



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

Module 2: Certificate Revocation and Chain Building

Microsoft Services





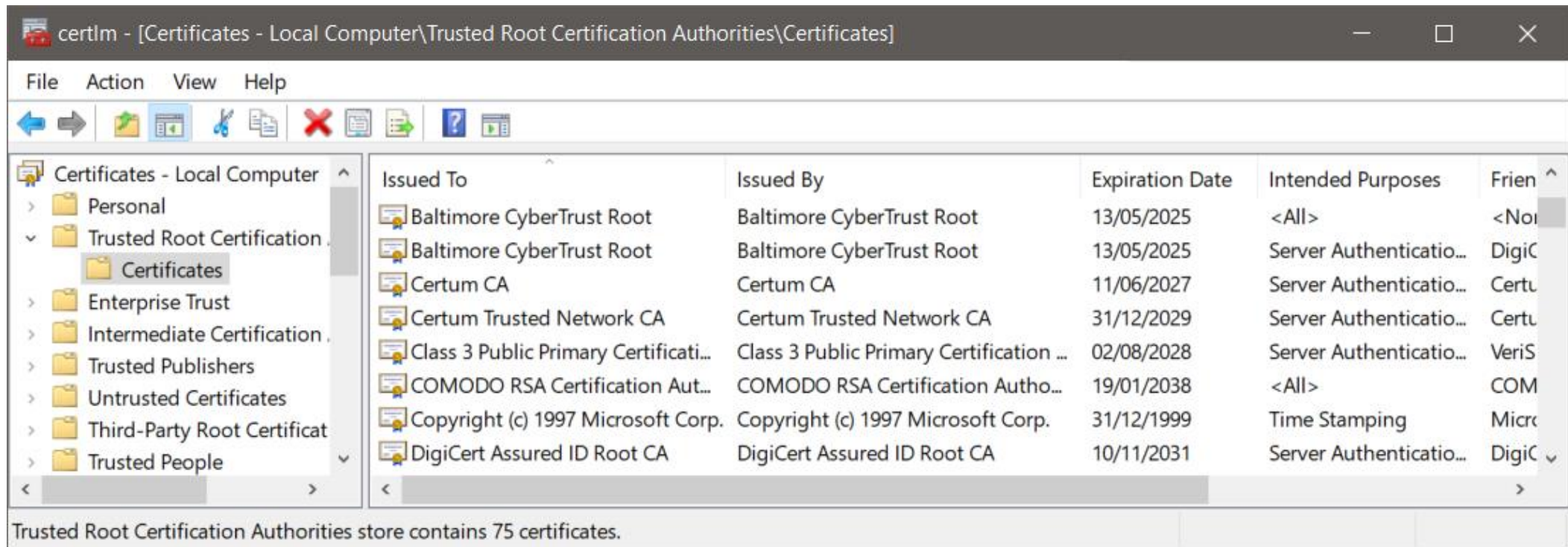
Module Overview

- Certificate Stores
- Certificate Verification and Chain Building
- Certificate Revocation Lists (CRLs)
- Designing and Configuring CDP Locations
- Revocation Cache
- Online Certificate Status Protocol (OCSP)
- Troubleshooting

Certificate Stores

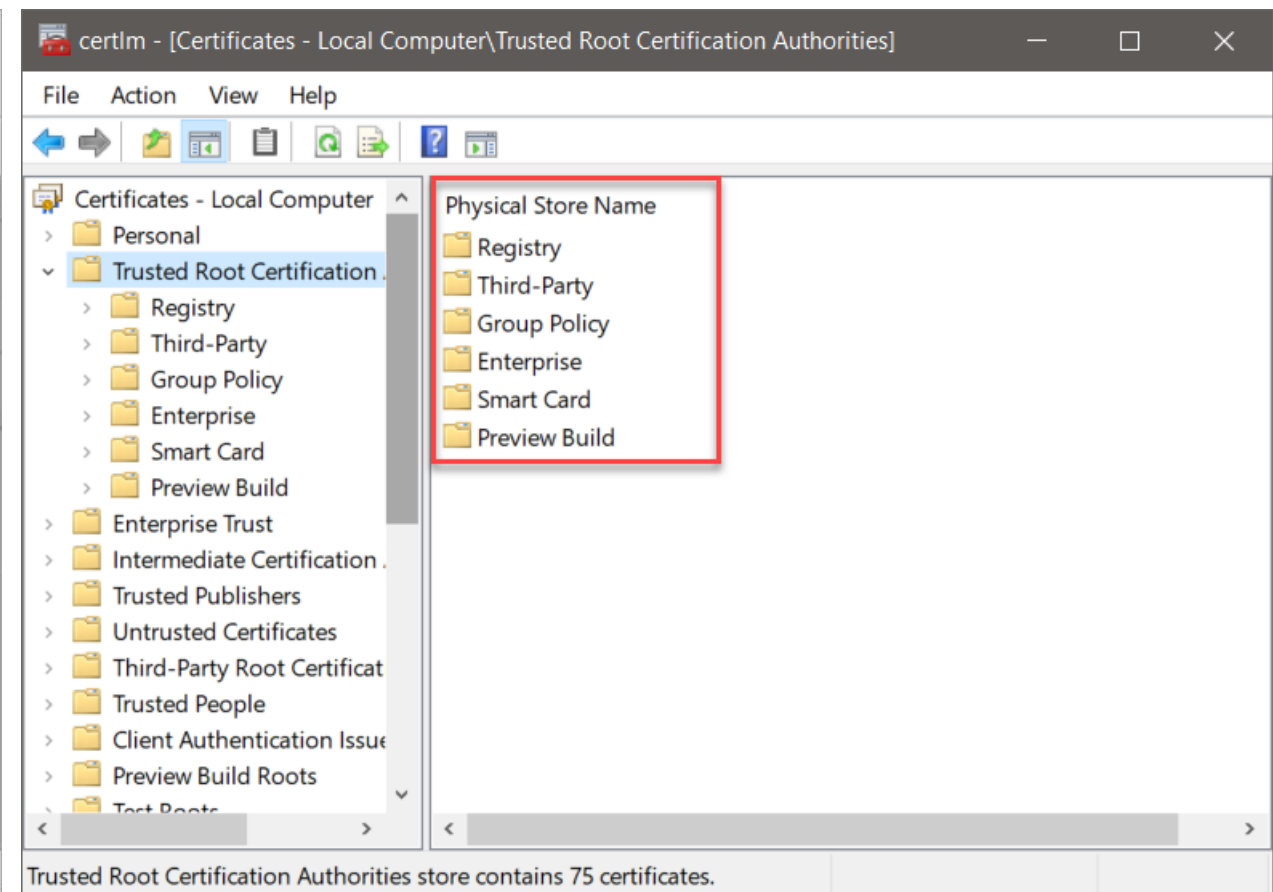
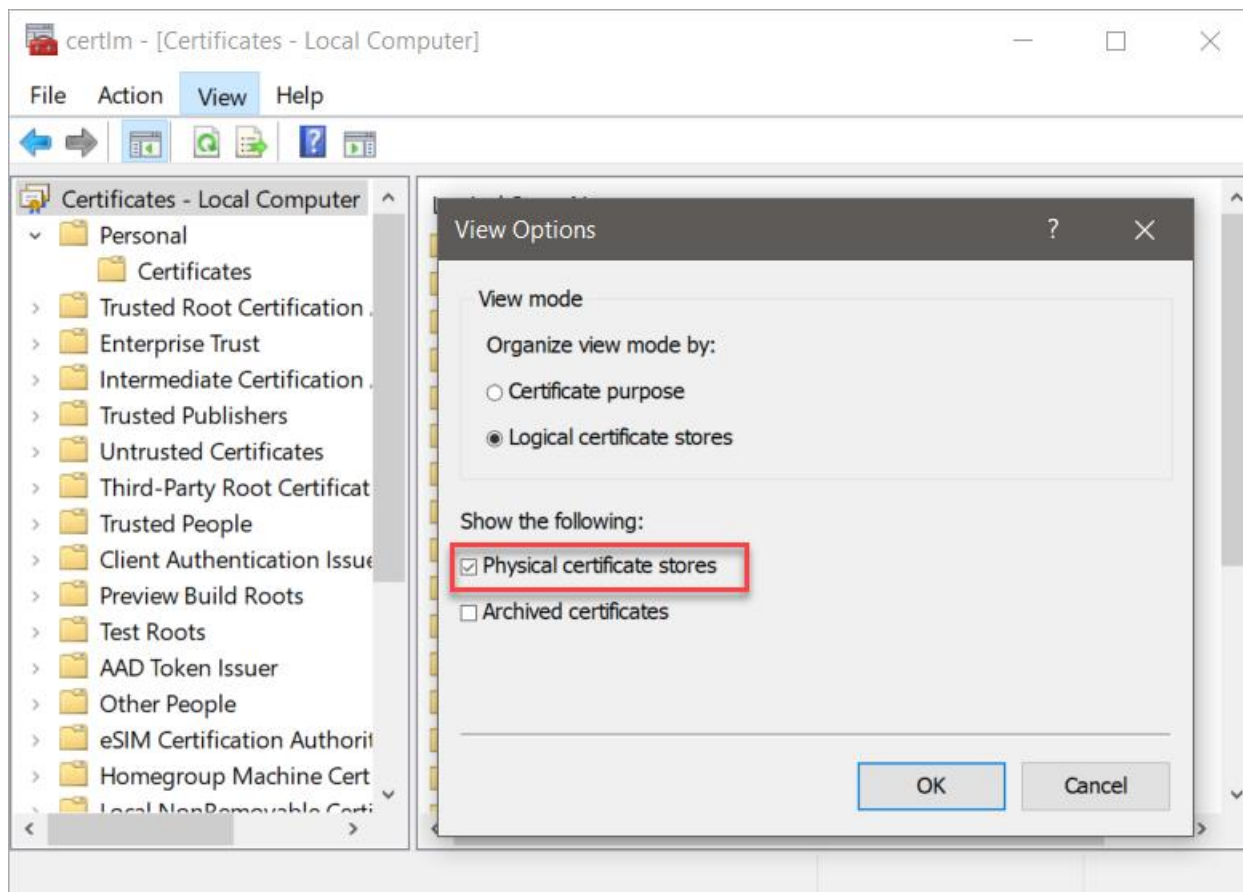
Certificate Stores

- Certificates saved in **physical stores**
- **Logical system store** is a collection of one or more physical stores
- MMC (certmgr.msc for current user or certlm.msc for local computer)
Display the logical view of each store by default



Certificate Stores (cont.)

