PKI
On
Windows Server 2012 R2
From Scratch

Sections at a Glance

- Overview of PKI
- Overview of Cryptography
- Certification Authority or CA
- Certificate Requests or Enrollment
- Configuring CA properties
- New Features of CA in Windows Server 2008 and onwards

Overview of PKI

What Is a PKI?

The combination of software, encryption technologies, processes, and services that enables an organization to secure its communications and business transactions

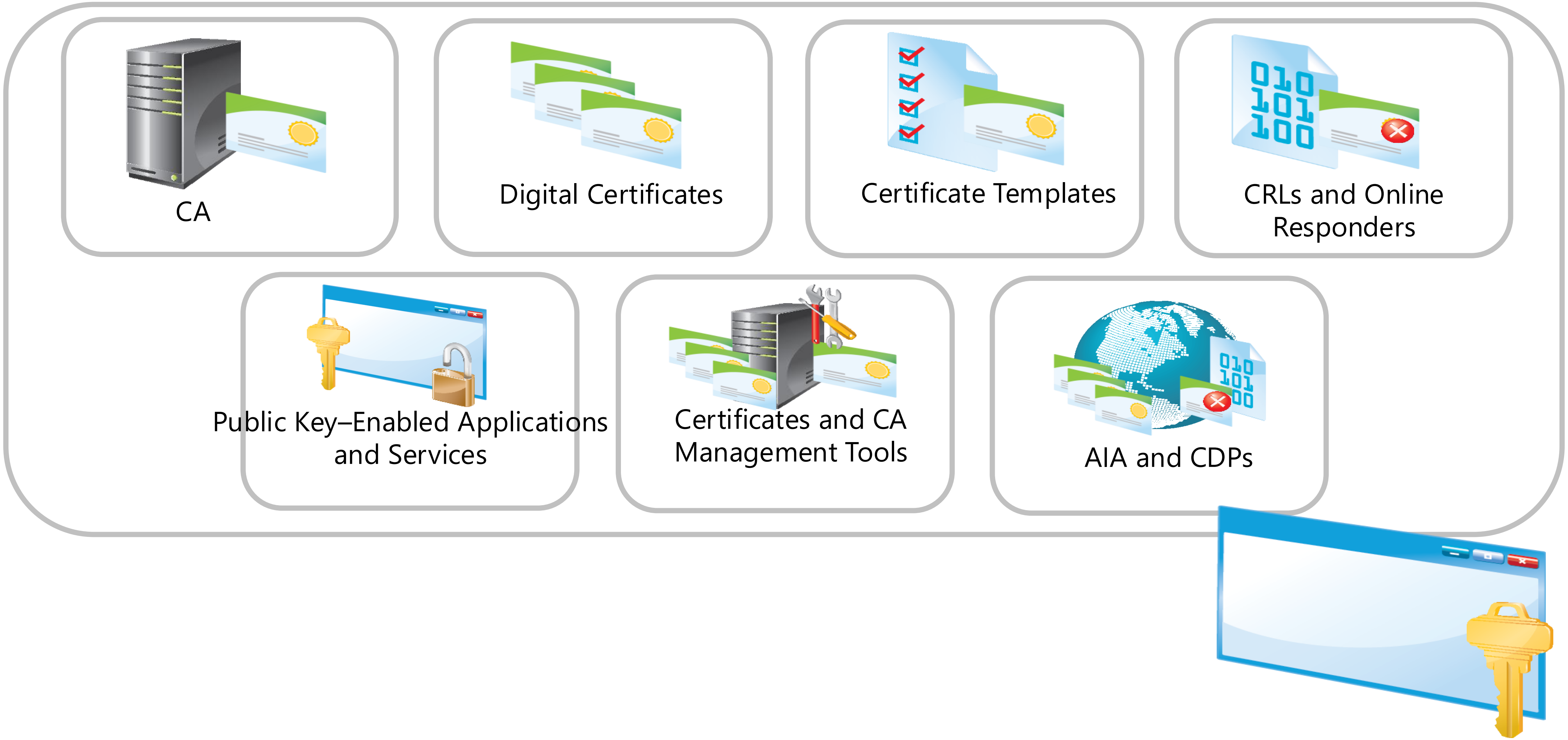
Requirement	PKI solutions
Confidentiality	Data encryption
Integrity	Digital signatures
Authenticity	Hash algorithms, message digests, digital signatures
Nonrepudiation	Digital signatures, audit logs
Availability	Redundancy

Uses of PKI?

- Client Server Authentication
- Signatures –
  - Drivers Signing
  - Emails
  - Tokens – ADFS

- Web Traffic (HTTPS)
- Encryption (Network Data, IPSec, EFS)
- Wireless
- Smart Cards

Components of a PKI Solution



CA

Digital Certificates

Certificate Templates

CRLs and Online Responders

Public Key–Enabled Applications and Services

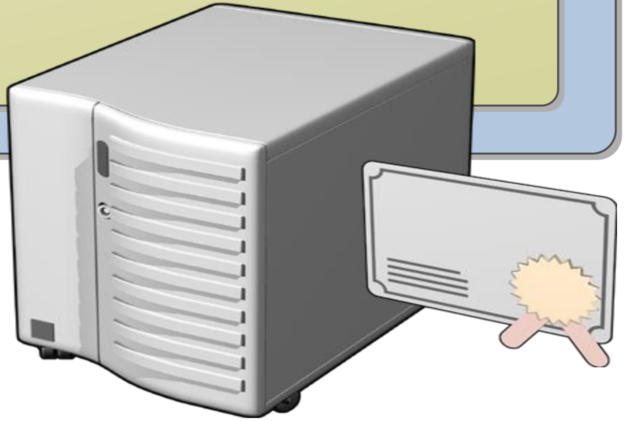
Certificates and CA Management Tools

AIA and CDPs

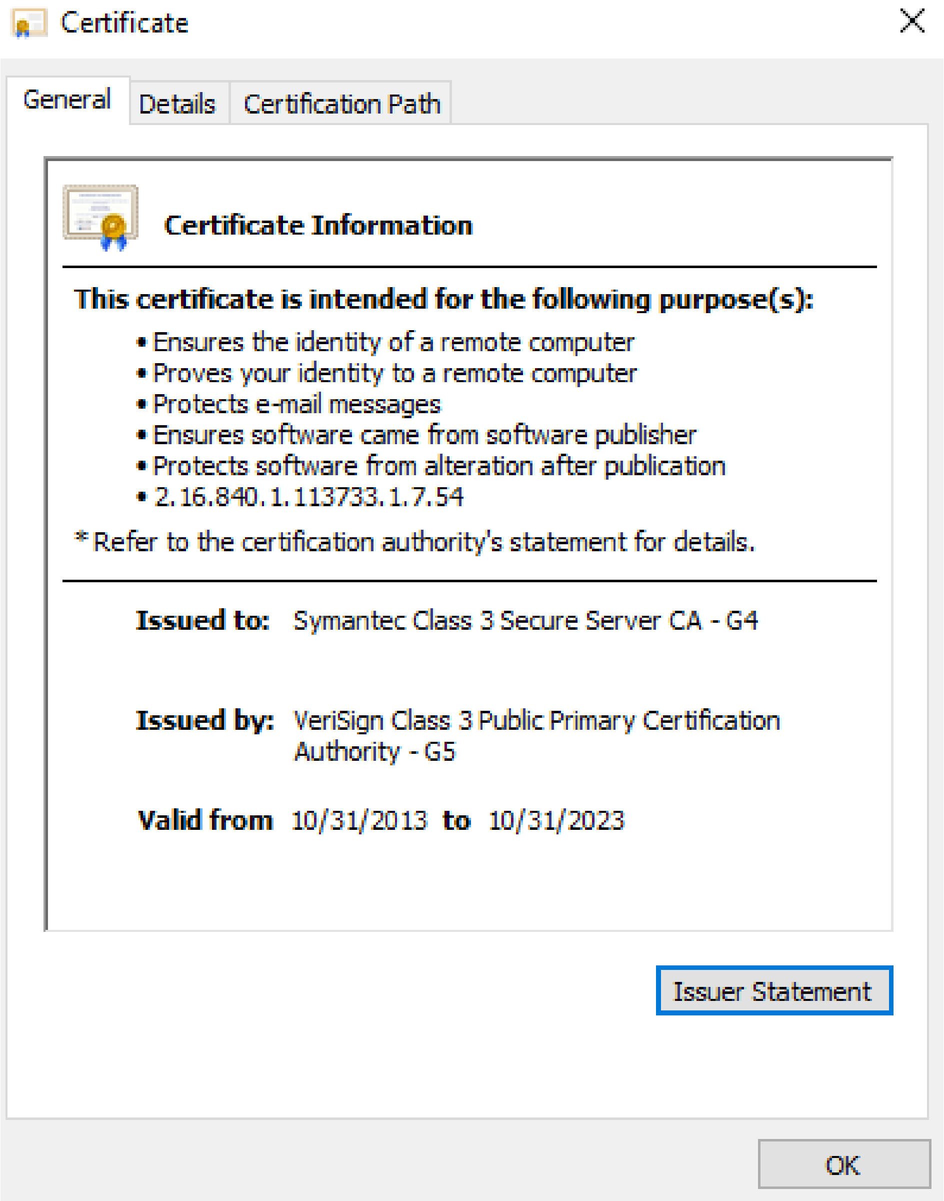
What Is a Digital Certificate?

A digital certificate:

- Verifies the identity of a user, computer, or program
- Contains information about the issuer and the subject
- Is signed by a CA



What Is a Digital Certificate?



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Protects e-mail messages
- Ensures software came from software publisher
- Protects software from alteration after publication
- 2.16.840.1.113733.1.7.54

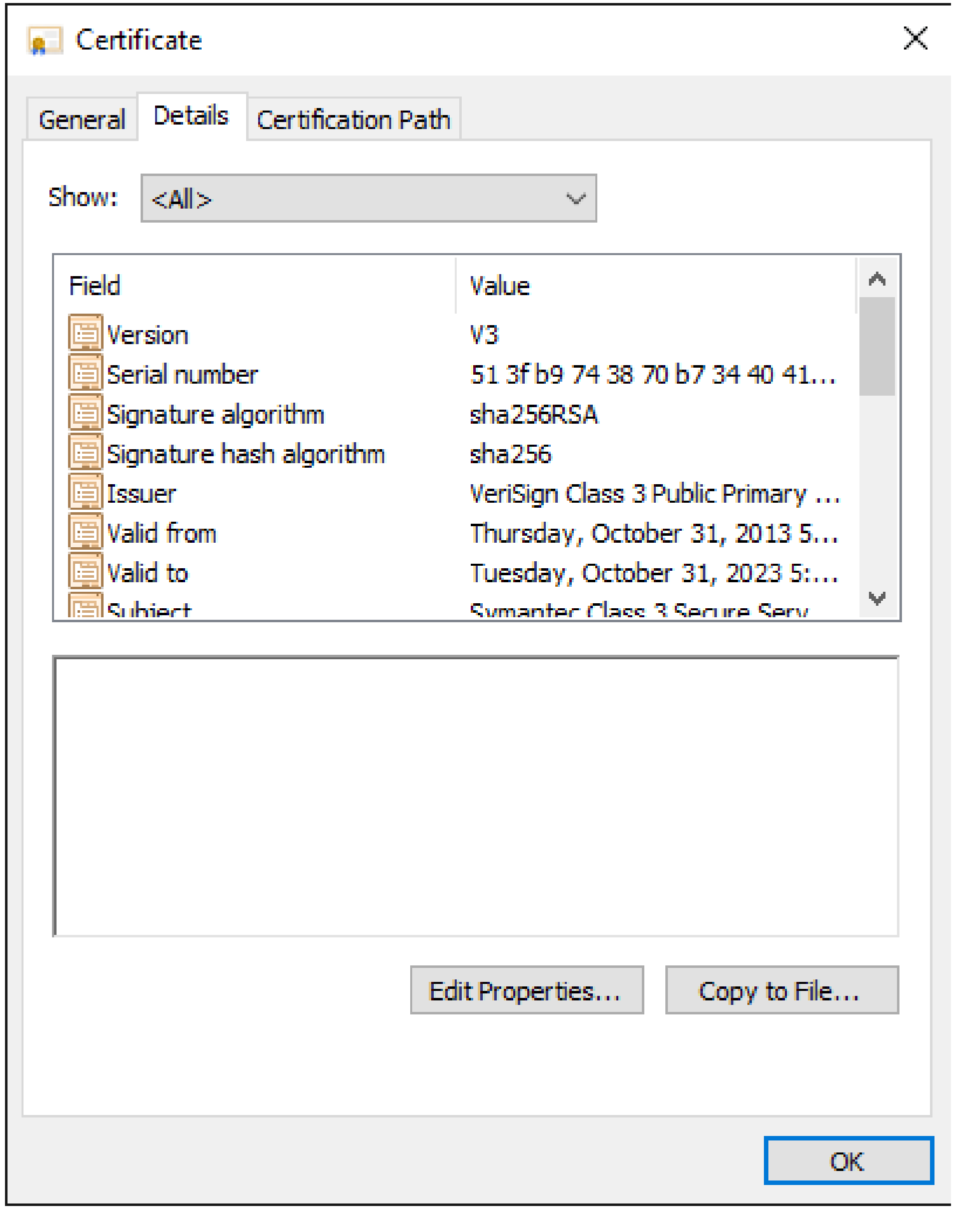
* Refer to the certification authority's statement for details.

Issued to: Symantec Class 3 Secure Server CA - G4

Issued by: VeriSign Class 3 Public Primary Certification Authority - G5

Valid from 10/31/2013 **to** 10/31/2023

What Are Certificate Extensions?



Show: <All>

Field	Value
Version	V3
Serial number	51 3f b9 74 38 70 b7 34 40 41...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	VeriSign Class 3 Public Primary ...
Valid from	Thursday, October 31, 2013 5:...
Valid to	Tuesday, October 31, 2023 5:...
Subject	Symantec Class 3 Secure Serv

Certificate extensions:

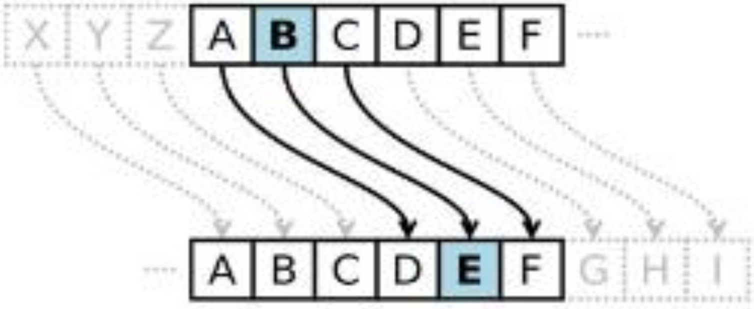
- Provide additional information about the subject
- Contain both version 1 and version 3 fields

Overview of Cryptography

What Cryptography is all about

- The art of protecting secrets using ciphers & codes.

