Microsoft

Windows Server Managing and Supporting Active Directory Certificate Services (ADCS)

Module 8: PKI Operations and Business Continuity

Module Overview

- Offline CA Maintenance
- Backup of PKI components
- CA certificate renewal
- CRL Maintenance
- Emergency Procedures
- CA Monitoring
- Documentation and Processes

Offline CA Maintenance

Offline CA Maintenance

General Tasks for offline CAs:

- Issue and publish CRLs
- Issue certificates to subordinate CAs
- CA certificate renewals
- Apply major release updates such as service packs

Offline CA Maintenance (cont.)

After Task execution:

- Take a new CA backup and save it to a location outlined in your key signing ceremony
- Take a new CA private key backup after a CA certificate renewal
- Power off the Offline CA and follow the steps in the key signing ceremony to secure the CA

Offline CA CRL Publishing

- Raise a change for that process
- Plan the publishing two or three weeks before the current CRL is going to expire
- Plan for issues during root CA start up
    - System start up can be done by server admins
    - Service start up should only be done by CA responsible together with auditors

Offline CA CRL Publishing (cont.)

- Issue new CRL: **Certutil -crl**
- Copy CRL to a disk or other removable media
- Shut down CA and verify storage and protection
- Process an audit log entry
- Publish the CRL(s) to the defined CDPs

Backup of PKI components

Backup Considerations

- Orphaned certificates
- Private key material presence
  - included in regular backups
  - separately backed up
  - additionally backed up
- Backup protection
  - Encryption
  - Access
  - Auditing

Backup Considerations (cont.)

- Backups containing CA private key material must be maintained and managed to the same level of security as the CA itself

- Documentation should exist for all Backup and Recovery processes and procedures

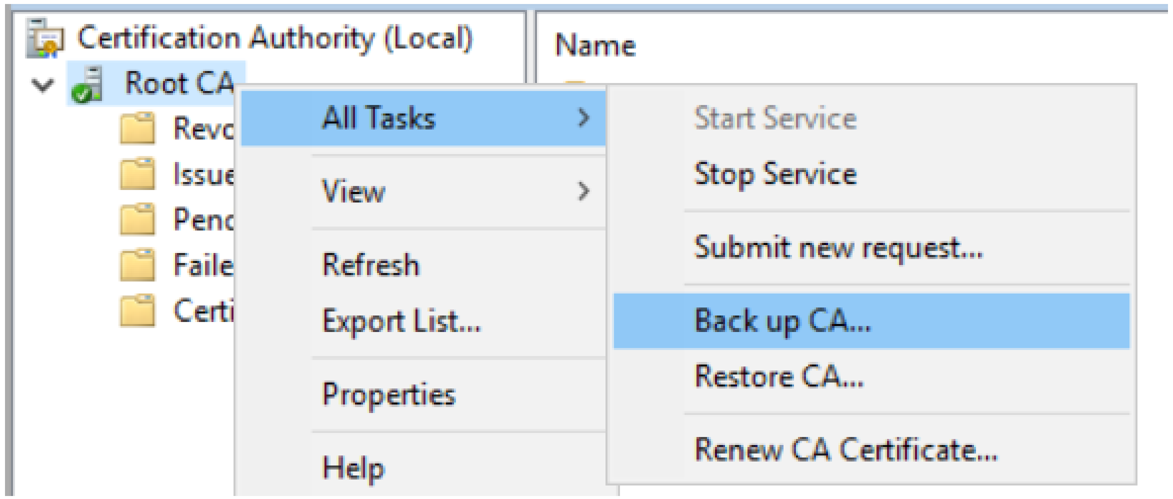
- Routine recovery exercises should be performed for all critical ADCS-related components to ensure integrity of the processes and recoverability of data (Microsoft generally recommends annually and after a major upgrade)

