authority Information Access (AIA) extension



12

Verify OCSP download  
certutil -urlfetch -verify  
certutil -url



13

## Renewing CA and OCSP

- Older CA certificate if still valid cannot sign OCSP responses
  - certutil -setreg ca\UseDefinedCACertInRequest 1
- Define new revocation config in OCSP

14



15



16

## Key Archival

- Signature keys
  - not necessary
- Online transaction keys
  - not necessary
- Encrypted data
  - necessary?
  - data recovery?

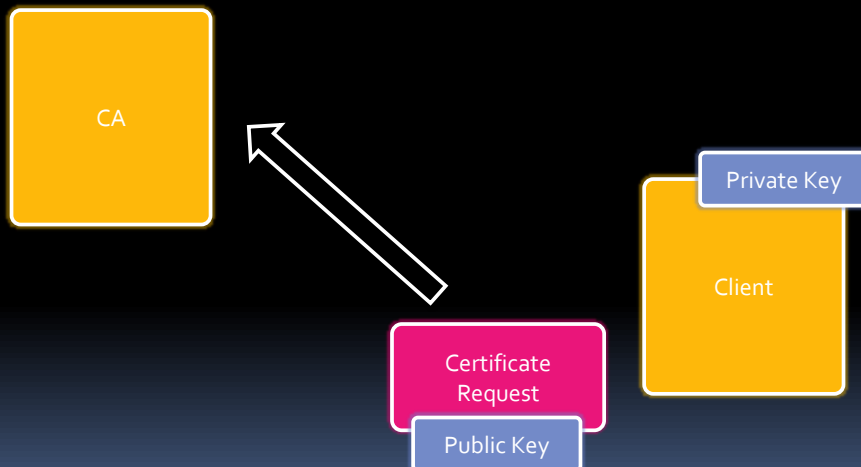


## Key Archival Requirements

- Windows 2003+ CA
- Windows XP/2003+ client
  - online DCOM enrollment
- 3DES encryption by default
- Windows 2008+ supports optional AES encryption with CNG

