Microsoft

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

Module 5: CA Security

Module Overview

- Exposure of CA Private Key
- Hardware Security Modules
- Zero Trust
- Securing Certification Authorities
- PKI Administrative Role Separation
- Additional PKI Administrative Roles
- Securing Certificate Templates
- Auditing

Exposure of CA Private Key

Private Key's Risk Exposure

- CA private key - the most important logical piece of data in PKI world
- CA private key might fall into the wrong hands:
  - physical hard disk can be stolen
  - backups can be compromised
  - virtualized CA can be accessed by different people (Hyper-V admins, storage admins)
- Stolen private key can be used to issue fraudulent certificates for unauthorized requestors.

Private Key storage (Local Computer)

Where are the CA’s private keys stored?

On the CA’s hard drive

DPAPI (Data Protection API) encrypts the private keys using the local computer account credentials

By default, CA keys are marked as exportable

In the CA computer’s memory

Note DPAPI only protects data at rest. It does not protect the private key if the system is up and running!

Hardware Security Modules

Private Key storage - HSM

- Where CA’s private keys can also be stored?

- **On an HSM** (Hardware Security Module)
- Implementing an HSM is the preferred option!

Features of HSM

- Hardware protection of valuable private keys
  - Isolated cryptography
  - Key generation
  - Non-exportability
  - Tamper protection

- Acceleration of cryptographic operations

Features of HSM (cont.)

- Enforces additional controls whenever the CA key is used (role separation, multiple eyes principle)

- Load balancing and failover in hardware modules using multiple HSMs linked together through a daisy chain

- Implementing an HSM is the answer to many (not all!) security threats but adds cost and complexity to your environment

Types of HSMs

- Dedicated

- Network

Risk Exposure to CA Backup

Risk exposure if HSM is not implemented

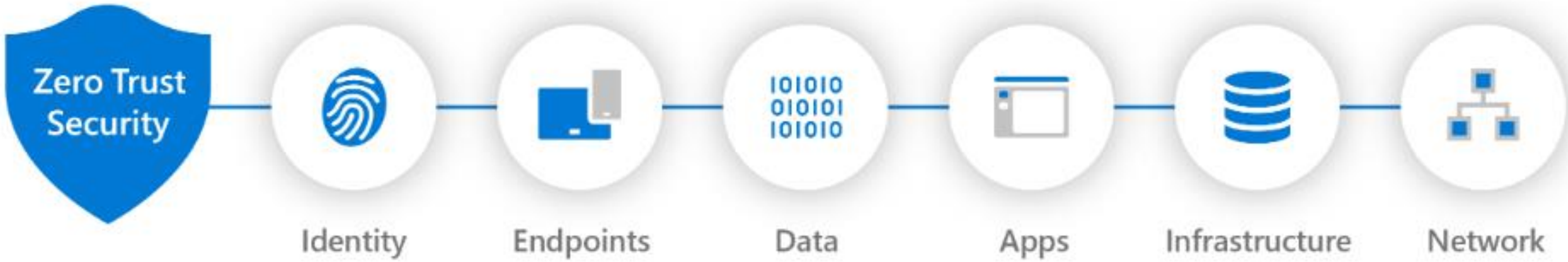
- Windows Server 2012 and later System State backup includes private keys
- Full disk, image-based backups and snapshots/checkpoints include private keys
- Memory dumps from CA server

Mitigation factors for backups including CA private keys

- Implement HSMs
- Store the backup in a tamper-evident bag and place it in a safe with limited access
- As CA keys almost never change, frequent backups are not necessary
- Ensure memory dump is saved on encrypted storage

Zero Trust

Zero Trust



- “**never trust, always verify**.”
- Users and devices, both inside and outside the corporate network, are deemed untrustworthy.
- Every access request is fully authenticated, authorized, and encrypted before granting access.
- Empower your users to work more securely anywhere and anytime, on any device.
- Enable digital transformation with intelligent security for today’s complex environment.
- Close security gaps and minimize risk of lateral movement.

Zero Trust Principles

Verify explicitly

- Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

Use least privileged access

- Limit user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity.

Assume breach

- Minimize blast radius for breaches and prevent lateral movement by segmenting access by network, user, devices, and app awareness. Verify all sessions are encrypted end to end.

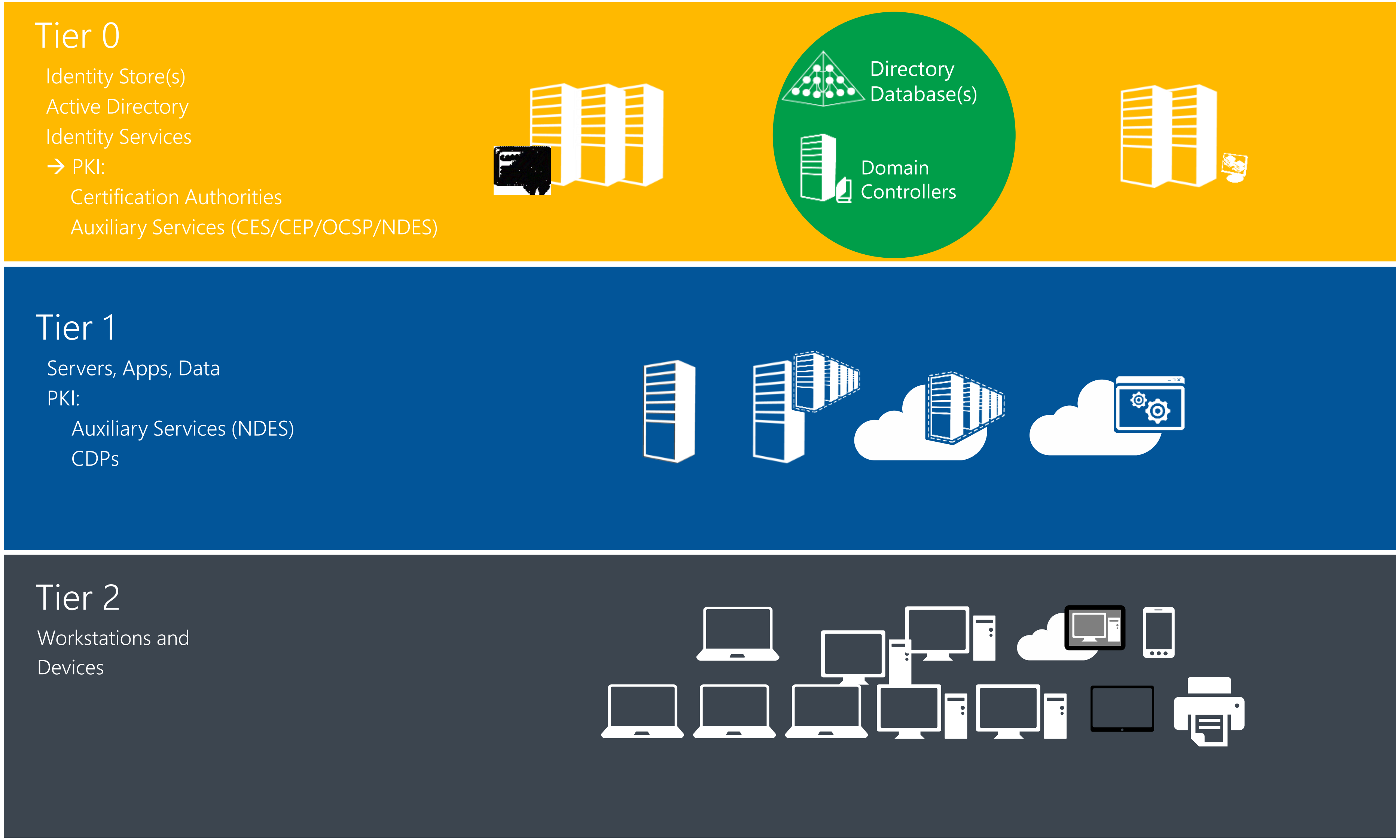
Use PKI to implement Zero Trust

Use certificates to protect:

- Identities (user and computer)
- Network Devices
- Mobile Devices
- Web and application servers
- Windows and non-windows workstations
- Wifi
- Vpn connection
- Smart Cards
- Windows Hello for Business (WHfB)
- Access to network resources

Securing Certification Authorities

PKI and Credential Tiering



Tier 0

Identity Store(s)
Active Directory
Identity Services
→ PKI:
Certification Authorities
Auxiliary Services (CES/CEP/OCSP/NDES)

Directory Database(s)

Domain Controllers

Tier 1

Servers, Apps, Data
PKI:
Auxiliary Services (NDES)
CDPs

Tier 2

Workstations and Devices

Tier 0

T0 credentials only usable in T0, for T0 (Identity) management tasks

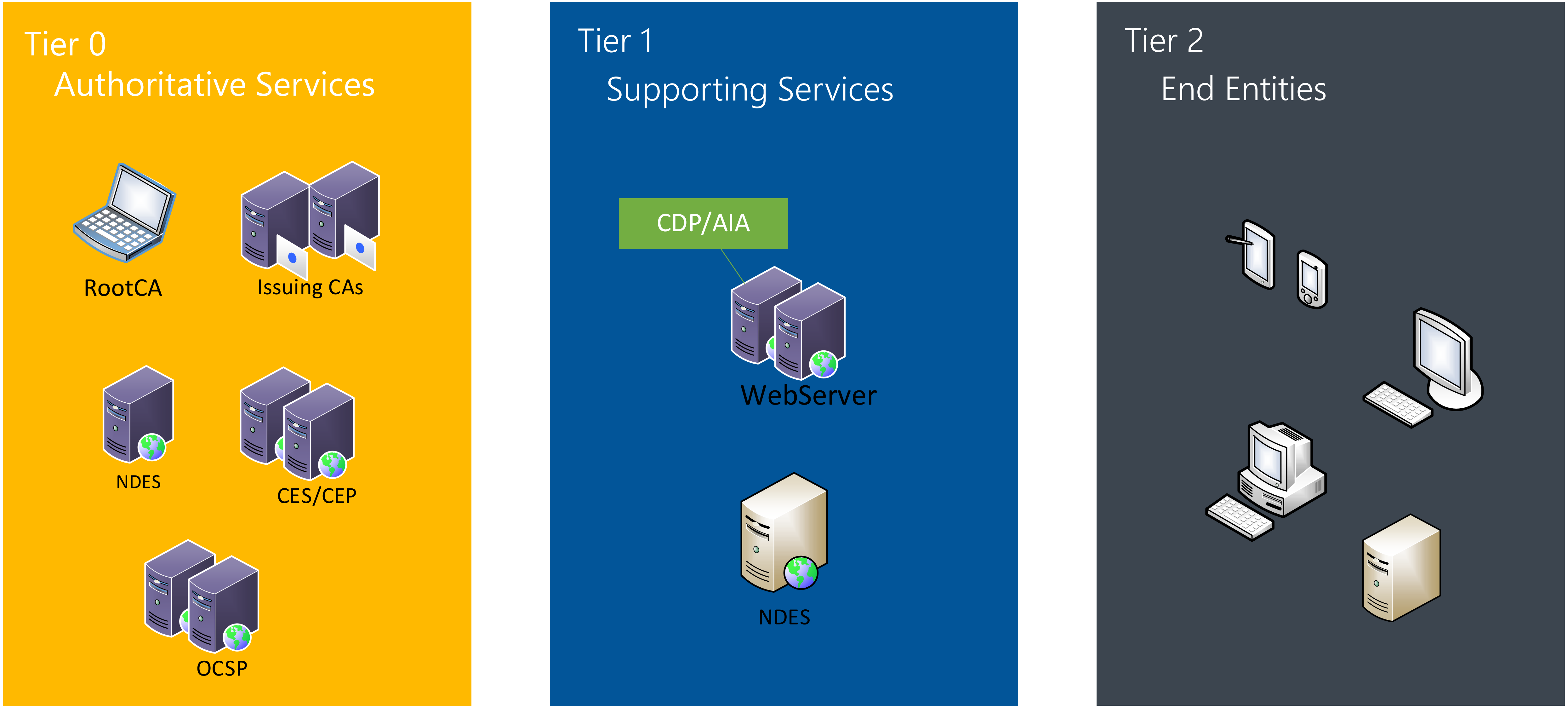
Tier 1

T1 credentials only usable in T1 for T1 management tasks

Tier 2

T2 credentials only usable in T2

PKI and Asset Tiering



Tier 0

Authoritative Services

RootCA

Issuing CAs

NDES

CES/CEP

OCSP

Tier 1

Supporting Services

CDP/AIA

WebServer

NDES

Tier 2

End Entities

Offline Certification Authorities

- Must be truly offline
- do not have a network interface
- are not joined to an Active Directory domain
- CRLs, certificates and cert requests must be copied manually
- If physical - keep it in a safe place (e.g. separate server cage, separate rack)
- If virtual - remove from hypervisor and store 2 copies on encrypted storage devices

Offline Certification Authorities

- Use dedicated media to transfer data
- Update the OS with major Service Packs and any updates that affect the logical operation of the CA and supportability of the OS
- Implement Security Auditing
- Use BitLocker or other full volume encryption method to encrypt hard disks

CA Hardening

- Block RDP and network logon for local accounts
- Enable and configure Windows Firewall
- Disable DMA
- Use encrypted hard disks
- Follow the guidelines of the Pass the Hash (PtH) whitepaper and related articles (http://aka.ms/pth)

CA Hardening (cont.)

- Use Microsoft Security Compliance Toolkit to build security baselines
- Disable Autoplay
- Rename Administrator and Guest accounts
- Do not re-use passwords!
- Do not install additional roles or software
- Disable services not required
- Restrict Remote Access
- Secure other channels for remote access (Remote Management Board, PowerShell Remoting)

CA Hardening (cont.)

- Restrict interactive logon
- Disable LM and NTLMv1 inbound authentication
- Use Protected Users security groups
- Connect to the CA only from hardened and restricted administrative hosts (http://aka.ms/cyberpaw)
- Usage of Authentication Policies and Authentication Policy Silos can help to restrict the scope of accounts
- Implement Multi-factor Authentication

Securing virtualized CAs

General:

- Use separate virtualization hosts for CAs and equivalent critical systems.
- Secure virtualization hosts differently from standard virtualization hosts.
- Protect the CA's private key by using HSMs.
- Don't use snapshot or bare-metal backups if the CA's private key is not secured by an HSM.
- Encrypt the virtualized hard disk to prevent uncontrolled boot or theft .

When using Windows Server 2016 (or above) Hyper-V:

- Use shielded VMs for the CAs.
- If no HSM can be used, protect the CA's private key by using the virtual TPM of the guest OS (this might affect signing performance).

Protecting the CA Service

- Enable and configure Windows Firewall
- Allow access only to required CA ports:
  - TCP 135
  - High ports
- Configure security settings and firewall rules to allow access only from systems which need to enroll certificates
- Use pre-defined enrollment stations (that is Smart Card enrollment)
- Registration authorities (e.g. NDES)
- Configure your CA to listed only on one, static port

Lesson Review

1. Where you can find CA private key?
2. What is the most important logical piece of data within a CA?
3. What security safeguards are implemented within a PKI to secure an entities private key?

PKI Administrative Role Separation

Common Criteria Role Separation

- … organizes CA administrators into separate task-based roles
- … prevents a condition where a single person can compromise the CA trust
- According to Common Criteria guidelines, **no single user may hold more than one PKI management role at the same time** (otherwise this account is blocked from administrative tasks)
- You need to assign multiple users the same role in case one holder of the role is sick, on holiday etc.