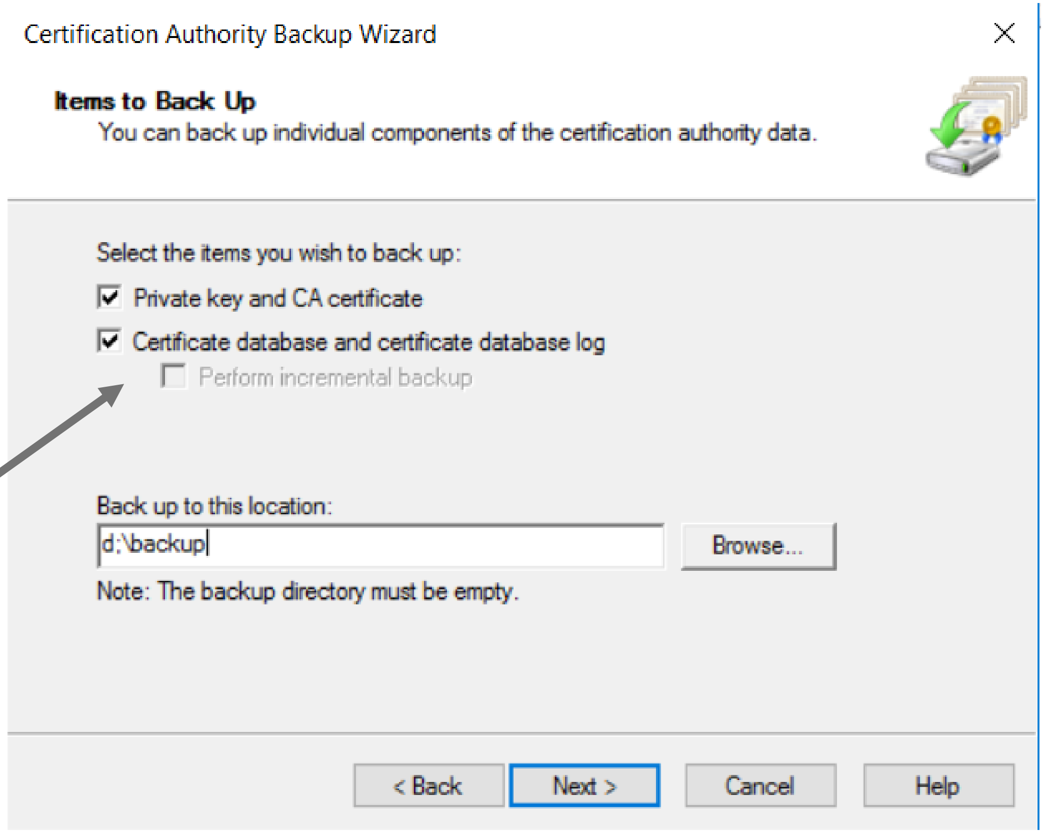
PKI Backup Checklist

- CA private key and database
- CA registry
- Setup and configuration files
- General CA information
  - Basic CA Information
  - CSP information
  - Published templates
- PKI objects in AD
- IIS configuration
- Additional PKI Services

CA private key and database

- From GUI:




Certification Authority Backup Wizard

Items to Back Up

You can back up individual components of the certification authority data.

Select the items you wish to back up:

☑ Private key and CA certificate

☑ Certificate database and certificate database log

□ Perform incremental backup

Back up to this location:

d:\backup

Note: The backup directory must be empty.

Perform incremental backup will be available if at least one backup was performed in the past

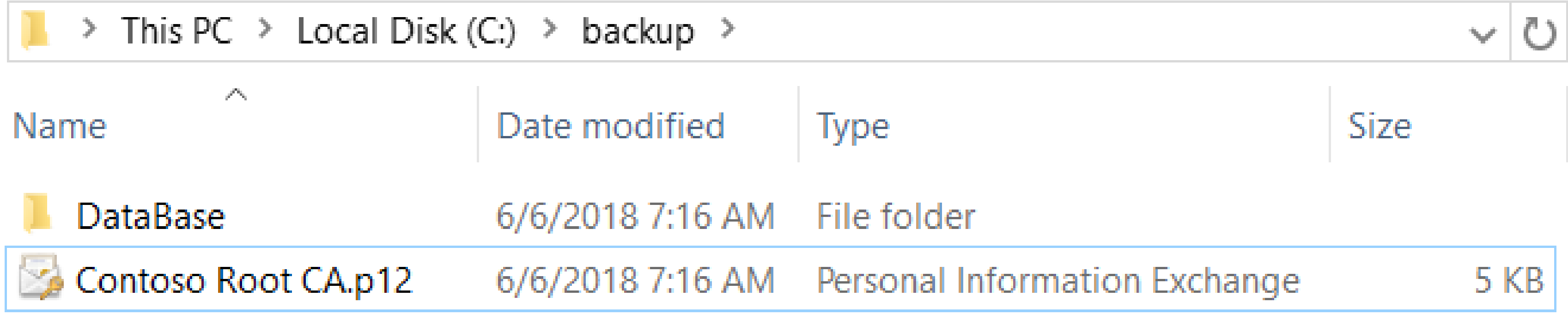
CA private key and database

- From Command line:

```
Certutil.exe –backupkey <BackupDirectory>
Certutil.exe –backupdb <BackupDirectory>
```

