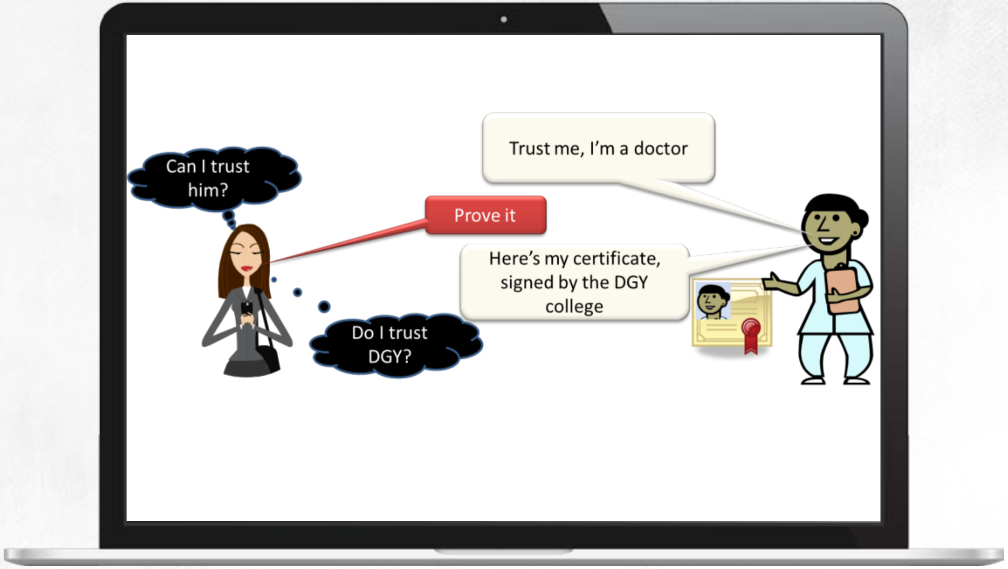
Public Key Infrastructure, or the ”Trust but verify” rule and How to deploy it

IT SECURITY ACADEMY
www.SecAcademy.com

How to build a trust relationship

Certificates are used to verify identity

To trust a certificate, you must trust the certification authority that issued the certificate