- Cryptography is the science of hiding information in plain sight, in order to conceal it from unauthorized parties.
  - Substitution cipher first used by Caesar for battlefield communications



Exchanging Secret Messages

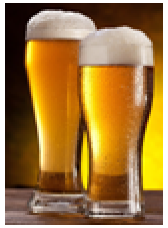
tsl'g fdks d cssn

Alice

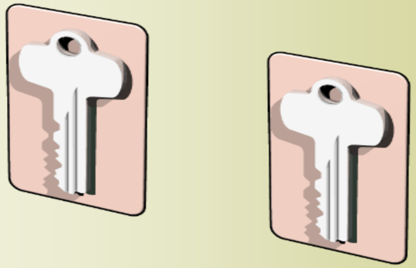
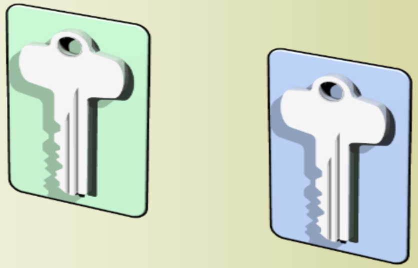
t = l
s = e
l = t
g = s
f = h
d = a
k = v
s = e
d = a
c = b
s = e
s = e
n = r

Bob

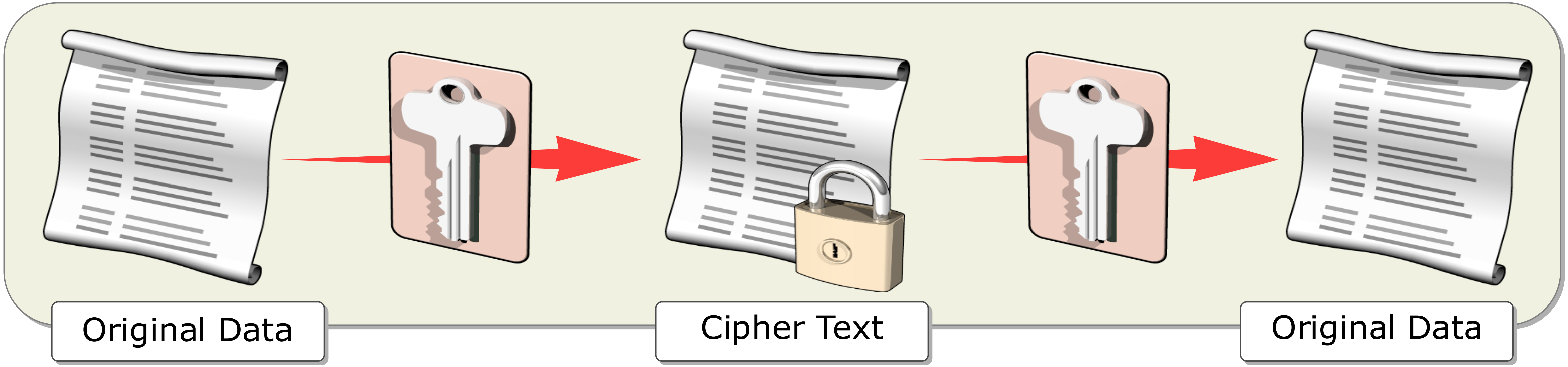
let's have a beer



Encryption Keys

Key type	Description
 Symmetric	- Same key is used to encrypt and decrypt the data - It protects the data from interception
 Asymmetric	- It consists of a public and private key - The private key is protected, the public key is widely distributed - If the private key is used to encrypt data, the public key is used to decrypt data, and vice versa

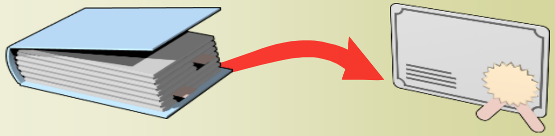
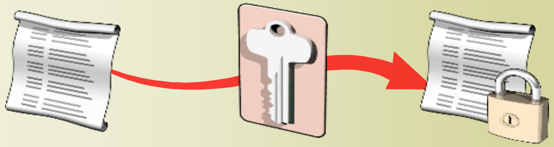
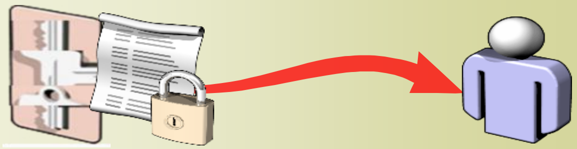
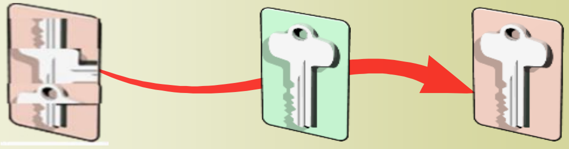
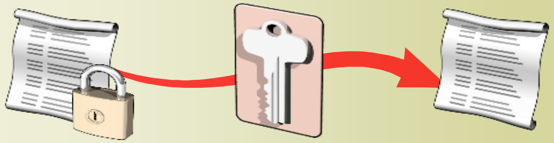
How Does Symmetric Encryption Work?



Symmetric encryption:

- Uses the same key
- Is often referred to as bulk encryption
- Is vulnerable if the symmetric key is obtained

How Does Public Key Encryption Work?

Requirement	Process
	1. The recipient’s public key is retrieved
	2. The data is encrypted with a symmetric key
	3. The symmetric key is encrypted with the recipient’s public key
	4. The encrypted symmetric key and encrypted data are sent to the recipient
	5. The recipient decrypts the symmetric key with her private key
	6. The data is decrypted with the symmetric key

Encryption Algorithms Cont..

- **DES**

  This is the 'Data Encryption Standard'. This is a cipher that operates on 64-bit blocks of data, using a **56-bit key**. It is a 'private key' system.

- **Triple DES**
  - 3 DES was designed to replace the original (DES) algorithm, which hackers eventually learned to defeat with relative ease. At one time, Triple DES was the recommended standard and the most widely used symmetric algorithm in the industry.
  - Triple DES uses three individual keys with 56 bits each. The total key length adds up to **168 bits**,

Encryption Algorithms Cont..

- **RSA**
  - RSA is a public-key encryption algorithm and the standard for encrypting data sent over the internet using key sizes **1,024 to 4,096 bit**. It also happens to be one of the methods used in our PGP and GPG programs.
  - Unlike Triple DES, RSA is considered an asymmetric algorithm due to its use of a pair of keys.
- **Blowfish**
  - Blowfish is yet another algorithm designed to replace DES. This symmetric cipher splits messages into blocks of 64 bits and encrypts them individually using key size of **32 – 448 bits**
  - Mostly used in e-commerce to secure payment systems.
  - known for both its tremendous speed and overall effectiveness as many claim that it has never been defeated

Encryption Algorithms

- **AES**
  - The Advanced Encryption Standard (AES) is the algorithm trusted as the standard by the U.S. Government and numerous organizations.
  - Although it is extremely efficient in **128-bit** form, AES also uses keys of **192 and 256 bits** for heavy duty encryption purposes.

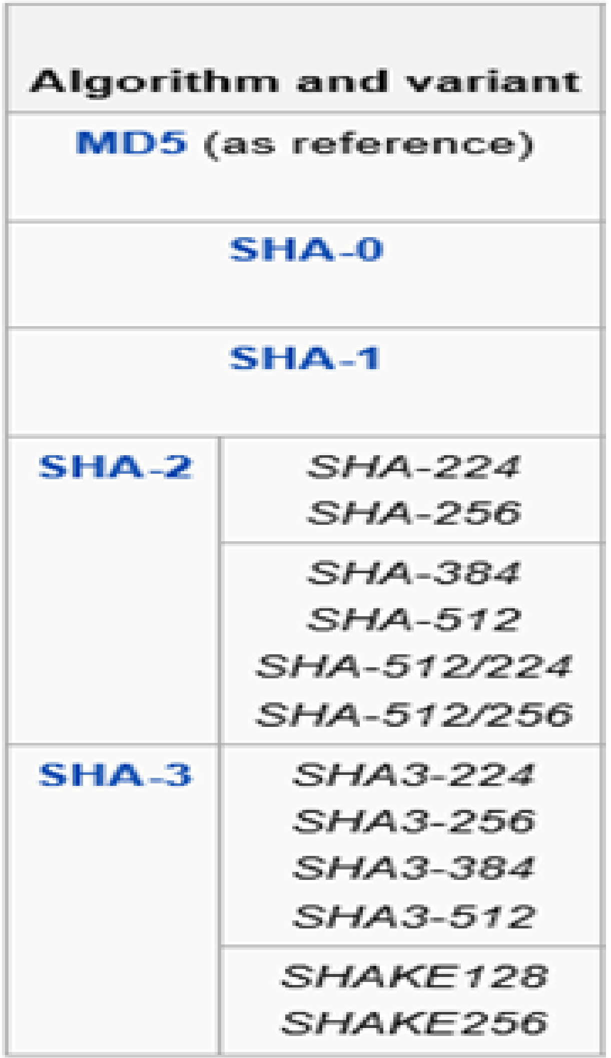
What is Digital Signature

Digital Signature Ensures:

- Verifies the identity of Author
- Content is not modified during transit
- All Certificates issued are signed by respective Certification Authority in the hierarchy

Hashing Algorithms

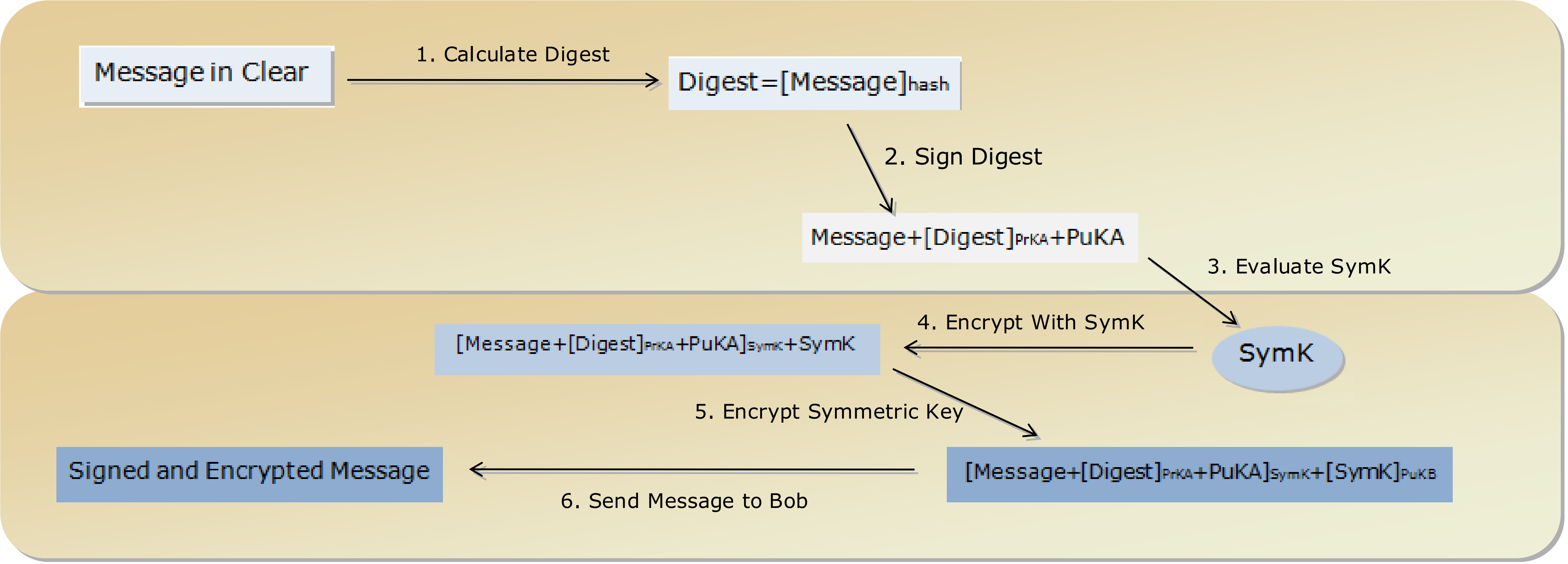
- Hashing means “fingerprints” of data



Algorithm and variant	
MD5 (as reference)	
SHA-0	
SHA-1	
SHA-2	*SHA-224* *SHA-256*
	SHA-384 *SHA-512* *SHA-512/224* *SHA-512/256*
SHA-3	*SHA3-224* *SHA3-256* *SHA3-384* *SHA3-512*
	SHAKE128 *SHAKE256*

Example of Encryption and Signing

Alice sending a signed and encrypted message to Bob



Message in Clear

1. Calculate Digest

$\text{Digest}=[\text{Message}]_{\text{hash}}$

2. Sign Digest

$\text{Message}+[\text{Digest}]_{\text{PrKA}}+\text{PuKA}$

3. Evaluate SymK

SymK

4. Encrypt With SymK

$[\text{Message}+[\text{Digest}]_{\text{PrKA}}+\text{PuKA}]_{\text{SymK}}+\text{SymK}$

5. Encrypt Symmetric Key

$[\text{Message}+[\text{Digest}]_{\text{PrKA}}+\text{PuKA}]_{\text{SymK}}+[\text{SymK}]_{\text{PuKB}}$