- You can switch the view to display the physical stores by
 - (View->Options -> Check 'Physical certificate stores')

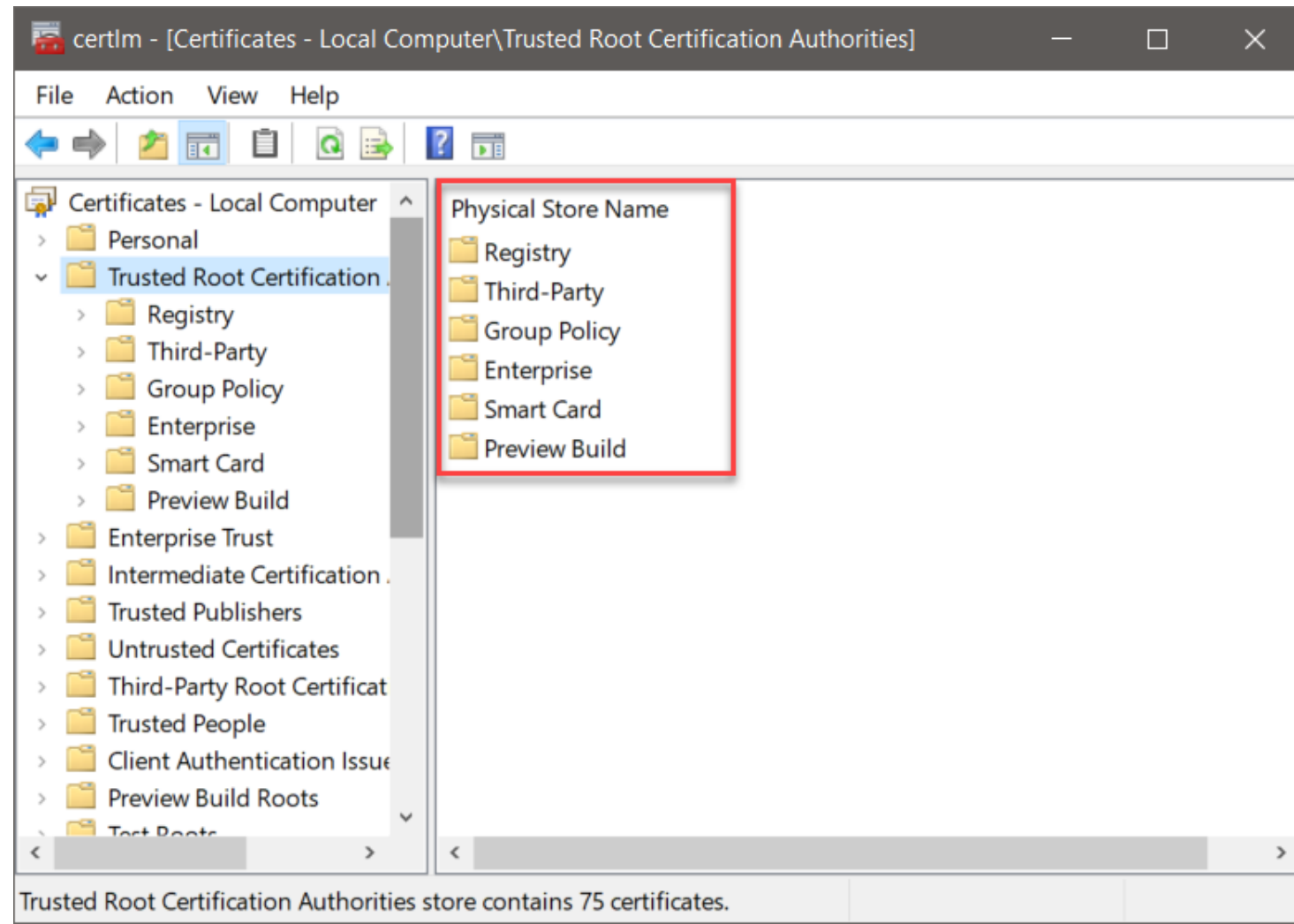


Certificate Stores (cont.)

- There are many physical stores available, including:

- Registry
- Local Computer (Hard Drive)
- Smart Card
- Enterprise
- Group Policy

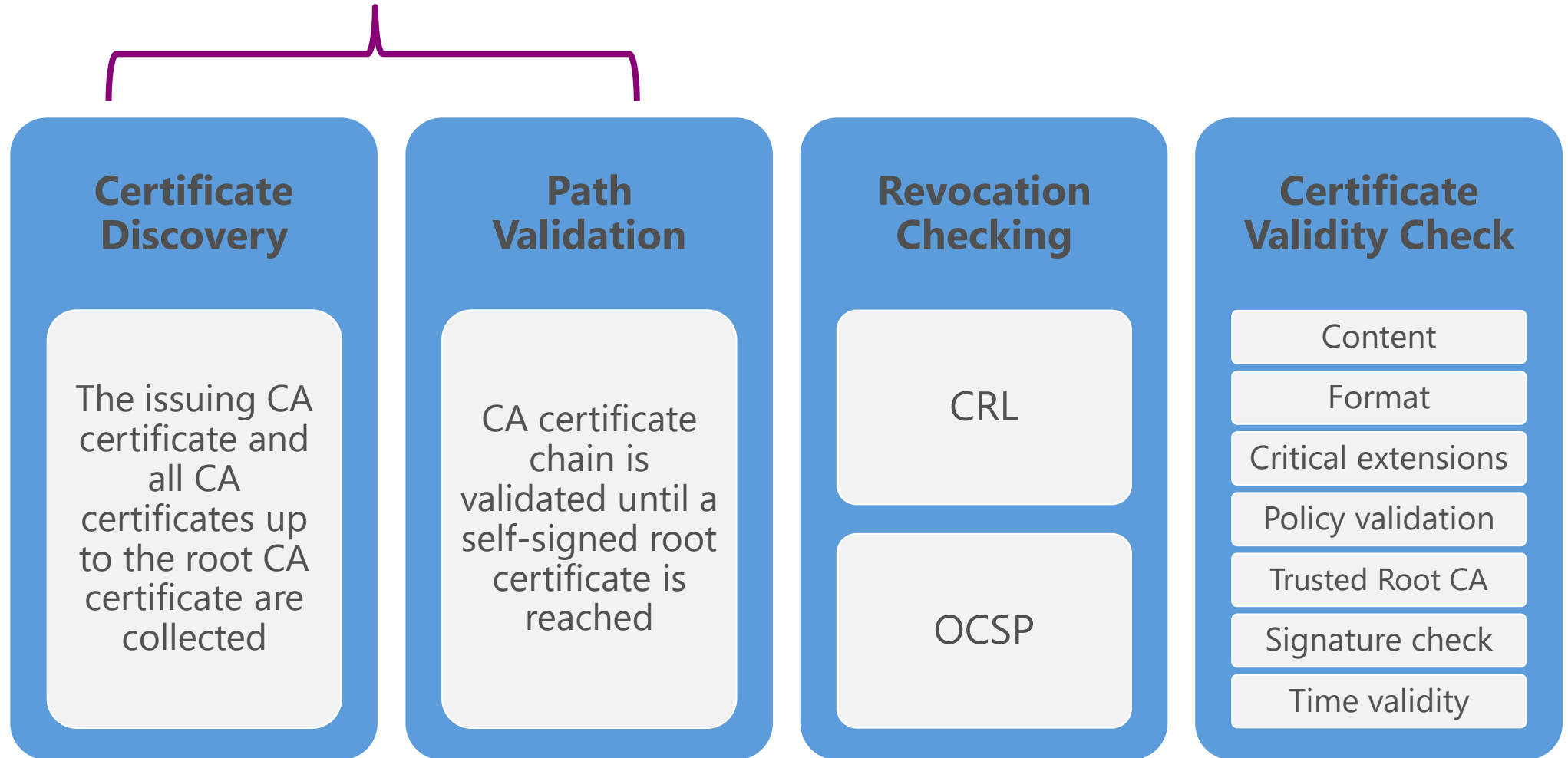
- Can be used for troubleshooting scenarios to easily identify certificate's source



Certificate Verification and Chain Building

The Pillars of Certificate Verification

Building the Certificate Chain



Trusted Root Certificates

- Root certificates are self-signed certificates issued to CAs
- Designated as trustworthy
- Trusted by adding them to a trusted root store (Trusted Root Certificate Authorities)



Subject: RootCA
Issuer: RootCA

Trusted Certificates Sources

Microsoft Root
Certificate Program
(installed with OS)

Installed from
Certification Authorities
AD container
(via GPO processing)

Installed from GPO
(Public Key Policies)

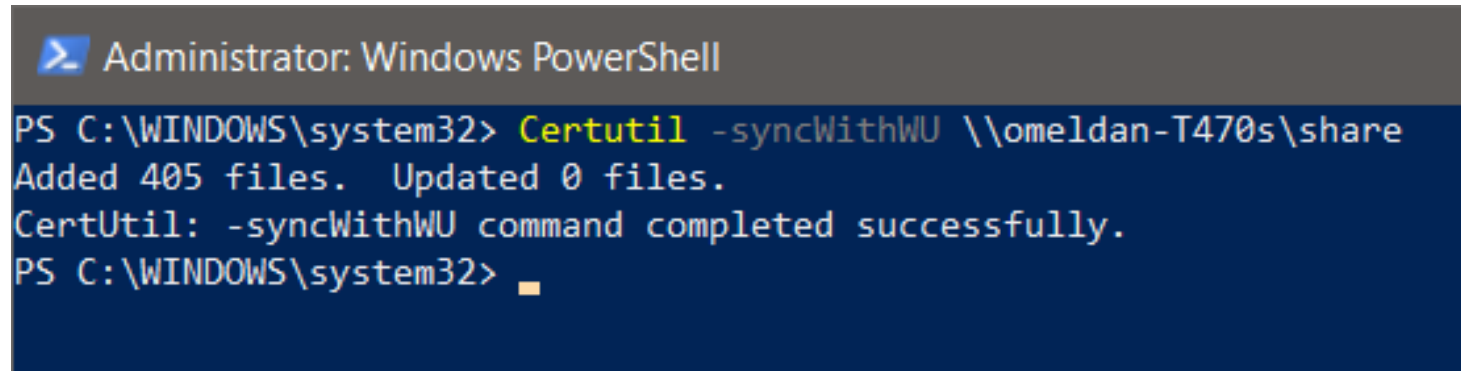
Other methods: MDM,
SCCM, scripts

Manually installed in
Computer's or User's
Trusted Root Store



Microsoft Root Certification Program

- The Microsoft Trusted Root Certificate enables trusted (and untrusted) root certificates to be downloaded from Windows Update servers and distributed automatically in Windows
- Can be downloaded manually using **Certutil -syncWithWU \\<Server>\<Share>**