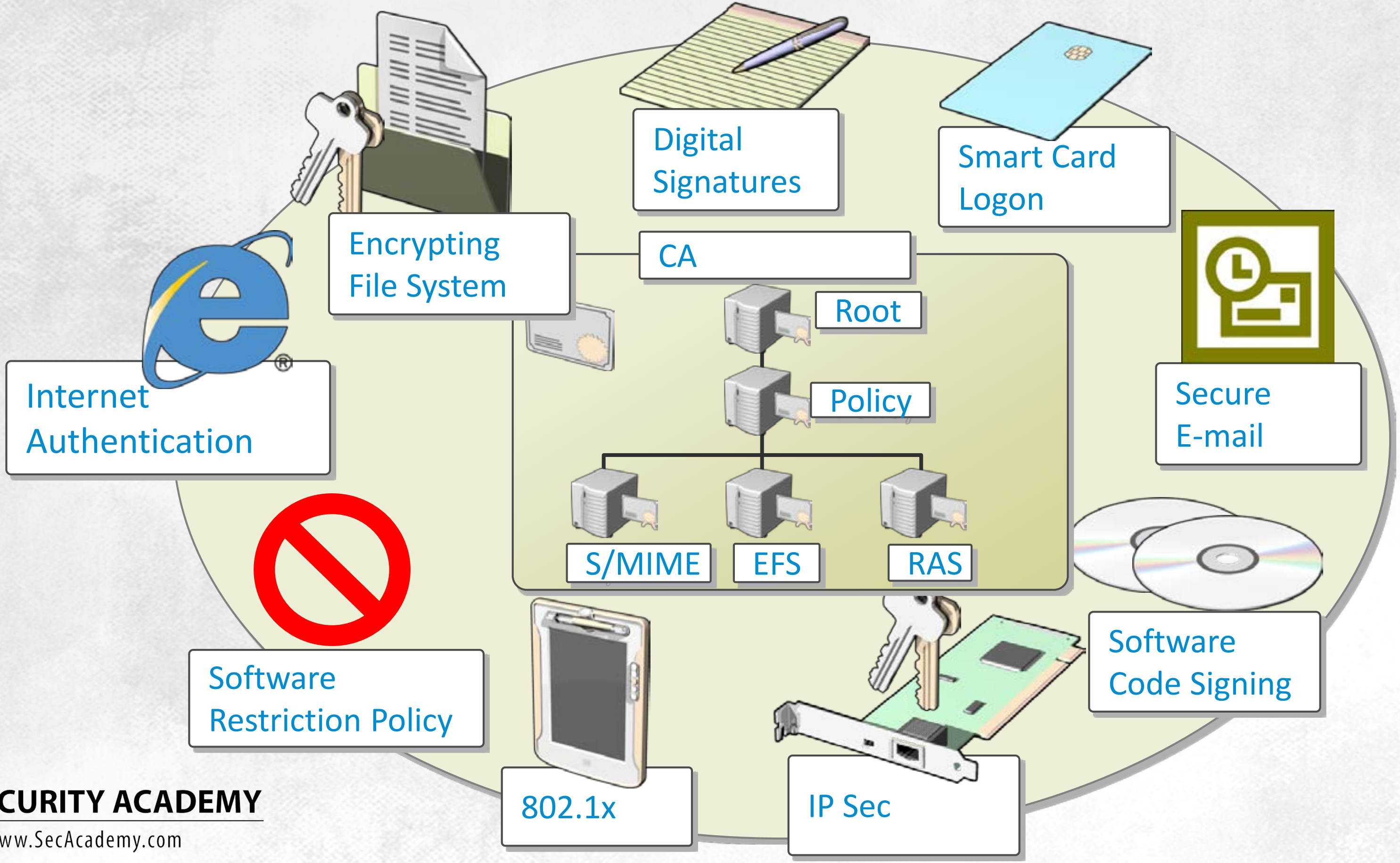


Public key infrastructure

A public key infrastructure is made up from:

- Certification authorities
- Certificates issued by CAs
- Certificate templates
- Certificate distribution points
- Certificate revocation list distribution points
- And software for using and managing a PKI

Public key infrastructure



Digital Signatures

Smart Card Logon

Encrypting File System

CA

Root

Policy

S/MIME

EFS

RAS

Internet Authentication

Secure E-mail

Software Code Signing

Software Restriction Policy

802.1x

IP Sec

Public key infrastructure

Deploying a PKI in Windows will allow you to:

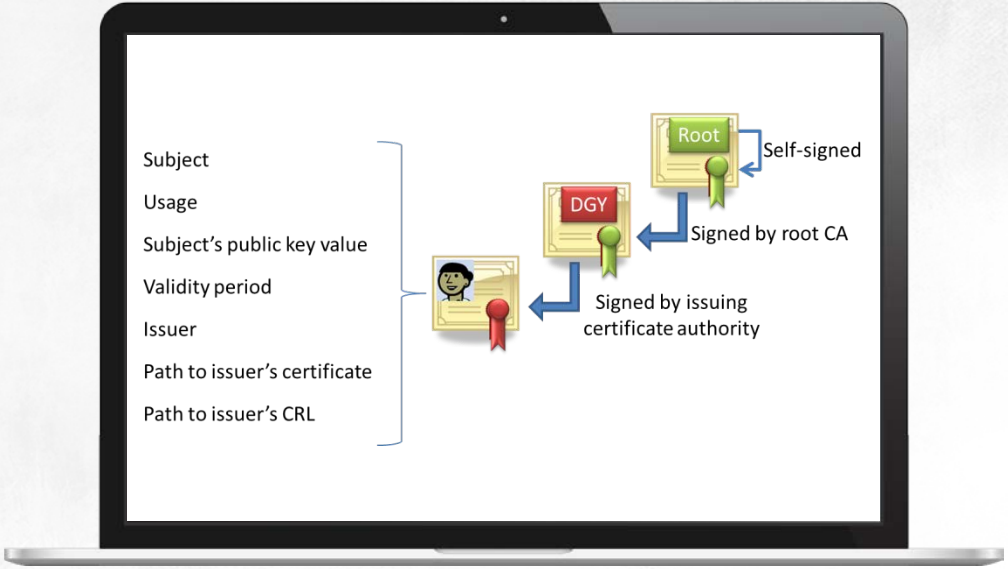
- Encrypt stored data using EFS
- Implement strong user authentication with the help of smart cards and the expanded version five of Kerberos
- Authenticate users and networked devices (both in wired and wireless networks) using the 802.1X standard
- Encrypt and digitally signed email messages using S/MIME
- Digitally sign programs
- Encrypt and digitally sign transmitted data using IPSec
- Verify the identity of web servers and guarantee the confidentiality and integrity of data transmitted across the servers and their clients, using SSL/TLS
- Enforce health policy compliance for networked devices, using NAP
- Use software restriction policies to block programs based on their manufacturer certificates

A public key infrastructure is a complex and fully functional but easy-to-deploy cryptography system