<BackupDirectory> specifies the directory in which the backup files are created.

- The specified value can be a relative or absolute path.
- If the specified directory does not exist, it is created.
- The backup files are created in a subdirectory named DataBase



Name	Date modified	Type	Size
DataBase	6/6/2018 7:16 AM	File folder	
Contoso Root CA.p12	6/6/2018 7:16 AM	Personal Information Exchange	5 KB

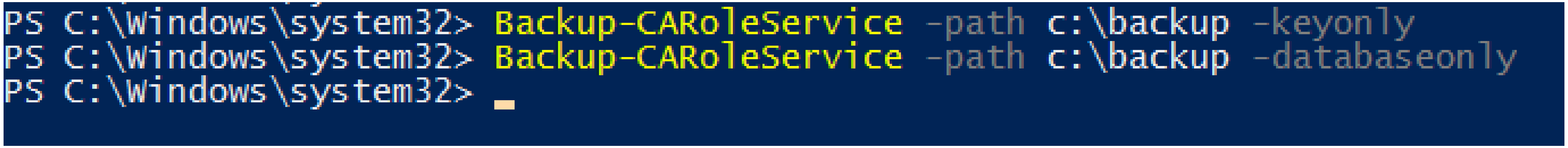
CA private key and database

- From PowerShell

  Backup-CARoleService -path c:\backup –keyonly

  Backup-CARoleService -path c:\backup -databaseonly

- Backup-CARoleService –keyonly without providing the password will protect private key with SID of the current user



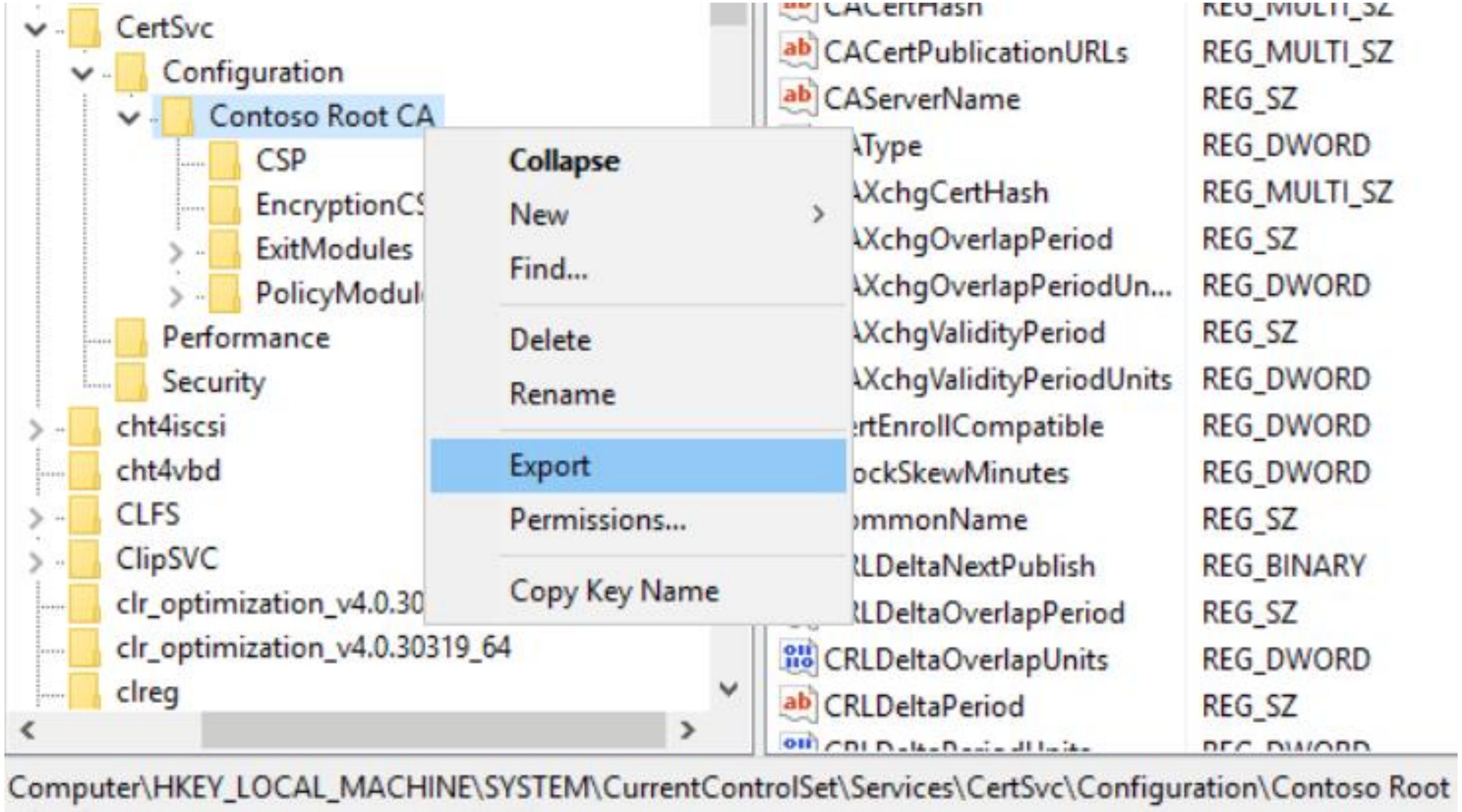
```
PS C:\Windows\system32> Backup-CARoleService -path c:\backup -keyonly
PS C:\Windows\system32> Backup-CARoleService -path c:\backup -databaseonly
PS C:\Windows\system32> _
```