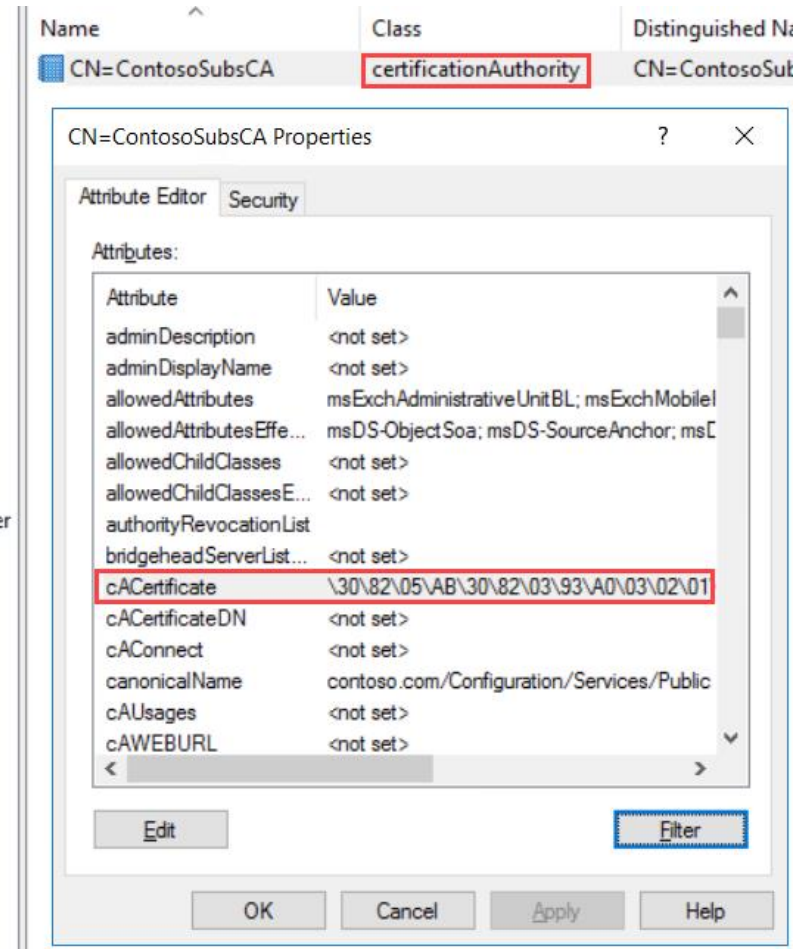
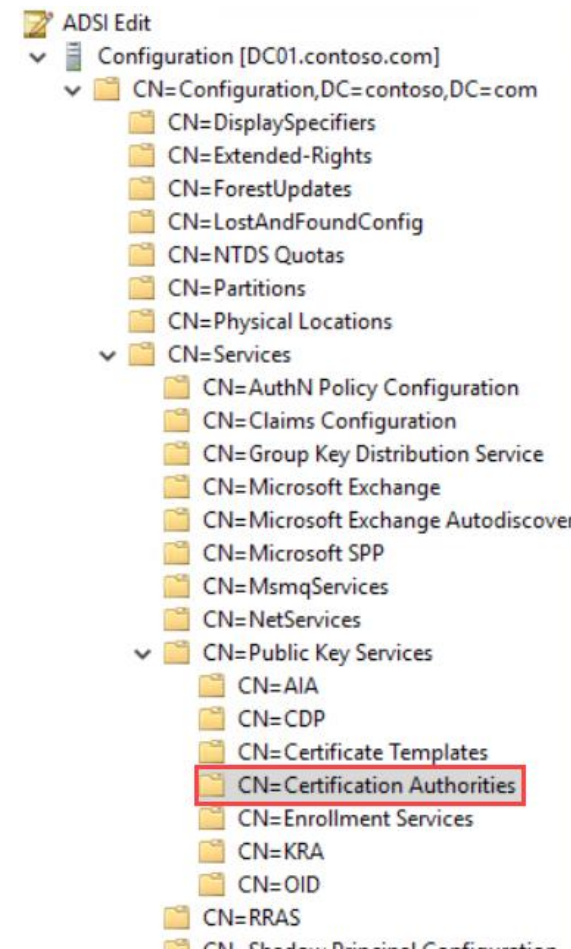


```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Certutil -syncWithWU \\omeldan-T470s\share
Added 405 files. Updated 0 files.
CertUtil: -syncWithWU command completed successfully.
PS C:\WINDOWS\system32>
```

- Microsoft Automatic Update URL can be changed for a disconnected environments using GPO and registry ([link](#))

"Certification Authorities" AD container

- "Certification Authorities" container contains 'certificateAuthority' objects
- CA certificates are written under 'cACertificate' attribute

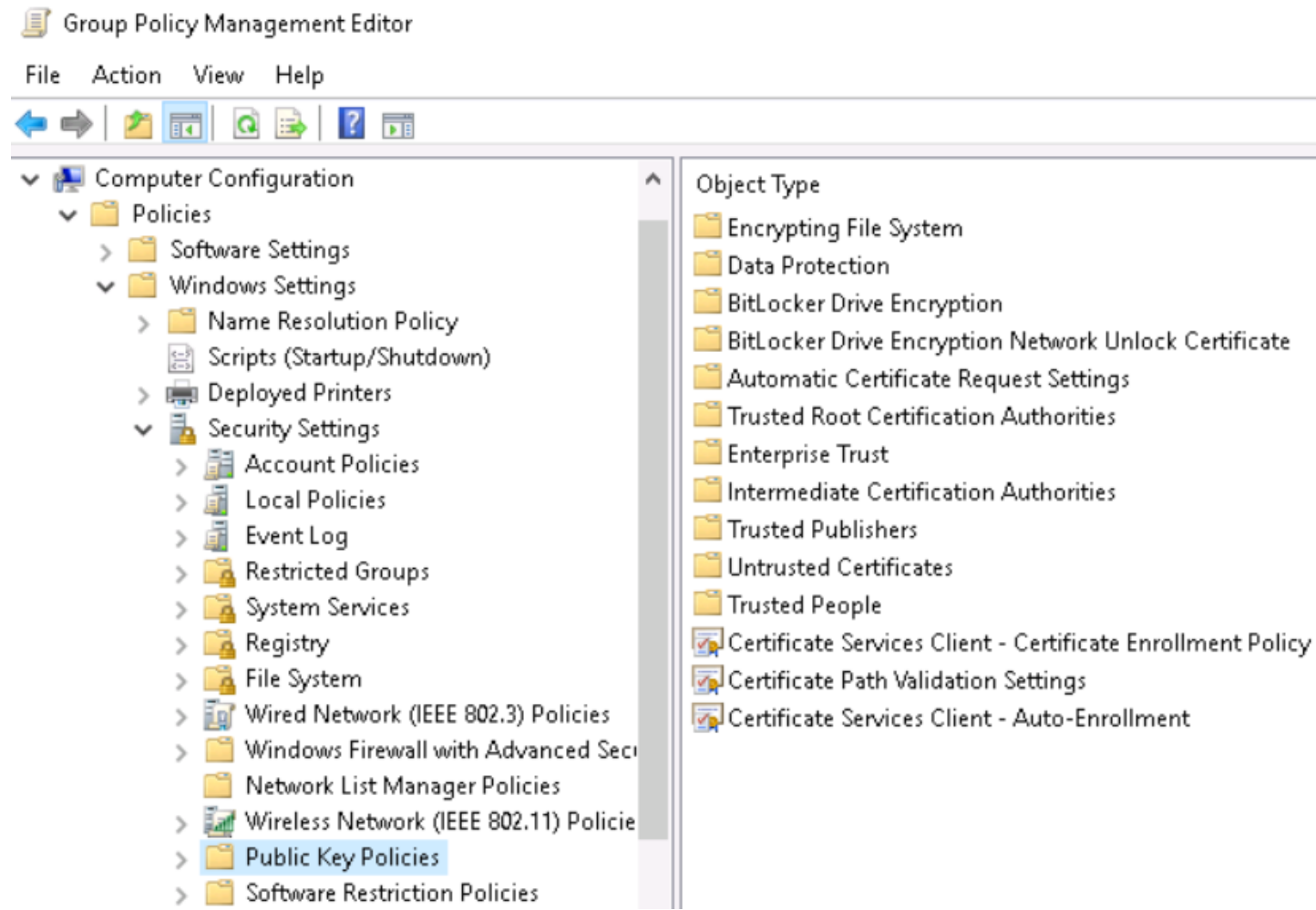


"Certification Authorities" AD container

- Certificates under "Certification Authorities" container are automatically deployed to Windows clients as part of Group Policy processing and saved under the Trusted Root Certification Authorities container
- Enterprise CA certificates are automatically installed to this container
- Root CA certificate can be installed manually using the command "Certutil -dspublish -f <PathToCertFile.cer> RootCA"