How to trust certificates

A certificate can only be trusted if the certificate for the root CA that issued it is on the list of trusted certification authorities

The root CA certificate is the basis of a trust relationship



Subject

Usage

Subject's public key value

Validity period

Issuer

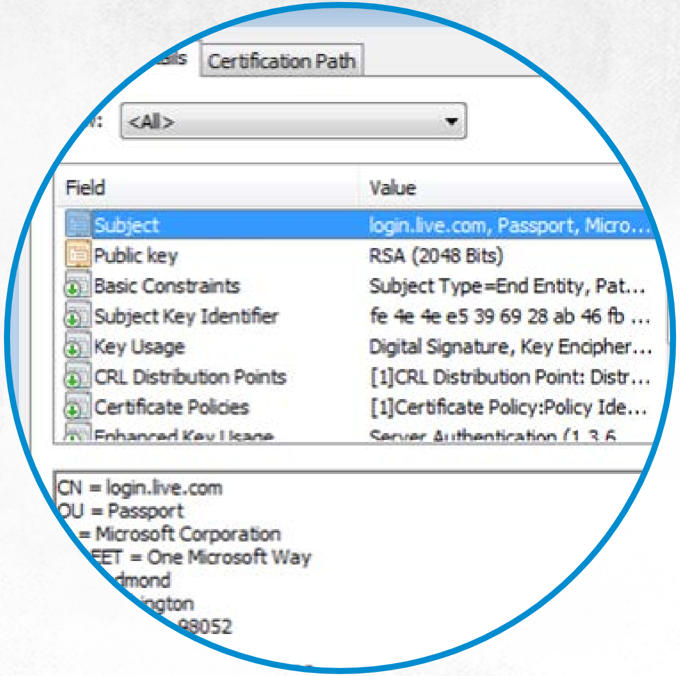
Path to issuer's certificate

Path to issuer's CRL

Certificates

All certificates that comply with the X.509 standard must have:

- Version number (most certificates nowadays comply with the third version of X.509)
- Subject's public key
- Serial number unique for all certificates issued by a given CA
- Certificate revocation list distribution points, or the URLs where you can check if a certificate is revoked
- URLs where you can obtain information on CAs with AIA extensions
- Information on enhanced key usage
- Certificate issuance policies and issuer statement

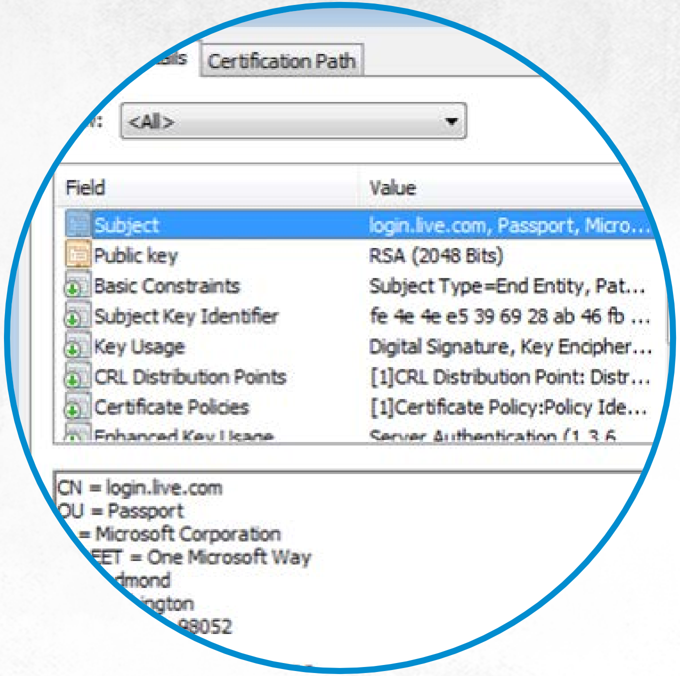


Field	Value
Subject	login.live.com, Passport, Micro...
Public key	RSA (2048 Bits)
Basic Constraints	Subject Type=End Entity, Pat...
Subject Key Identifier	fe 4e 4e e5 39 69 28 ab 46 fb ...
Key Usage	Digital Signature, Key Encipher...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Enhanced Key Usage	Server Authentication (1.3.6

CN = login.live.com
OU = Passport
= Microsoft Corporation
EET = One Microsoft Way
dmond
ington
98052

Certificates

Certificates are digitally signed by issuing certification authorities, and any changes made to the certificate will cause it to be revoked