CA private key and database

- If a hardware security module (HSM) is used by the CA, back up the private keys by following procedures provided by the HSM vendor

CA Registry

reg export HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration <output file.reg>



CACertHash	REG_MULTI_SZ
CACertPublicationURLs	REG_MULTI_SZ
CAServerName	REG_SZ
Type	REG_DWORD
XchgCertHash	REG_MULTI_SZ
XchgOverlapPeriod	REG_SZ
XchgOverlapPeriodUn...	REG_DWORD
XchgValidityPeriod	REG_SZ
XchgValidityPeriodUnits	REG_DWORD
rtEnrollCompatible	REG_DWORD
ockSkewMinutes	REG_DWORD
mmonName	REG_SZ
LDeltaNextPublish	REG_BINARY
LDeltaOverlapPeriod	REG_SZ
CRLDeltaOverlapUnits	REG_DWORD
CRLDeltaPeriod	REG_SZ
CRLDeltaPeriodUnits	REG_DWORD

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Contoso Root

Setup and configuration files

- Setup and configuration files (capolicy.inf, policy.inf, configuration scripts)
  - If a **policy.inf** file was used to apply policies to the CA it should also be saved
  - The **CAPolicy.inf** file is located in the *%SystemRoot%* directory, which is usually *C:\Windows*
  - If a scripted setup (e.g. with PowerShell) was used, this files should also be backed up
  - Usually a post setup script will be used to apply the final configuration to the CA. This script will provide useful information for the migration and for the rebuild documentation
  - Automated scripts/jobs (e.g. CRL copy job, automated backup, etc.)