Common Criteria Roles

Roles	Security Permission	Description
CA Administrator	Manage CA	Configure and maintain the CA. This CA role includes the ability to assign all other CA roles and to renew the CA certificate
Certificate Manager	Issue and Manage Certificates	Approve certificate enrollment and revocation requests
Backup Operator	Back up and restore files and directories	Perform system backup and recovery. Backup is an OS feature
Auditor	Manage auditing and security log	Configure, view and maintain audit logs. Auditing is an OS feature

Configure “Common Criteria Role Separation” in Windows

- Not enforced by default
- When enforced, **no Windows account can have two roles at the same time**
- Configured on the CA using

  ```
  certutil -setreg CA\RoleSeparationEnabled 1
  ```

Additional PKI Administrative Roles

Additional Administrative Roles

In addition to Common Criteria roles, you can define Windows-based CA administrative roles

Roles and Groups	Security Permissions	Description
CA Administrator	• Acts as "service provider" for the service CA • Can restart the service • Modify CA configuration	• Often CA Administrator and Certificate Template Manager will be combined in one group.
Certificate Manager	• Manage certificate issuance and revocation	
Certificate Template Manager	• Can configure certificate templates.	• Often CA Administrator and Certificate Template Manager will be combined in one group.
Key Recovery Agent	• Can decrypt BLOBs using his/her Private KRA key.	
User Manager	• Manages users and their associated information in the Active Directory	
Enrollment Agent	• Can request certificates on behalf of other users.	• User must request a certificate with the Certificate Request Agent OID.

Multi-Factor Authentication for CA

- Multifactor authentication recommended for PKI management roles:
  - PKI Administrator
  - Certificate Manager
  - Backup Operator
  - Audit Manager
  - Key Recovery Manager
- If you implement smart card authentication for the management roles, ensure that you will be able to log on to CA computers at any time
- Smart Card authentication is not an option for non-domain joined computers

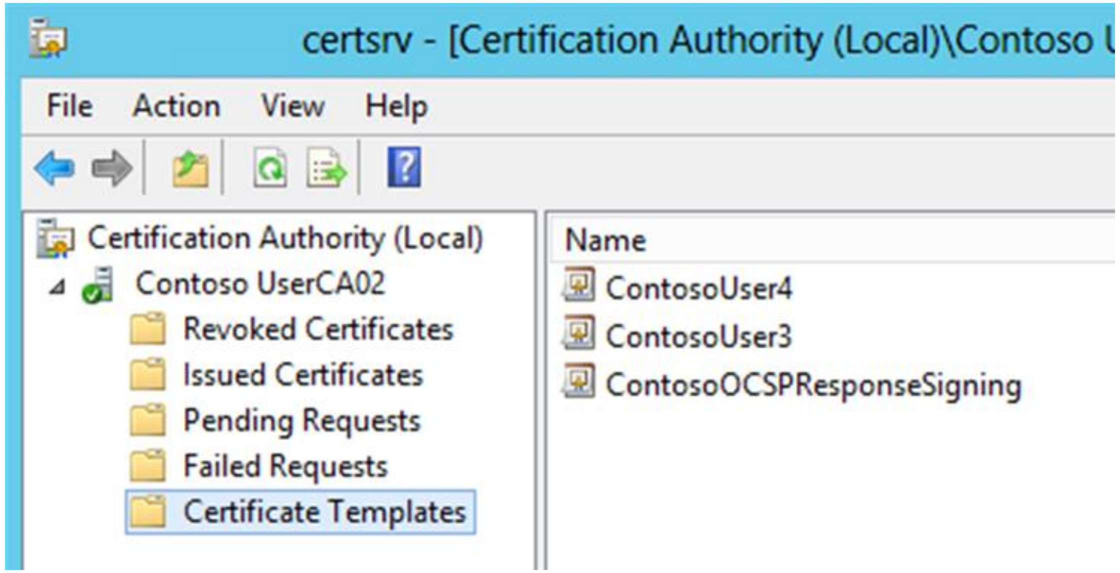
Security Certificate Templates

Securing Certificate Templates

- Remove Overly Broad Enroll or Autoenroll Permissions
- Remove Unused Templates from Certification Authorities
- Secure Templates that Allow You to Specify the Subject in the Request (SAN)
- Do not enable EDITF_ATTRIBUTESUBJECTALTNAME2 flag (certutil –getreg policy\EditFlags)
- For high sensitivity certificates:
  - Implement certificate manager approval
  - Implement additional signatures on requests
  - Implement monitoring of certificates issued by the template

Limit Types of Certificates a CA can issue

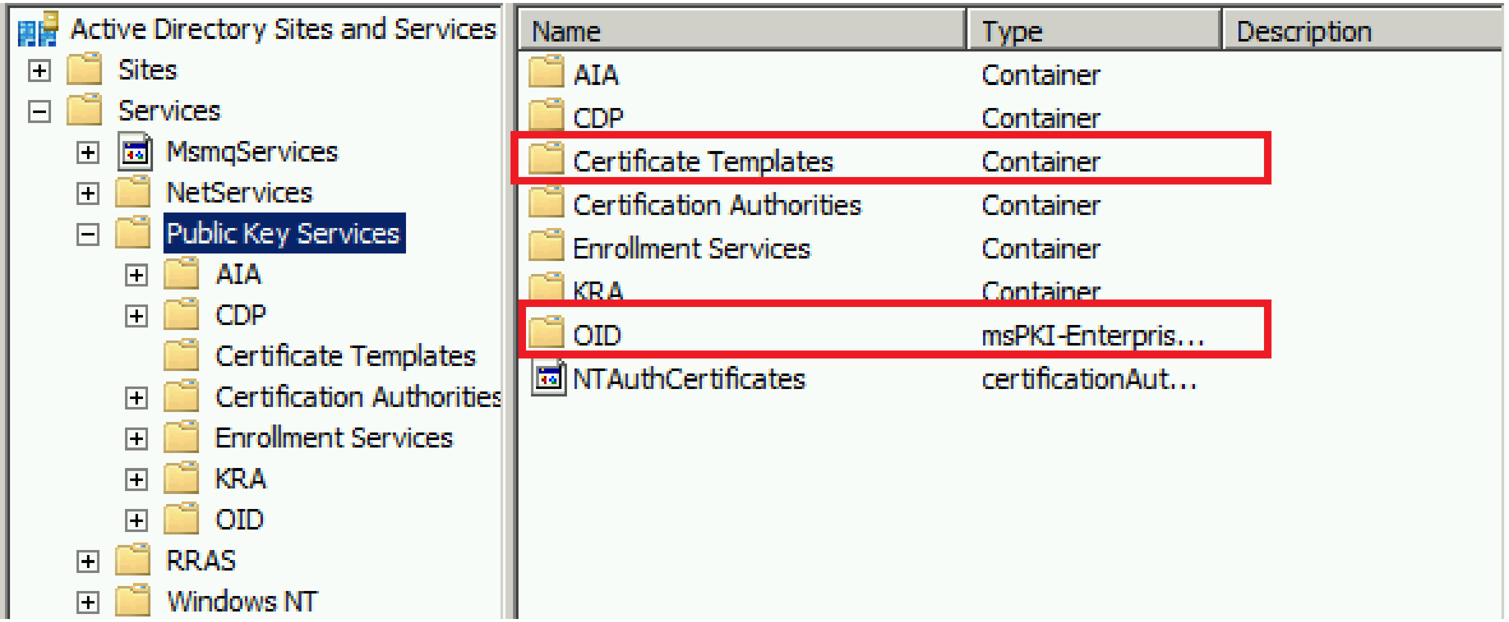
- CA can only issue certificates listed in its Certificate Templates container
- Remove default and unnecessary certificate templates
- Remove overly broad Enroll or Autoenroll permissions
- Secure templates that allow you to specify the subject in the request
- Limit the number of templates
- Limit Enroll permissions
- Enforce Certificate Manager approval
- Control user added SANs



ContosoUser4
ContosoUser3
ContosoOCSPResponseSigning

Delegate Control to Manage Templates

- Permission to create templates can be delegated
- Permissions to create OIDs can be granted to Certificate Template Managers



- Active Directory Sites and Services
  - Sites
  - Services
    - MsmqServices
    - NetServices
    - Public Key Services
      - AIA
      - CDP
      - Certificate Templates
      - Certification Authorities
      - Enrollment Services
      - KRA
      - OID
    - RRAS
    - Windows NT

Name	Type	Description
AIA	Container	
CDP	Container	
Certificate Templates	Container	
Certification Authorities	Container	
Enrollment Services	Container	
KRA	Container	
OID	msPKI-Enterpris...	
NTAuthCertificates	certificationAut...	