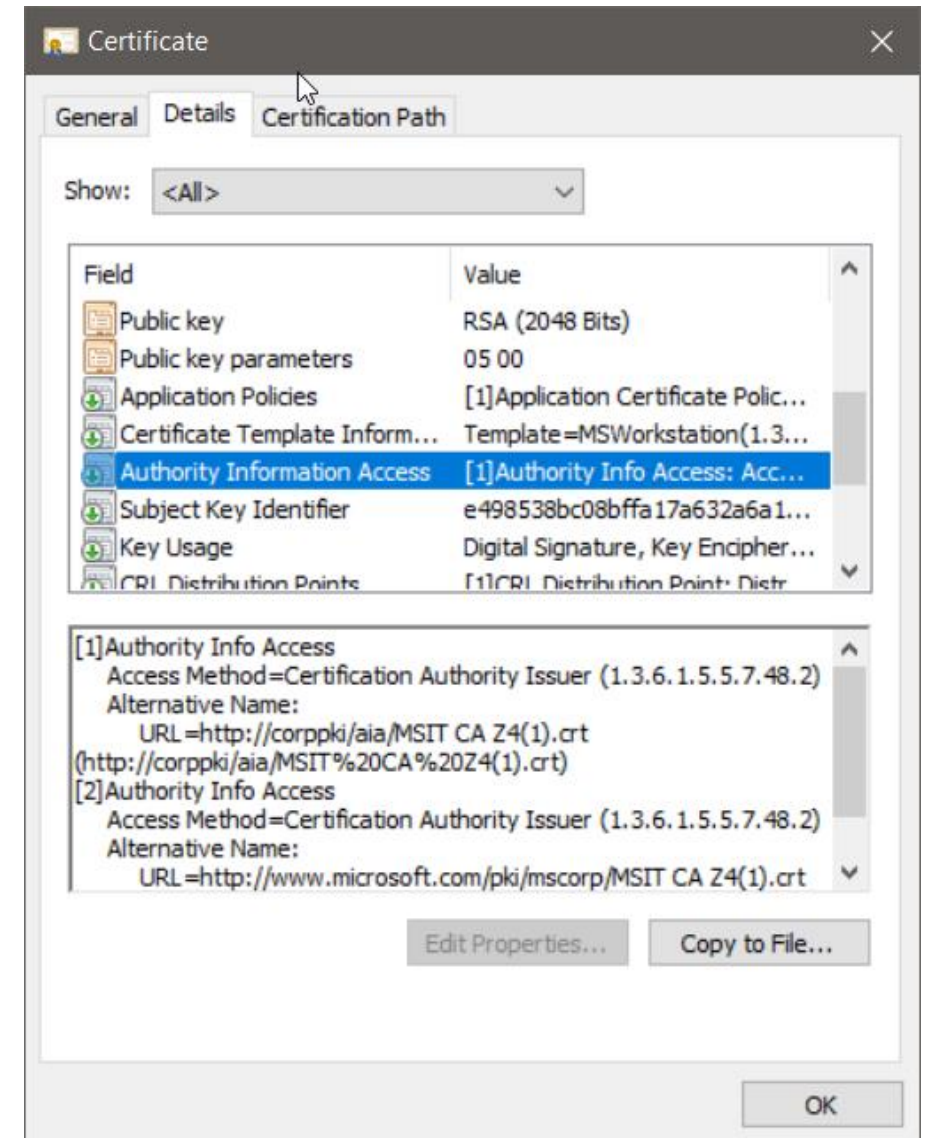
Group Policy

- Group Policy can be used to distribute certificates to different locations, as shown in the screenshot below:



Authority Information Access (AIA)

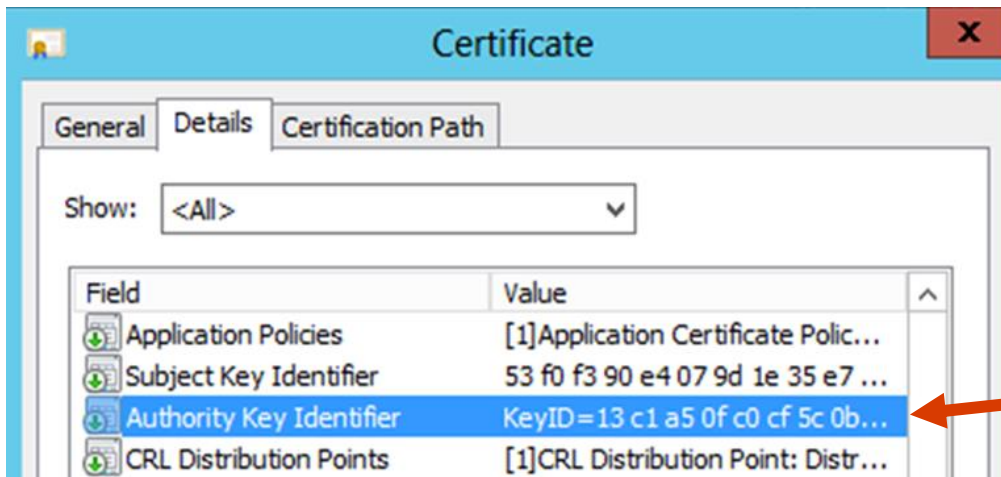
- The AIA (Authority Information Access) extension indicates how to access CA information (CA certificate) and services (OCSP)



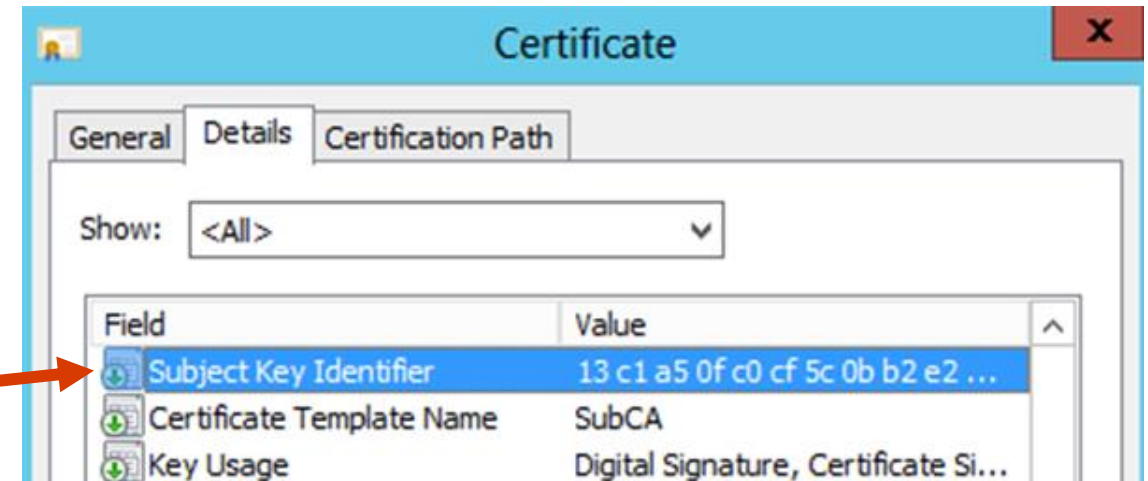
Chain Building: Arranging Certificates

- **AKI** (Authority Key Identifier) and **SKI** (Subject Key Identifier) extensions are used by the chaining engine to determine what certificate was used to sign a presented certificate
- By default, hash of the public key is used