6. Send Message to Bob

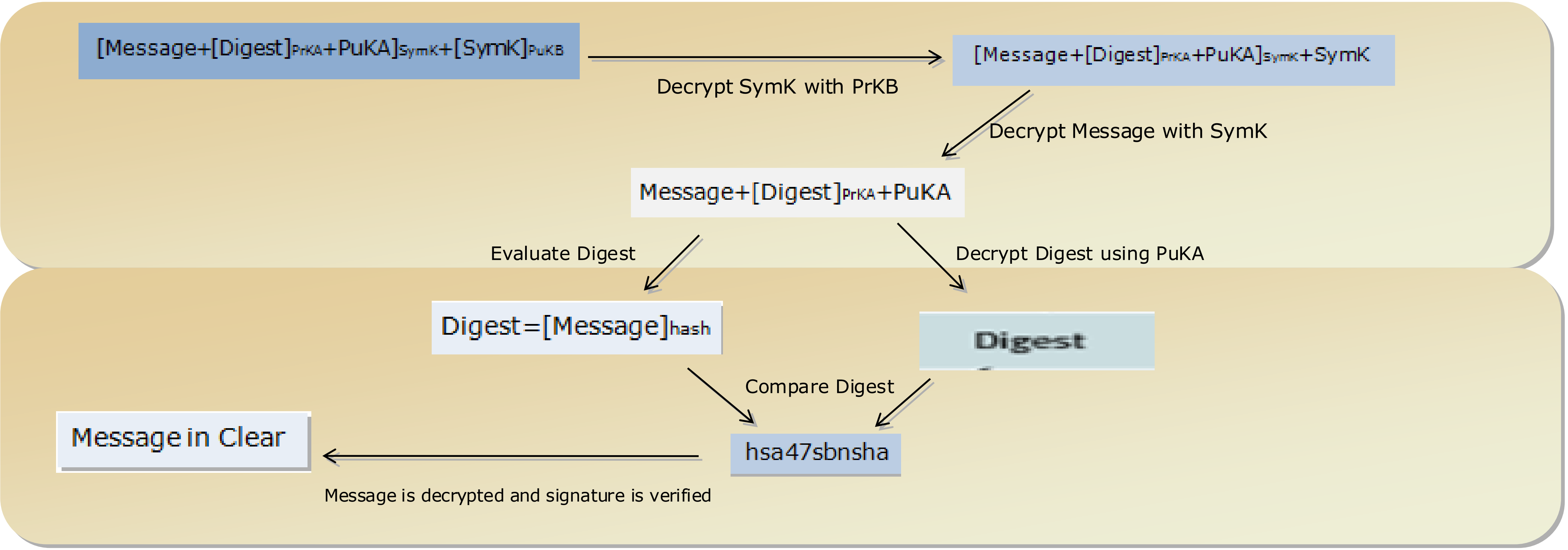
Signed and Encrypted Message

Legend

PrKA	Alice's Private Key
PuKA	Alice's Public Key
PuKB	Bob's Public Key
SymK	One time symmetric key
Hash	Hashing alogorithm

Decryption and Verifying Message

Bob Decrypting and Verifying message sent by Alice



$[Message+[Digest]_{PrKA}+PuKA]_{SymK}+[SymK]_{PuKB}$

Decrypt SymK with PrKB

$[Message+[Digest]_{PrKA}+PuKA]_{SymK}+SymK$

Decrypt Message with SymK

$Message+[Digest]_{PrKA}+PuKA$

Evaluate Digest

Decrypt Digest using PuKA

$Digest=[Message]_{hash}$

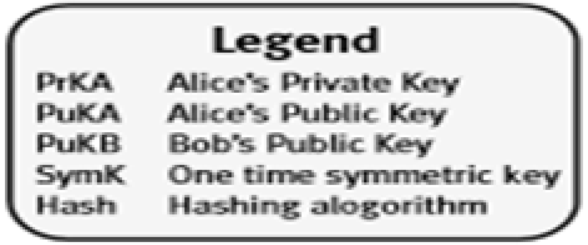
Digest

Compare Digest

hsa47sbnsha

Message in Clear

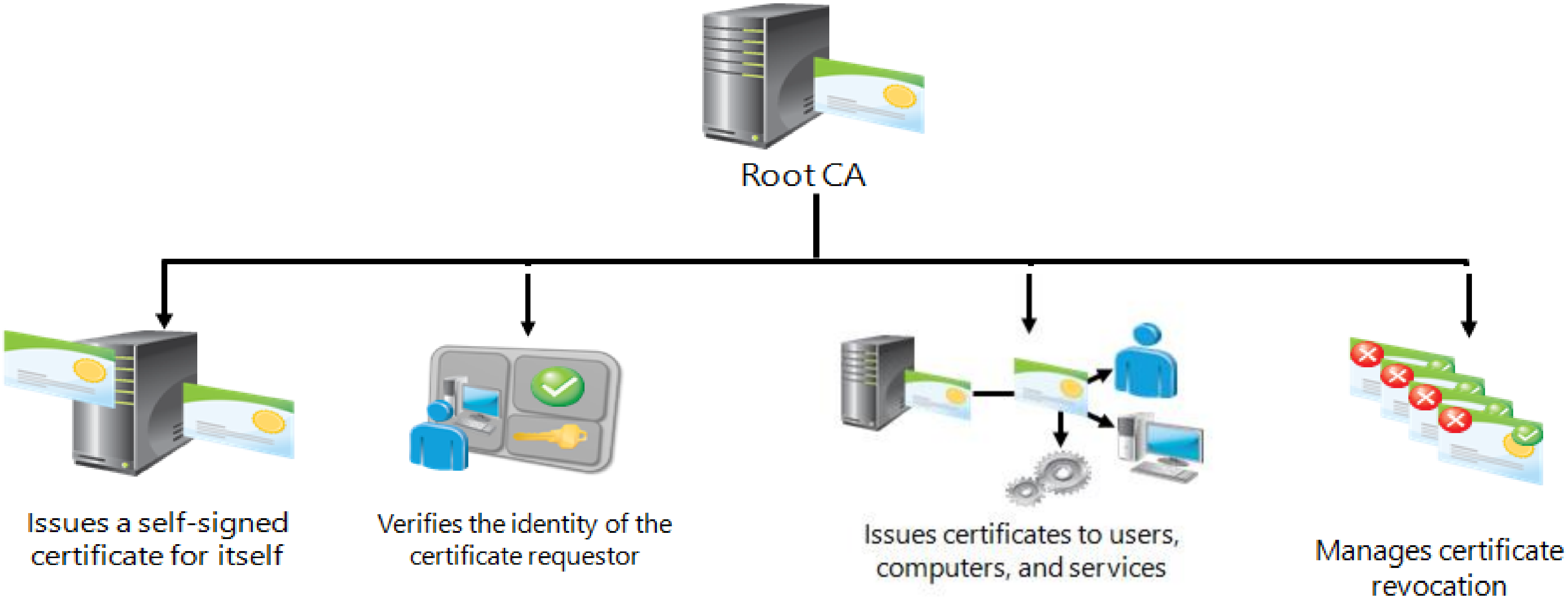
Message is decrypted and signature is verified



Legend	
PrKA	Alice's Private Key
PuKA	Alice's Public Key
PuKB	Bob's Public Key
SymK	One time symmetric key
Hash	Hashing alogorithm

Certification Authority or CA

What Are CAs?



Root CA

Issues a self-signed certificate for itself

Verifies the identity of the certificate requestor

Issues certificates to users, computers, and services

Manages certificate revocation

Overview of the AD CS Server Role in Windows Server 2012

CA

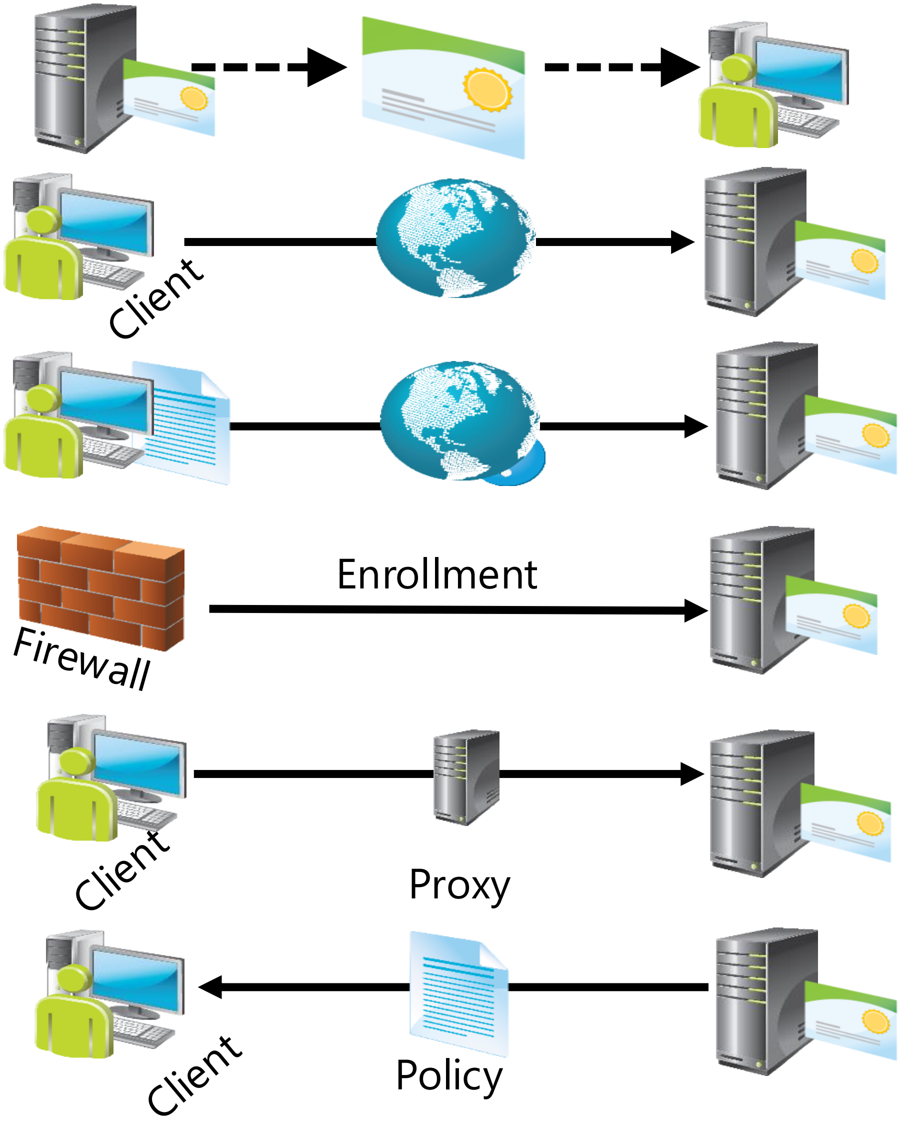
CA Web enrollment

Online Responder

NDES

CES

CEP



Public vs. Private CAs

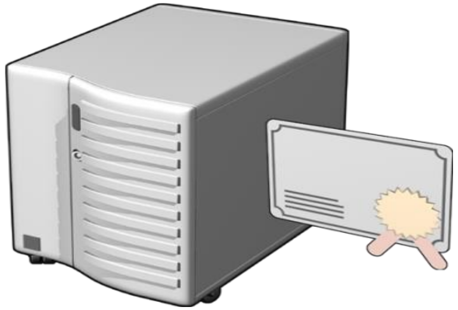
Internal private CAs:

- Require greater administration than external public CAs
- Cost less than external public CAs, and provide greater control over certificate management
- Are not trusted by external clients by default
- Offer advantages such as customized templates and autoenrollment

External public CAs:

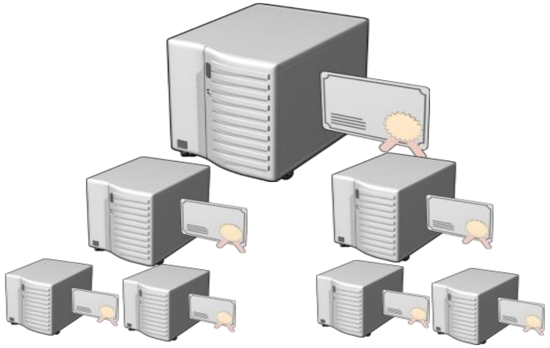
- Are trusted by many external clients
- Have slower certificate procurement

Types of Certification Authorities



Root CA

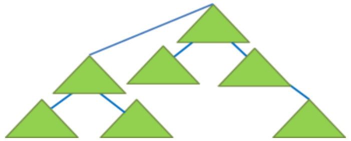
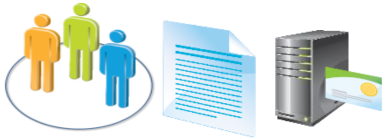
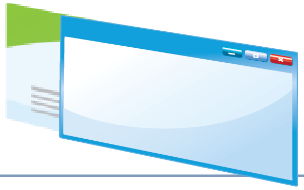
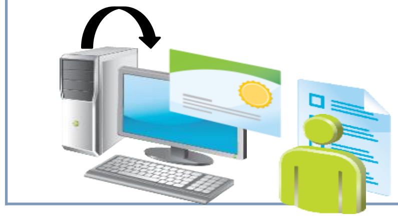
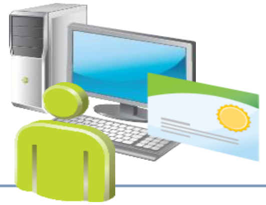
- Is the most trusted type of CA in a PKI infrastructure
- Is a self-signed certificate
- Issues certificates to other subordinate CAs
- Possesses physical security and the certificate issuance policy that are typically more rigorous than subordinate CAs



Subordinate CA

- Is issued by another CA
- Addresses specific usage policies, organizational or geographical boundaries, load balancing, and fault tolerance
- Issues certificates to other CAs to form a hierarchical PKI infrastructure