Lesson Review

1. When enabling role separation on a CA unsing:

"certutil -setreg CA\RoleSeparationEnabled 1", how can you ensure that no one is able to override this setting?

Auditing

Audit Active Directory Objects and Attributes

Audit and alert on changes to:

- **Critical groups** that control access to the CA (e.g., groups containing users with elevated rights to manage CAs, Registration Authorities, and enroll for important certificate types)
- Membership to the "**Cert Publishers**" domain local group(s)
- Accounts that have **privileged access** to Enterprise PKI components, including attributes (e.g., cn, name, sAMAccountName, userPrincipalName, or userAccountControl)
- Accounts used by **software packages** authoritative as a Registration Authority to a CA (e.g., mobility, SSL intercept, or identity management solutions, 3rd-party certificate management applications, etc…)
- **Unauthorized changes** to certificate templates

Other Activities

Record and review non-electronic activities that may impact PKI security

- Authorizations and change control permitting CA access and activities
- Authorizations and change control permitting access to any secure storage locations containing PKI backups or sensitive data (e.g., safes/vaults, archive facility, encrypted removable media, etc…)
- Entry and exit to the secure area where PKI hardware is located or operated (e.g., access to secure CA server racks/cage, access to the server room where the CAs are located, review of camera footage, etc.)
- Access and use of Hardware Security Modules (HSMs) and any tokens used to activate the HSMs

Auditing Configuration

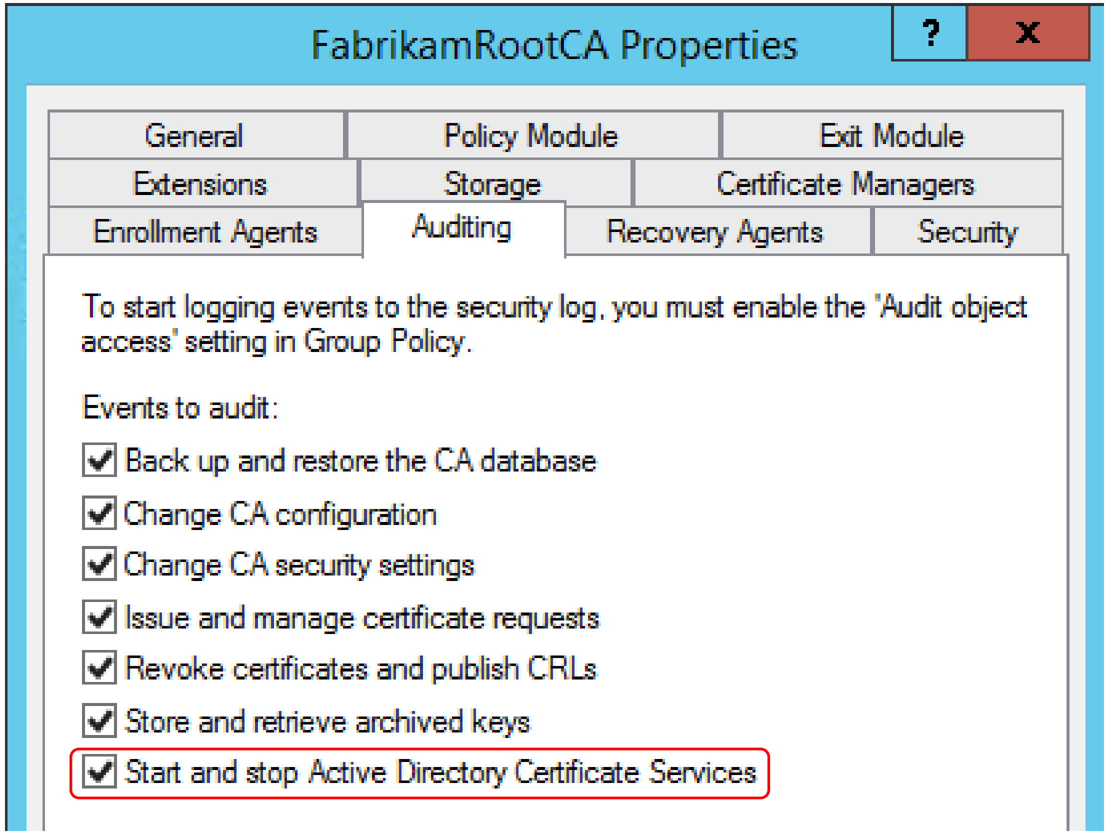
- In order to audit a variety of events related to the management and activities of a certification authority (CA), it is recommended to enable the following audit settings, using any of the following tools:
  - CA level auditing
    - Certification Authority Snap-in
    - Certutil.exe command
  - Operating System Level auditing
    - Security Policy (local/GPO)
  - CA Registry auditing
    - Regedit
    - Security Policy (local/GPO)
  - Certificate Template auditing
    - Certutil.exe command
    - AD Object auditing of Templates

CA Auditing

- Enable Auditing on the CA

```
Certutil -setreg CA\AuditFilter 127
```

Note: Auditing of certsvc start and stop causes a delay in the service starting and stopping, which should be expected to increase as the database grows



To start logging events to the security log, you must enable the 'Audit object access' setting in Group Policy.

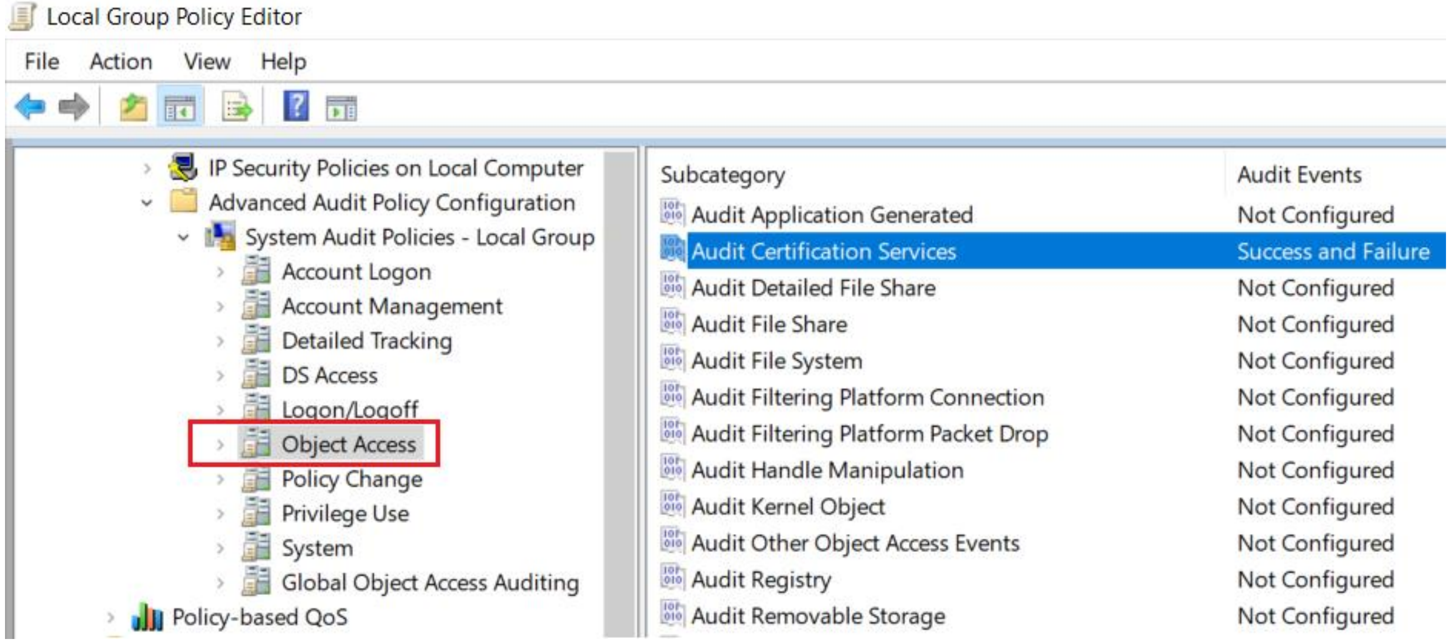
Events to audit:

☑ Back up and restore the CA database
☑ Change CA configuration
☑ Change CA security settings
☑ Issue and manage certificate requests
☑ Revoke certificates and publish CRLs
☑ Store and retrieve archived keys
☑ Start and stop Active Directory Certificate Services

OS Auditing

Local or Group Policy:

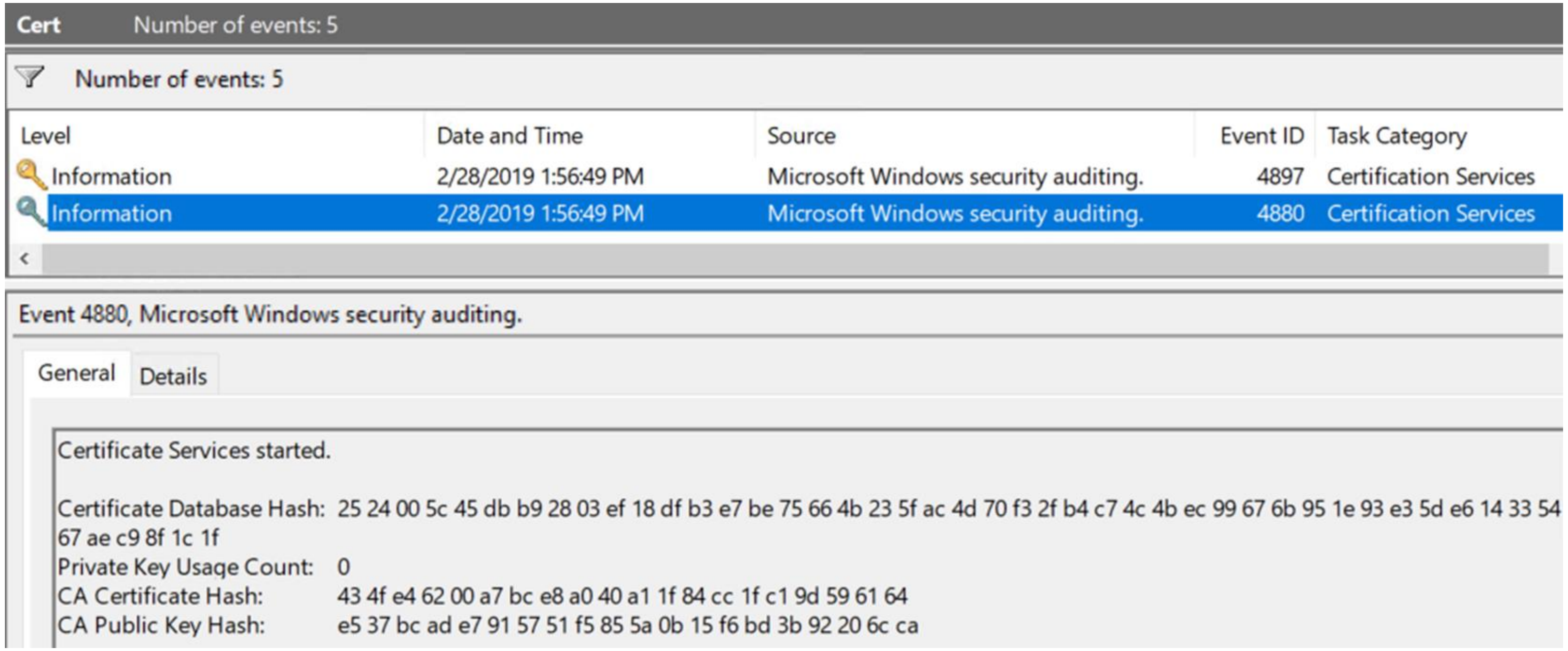
Advanced Audit Policy Configuration > System Audit Policies > Object Access > Audit Certification Services


Local Group Policy Editor
File
Action
View
Help
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
System Audit Policies - Local Group
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing
Policy-based QoS

Subcategory	Audit Events
Audit Application Generated	Not Configured
Audit Certification Services	Success and Failure
Audit Detailed File Share	Not Configured
Audit File Share	Not Configured
Audit File System	Not Configured
Audit Filtering Platform Connection	Not Configured
Audit Filtering Platform Packet Drop	Not Configured
Audit Handle Manipulation	Not Configured
Audit Kernel Object	Not Configured
Audit Other Object Access Events	Not Configured
Audit Registry	Not Configured
Audit Removable Storage	Not Configured

Example of a CA security event

Events are saved in Security log, and can be filtered based on Source and Task Category