End-Entity Certificate

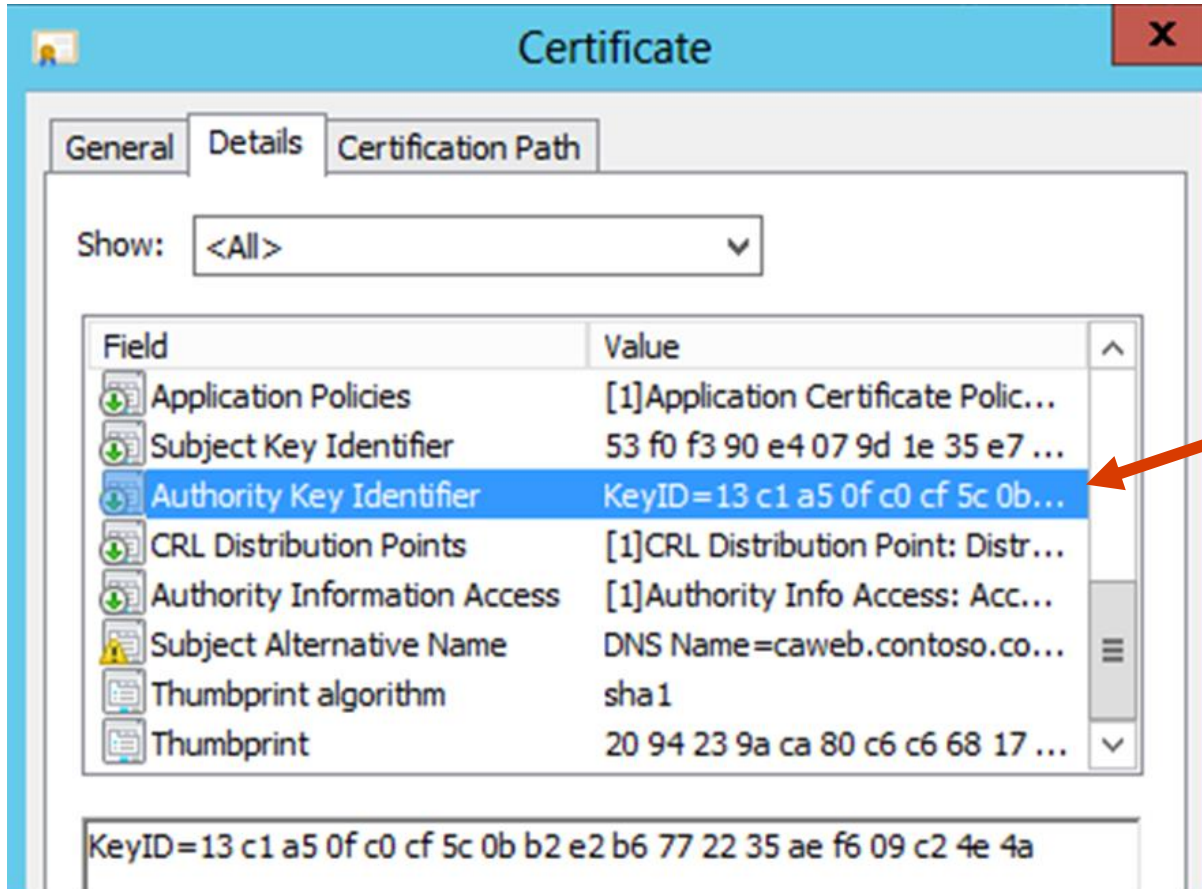


Issuing CA Certificate

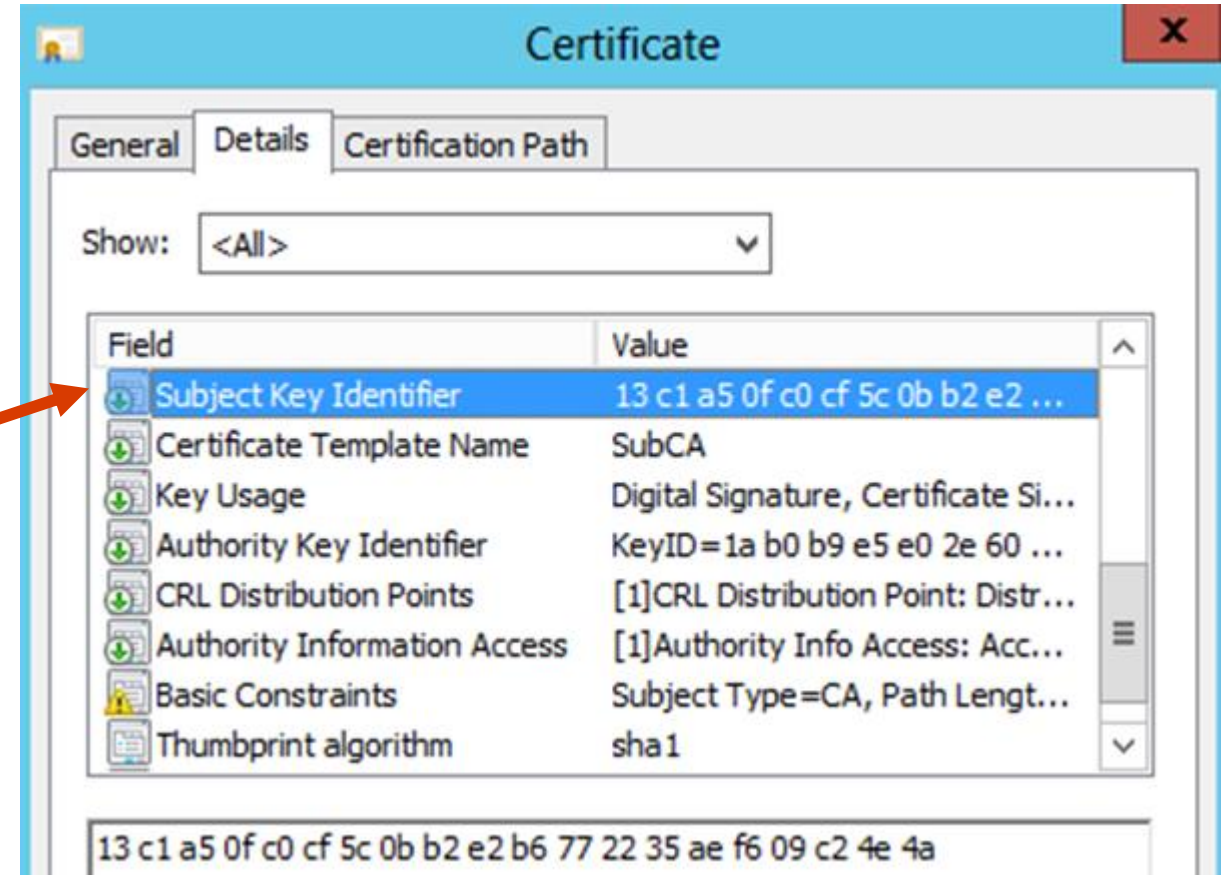


Chain Building: Arranging Certificates

End-Entity Certificate



Issuing CA Certificate



AKI in End-Entity certificate matches SKI in Issuing CA certificate



Lesson Review

Question 1:

AIA is one of the certificate extensions. What does it stand for and what its purpose?

AIA stands for Authority Information Access. It used to indicate how to access the CA services, including the CA certificate.

Question 2:

What is the preferred locations for certificates when building certificate chain?

Cached and local certificate store.

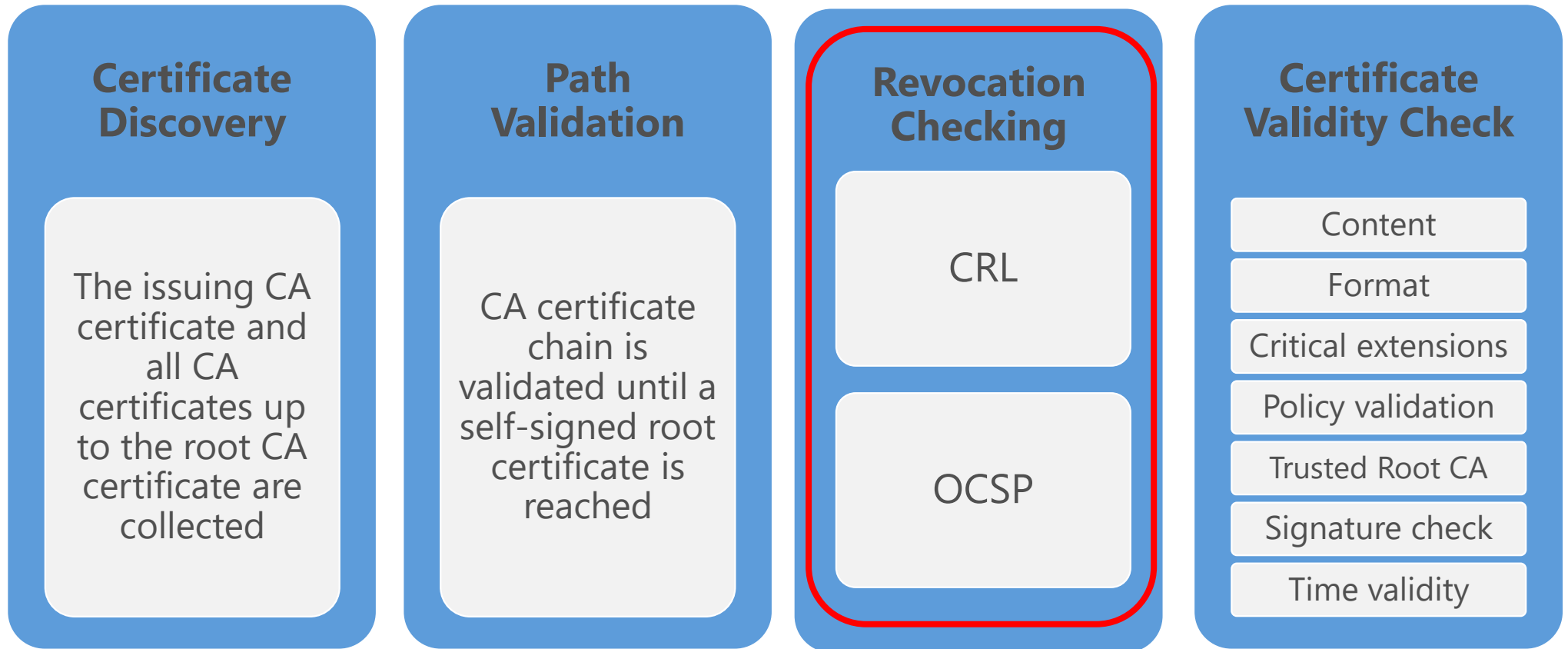
Question 3:

To build the certificate chain, which two attributes must match?

AKI (in issued certificate) must match SKI (in issuer certificate)

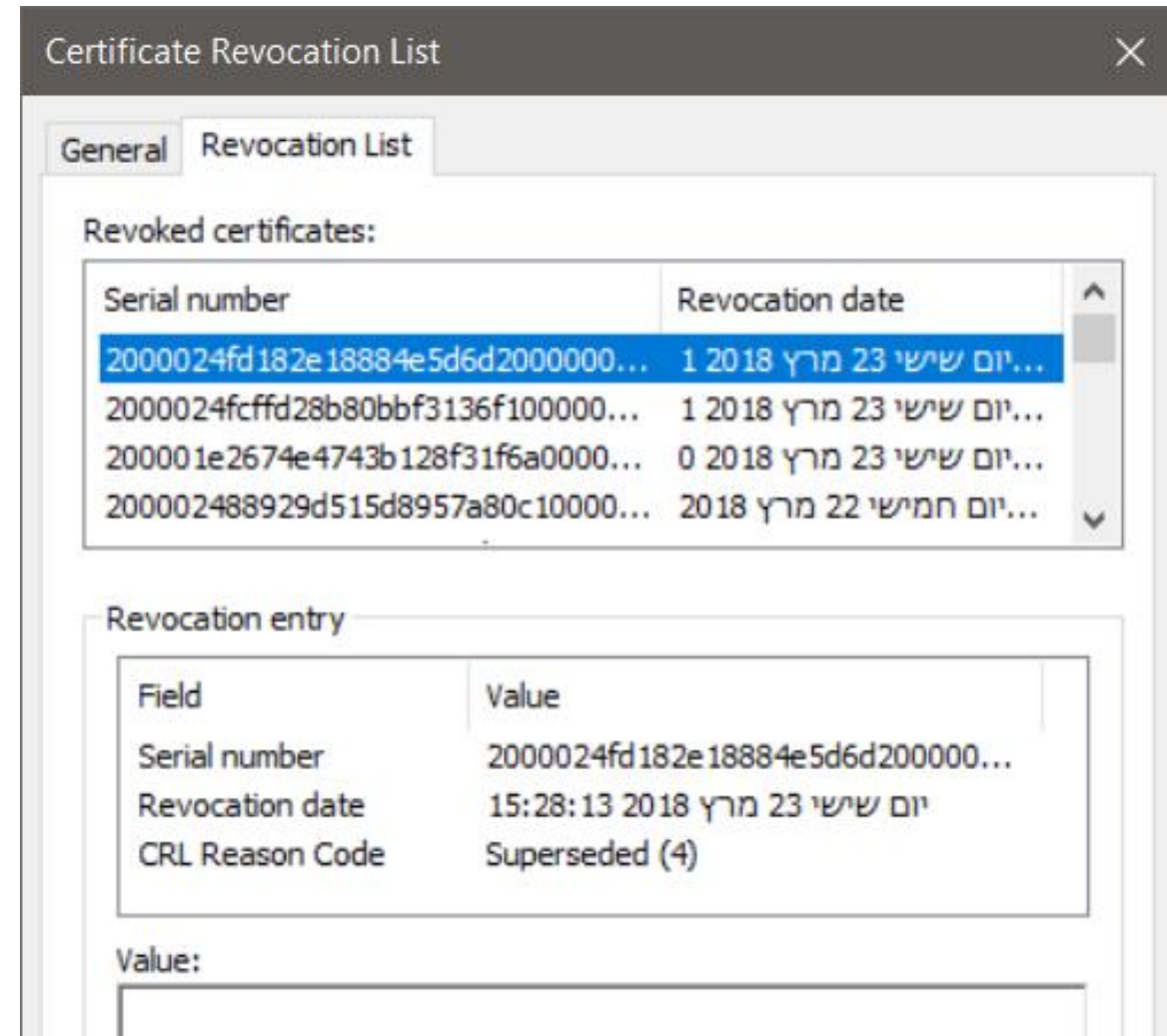
Certificate Revocation Lists (CRLs)