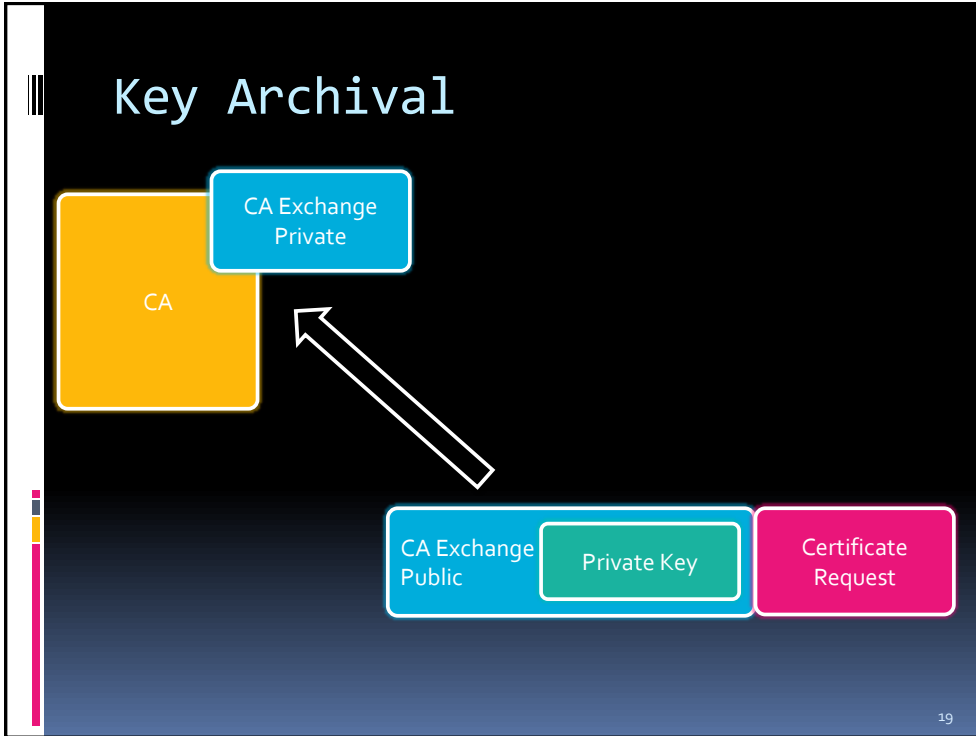
17

## Standard certificate request without private key

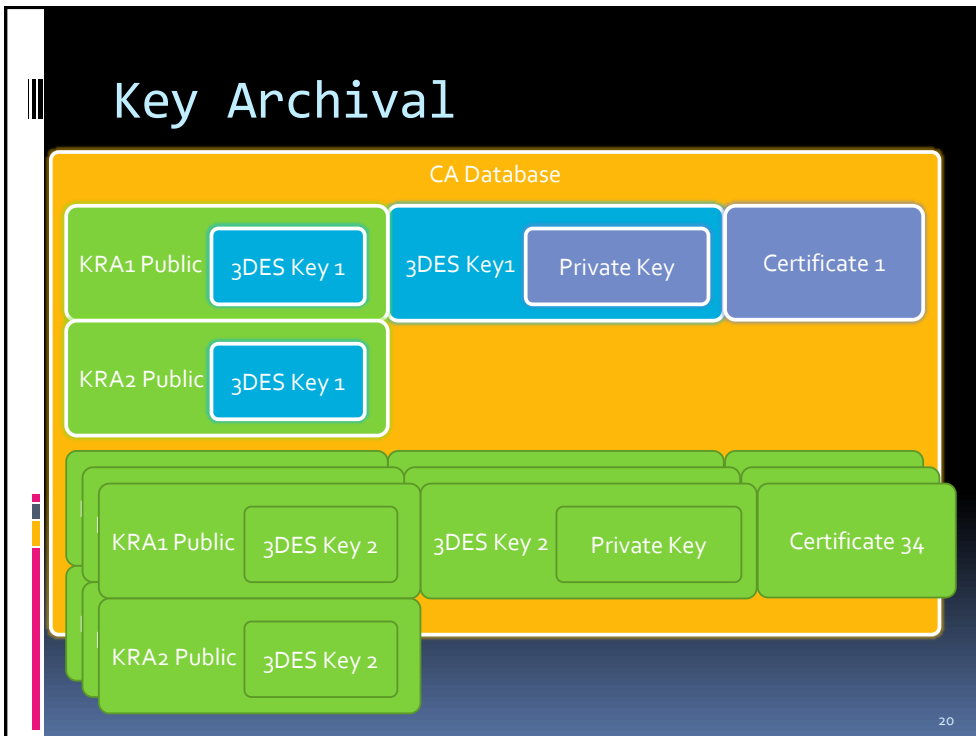


18

18



19



20

## Several KRA keys philosophy

- Randomly selected
  - no one knows what keys he/she will recover
- More simultaneously used
  - one of the people can recover
  - not all-of-them, **just one-of-them** principle
- Smooth preparation for ongoing **KRA expiration**

21

## CAKeyExchange and Suite-B

- CERTUTIL -setreg CA\EncryptionCSP\CNGEncryptionAlgorithm AES
- CERTUTIL -setreg CA\EncryptionCSP\SymmetricKeySize 128
- CERTUTIL -setreg CA\EncryptionCSP\CNGPublicKeyAlorithm ECDH\_P256
- CERTUTIL -setreg CA\EncryptionCSP\KeySize 256

22

## Recovering the keys

- CERTUTIL -getkey
  - to obtain encrypted PKCS7 .BIN from CA
  - do not need RA private key yet
- CERTUTIL -recoverkey
  - requires RA private key
  - produces .PFX from the .BIN PKCS7 file

23

## Recovering the keys -getkey

```
Administrator: C:\Windows\system32\cmd.exe
C:\>
C:\>certutil -getkey 5e00000526c14175c81efca2400000000052 \\dc1\public\zachrama.bin
Recovery blobs retrieved: 1
----- Retrieved, but not Recovered -----

"EMICA.gopas.virtual\GOPAS Issuing Online CA"
Serial Number: 5e00000526c14175c81efca2400000000052
Subject: CN=raon
KeyId: ac07f5739a9dc83f4e0e6e26d488307eb53c7ab
Cert Hash(sha1): 73b0e3efc025d22bcd973a19547f72d7ad72cb
Recovery blob file: \\dc1\public\zachrama.bin
One of the following key Recovery Agent certificates is required to recover the key:
RA cert[0]:
Serial Number: 5e000004cf2a6aed4993d3d640000000004c
Subject: CN=obnovovac-1, OU=People, OO=Company, DC=gopas, DC=virtual
NotBefore: 10. 10. 2014 18:50
NotAfter: 9. 10. 2016 10:50
Template: GP5KeyRecoveryAgent, GPS Key Recovery Agent
Key Id Hash(md5): 30fd475fe6bd5029968042bfff35f3d75
Key Id Hash(sha256): 5120d13fe5d7b22677d988fe732807efca2115fd1bb9450bcc1f78an77f694e7
Cert Hash(sha1): c886a1d973c62a6e8c039560564293c4c1f08f7a
Cert Hash(sha256): 08e5655cf6bb00f2e672b27203791bdf8f07744114fbf946915628e28958ca99
Signature Hash: 2c0ba79a67ca9bbf0f1cb7bf25a0ab309e028986e008065b7379814b7a70779762c14ac723e654b1bb07Fa24735216
RA cert[1]:
Serial Number: 50000004e0389ab374437f5800000000004e
Subject: CN=obnovovac-2, OU=People, OO=Company, DC=gopas, DC=virtual
NotBefore: 10. 10. 2014 18:53
NotAfter: 9. 10. 2016 10:51
Template: GP5KeyRecoveryAgent, GPS Key Recovery Agent
```

24

## RecoverKey into final PFX

```
C:\Windows\system32\cmd.exe
C:\>
C:\>certutil -recoverkey \\dc1\public\chranemy-kas11.bin \\dc1\public\obnoveny-kas11.pfx

Computed Hash: ...
0000 8a 94 24 86 88 95 d5 c5 f0 44 d0 80 bf 9d a7 1c
0010 29 62 c4 ba 64 b9 5f 34 f9 b2 5a 1f 04 83 ad aa

User Certificate:
Serial Number: 1900000034d6806ecc26049c47000000000034
Issuer: CN-GOPAS Online Issuing CA, DC-gopas, DC-virtual
Subject: CN-Kas11
Cert Hash(sha1): F3 33 ea 60 d1 a3 34 b3 62 5c 76 53 71 23 c1 a8 4c 37 75 4d
Enter new password:
Confirm new password:
CertUtil: -RecoverKey command completed successfully.

C:\>
```

25

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

# THANK YOU!

26