Cert Number of events: 5

Number of events: 5

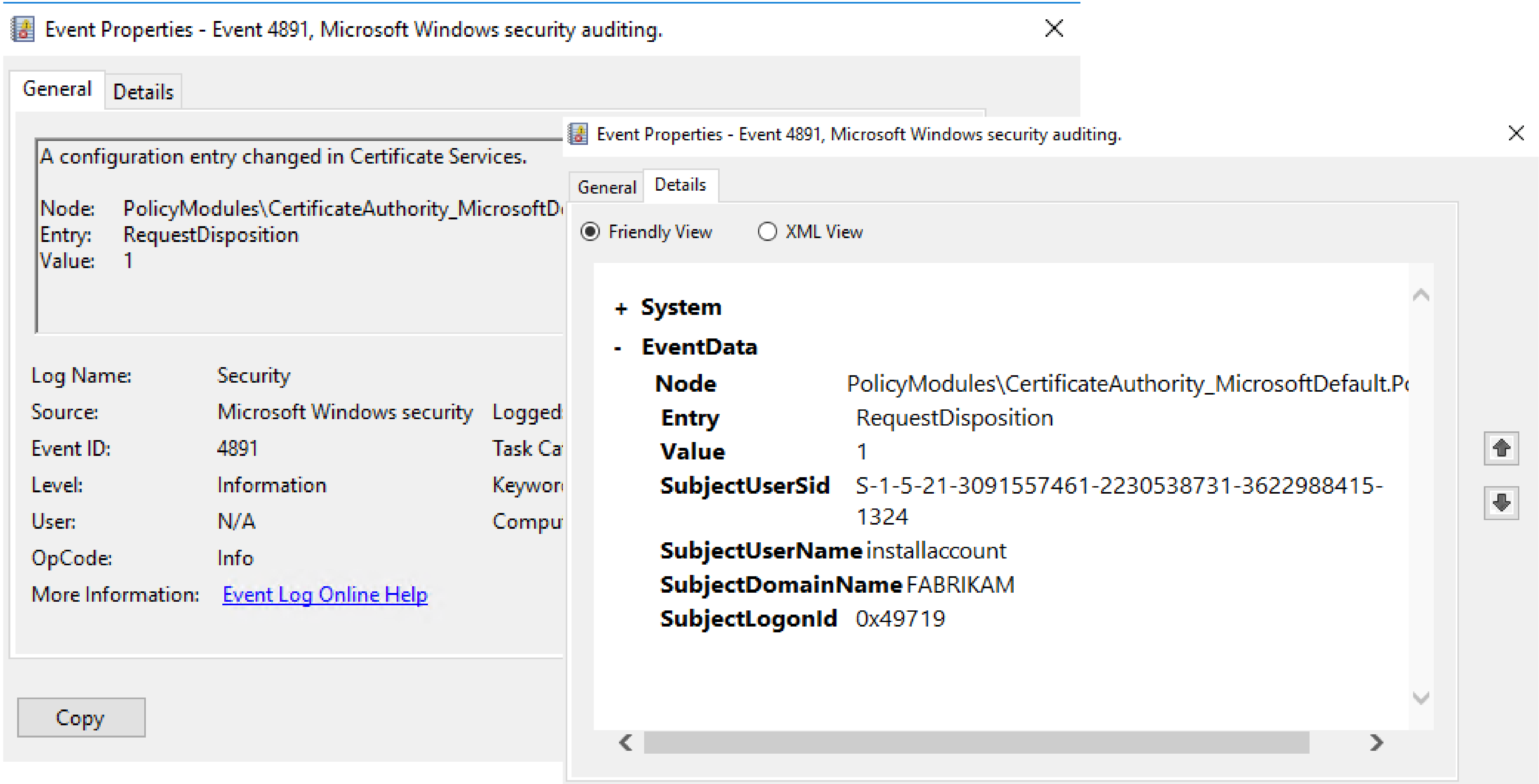
Level	Date and Time	Source	Event ID	Task Category
Information	2/28/2019 1:56:49 PM	Microsoft Windows security auditing.	4897	Certification Services
Information	2/28/2019 1:56:49 PM	Microsoft Windows security auditing.	4880	Certification Services

Event 4880, Microsoft Windows security auditing.

```
Certificate Services started.

Certificate Database Hash:  25 24 00 5c 45 db b9 28 03 ef 18 df b3 e7 be 75 66 4b 23 5f ac 4d 70 f3 2f b4 c7 4c 4b ec 99 67 6b 95 1e 93 e3 5d e6 14 33 54
67 ae c9 8f 1c 1f
Private Key Usage Count:    0
CA Certificate Hash:        43 4f e4 62 00 a7 bc e8 a0 40 a1 1f 84 cc 1f c1 9d 59 61 64
CA Public Key Hash:         e5 37 bc ad e7 91 57 51 f5 85 5a 0b 15 f6 bd 3b 92 20 6c ca
```

Security Audit Sample Event



Event Properties - Event 4891, Microsoft Windows security auditing.

A configuration entry changed in Certificate Services.

Node: PolicyModules\CertificateAuthority_MicrosoftD
Entry: RequestDisposition
Value: 1

Log Name:	Security	
Source:	Microsoft Windows security	Logged
Event ID:	4891	Task Ca
Level:	Information	Keywor
User:	N/A	Compu
OpCode:	Info	
More Information:	Event Log Online Help	

Event Properties - Event 4891, Microsoft Windows security auditing.

● Friendly View ○ XML View

+ System

- EventData

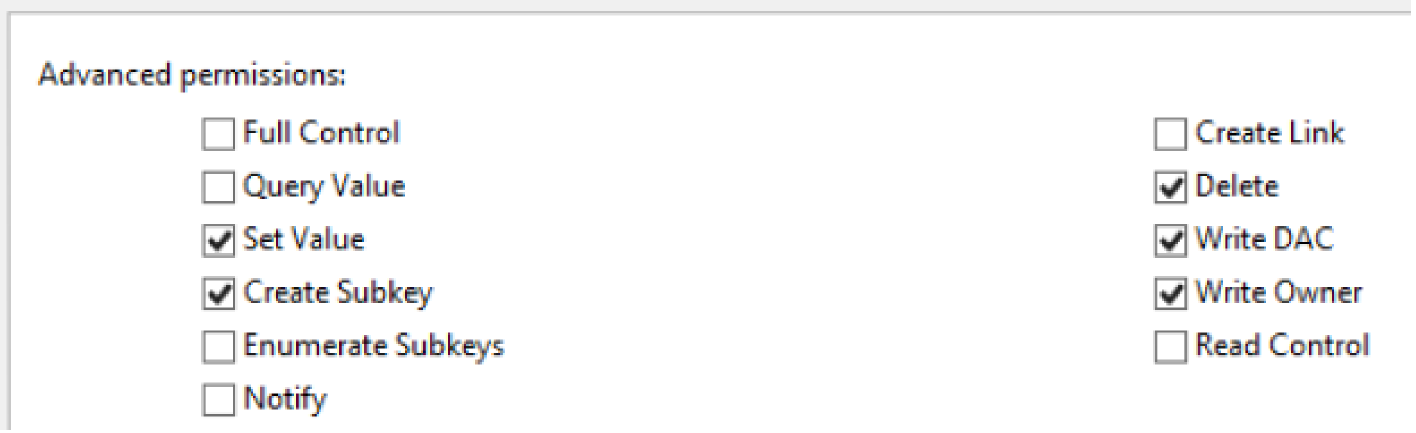
Node	PolicyModules\CertificateAuthority_MicrosoftDefault.P
Entry	RequestDisposition
Value	1
SubjectUserSid	S-1-5-21-3091557461-2230538731-3622988415-1324
SubjectUserName	installaccount
SubjectDomainName	FABRIKAM
SubjectLogonId	0x49719

Enable auditing on CA Registry

Local or Group Policy:

Advanced Audit Policy Configuration > System Audit Policies > Object Access > Audit Registry

Enable auditing on registry HKLM\System\Services\CurrentControlSettings\CertSvc\Configuration\



Advanced permissions:

- □ Full Control
- □ Query Value
- ☑ Set Value
- ☑ Create Subkey
- □ Enumerate Subkeys
- □ Notify
- □ Create Link
- ☑ Delete
- ☑ Write DAC
- ☑ Write Owner
- □ Read Control