Field	Value
Subject	login.live.com, Passport, Micro...
Public key	RSA (2048 Bits)
Basic Constraints	Subject Type=End Entity, Pat...
Subject Key Identifier	fe 4e 4e e5 39 69 28 ab 46 fb ...
Key Usage	Digital Signature, Key Encipher...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Enhanced Key Usage	Server Authentication (1.3.6

CN = login.live.com
OU = Passport
= Microsoft Corporation
EET = One Microsoft Way
dmond
ngton
98052

Certificate life cycle

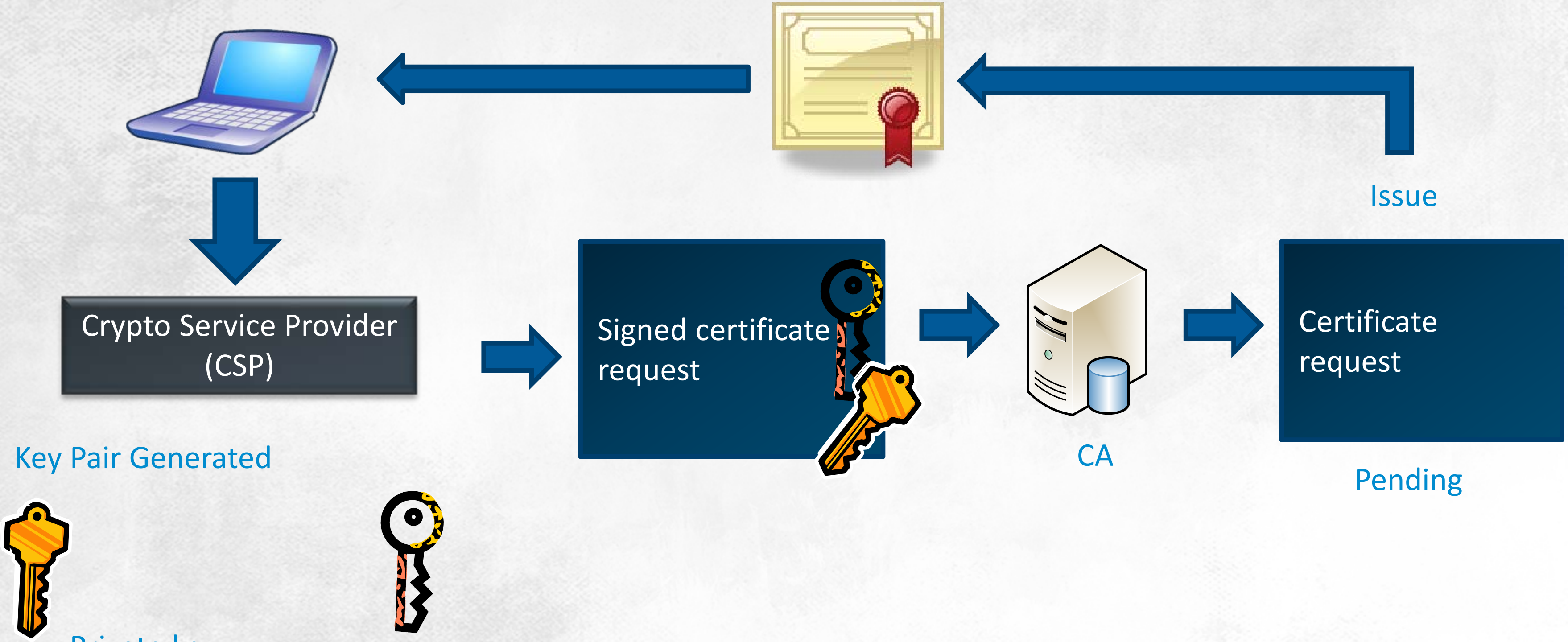
- CA receives a certificate request
- If the request is authorised, the CA issues the certificate
- The certificate is delivered to the user, host or service
- Applications in the PKI use the certificate correspondingly to its usage and purposes
- The certificate expires (it may also be revoked prior to expiry). From this point on, it is impossible to use the certificate
- The CA receives a request to renew the existing certificate. If it is authorised, the certificate is renewed and can be used again

Certificate life cycle

A certificate must be validated before it can be used. Validating a certificate is a two-stage process:

- A certificate is correct (trusted) only if it was signed by a trusted CA, and that's why trusted root CA certificates are downloaded first. At this stage the system checks certificates submitted by AIA points and the group policy applicable for the computer as well as certificates cached earlier
- Next, the system checks the validity of all certificates on the path between the trusted CA and the checked certificate

Certificate issuing



Crypto Service Provider (CSP)

