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

KEY ARCHIVAL, OCSP

1

Enterprise PKI

ONLINE CERTIFICATE STATUS PROTOCOL

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 kB / (1450 B * 5) = 124 x better = 36 Mbps

OCSP vs. CRL scenario (private CA)

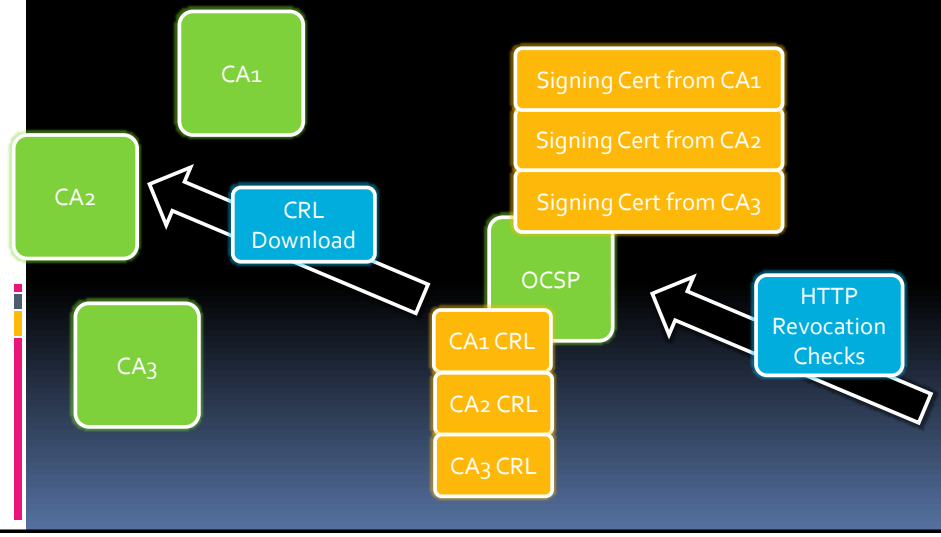
- Private CRL
  - 900 kB
  - 10 days expiration
  - ~ 50 000 clients?
  - = 4 Mbps constant traffic
- Private OCSP
  - 1450 B OCSP response
  - 10 days expiration based on CRL
  - ~ 50 000 clients?
  - 50 services touched by each client
  - mutual certificate validation
  - = 900 kB / (2 * 50 * 1450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

OCSP preference count

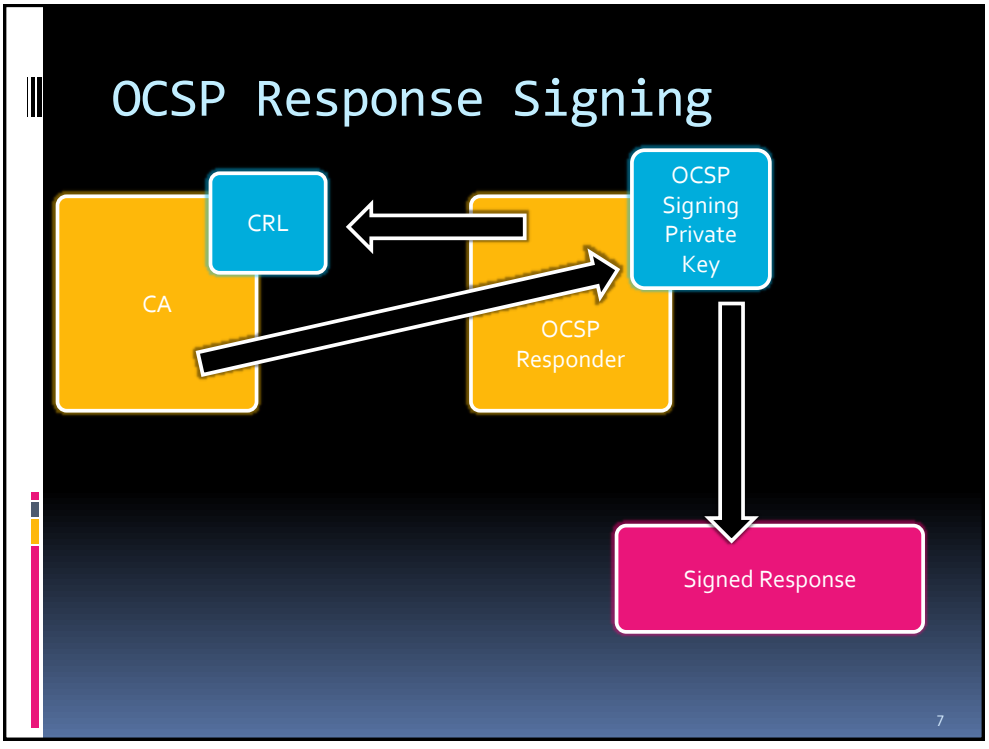
- CryptnetCachedOcspSwitchToCrlCount
- HKLM\Software\Policies\Microsoft\SystemCertificates\ChainEngine\Config