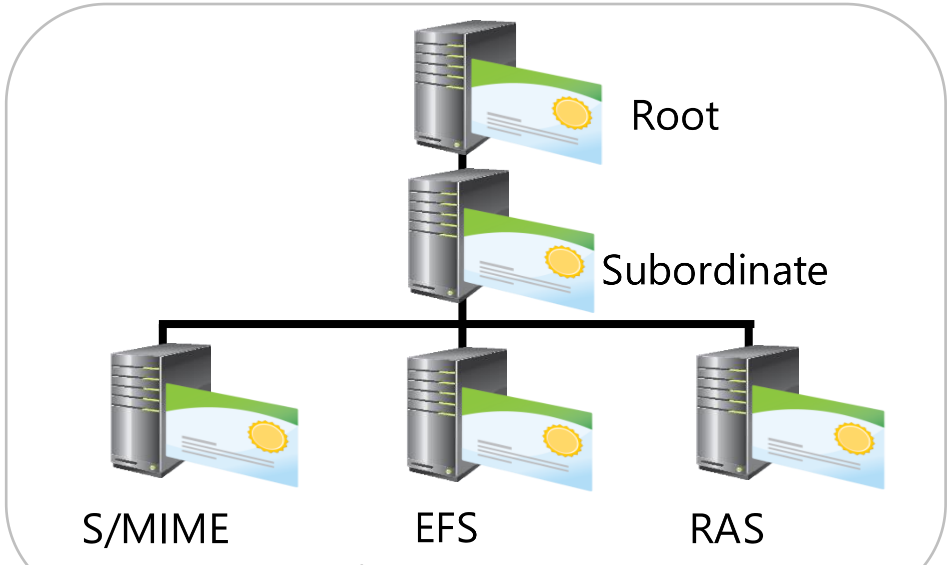
Stand-Alone vs. Enterprise CAs

Stand-alone CAs		Enterprise CAs	
	Must be used if any CA (root/intermediate/policy) is offline, because a stand-alone CA is not joined to an AD DS domain		Requires the use of AD DS
			Can use Group Policy to propagate certificate to trusted root CA certificate store
	Users provide identifying information and specify type of certificate		Publishes user certificates and CRLs to AD DS
	Does not require certificate templates		Issues certificates based upon a certificate template
	All certificate requests are kept pending until administrator approval		Supports autoenrollment for issuing certificates

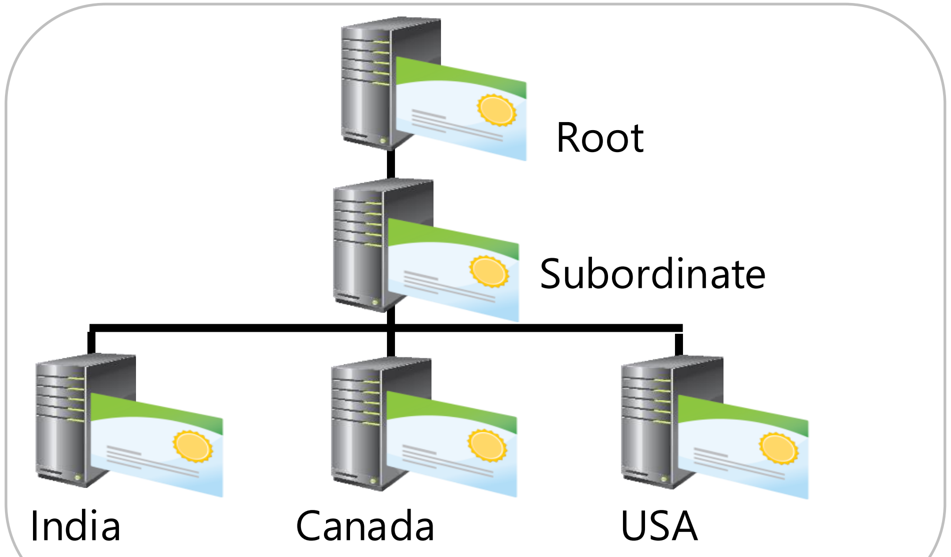
Considerations for Deploying a Root CA

- Computer name and domain membership cannot change
- When you plan private key configuration, consider the following:
  - CSP or KSP
  - Key character length with a default of 2,048
  - The hash algorithm that is used to sign certificates issued by a CA
- When you plan a root CA, consider the following:
  - Name and configuration
  - Certificate database and log location
  - Validity period

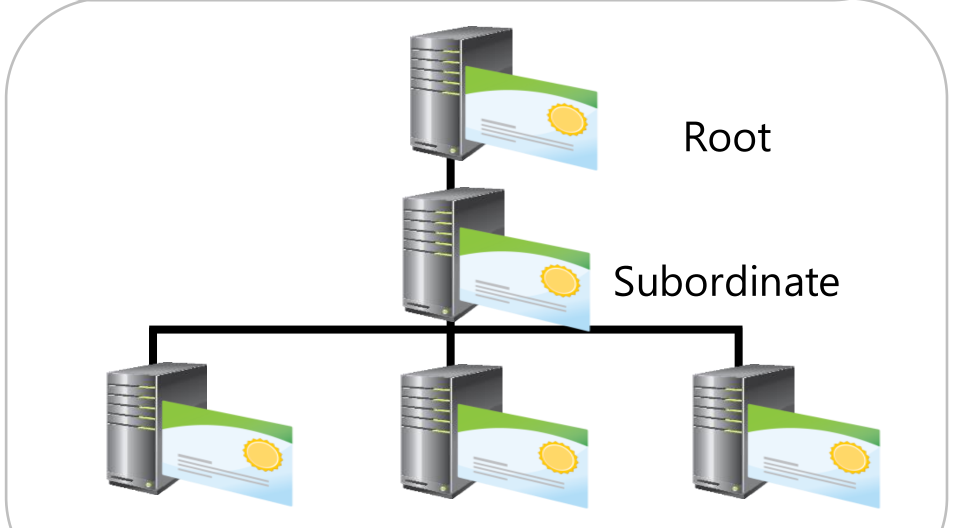
Considerations for Deploying a Subordinate CA



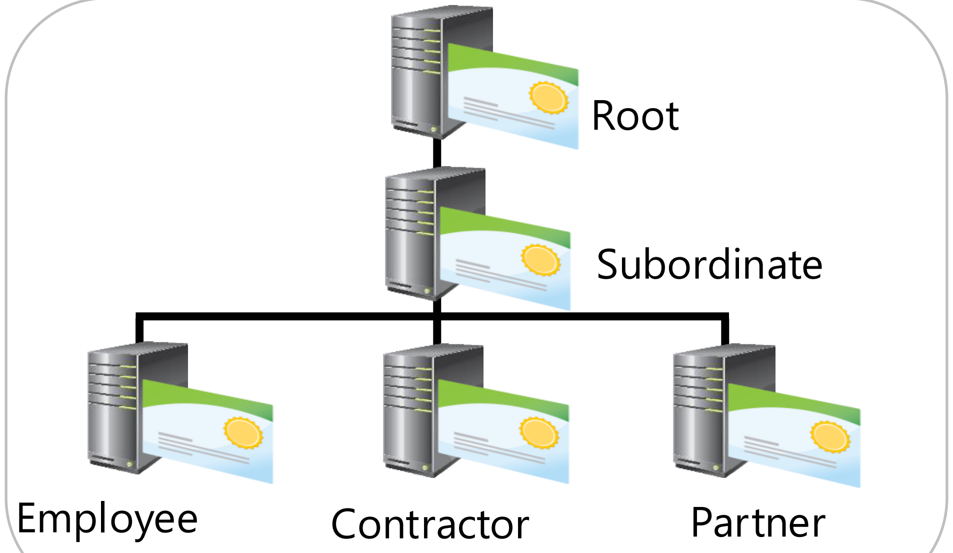
Certificate Uses



Locations

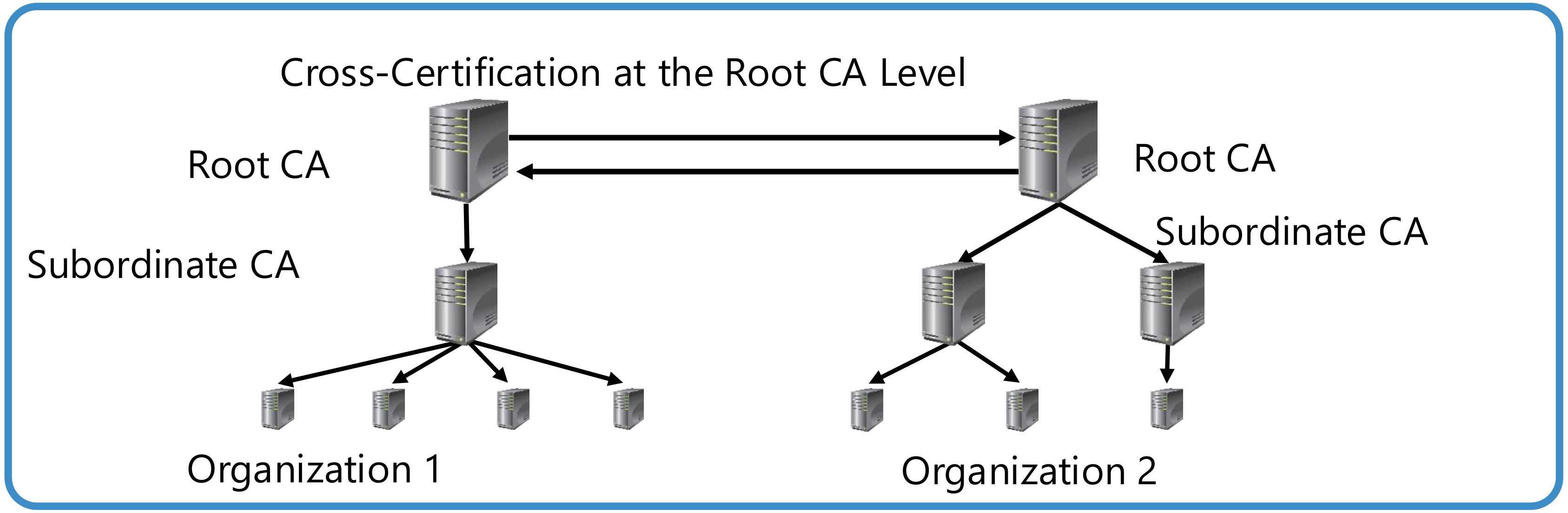


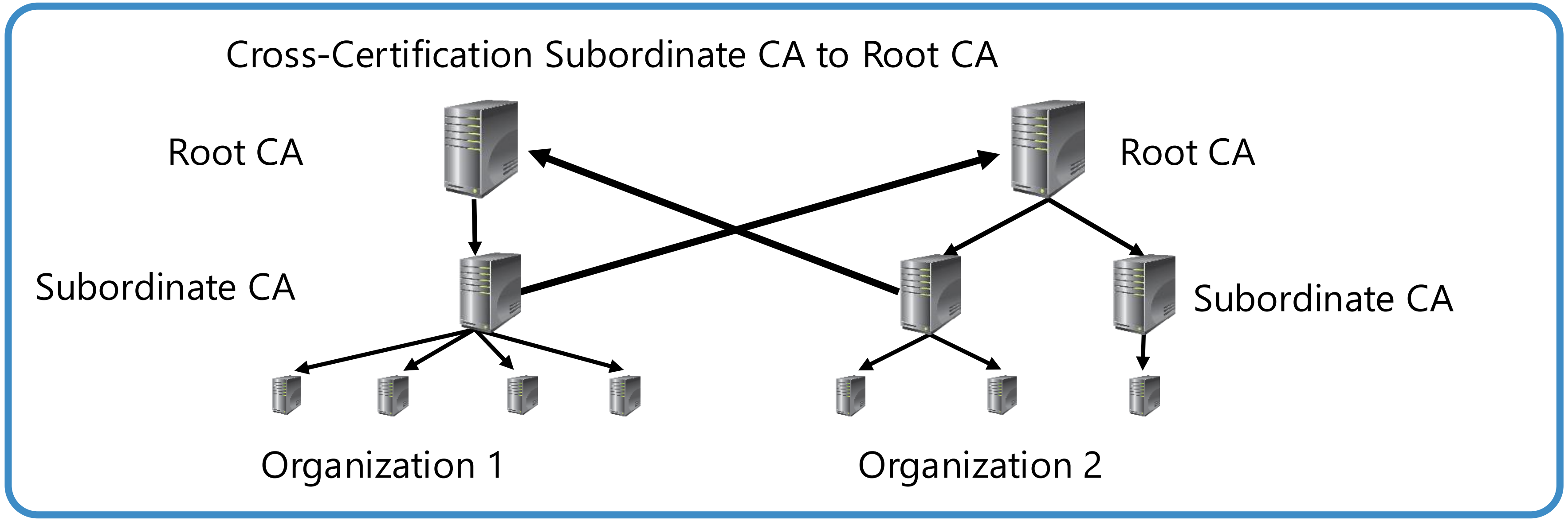
Load Balancing



Organizational Divisions

What Is a Cross-Certification Hierarchy?





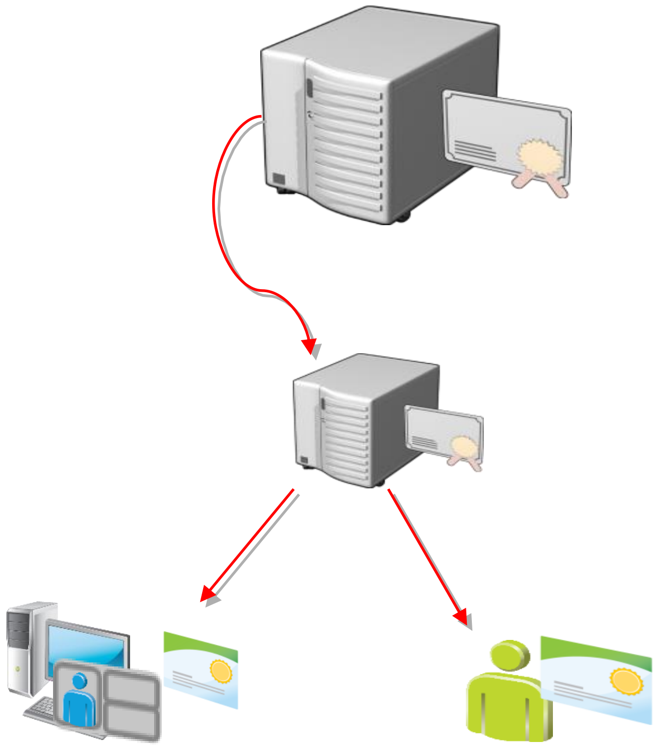
Demonstration: Deploying a Root CA and Subordinate CA

In this demonstration, you will see how to -

1. Deploy an Standalone Root CA on Windows Server 2016
2. Deploy an Enterprise Subordinate Ca on Windows Server 2016

Migrating Hashing Algorithm from SHA1 to SHA2

- Windows are no longer trusting certificates signed with SHA-1 after January 1, 2017. (Applicable on External Certificates)
- Windows 2008 and onwards CA supports SHA-2
- Before migrating to SHA-2, thoroughly check all applications if they support SHA-2 signed certificates.
- CSP doesn't support SHA-2, have to switch CA key to KSP



Migrating Hashing Algorithm from SHA1 to SHA2 (Root CA)

1. Backup CA and CA registry key
2. Stop CA service
3. Check if CA is using CSP or KSP
4. If using HSM for storing certificate key, please check with HSM vendor for steps on migrating from CSP to KSP (Optional)
5. Delete CA certificate along with private key from local machine store
6. Migrate CA certificate and private key from CSP to KSP (this step is optional but has to be done on windows server 2012 R2)
7. Import CA certificate in the machine store
8. Import modified configuration and encryption registry file into machine registry
9. Changing Hashing algorithm from SHA1 to SHA2
10. Start CA service
11. Renew CA certificate
12. Run CERTUTIL –CRL to generate a new CRL signed with SHA-2 certificate

Migrating Hashing Algorithm from SHA1 to SHA2 (Sub CA)

1. Backup CA and CA registry key
2. Stop CA service
3. Check if CA is using CSP or KSP
4. If using HSM for storing certificate key, please check with HSM vendor for steps on migrating from CSP to KSP (Optional)
5. Delete CA certificate along with private key from local machine store
6. Migrate CA certificate and private key from CSP to KSP (this step is optional but has to be done on windows server 2012 R2)
7. Import CA certificate in the machine store
8. Import modified configuration and encryption registry file into machine registry
9. Changing Hashing algorithm from SHA1 to SHA2
10. Start CA service
11. Publish RootCA new CRL and certificate
12. Renew CA certificate by requesting offline from Root CA
13. Run CERTUTIL –CRL to generate a new CRL signed with SHA-2 certificate

Certificate Request
or
Enrollment

Types of Certificate Enrollment

- Web enrollment
- MMC
- Auto enrollment
- Certreq.exe or offline Request
- Certificate Enrollment Policy (CEP) – New in server 2008 R2
- Certificate Enrollment Service (CES)- New in Server 2008R2

What Are Certificate Templates?