General CA Information

- Basic CA Information

  certutil -v -cainfo > <output file.txt>

- CSP information

  certutil –getreg CA\CSP > <output file.txt>

- Published templates

  certutil -v -catemplates > <output file.txt>

PKI objects in AD

AD Configuration NC

CN=Public Key Services, Configuration, CN=Services, DC=<ForestRootdomain>

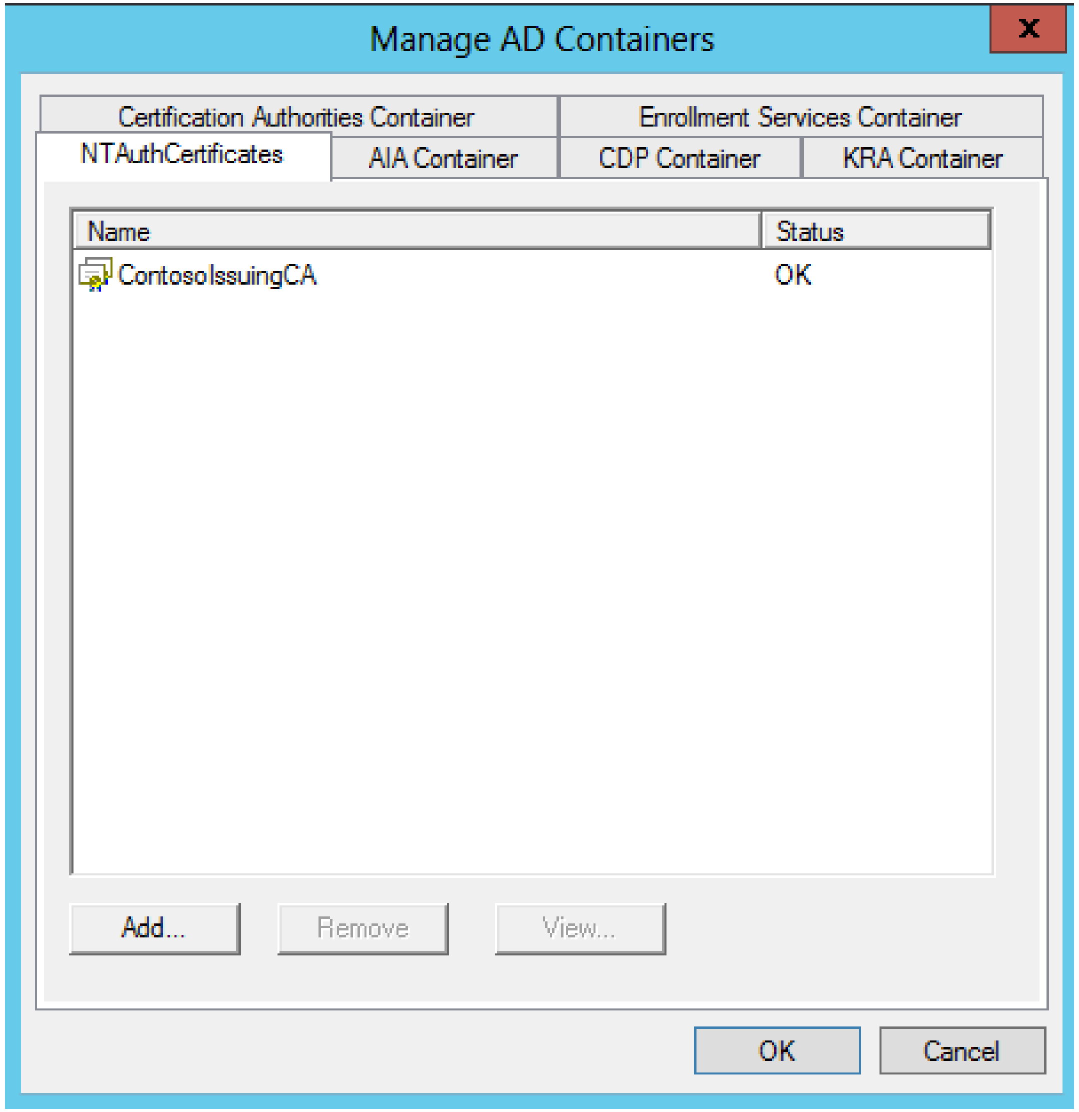
Tools

ADSIedit.msc

LDAP.exe

Enterprise PKI (PKIview.msc)