5

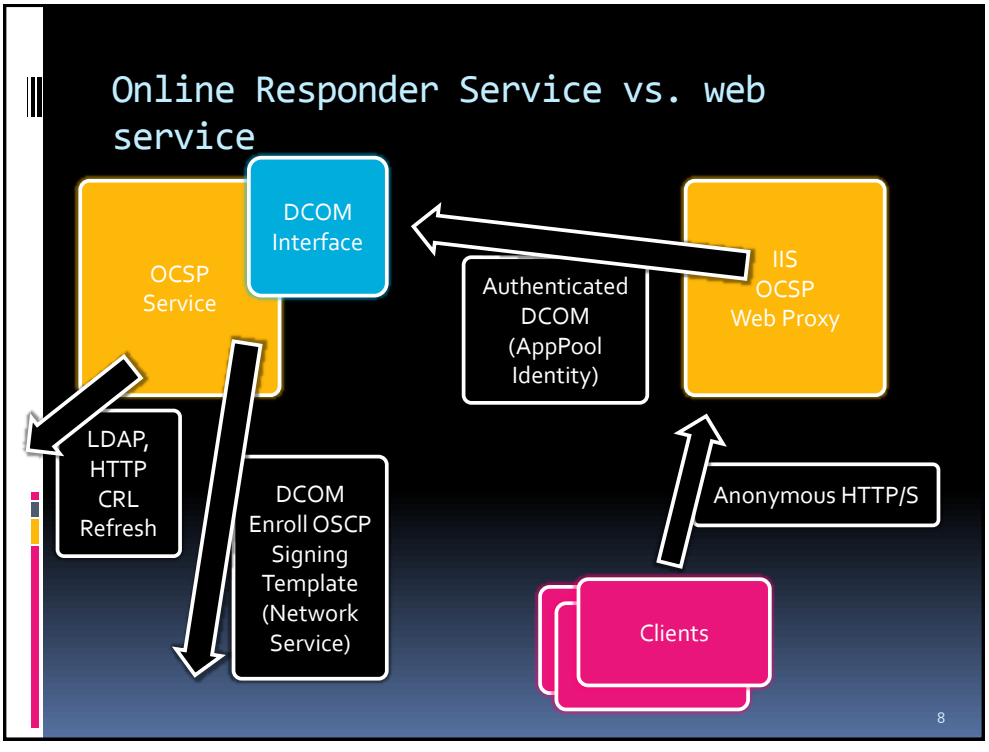
OCSP Responder Certificates and CRLs



6

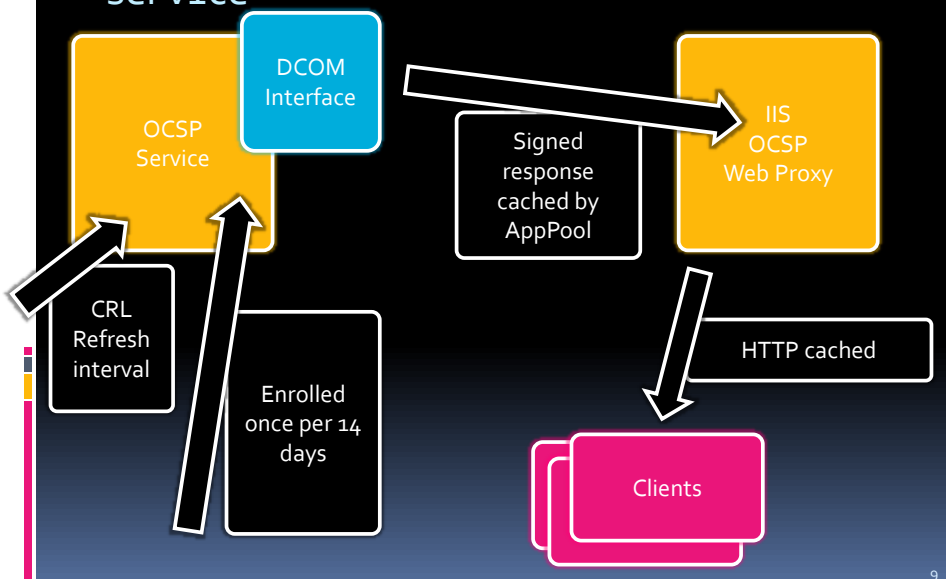

OCSP Response Signing
CRL
CA
OCSP Signing Private Key
OCSP Responder
Signed Response
7