The Pillars of Certificate Verification



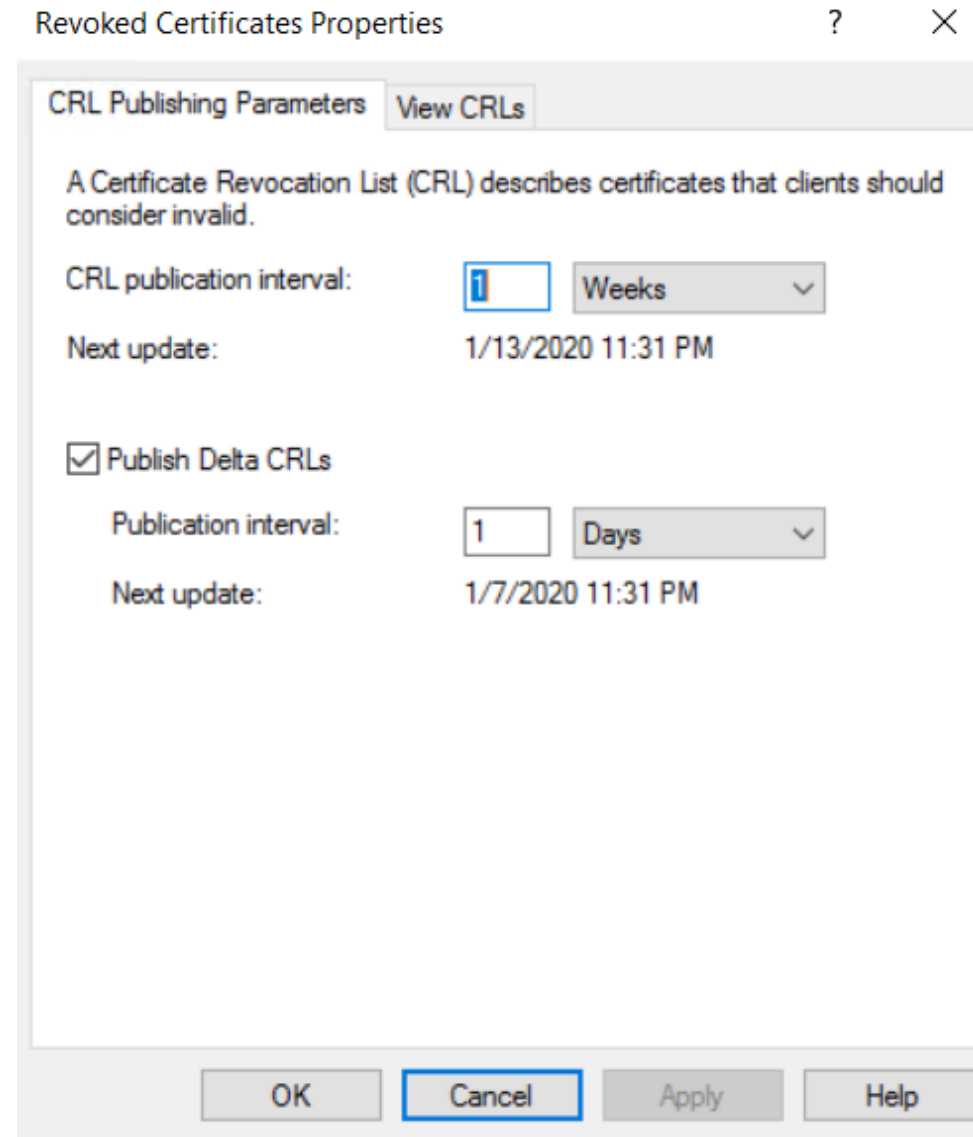
CRL Definition

- A CRL is a digitally signed list including information of all the certificates which have been revoked for a specific CA
- Applications or systems can perform CRL checking to determine a presented certificate's revocation status



CRL Publishing

- Generated and published periodically (every 1 week by default)
- The CA publishes the CRL to the local filesystem but can also publish it to a publicly accessible location



CRL Check

- CRL verification depends on application's settings:
 - Behavior might be hardcoded / Controlled and managed by the administrator

Certificate Revocation List Configuration

Download CRL: ☐

CRL Distribution URL:

Retrieve CRL: ☒ Automatically 5 Minutes before expiration.
☐ Every 1 Hours

If download failed, wait 10 Minutes before retry.

Bypass CRL Verification if CRL is not Received: ☐

Ignore CRL Expiration: ☐

⚠ = Required fields

Client Certificate Validation Session Resumption Advanced Server Settings

Enable CRL Checking: ☐

Retrieval Timeout: 5 seconds

Expiration Grace Period: 0 seconds

Allow Missing CDP Attribute: ☒

☐ CRL Cache Timeout Period: 168 hours

Default LDAP Server Name:

Verify that Client Certificates are published to user accounts (Active Directory accounts and EAP-TLS only) ☐

CRL Validity

- **Effective date**

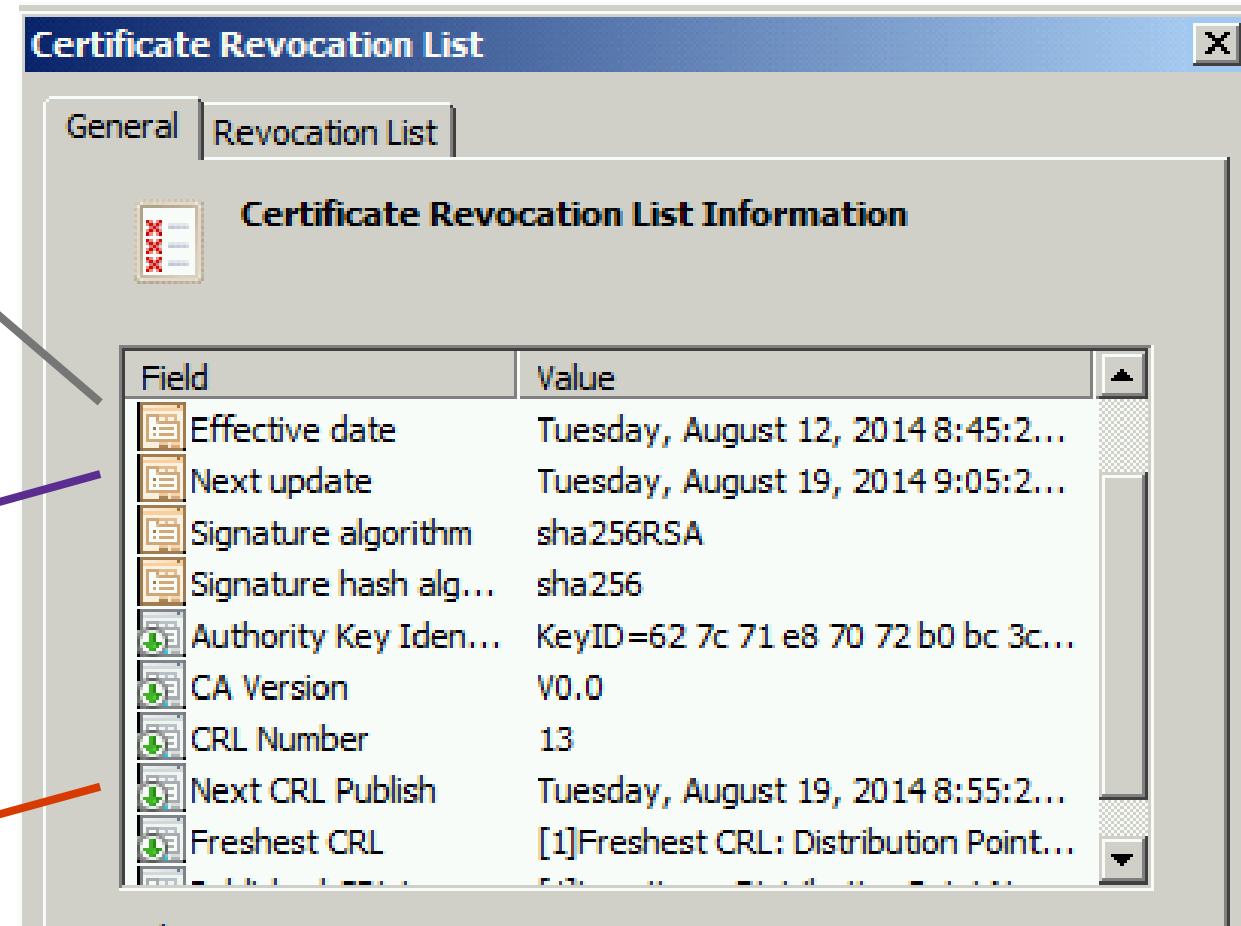
Indicates the start of CRL validity. Back-dated by 10 minutes by default (can be controlled using 'ClockSkewMinutes' registry key)

- **Next update**

Indicates time when this CRL expires and becomes invalid

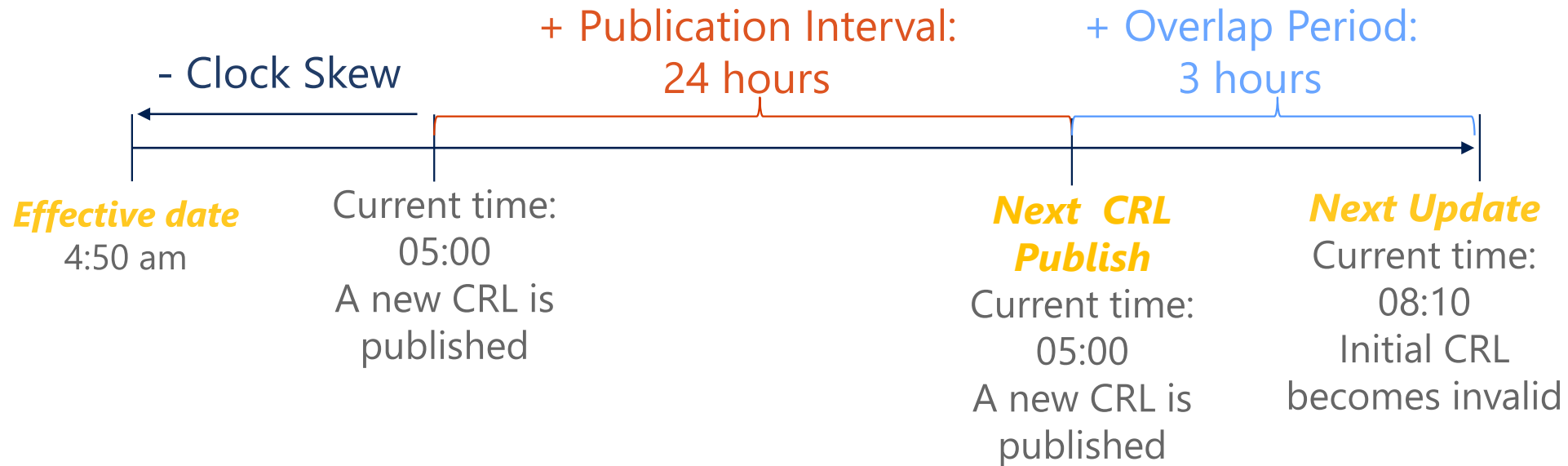
- **Next CRL Publish**

Indicates at which time a new CRL will be published by the CA



CRL Overlap Period

- CRL overlap used to ensure that a new CRL is available before the first CRL is expired



CRL Overlap Period (Cont.)