GPOs containing PKI related settings



Name	Status
ContosoIssuingCA	OK

Lesson Review

1. What are the key elements for CA backup/restore?

CA certificate renewal

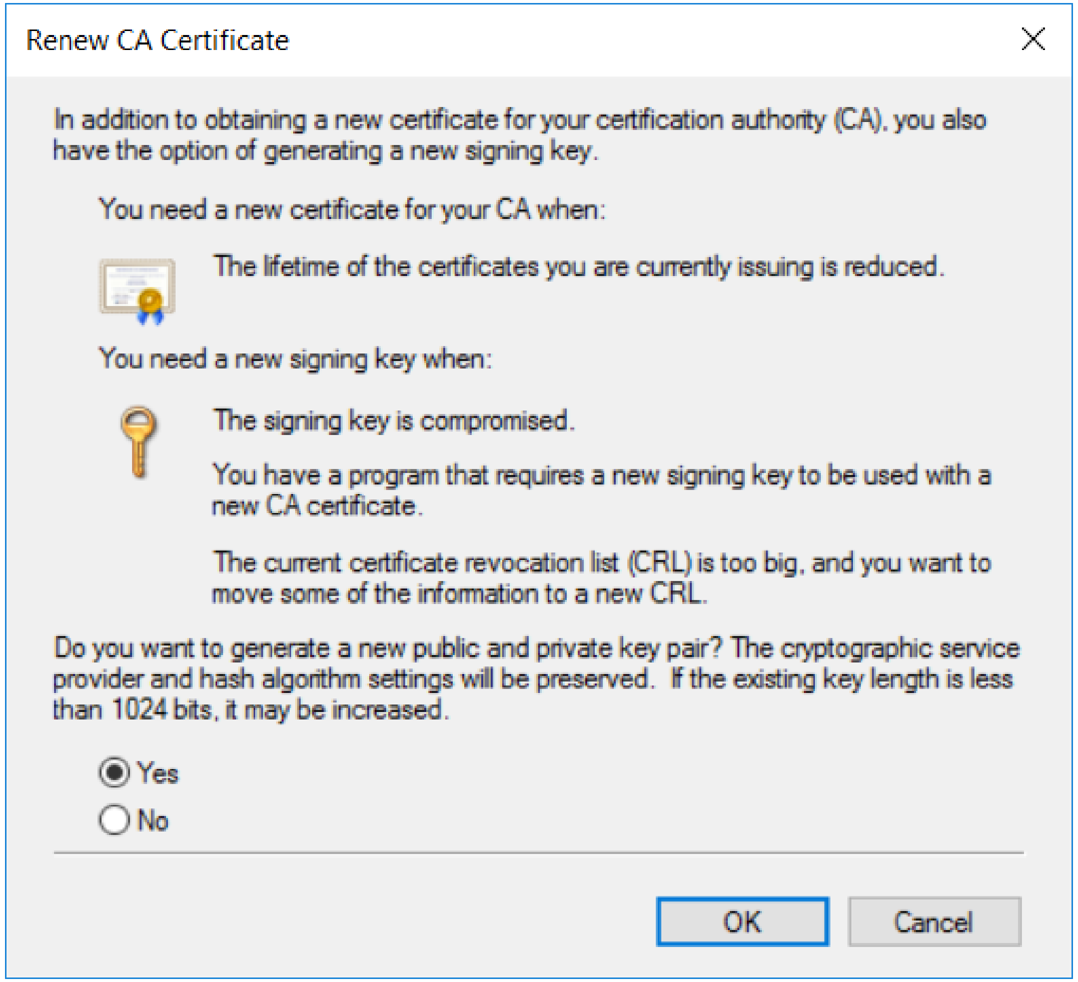
CA certificate renewal

- **Reasons for CA certificate renewals:**
    - Extending lifetime of a CA
    - Increasing the key size of the CA
    - Changing hash algorithm of the CA certificate
    - Changing CDP or AIA locations of the parent CA
    - Adding certificate policies to the CA (qualified subordination)
    - CRL partitioning

CA certificate renewal

2 options:

- Renewal with **New private key**
- Renewal with **Same private key**



Renew CA Certificate

In addition to obtaining a new certificate for your certification authority (CA), you also have the option of generating a new signing key.

You need a new certificate for your CA when:

The lifetime of the certificates you are currently issuing is reduced.

You need a new signing key when:

The signing key is compromised.

You have a program that requires a new signing key to be used with a new CA certificate.

The current certificate revocation list (CRL) is too big, and you want to move some of the information to a new CRL.

Do you want to generate a new public and private key pair? The cryptographic service provider and hash algorithm settings will be preserved. If the existing key length is less than 1024 bits, it may be increased.