7


Online Responder Service vs. web service
DCOM Interface
OCSP Service
Authenticated DCOM (AppPool Identity)
IIS OCSP Web Proxy
LDAP, HTTP CRL Refresh
DCOM Enroll OSCP Signing Template (Network Service)
Anonymous HTTP/S
Clients
8

8

Online Responder Service vs. web service



9

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

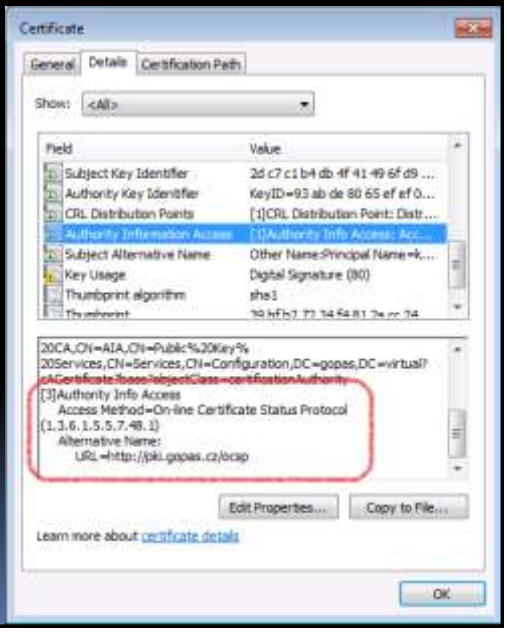
10

10

Configuring AIA OCSP path in CA settings

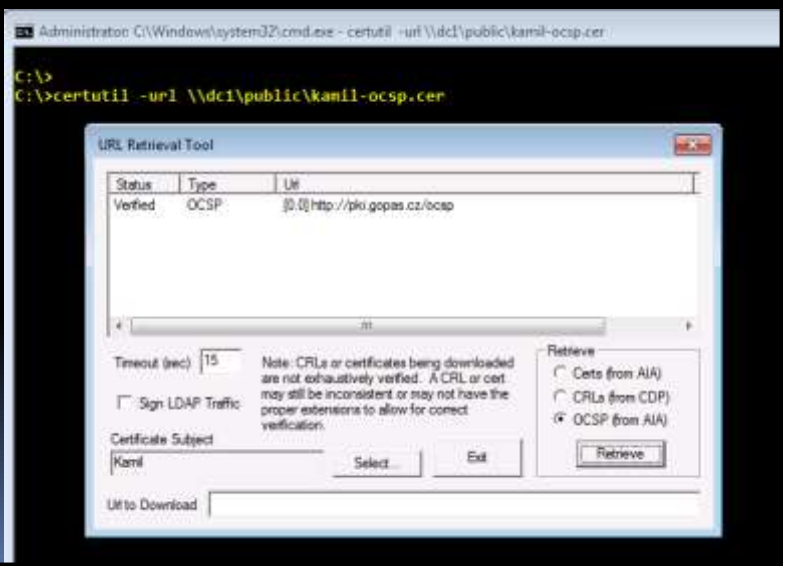
11

OSCP url included in Authority Information Access (AIA) extension



12

Verify OCSP download
certutil –urlfetch –verify
certutil -url



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

Enterprise PKI

KEY ARCHIVAL

Key Archival

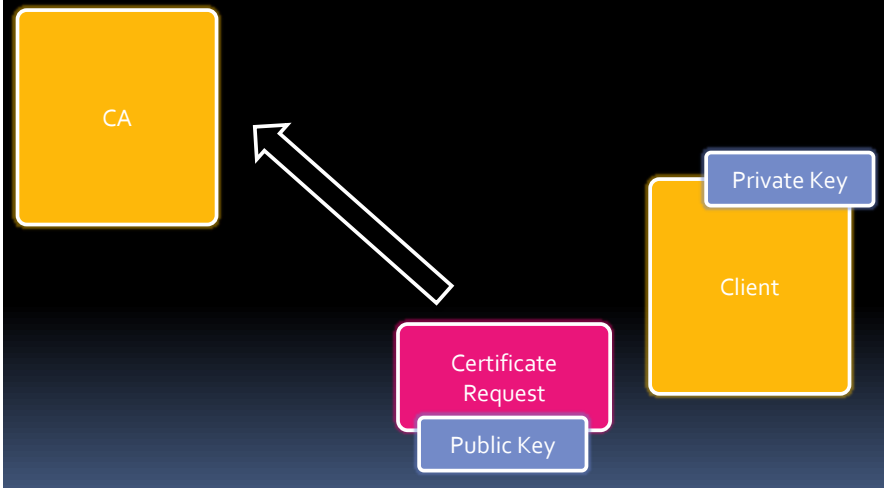
- Signature keys
  - not necessary
- Online transaction keys
  - not necessary
- Encrypted data
  - necessary?
  - data recovery?