Enable Auditing on CA Templates

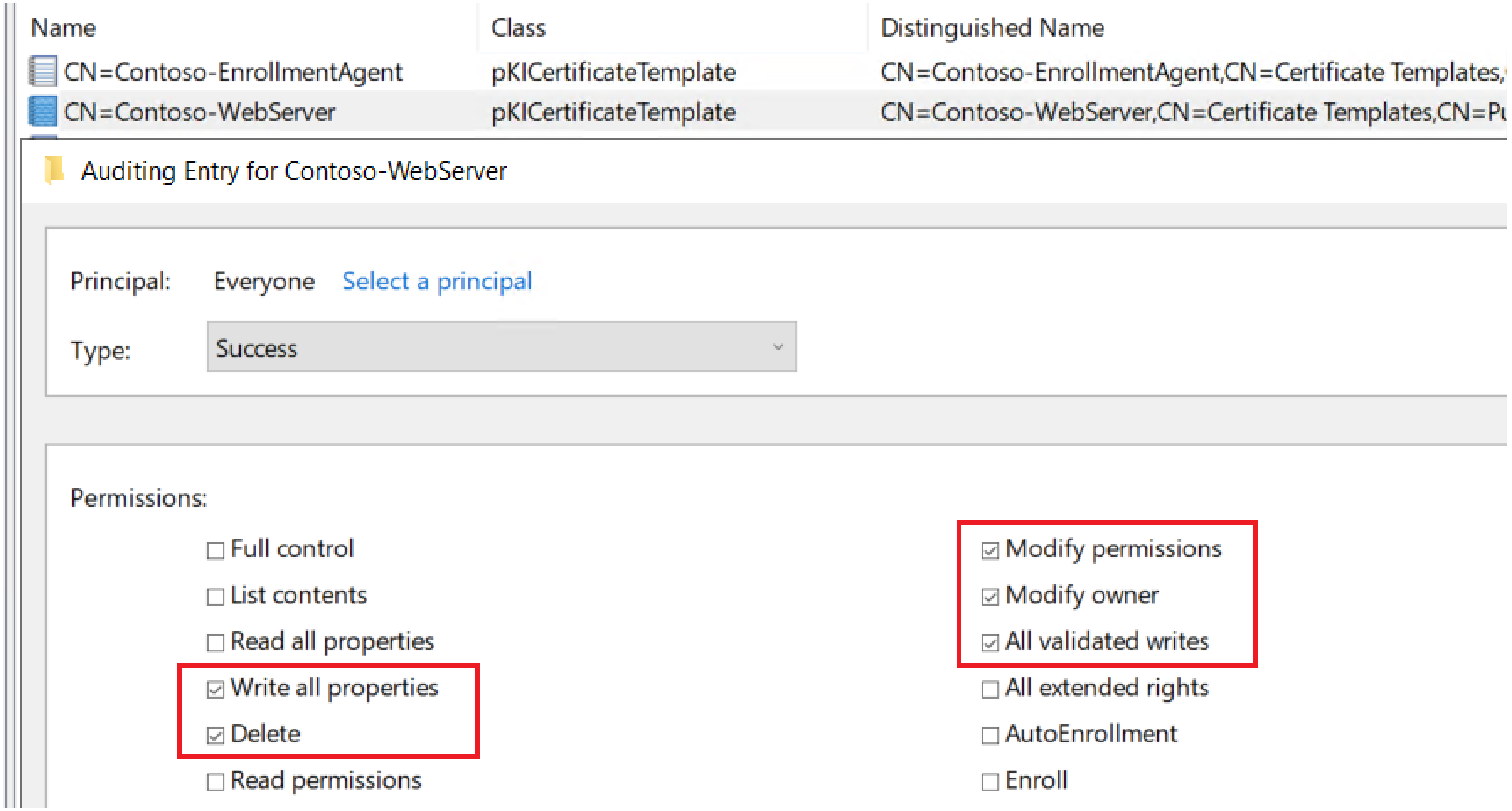
- AD CS includes several audit events that allow monitoring of changes to certificate templates that are actively being used by a CA. The following audit events are available:
  - Certificate Services loaded a template (Event ID 4898)
  - A Certificate Services template was updated (Event ID 4899)
  - Certificate Services template security was updated (Event ID 4900)

```
certutil –setreg policy\EditFlags +EDITF_AUDITCERTTEMPLATELOAD
```

CA Templates Auditing

- When auditing templates, consider the following scenarios:
  - Changes to templates that add new EKUs (Code Signing, Enrollment Agent, Smart Card Logon, etc.)
  - Addition of unexpected new templates on the CA
  - Changes to permissions for enrollment
  - Changes to permissions for write access to a template
  - Assignment of new templates that allow “supply in request” to build the subject
  - List of templates which are loaded during CA service startup

DS Access Auditing of Template



Name	Class	Distinguished Name
CN=Contoso-EnrollmentAgent	pKICertificateTemplate	CN=Contoso-EnrollmentAgent,CN=Certificate Templates,
CN=Contoso-WebServer	pKICertificateTemplate	CN=Contoso-WebServer,CN=Certificate Templates,CN=Pu

Auditing Entry for Contoso-WebServer

Principal: Everyone

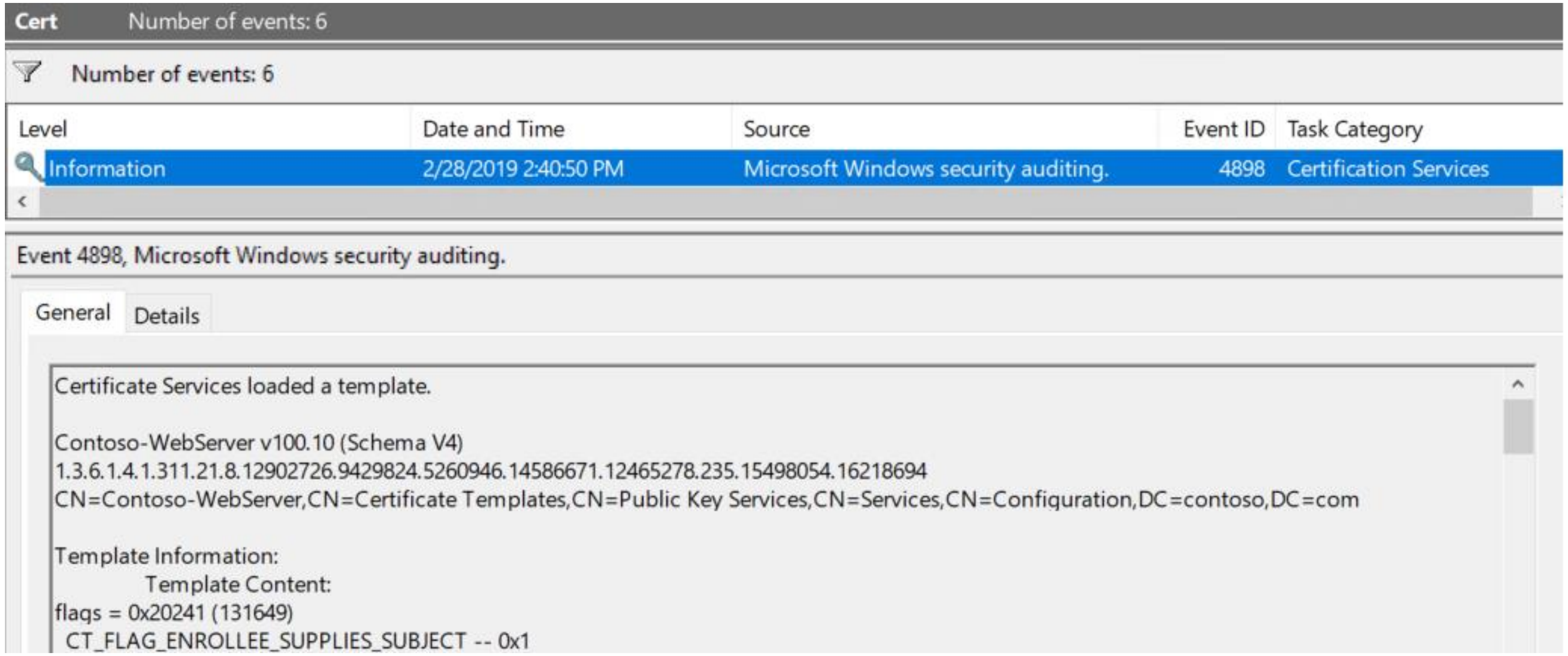
Type: Success

Permissions:

- □ Full control
- □ List contents
- □ Read all properties
- ☑ Write all properties
- ☑ Delete
- □ Read permissions
- ☑ Modify permissions
- ☑ Modify owner
- ☑ All validated writes
- □ All extended rights
- □ AutoEnrollment
- □ Enroll

Example of a security event on-Template Auditing

In the security log you can see event 4898 indicating template being loaded from Active Directory to CA server



Level	Date and Time	Source	Event ID	Task Category
Information	2/28/2019 2:40:50 PM	Microsoft Windows security auditing.	4898	Certification Services