A certificate template defines:

- The format and contents of a certificate
- The process for creating and submitting a valid certificate request
- The security principals that are allowed to read, enroll, or use autoenrollment for a certificate that will be based on the template
- The permissions required to modify a certificate template

Certificate Template Versions in Windows Server 2012

Version 1:

- Introduced in Windows 2000 Server, provides for backward compatibility in newer versions
- Creates by default when a CA is installed
- Cannot be modified (except for permissions) or removed, but can be duplicated to become version 2 or 3 templates, which can then be modified

Version 2:

- Default template introduced with Windows Server 2003
- Allows customization of most settings in the template
- Several preconfigured templates are provided when a CA is installed

Version 3:

- Supports advanced Suite B cryptographic settings
- Includes advanced options for encryption, digital signatures, key exchange, and hashing
- Only supports Windows Server 2008 and Windows Server 2008 R2 servers
- Only supports Windows Vista and Windows 7 client computers

Version 4:

- Available only for Windows Server 2012 and Windows 8 clients
- Supports both CSPs and KSPs
- Supports renewal with the same key

WEB Enrollment

- Domain joined and NON-Domain clients can request certificates using web enrollment.
- Need to access http://certservername/certsrv
- Allow you to download CA chain certificate
- Allow you to view the pending request

Requesting certificate via MMC

- Only domain joined clients able to request certificate via MMC console.

Requesting certificate via Certreq: Offline Request

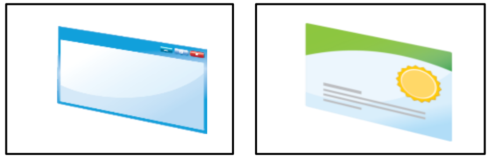
- **Certreq.exe -new <*RequestPolicy.inf*><*CertificateRequest.req*>**

- **certreq -submit -config "<*ServerName\CAName*>" "<*CertificateRequest.req*>" "<*CertificateResponse.cer*>“**

- **certreq –retrieve -config "<*ServerName\CAName*>" <*RequestID*> "<*CertificateResponse.cer*>“**

- **certreq –accept -config "<*ServerName\CAName*>" "<*CertificateResponse.cer*>"**

Requesting a Certificate using Autoenrollment



Certificate template

A certificate template is configured to Allow, Enroll, and Autoenroll permissions for users who receive the certificates

CA

The CA is configured to issue the template

Group Policy Object

An Active Directory Group Policy Object should be created to enable autoenrollment. The GPO should be linked to the appropriate site, domain, or organizational unit

Client machine

The client machine receives the certificates during the next Group Policy refresh interval

CA Policy and Exit Modules

- The policy module determines the action that is performed after the certificate request is received
- The exit module determines what happens with a certificate after it is issued
- Each CA is configured with default policy and exit modules
- The FIM CM 2010 deploys custom policy and exit modules
- The exit module can send email or publish a certificate to a file system
- You have to use certutil to specify these settings, as they are not available in the CA administrator console

https://msdn.microsoft.com/en-us/library/aa388216.aspx

Hands-On:

Encrypting and Decrypting a File with Certificate

Hands On: Securing a website using a Certificate

Configuring CA Properties

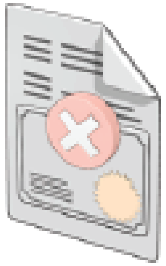
Configuring CA Administration and Security

- You can establish role-based administration for the CA hierarchy by defining the following roles:
  - CA administrator
  - Certificate manager
  - Backup operator
  - Enrollees
- You can assign the following permissions on the CA level:
  - Read
  - Issue and Manage Certificates
  - Manage CA
  - Request Certificates

What are CRLs and CDPs

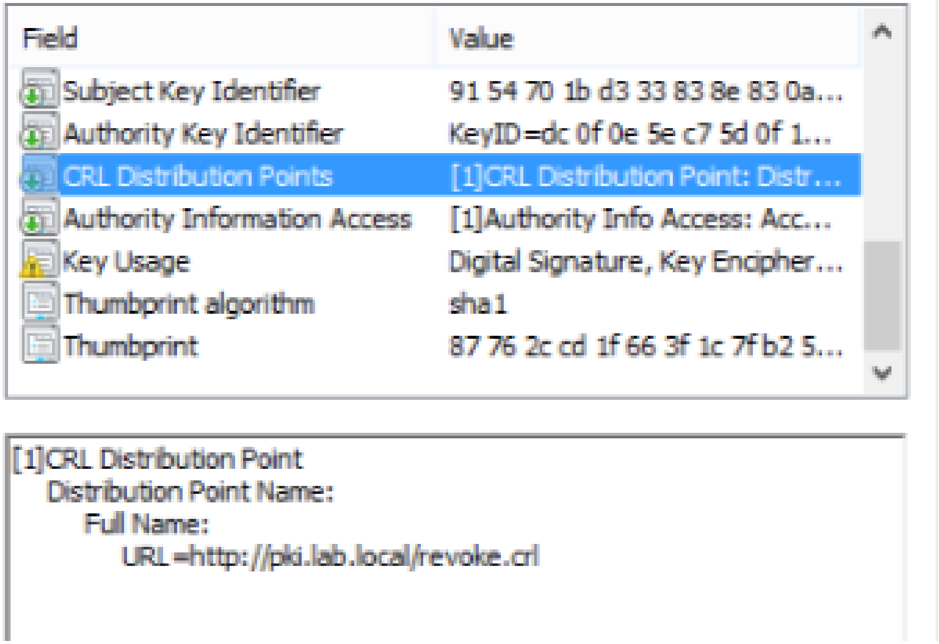
Purpose of CRLs:

- List of revoked certificates
- Publish periodically or on demand
- Can be retrieved and cached by client computers



Purpose of CDPs:

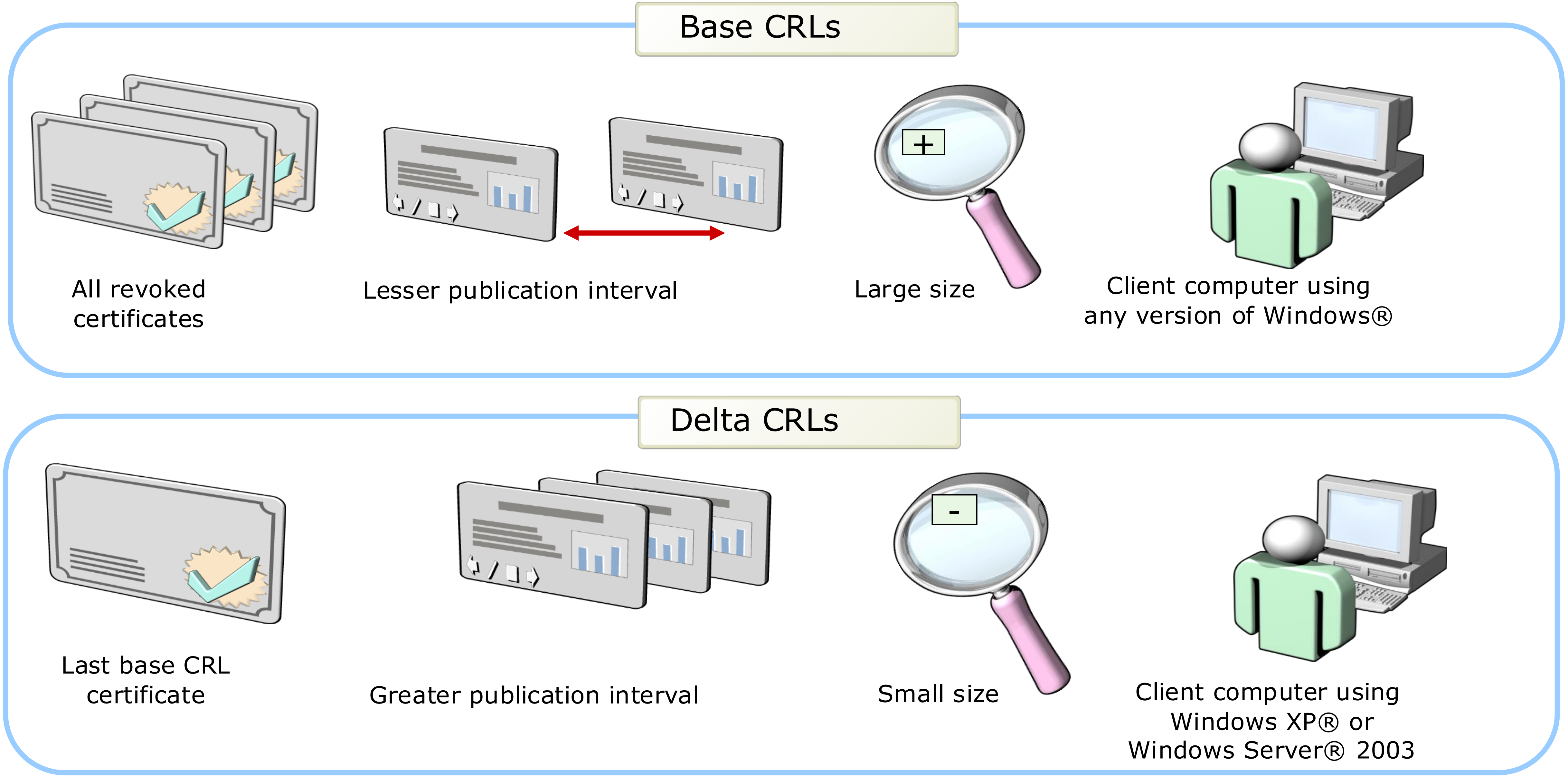
- Distribution point for CRLs
- Distributed as part of a certificate
- Can be updated but won't affect issued certificates



Field	Value
Subject Key Identifier	91 54 70 1b d3 33 83 8e 83 0a...
Authority Key Identifier	KeyID=dc 0f 0e 5e c7 5d 0f 1...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Key Usage	Digital Signature, Key Encipher...
Thumbprint algorithm	sha1
Thumbprint	87 76 2c cd 1f 66 3f 1c 7f b2 5...

```
[1]CRL Distribution Point
     Distribution Point Name:
          Full Name:
               URL=http://pki.lab.local/revoke.crl
```