- CRL overlap period can be configured using:
 - Certutil -setreg CA\CRLOverlapUnits 12
 - Certutil -setreg CA\CRLOverlapPeriod "Hours"

Administrator: Windows PowerShell

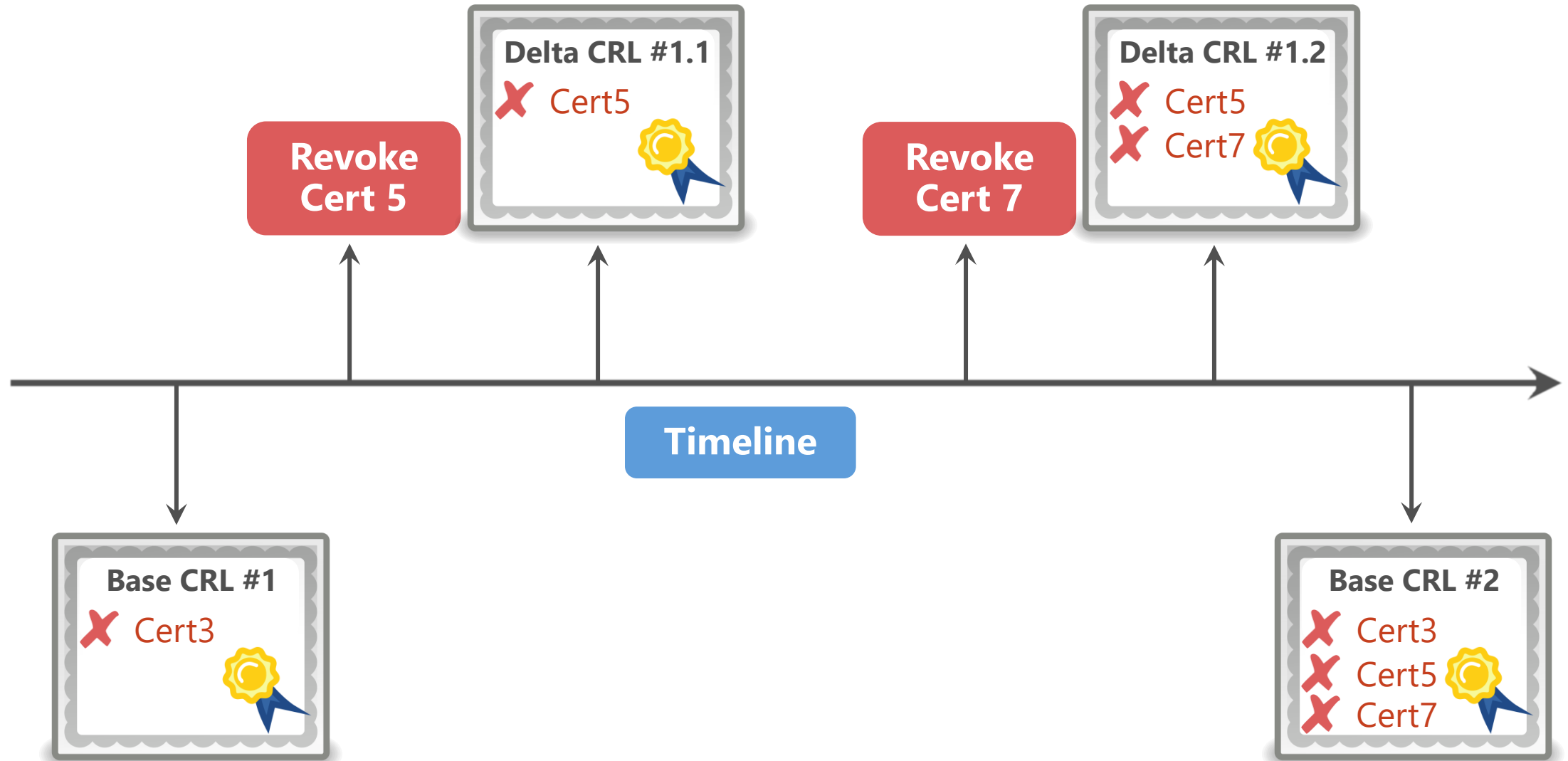
```
[casub01]: PS C:\> certutil -setreg CA\CRLOverlapPeriodUnits 12
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\SubCA\CRLOverlapPeriodUnits:
New Value:
    CRLOverlapPeriodUnits REG_DWORD = c (12)
Certutil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
[casub01]: PS C:\> _
```

- Even if the overlap registry keys are not set for base CRLs, a default overlap value of 10% of the CRL's lifetime is used
- Overlap periods can never exceed the configured validity time

Delta CRLs

- Delta CRLs contain the list of revoked certificates since the last base CRL issuance
- Version 2 of the CRL introduced the concept of Delta CRLs, which are differential revocation lists published on a more regular basis than the (base) CRL
- Keep in mind that a valid copy of both (delta and base CRL) must be available to perform a successful revocation check
- in a Windows CA, the delta CRL is published with the same name as the CRL with a "+" appended

Delta CRLs – How CRLs are published





Lesson Review

Question 1:

Assume that Delta CRLs are implemented for a CA, but for some reason a new Delta CRL cannot be published.

However, as the Base CRL is still valid, the CA administrator feels safe because he is quite sure that PKI clients will use the Base CRL for revocation check.

True or False?

It depends on the client/application. For clients understanding the Delta CRL extension, the revocation will be failed.



Lesson Review

Question 2:

You configured the following settings on your Issuing CA:

CRL publication interval= 16 hours

Overlap period = 8 hours

At 08:00, the CA issues a new CRL.
one hour later, the CA crashes.

At which time and day will you be in a deep trouble (unless you manage to restore normal operation)?

After 24 hours, at 08:00 next morning (08:10 if we would like to include the default time skew as well)

Designing and Configuring CDP Locations

Overview

- CDP (CRL Distribution Point) – Location accessible by clients to download CRL
- The CDP repositories can be either LDAP, HTTP or UNC
- If a time-valid object is not found in the cache, the network retrieval process starts
- Availability and validity of revocation information is crucial for a PKI

LDAP vs HTTP

- When publishing on HTTP and LDAP path, the order IS important
- Attempt to use a HTTP location that can be accessed both internally and externally
- Keep in mind that a certificate and CRL containing an AD LDAP path leaks the internal domain name when being used on the Internet

LDAP CDP Pros	HTTP CDP Pros
Replication to any DC in the forest: <ul style="list-style-type: none">• High-availability• Site-awareness	<ul style="list-style-type: none">• Compatible with most 3rd party products• Anonymous download possible• Can be published on the Internet easily• Firewall and proxy friendly

Aggressiveness vs. Manageability

- Short (Delta) CRL validity periods
 - Allows more aggressive revocation information publishing.
 - Requires more careful monitoring and disaster recovery/mitigation planning when a CRL cannot be provided in time.
- Long (Delta) CRL validity periods
 - May give the PKI admins a false sense of comfort regarding high availability of revocation information.

Revocation Cache

Disk Cache

- Maintains copies of all CRL and OCSP responses retrieved
- Items are maintained until their validity period expires
- Every user (including System, Network Service and Local Service) has his own disk cache
- Disk locations on Windows:
 - Per User: C:\Users\Username\AppData\LocalLow\Microsoft\CryptnetUrlCache
 - Per Computer: C:\Windows\System32\Config\SystemProfile\AppData\LocalLow\Microsoft\CryptnetUrlCache

View and Flush Disk Cache

- To view the contents of the disk cache
 - `certutil -urlcache crt`
 - `certutil -urlcache ocsp`
- To flush the disk cache:
 - `certutil -urlcache crt delete`
 - `certutil -urlcache ocsp delete`
 - `certutil -urlcache * delete`
- These commands will flush the disk cache of whoever's security context they are running in.

Memory Cache

- Contains revocation information used by a specific process
- Maintained within the memory used by the calling process
- When the process terminates, the memory is released, and the memory cache is flushed
- To immediately invalidate all items from the memory cache:
`certutil -setreg chain\ChainCacheResyncFiletime @now`

Pre-fetching

- Pre-fetching enables a CryptoAPI client to download updates to revocation information used previously to validate certificates before they are needed.
- Pre-fetching was implemented to improve the performance of revocation checking.
- Pre-fetching only writes the revocation information to the file cache. It does not influence the application's in-memory cache.