● Yes

○ No

CA Certificate Renewal – Same Key Pair

- Does not affect Trust or chaining
- All new certificates are singed using same private key
- Existing CRL is maintained
- Preferred from usability perspective

CA Certificate Renewal – New Key Pair

- Trust must be re-established/propagated
- More complex chaining
- Subject Key Identifier (SKI) changes
- All new certificates are signed using new private key
- New CRL is created with incremental index in file name (e.g., “Fabrikam Root CA(1).crl”)
- Inherently problematic for non-LDAP aware relying parties
- Recommended from security perspective

CA Certificate Renewal – New Key Pair (cont.)

- Cross-certificates are generated to provide a chaining mechanism for domain-joined clients until the new CA certificate is distributed and must be published to Active Directory

```
certutil –dspublish –f <CAName(0-1).crt> CrossCA
certutil –dspublish –f <CAName(1-0).crt> CrossCA
```

- Recommended only for the following scenarios:
  - CRL partitioning
  - Key compromise
  - Application requirement

CA Renewal Best practices

- Validity period of child CA should be no more than 50% of its parent
- Renewal of the CA certificate should be conducted in a way so that leaf certificates can be always issued with full lifetime:

  Example:
  Root CA – valid for 9 years – renewal at 4th-5th year, if Issuing CA is valid for 4 years

  Issuing CA – valid for 4 years – renewal at 2nd year, if end-entity certificates are typically valid for 2 years

- Every 2nd renewal with new private key

CRL Maintenance

CRL Maintenance

- Controlling CRL Size
  - Do not publish expired certificates on a CRL until forced due to legal issues
  - CRL size is increasing linear (52 bytes each entry)
    - Serial number size changed from 19 bytes (Windows Server 2008) to 38 bytes with introduction of Windows Server 2012
  - Plan with CRL partitioning after 100k enrolled or revoked certificates
  - Plan for IDP (Issuing Distribution Point) 3rd party client support

- Remove Expired CRLs (if configured to be stored in the database)
  - In the CA database, all CRLs can be stored on long term for audit purposes

Emergency Procedures

CRL Re-Signing/ Emergency CRL Signing

Manually extending the validity time of a CRL during:

- CA Migration
- CA Recovery
- Disaster Recovery

certutil -sign <existing CRL file name> <resigned CRL file name>

certutil -dspublish <resigned CRL file name>

During this procedure you can add and remove serial numbers of revoked certificates to or from CRL