Type of CRLs



Base CRLs

All revoked certificates

Lesser publication interval

Large size

Client computer using any version of Windows®

Delta CRLs

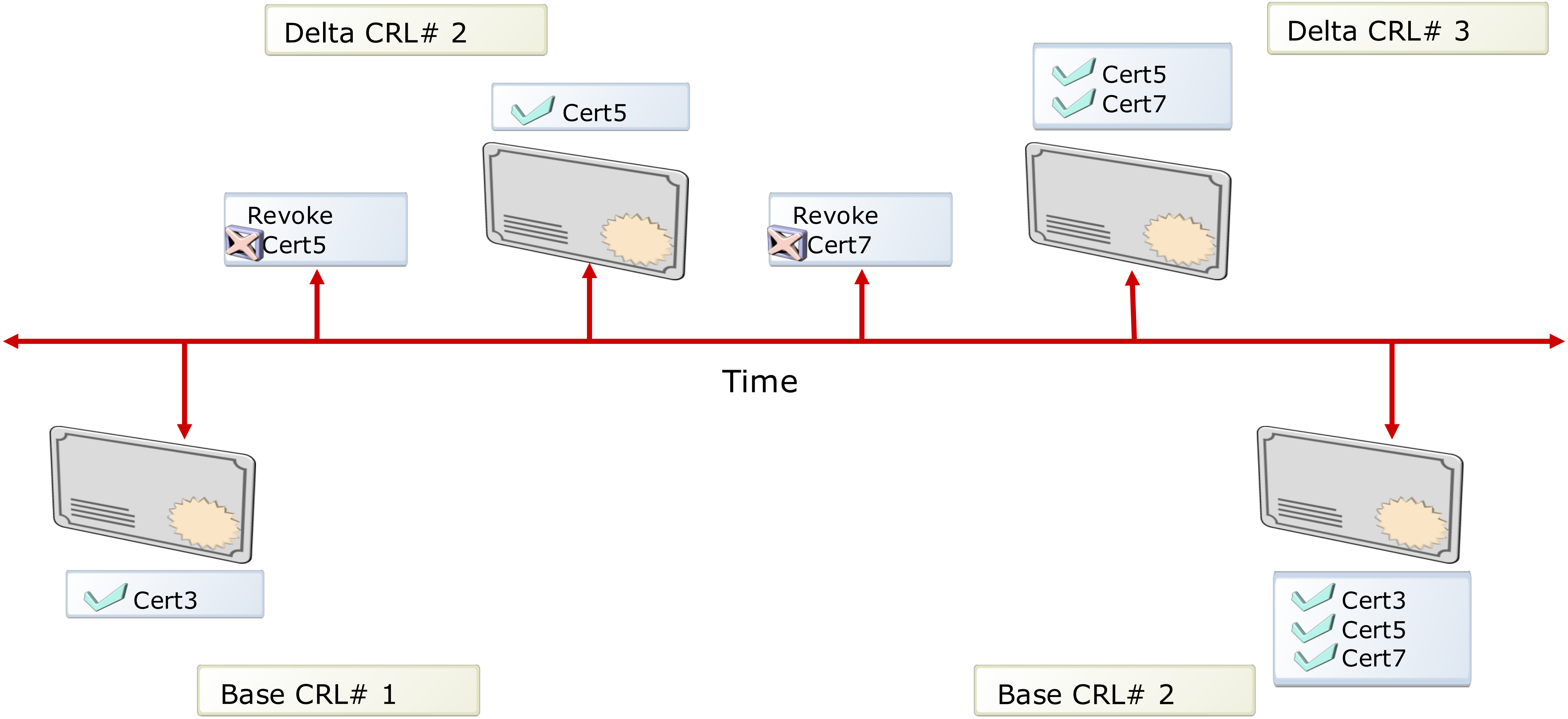
Last base CRL certificate

Greater publication interval

Small size

Client computer using Windows XP® or Windows Server® 2003

How CRLs Are Published



Delta CRL# 2

✓ Cert5

Revoke
✗ Cert5

Revoke
✗ Cert7

✓ Cert5
✓ Cert7

Delta CRL# 3

Time

✓ Cert3

Base CRL# 1

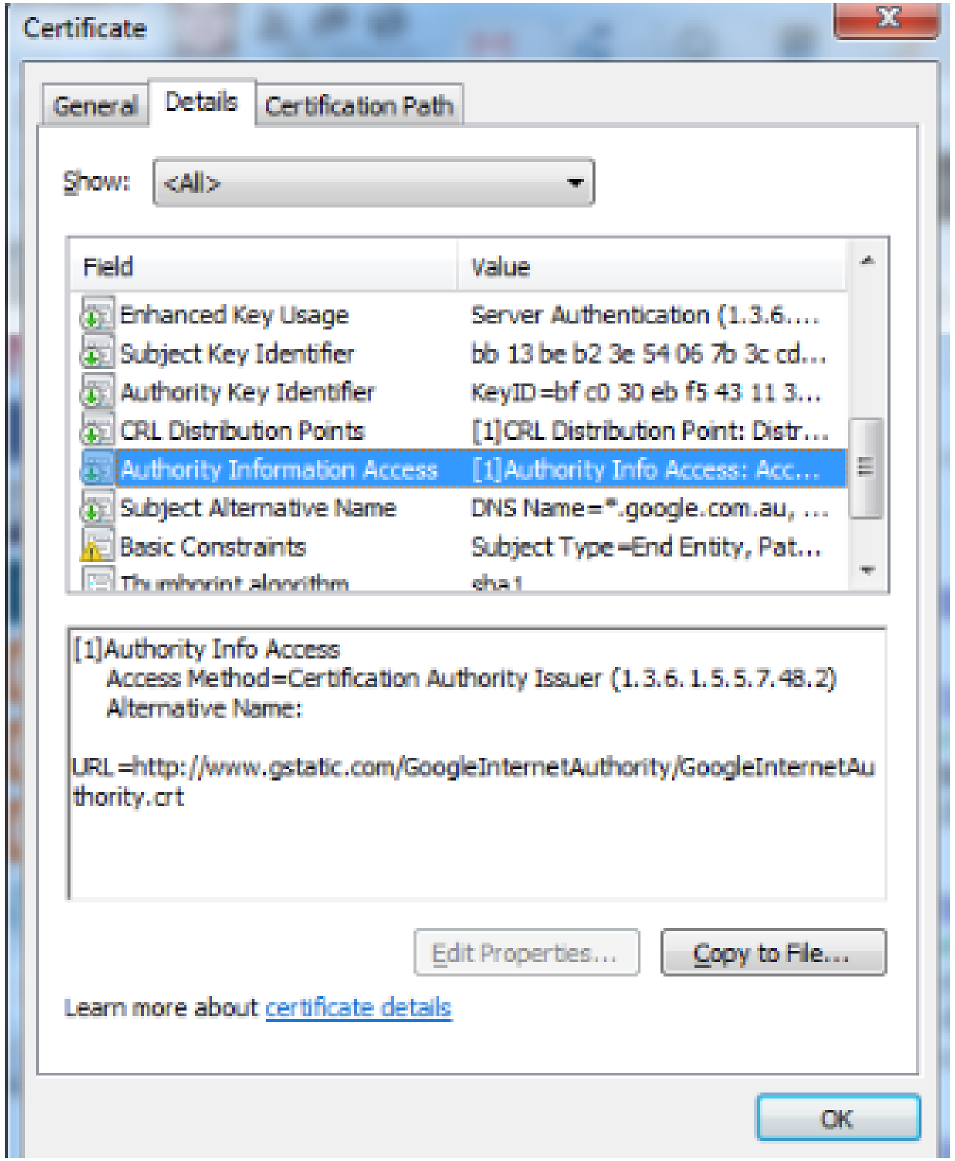
Base CRL# 2

✓ Cert3
✓ Cert5
✓ Cert7

Authority Information Access or AIA Extension

Authority information access locations:

Authority information access locations are URLs that are added to a certificate in its authority information access extension. These URLs can be used by an application or service to retrieve the issuing CA certificate. These CA certificates are then used to validate the certificate signature and to build a path to a trusted certificate.



Show: <All>

Field	Value
Enhanced Key Usage	Server Authentication (1.3.6....
Subject Key Identifier	bb 13 be b2 3e 54 06 7b 3c cd...
Authority Key Identifier	KeyID=bf c0 30 eb f5 43 11 3...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Subject Alternative Name	DNS Name=*.google.com.au, ...
Basic Constraints	Subject Type=End Entity, Pat...
Thumbprint algorithm	sha1

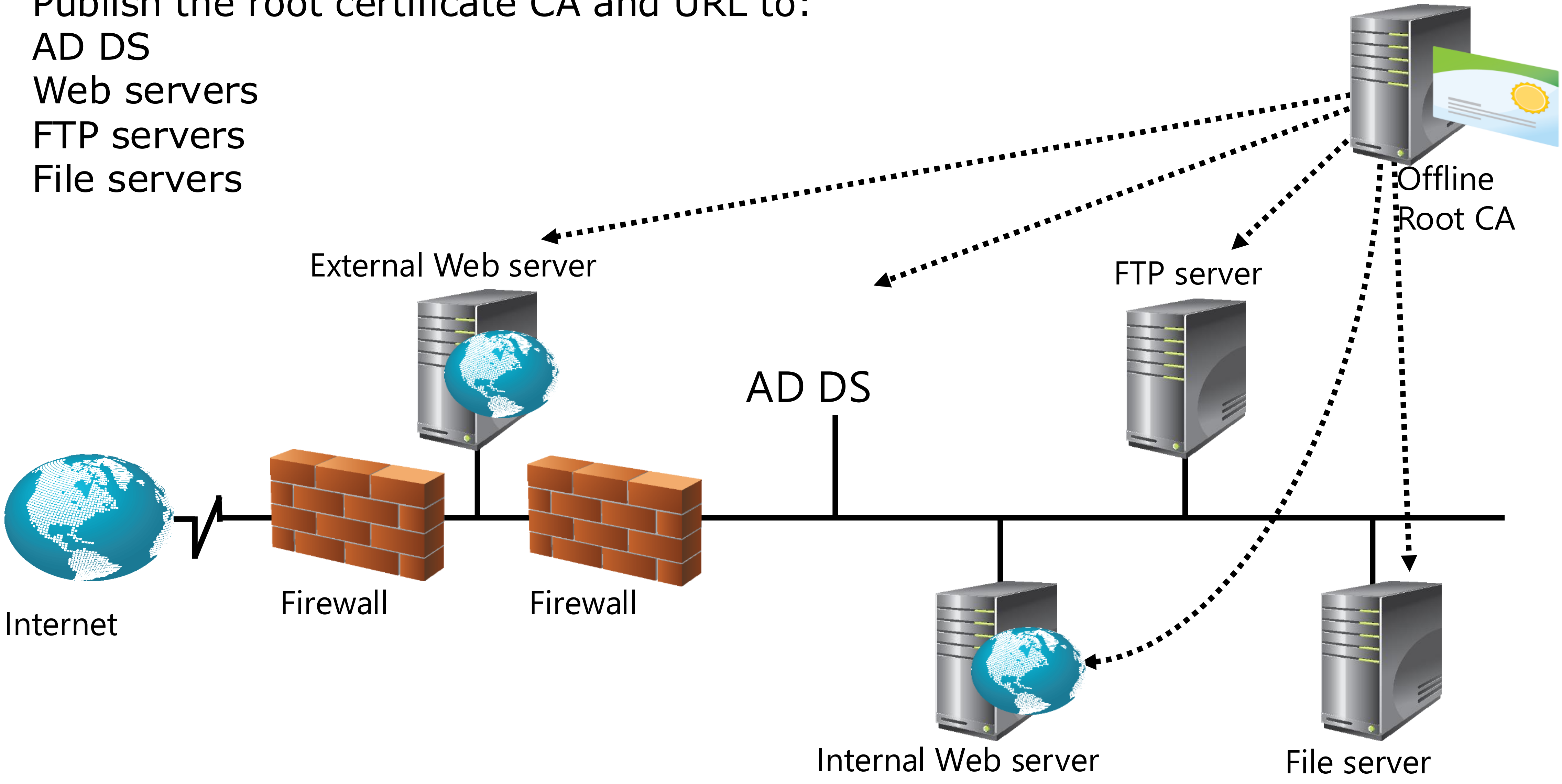
```
[1]Authority Info Access
     Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
     Alternative Name:

URL=http://www.gstatic.com/GoogleInternetAuthority/GoogleInternetAuthority.crt
```

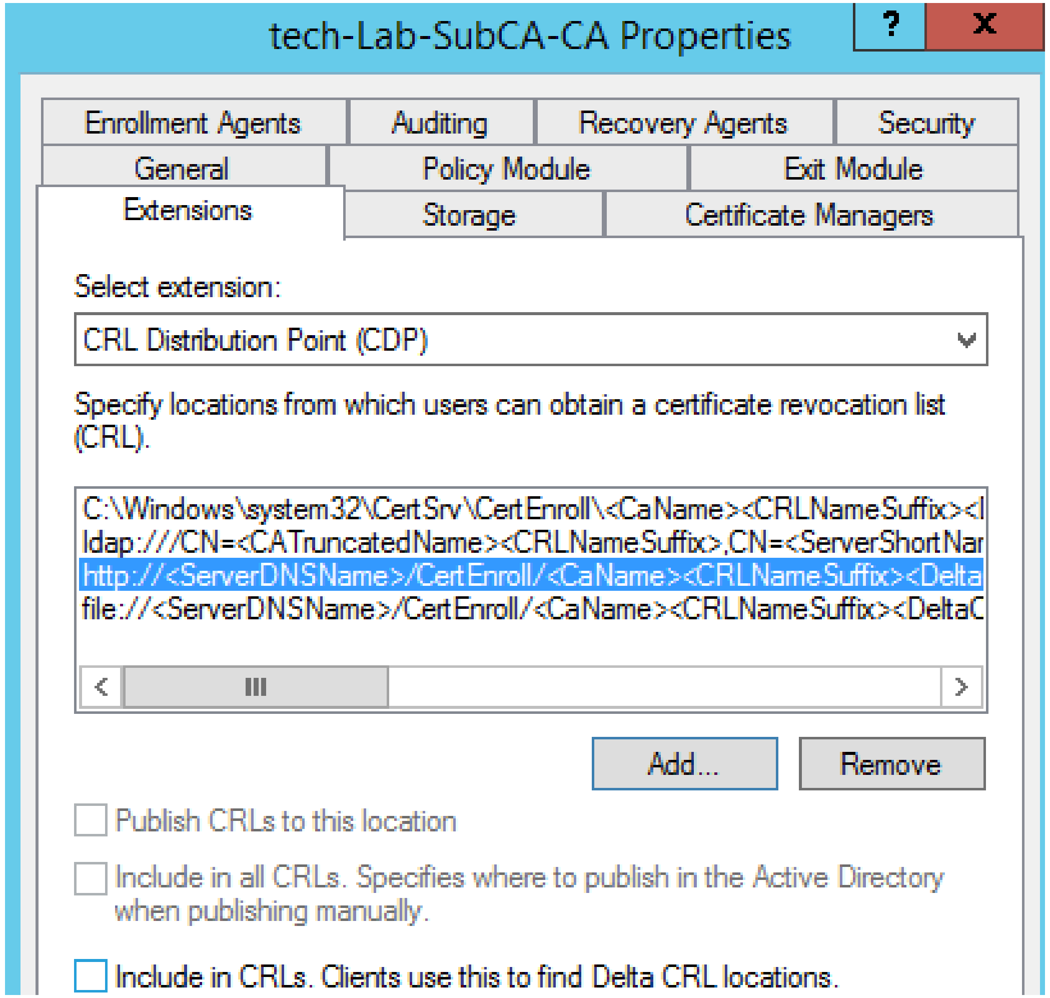
Learn more about certificate details

Considerations for Publishing AIAs and CDPs

Publish the root certificate CA and URL to:
AD DS
Web servers
FTP servers
File servers



Configuring AIA and CDP extensions



Select extension:

CRL Distribution Point (CDP)