Lesson Review

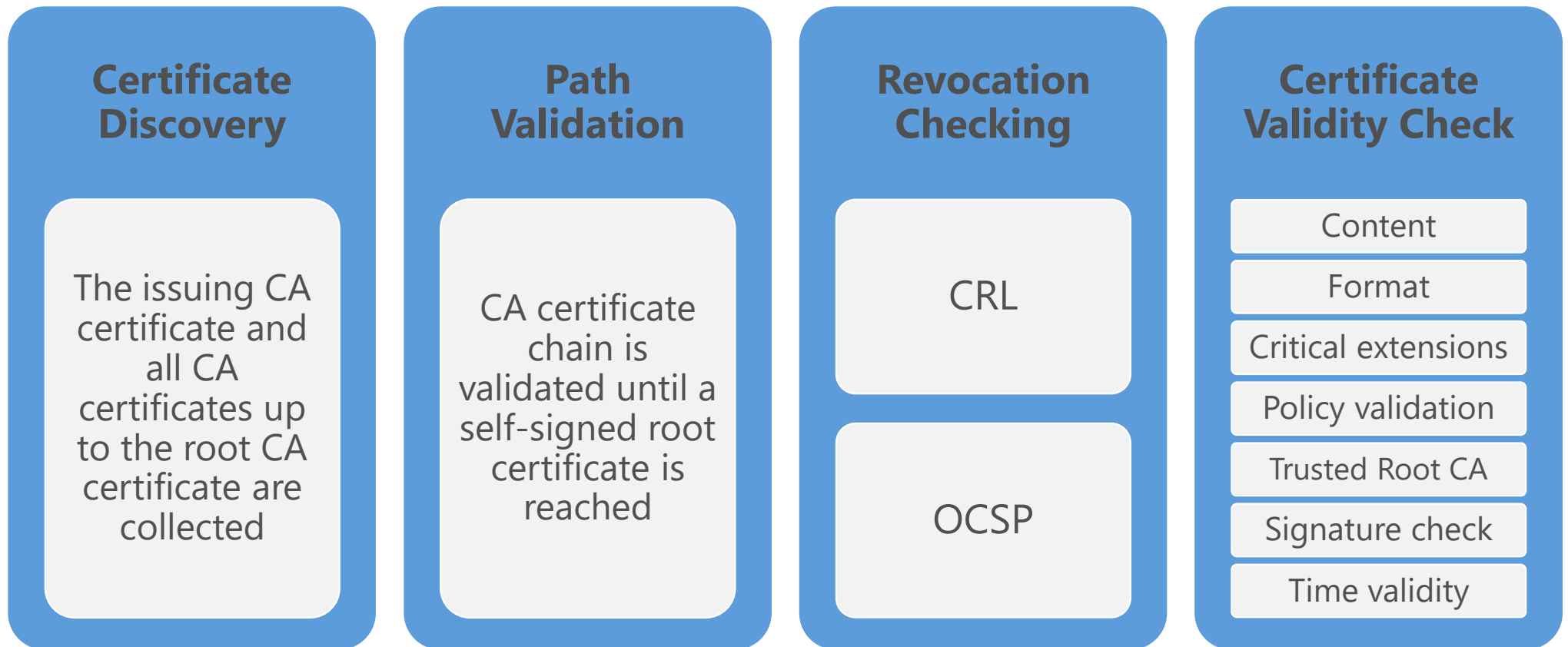
Question 1:

What is the major advantage of HTTP CDP over LDAP?

HTTP CDP does not require authentication and limit the exposure of internal namespace.

Online Certificate Status Protocol (OCSP)

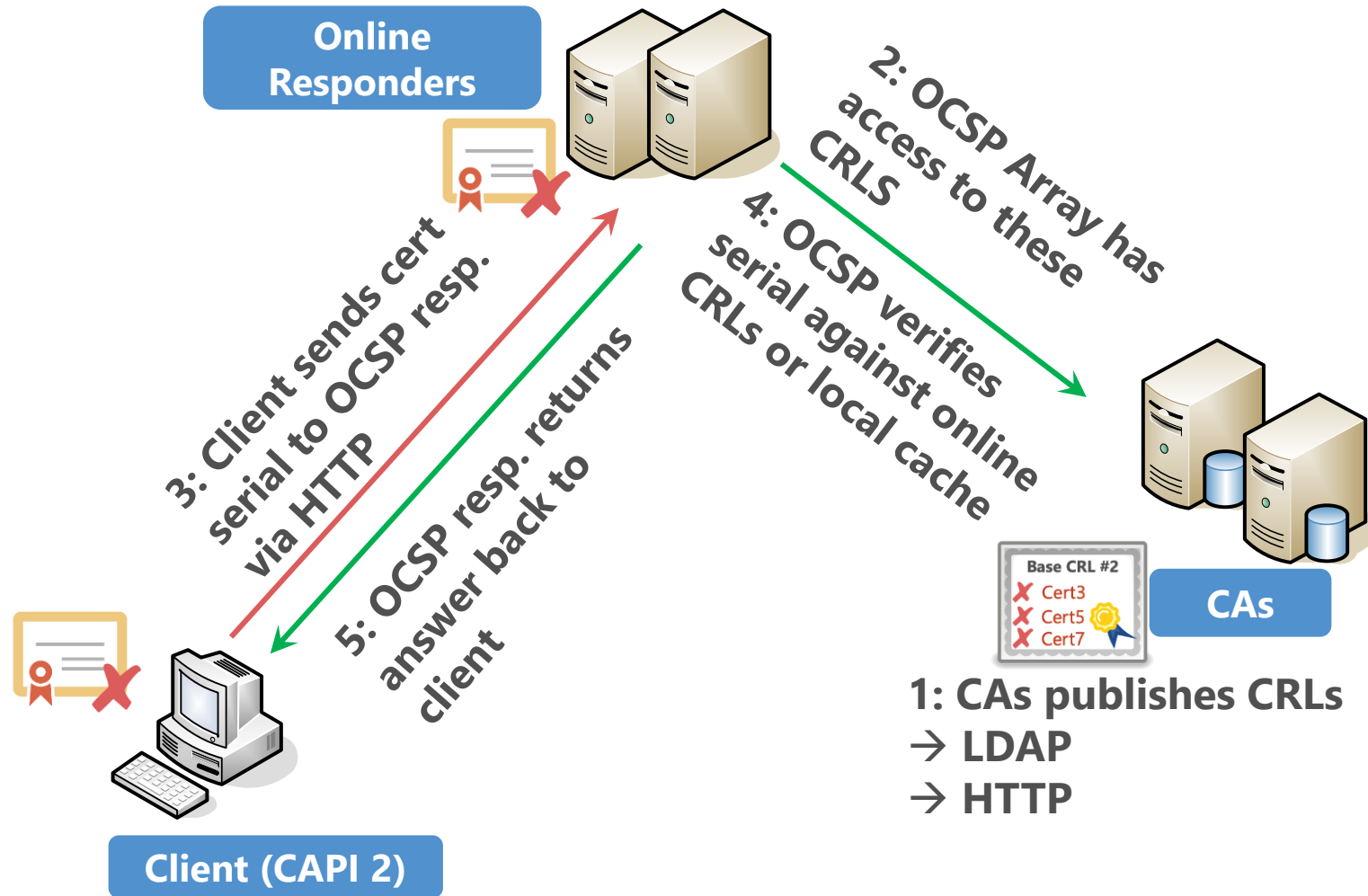
The Pillars of Certificate Verification



OCSP in a Nutshell

- OCSP stands for Online Certificate Status Protocol
- OCSP client sends HTTP or HTTPS request to OCSP responder to get revocation status for a specific certificate by providing its serial number
- OCSP responder replies with a signed response that includes the revocation status of the requested certificate, based on its cached knowledge from the CRL issued by the CA
- OCSP client validates the signature of the response prior to accepting and caching it

OCSP Mechanics



Troubleshooting

Troubleshooting Revocation Issues

Revocation Problem?

- Windows App/System Event Log
- Application-specific Log

Need more Details?

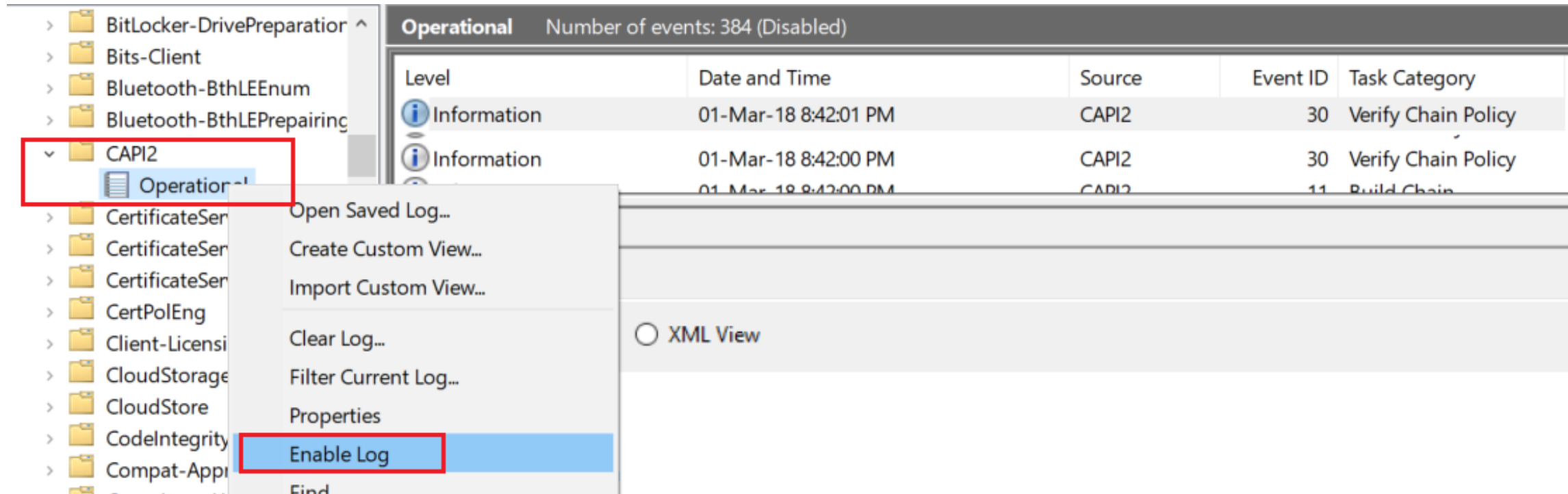
- Enable CAPI2 logging
- Certutil -verify [urlfetch] certfile.cer
- Certutil -url certfile.cer (GUI)

Unable to download?

- Proxy or Firewall between client and CDP/OCSP?
- User vs. system security context

CAP12 Logging

- Disabled by default
- Located in Event Viewer under:
Applications and Services > Microsoft > Windows > CAP12





Lesson Review

Question 1:

Is there a high availability option exist for OCSP Responder?

Yes, OCSP Array.

Question 2:

What does the command
`certutil -url certfile.cer` used for?

Open a GUI to verify certificate's CRL and AIA status



Module Summary

- Chain building and revocation checking
 - Chain building and validation
 - Revocation checking
 - Troubleshooting chain building and revocation checking
- CRLs
 - Base CRL's and delta CRL's
 - CRL overlap
 - CRL publication design principles
- OCSP Overview