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

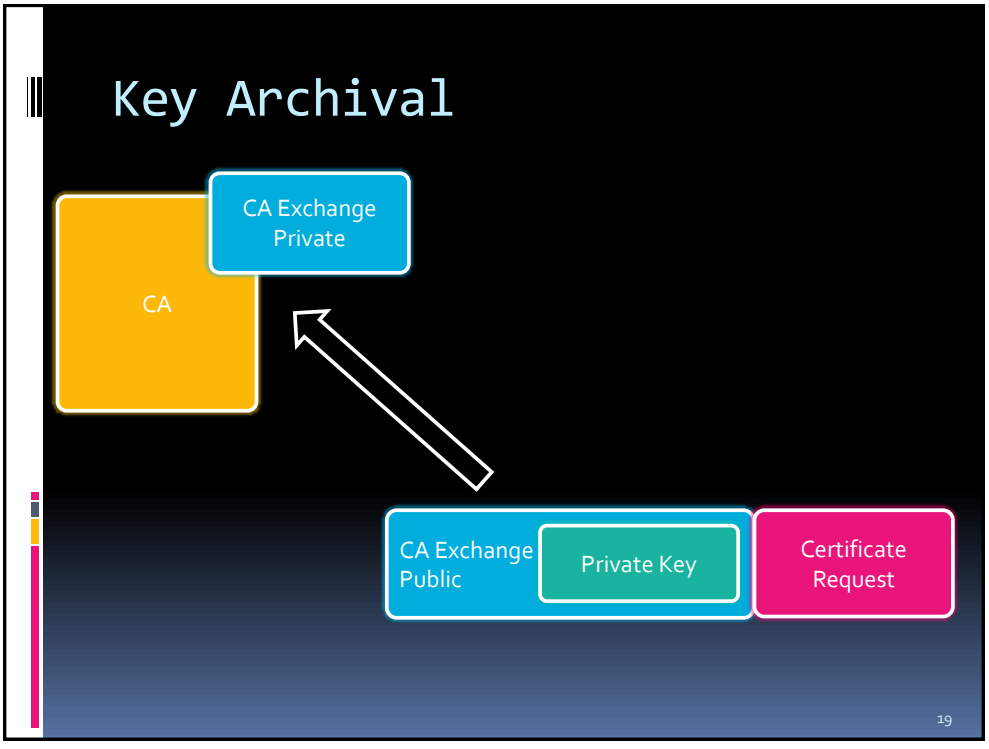
17

Standard certificate request without private key

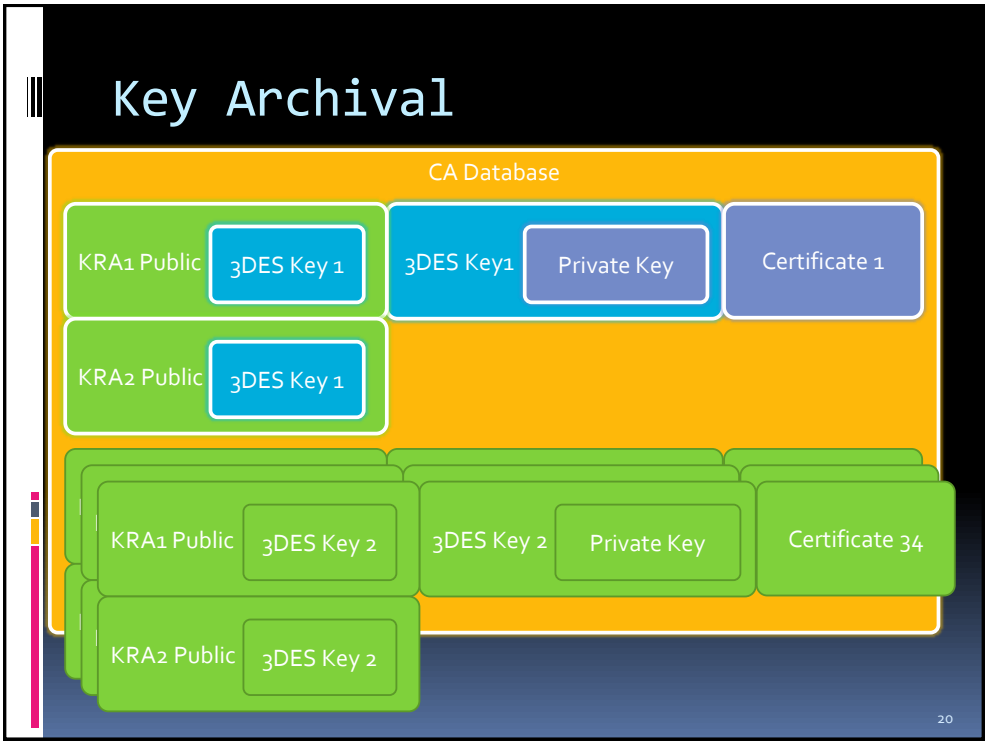


18

18


Key Archival
CA Exchange Private
CA
CA Exchange Public
Private Key
Certificate Request
19

19


Key Archival
CA Database
KRA1 Public
3DES Key 1
3DES Key1
Private Key
Certificate 1
KRA2 Public
3DES Key 1
KRA1 Public
3DES Key 2
3DES Key 2
Private Key