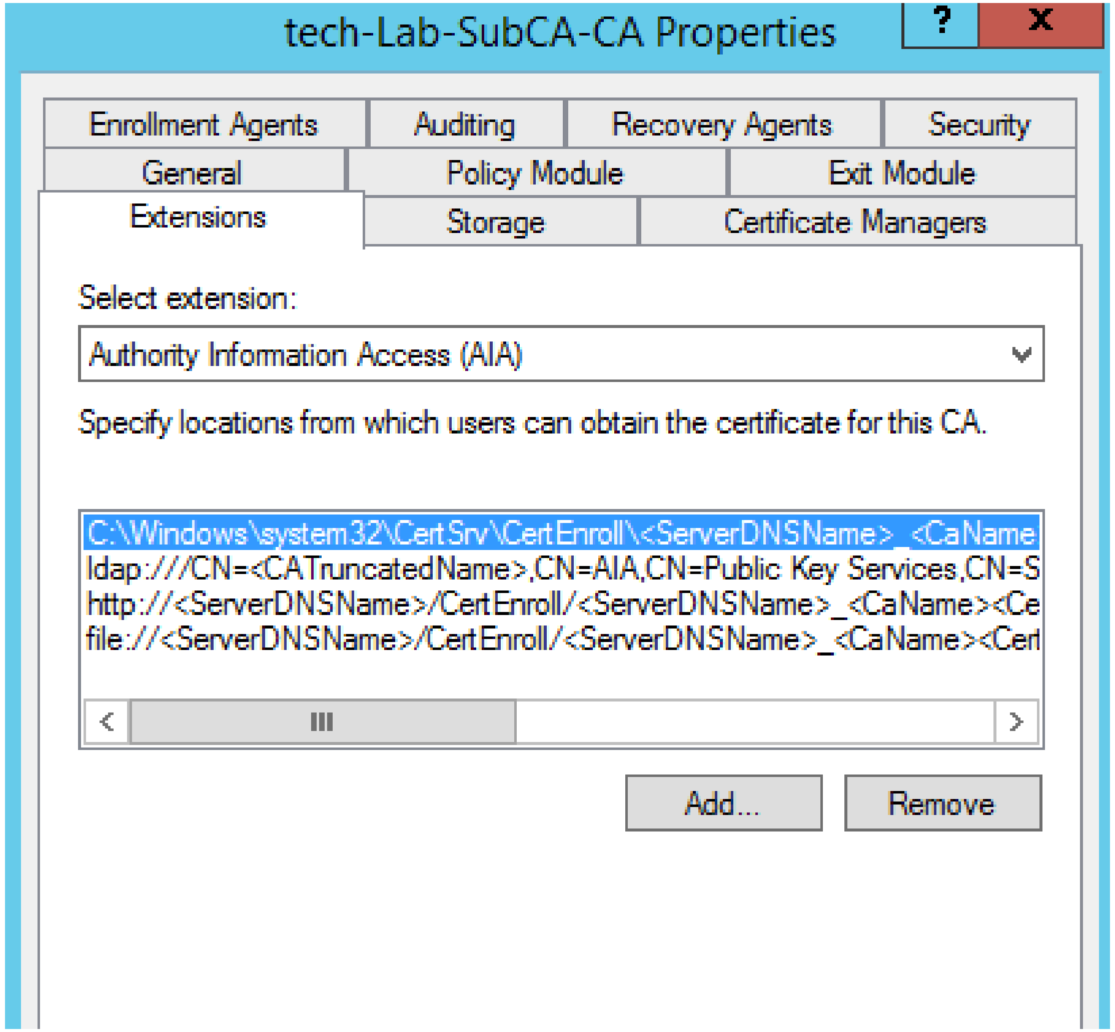
Specify locations from which users can obtain a certificate revocation list (CRL).

```
C:\Windows\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix><I
ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortNar
http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><Delta
file://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaC
```

□ Publish CRLs to this location

□ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

□ Include in CRLs. Clients use this to find Delta CRL locations.



Select extension:

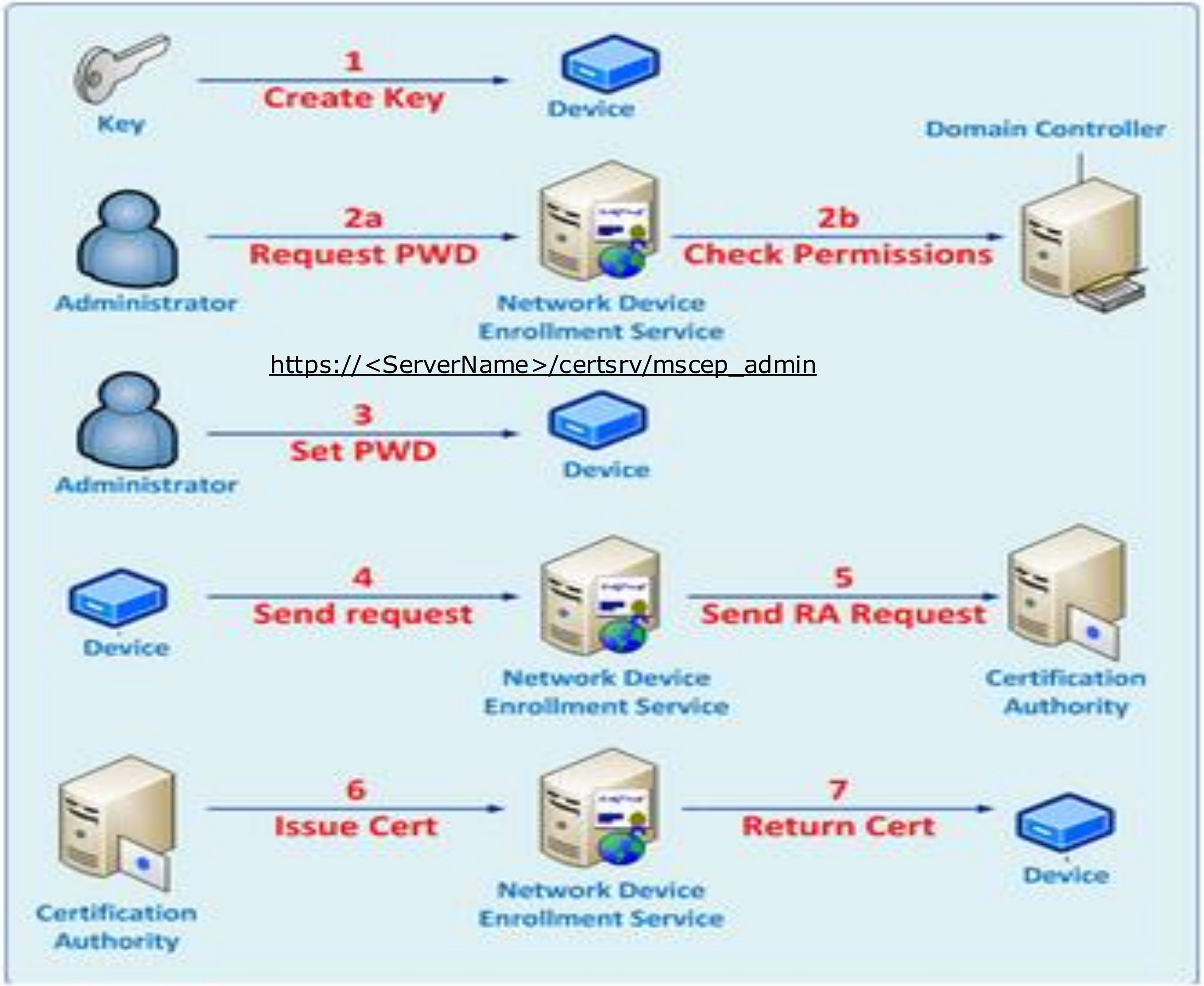
Authority Information Access (AIA)

Specify locations from which users can obtain the certificate for this CA.

```
C:\Windows\system32\CertSrv\CertEnroll\<ServerDNSName>_<CaName
ldap:///CN=<CATruncatedName>,CN=AIA,CN=Public Key Services,CN=S
http://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><Ce
file://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><Cert
```

New Roles in Certificate Services

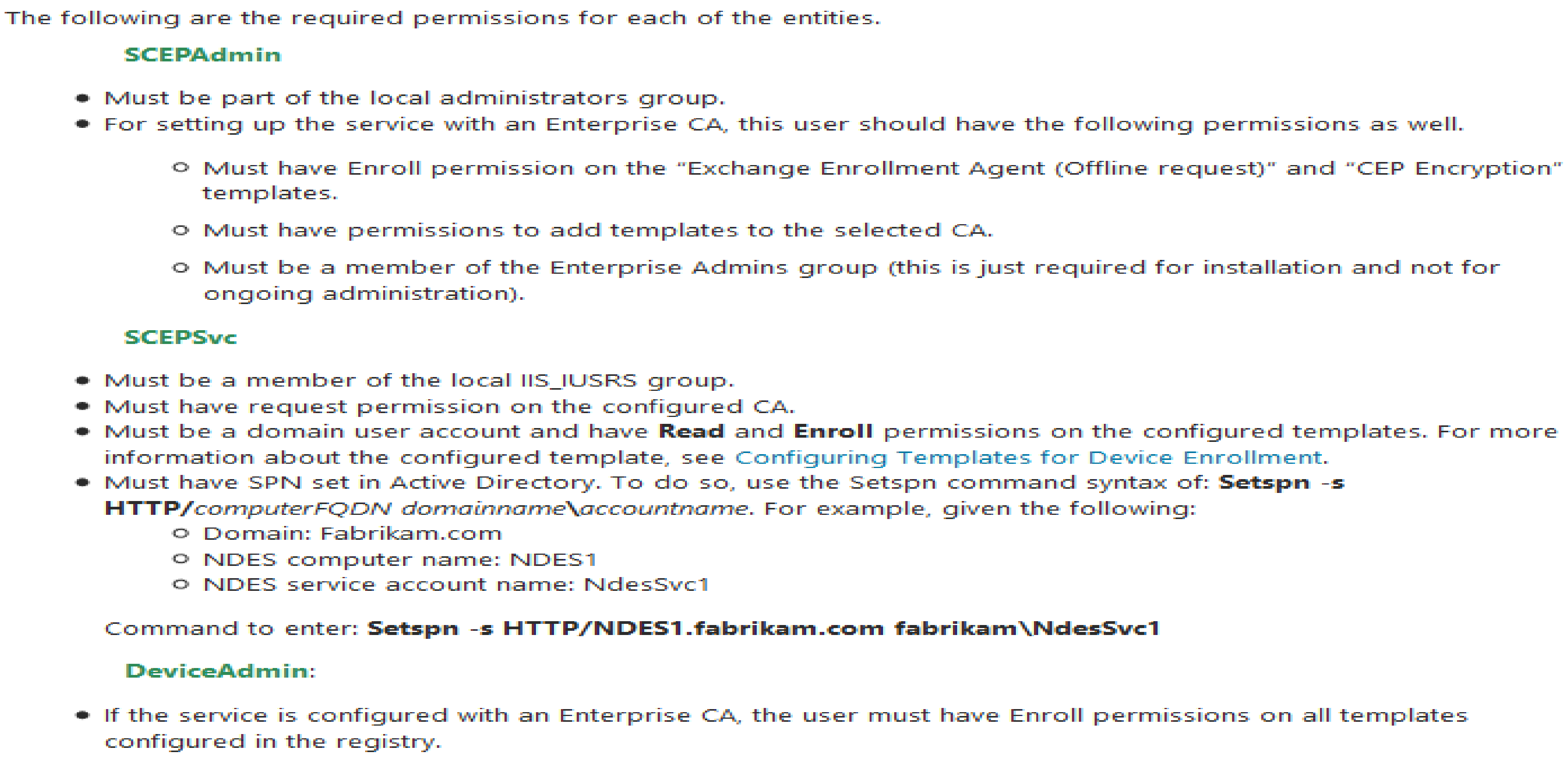
Network Device Enrollment Service



https://<ServerName>/certsrv/mscep_admin

Hands On: Configuring NDES

Pre-requisite for NDES installation



The following are the required permissions for each of the entities.

SCEPAdmin

- Must be part of the local administrators group.
- For setting up the service with an Enterprise CA, this user should have the following permissions as well.
  - Must have Enroll permission on the "Exchange Enrollment Agent (Offline request)" and "CEP Encryption" templates.
  - Must have permissions to add templates to the selected CA.
  - Must be a member of the Enterprise Admins group (this is just required for installation and not for ongoing administration).

SCEPSvc

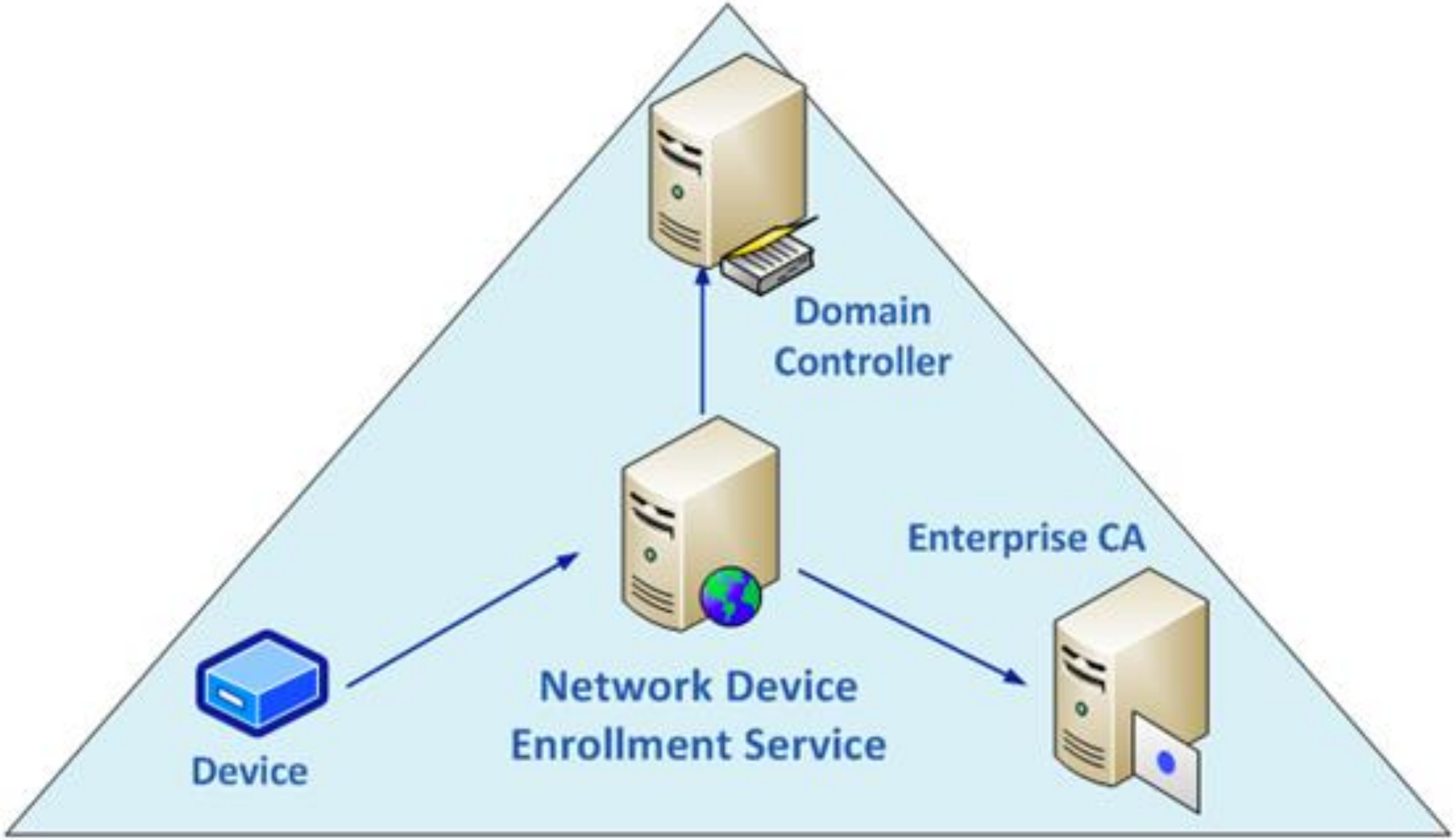
- Must be a member of the local IIS_IUSRS group.
- Must have request permission on the configured CA.
- Must be a domain user account and have **Read** and **Enroll** permissions on the configured templates. For more information about the configured template, see Configuring Templates for Device Enrollment.
- Must have SPN set in Active Directory. To do so, use the Setspn command syntax of: **Setspn -s HTTP/***computerFQDN domainname*\*accountname*. For example, given the following:
  - Domain: Fabrikam.com
  - NDES computer name: NDES1
  - NDES service account name: NdesSvc1