Event 4898, Microsoft Windows security auditing.

```
Certificate Services loaded a template.

Contoso-WebServer v100.10 (Schema V4)
1.3.6.1.4.1.311.21.8.12902726.9429824.5260946.14586671.12465278.235.15498054.16218694
CN=Contoso-WebServer,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=contoso,DC=com

Template Information:
            Template Content:
flags = 0x20241 (131649)
  CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT -- 0x1
```

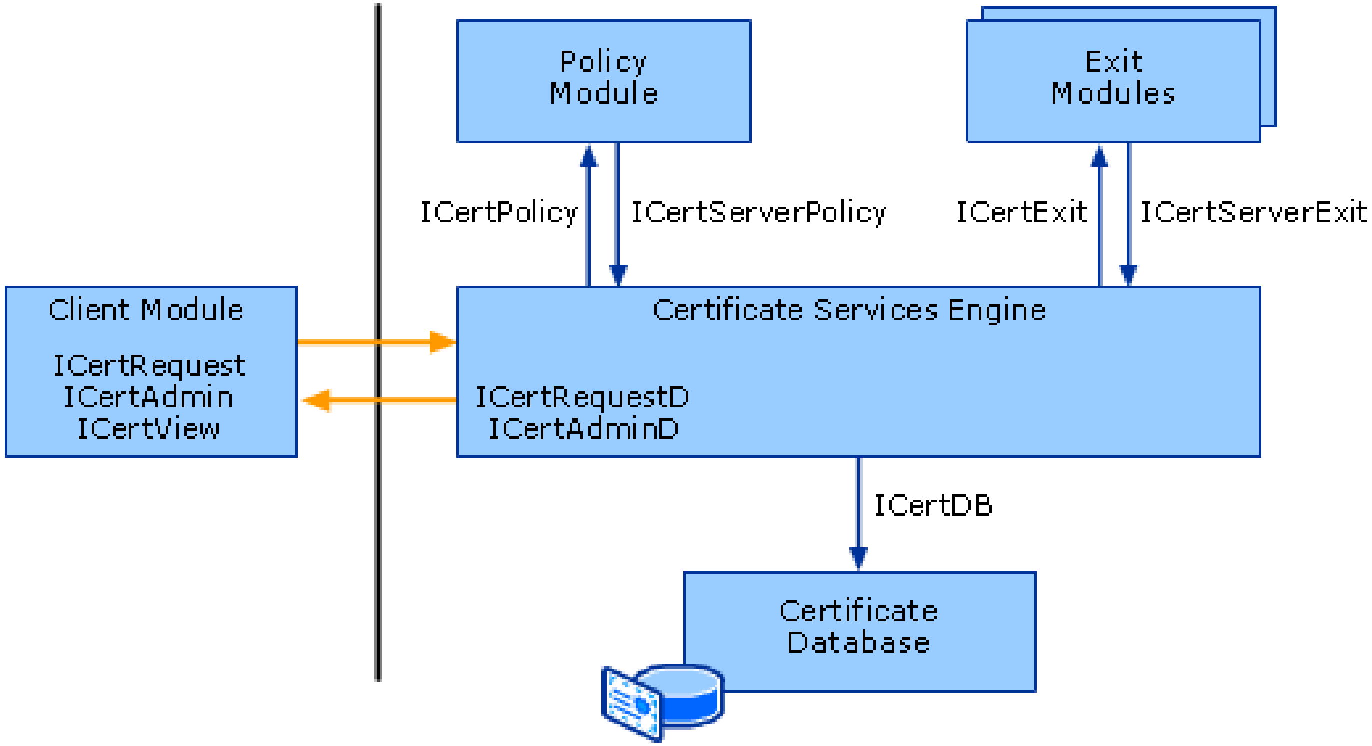
Exit Modules

Exit Module Functionality

- Called by the certificate services engine
- Notified of a certificate services event
- Callback possibility to query CA database about stored data
- Provides protocol-based publishing of certificates and CRLs
  - The default protocols are defined by the certificate services protocols specification https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-cersod/ec4bb597-9e73-4d2b-a768-621239e21fca
- Can be completely exchanged with or added by a custom developed module
  - A custom exit module can extend the specified default protocols https://docs.microsoft.com/en-us/windows/win32/seccrypto/exit-modules
- Multiple exit modules can be utilized in parallel

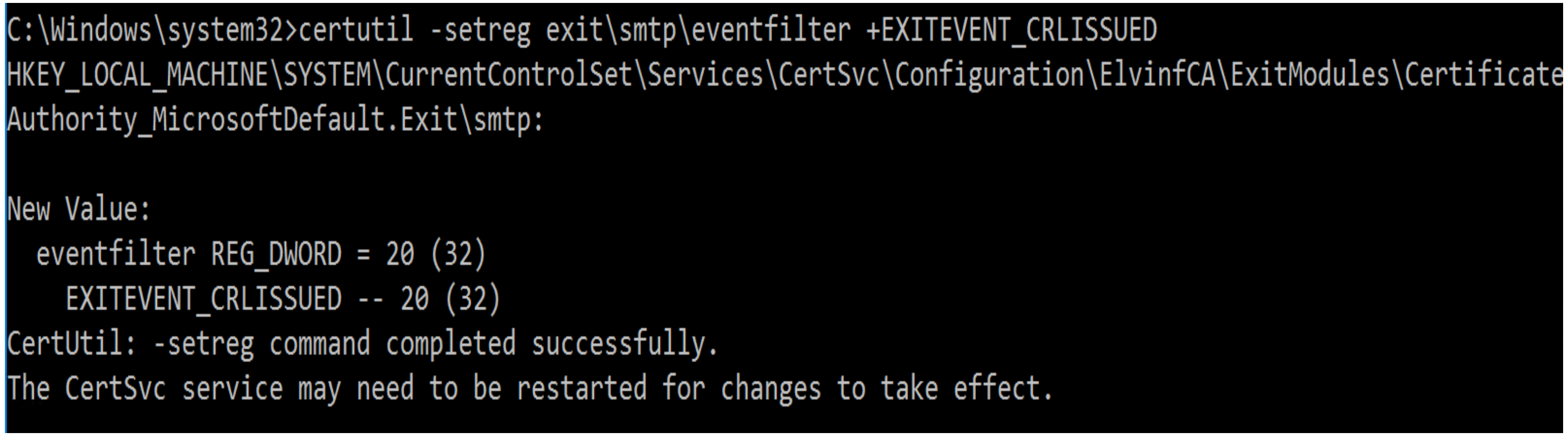
Exit Modules

- SMTP Exit Module is a component that is triggered after certificate request is processed or after any other event
- Examples:
  - Windows Default (saves certs to file system and AD)
  - SMTP Exit module (sends email notifications)
  - SQL Exit module (custom module that saves certs to the database)
  - MIM CM Exit module



SMTP Module Script

- SMTP Exit Module can be configured using a script provided by Microsoft
- Configurable items:
  - Scope
  - SMTP server address
  - Authentication
  - SSL



```
C:\Windows\system32>certutil -setreg exit\smtp\eventfilter +EXITEVENT_CRLISSUED
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\ElvinfCA\ExitModules\Certificate
Authority_MicrosoftDefault.Exit\smtp:

New Value:
  eventfilter REG_DWORD = 20 (32)
    EXITEVENT_CRLISSUED -- 20 (32)
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
```

Lesson Review

1. To enable auditing, what settings have to be enabled?

M05 - CA Security

- Exercise 1: Applying Roles Groups to your CAs
- Exercise 2: Finalizing Delegation of Public Key Services Container
- Exercise 3: Enable Security Auditing for all CAs
- Exercise 4: Assign necessary privileged to CA Administrators
- Exercise 5: Enable SMTP Exit module

Questions?