Also it is possible to add or remove extensions from the CRL

Lesson Review

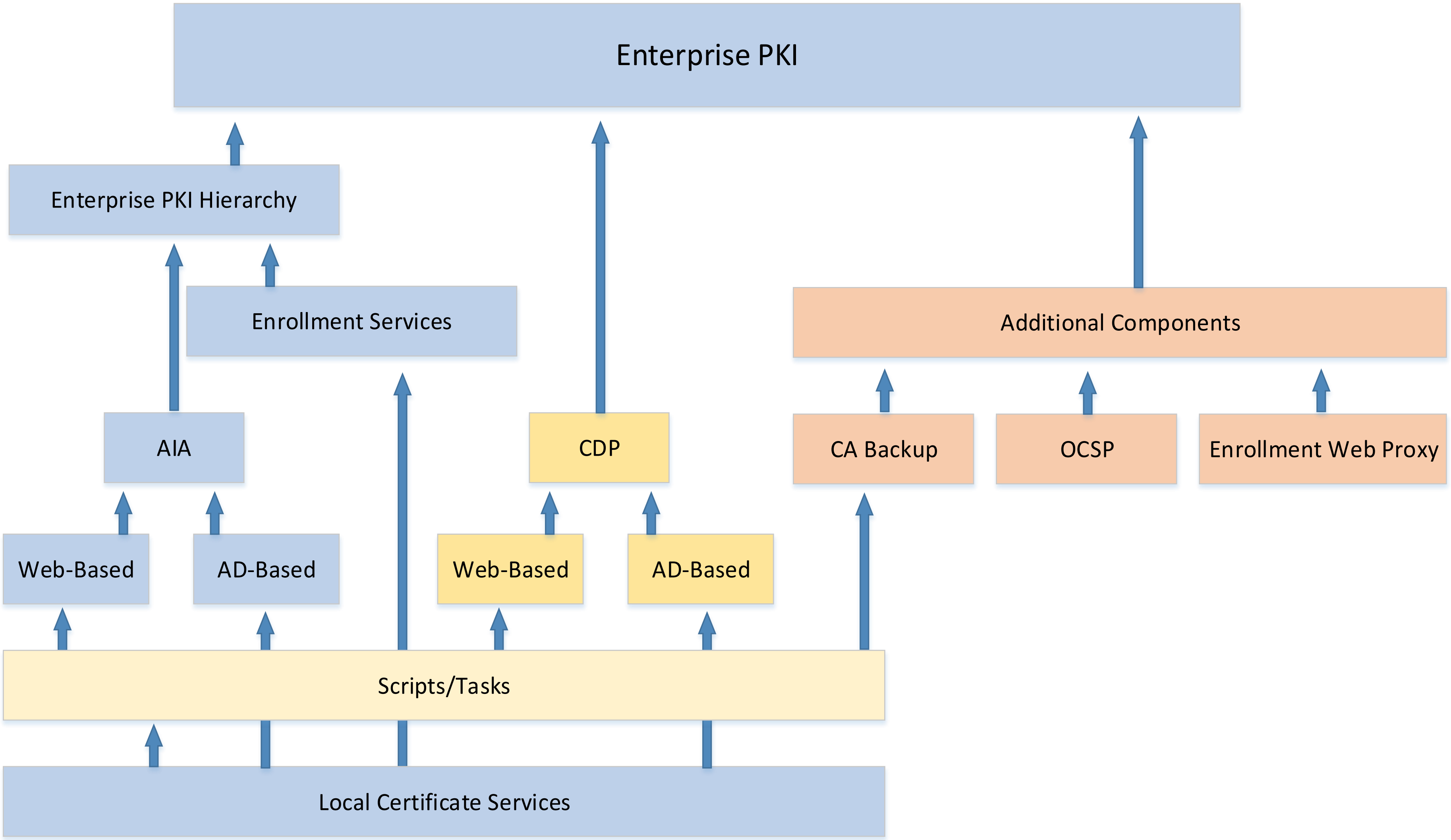
1. Why would you renew a CA certificate?
2. How should a CA lifecycle and renewal plan looks like?
3. Explain CRL partitioning.

CA Monitoring

Monitoring: Service vs. Application

- Service
  - e.g. Active Directory Certification Authority Service
- Application
  - Looking at the PKI as an overall Application including all attached components, services and tasks and includes performance data

Complete PKI Health Rollup



Lesson Review

1. What functionality does an exit module provide?
2. Explain the phrase "PKI Health Rollup"

Documentation and Processes

Written Policies

- **Certificate Policy (CP)** - set of rules that indicates the applicability of a certificate to a particular group of clients or applications that have common security requirements
- **Certificate Practice Statement (CPS)** - statement of the practices that IT uses to manage the certificates that it issues

Offline CA handling documentation

- Retrieval and stand-up
- Rebuild
- Disaster recovery
- CA certificate renewal
- Publishing CA certificate and CRL

Online CA handling documentation

- Rebuild
- Disaster recovery
- CA certificate renewal
- Emergency CRL signing
- HSM access and operations (if HSM is used)

Required CA documentation

Server	CA Configuration	User Configuration
Operating System (OS) version and patches needed	CAPolicy.Inf	Certificate Template Definitions
Names used by the CAs	CSP used to protect CA's private key	Certificate Templates Published
Network configuration	Key length and algorithm of the CA certificate	Permissions and User rights
Logical partitioning of the CA	Pre and Post installation scripts	
CA data and log path	Properties of the CA	
Audit settings (for both server and CA)	CRL and AIA distribution points	

Other maintenance tasks:

- Test CA private key backup
- Sign a certificate or CRL:

```
Certutil -sign CRLFileName.crl NewCRL.crl
Certutil -sign CertFileName.cer NewCertFile.cer
```

- Verify success:

```
Certutil: -sign command completed successfully
```

Lesson Review

1. What documentations are required for CA?

PKI Operations and Business Continuity - Best Practices

- Perform emergency CRL signing
- Extend the lifetime of CRLs
- Perform a reliable CA backup
- Restore the CA service to full functionality

LAB

Module Summary

- Understand PKI components required for Backup and Restore
- Maintaining and operating a CA
- Dealing with CRL maintenance
- Importance of monitoring the complete PKI
- PKI Documentation

Questions?