Command to enter: **Setspn -s HTTP/NDES1.fabrikam.com fabrikam\NdesSvc1**

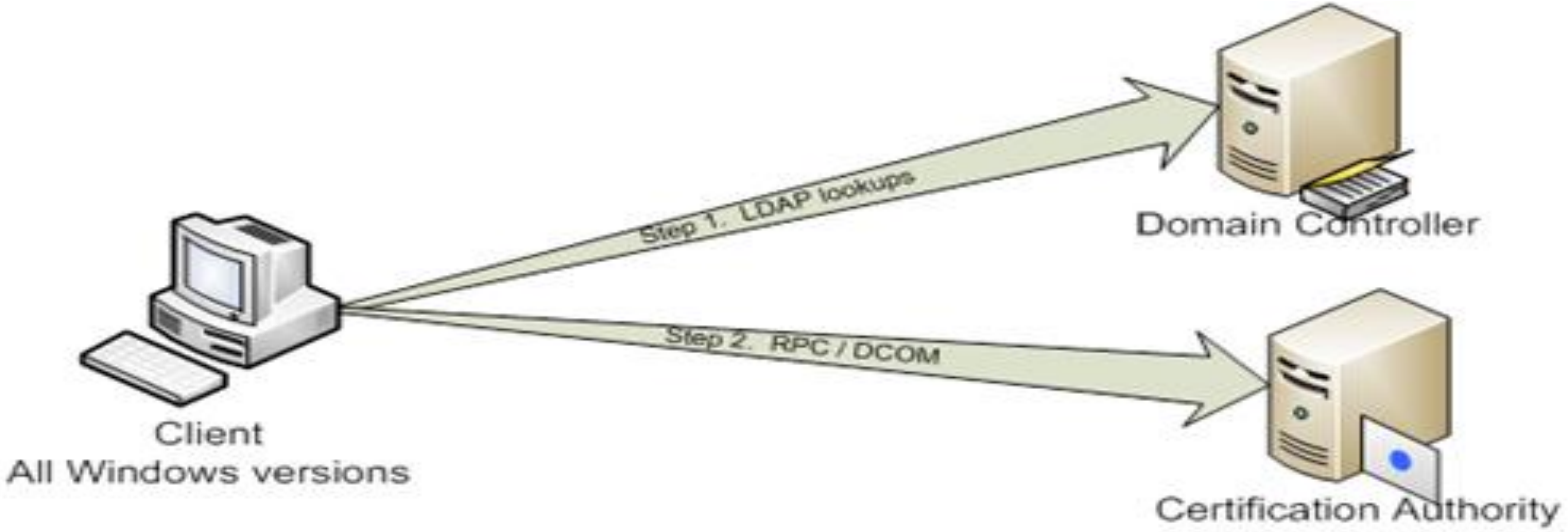
DeviceAdmin:

- If the service is configured with an Enterprise CA, the user must have Enroll permissions on all templates configured in the registry.

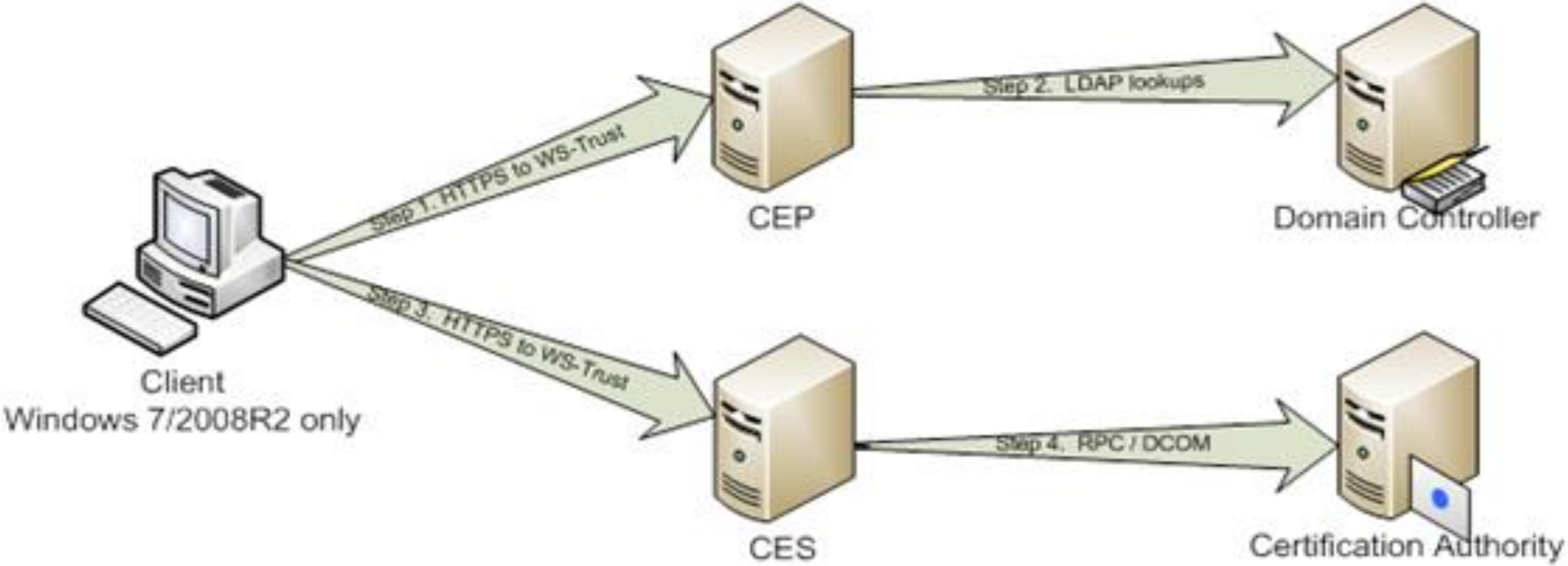
Hands On: Configuring NDES



Certificate enrollment without CEP / CES



Certificate enrollment with CEP / CES



Certificate Enrollment Service (CES)

- CES is another web service that allows users and computers to perform certificate enrollment by using the HTTPS protocol.
- Together with the CEP web service, CES enables policy-based certificate enrollment when the client computer is not a member of a domain or when a domain member is not connected to the domain.
- CEP/CES also enables cross-forest policy-based certificate enrollment for Windows 7 or Windows Server 2008 R2 clients
- CES role will require Kerberos delegation to be configured because it impersonates the user to the CA DCOM interface.

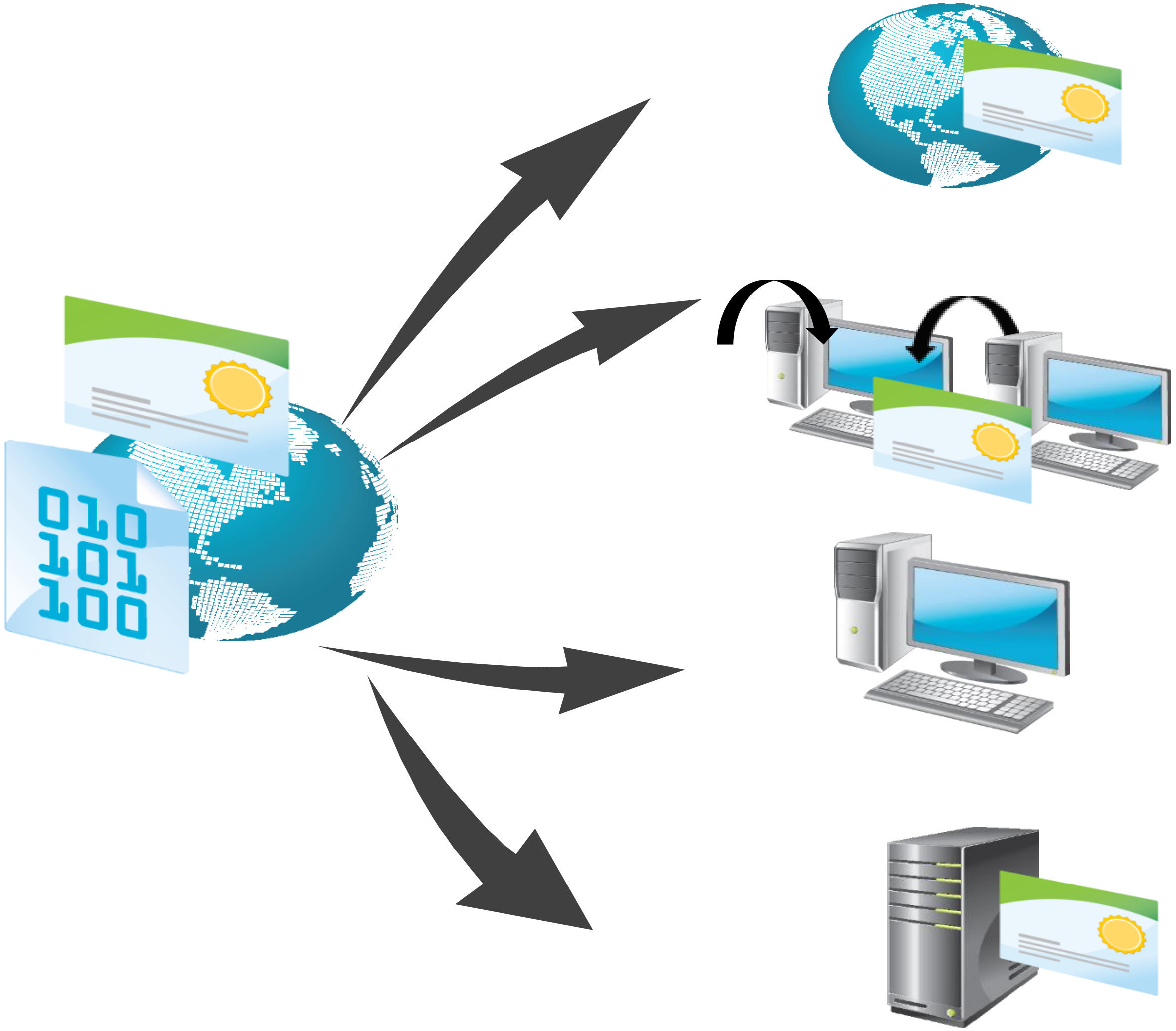
Certificate Enrollment Policy (CEP)

- CEP is a web service that enables users and computers to obtain certificate enrollment policy information. This information includes what types of certificates can be requested and which CAs can issue them.
- Only available on Windows Server 2008 R2 above and the only clients that are capable of requesting certificates via CEP and CES is Windows 7 and Windows Server 2008 R2 above
- Roles can be used with Windows Server 2003, 2008, 2008R2 and 2012R2 Certification Authorities (CA).

Demonstration: Configuring CEP and CES

In this demonstration, you will see how to configure CES and CEP servers

What Is an Online Responder?



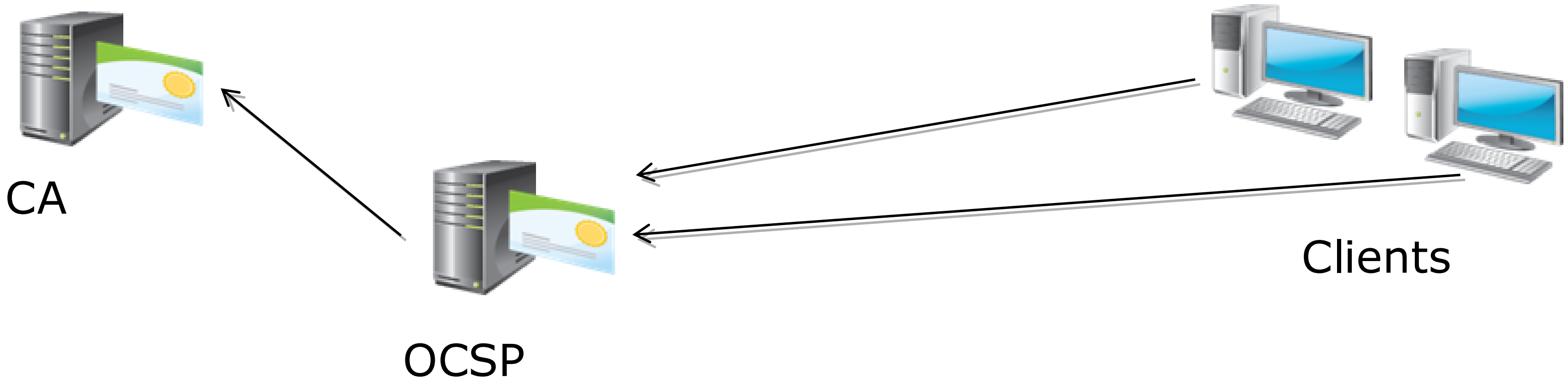
Uses OCSP validation and revocation checking using HTTP

Receives and responds dynamically to individual requests

Supports only Windows Server 2008, Windows Vista, and newer Windows operating systems

Functions as a responder to multiple CAs

How OCSP works



Demonstration: Configuring an Online Responder

In this demonstration, you will see how to configure an Online Responder