Certificate 34
KRA2 Public
3DES Key 2
20

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

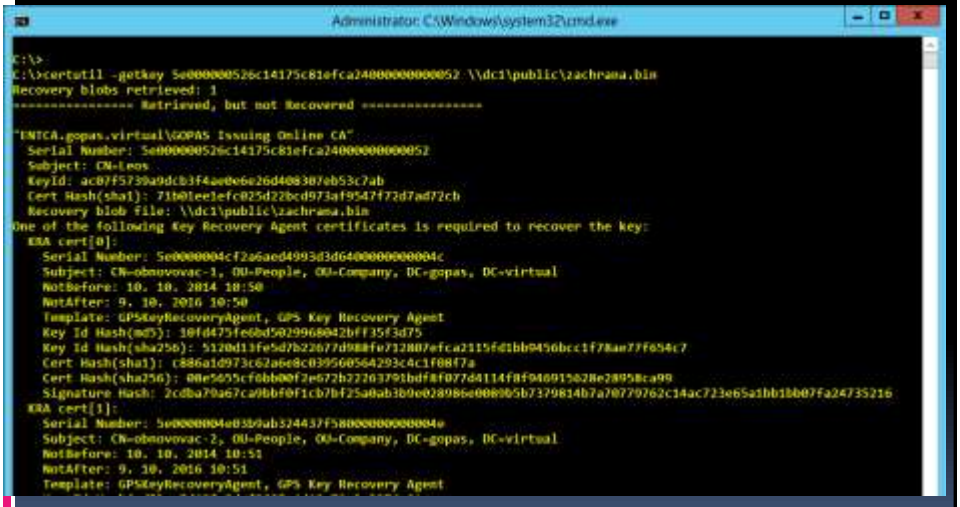
CAKeyExchange and Suite-B

- 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

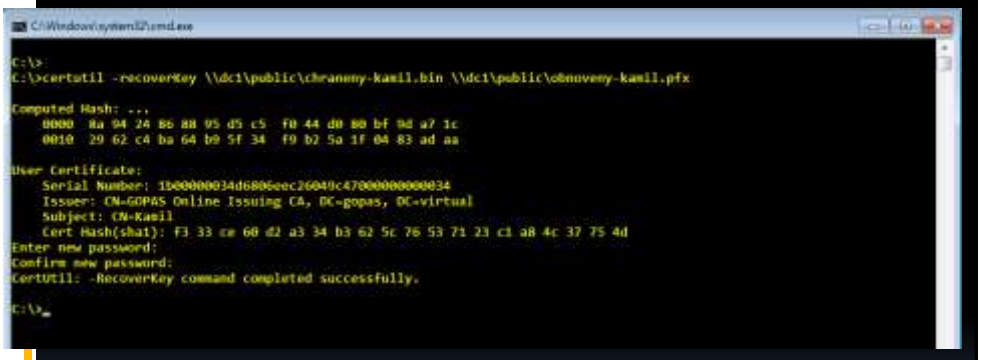
Recovering the keys

- 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

Recovering the keys -getkey



RecoverKey into final PFX



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

THANK YOU!