Key Pair Generated

Signed certificate request

CA

Certificate request

Pending

Issue

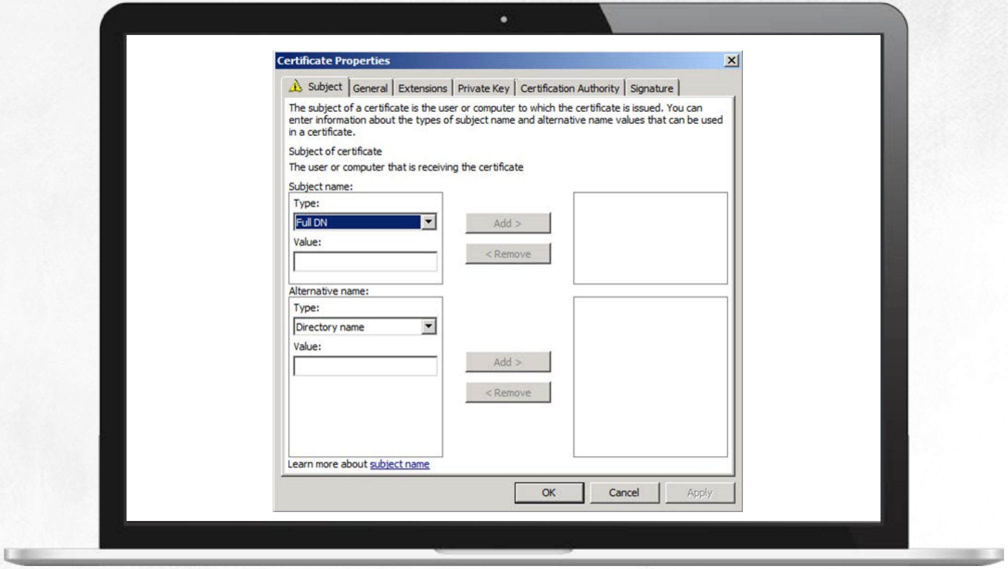
Private key stored to profile or HSM

Public key sent to CA

Certificate request

Requests may be made:

- Through the Certificates MMC
- Through a CA website
- Automatically



Certificate Properties

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate

The user or computer that is receiving the certificate

Subject name:

Type: Full DN

Value:

Alternative name:

Type: Directory name

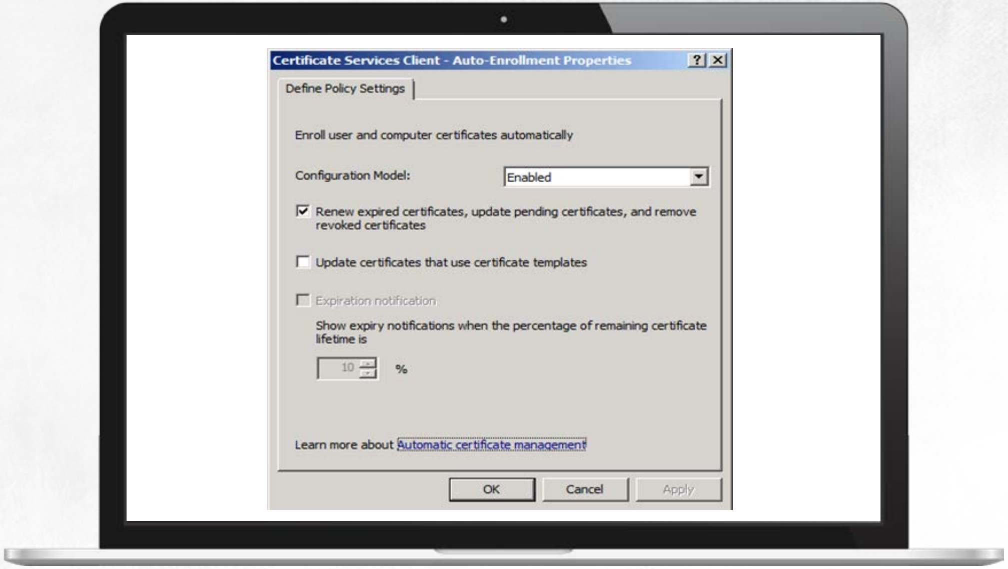
Value:

Learn more about subject name

Certificate request

Requests may be made:

- Through the Certificates MMC
- Through a CA website
- Automatically



Certificate Services Client - Auto-Enrollment Properties

Enroll user and computer certificates automatically

Configuration Model: Enabled

☑ Renew expired certificates, update pending certificates, and remove revoked certificates

☐ Update certificates that use certificate templates

☐ Expiration notification

Show expiry notifications when the percentage of remaining certificate lifetime is

10 %

Learn more about Automatic certificate management

Certificate verification

To be trusted (accepted) the certificate:

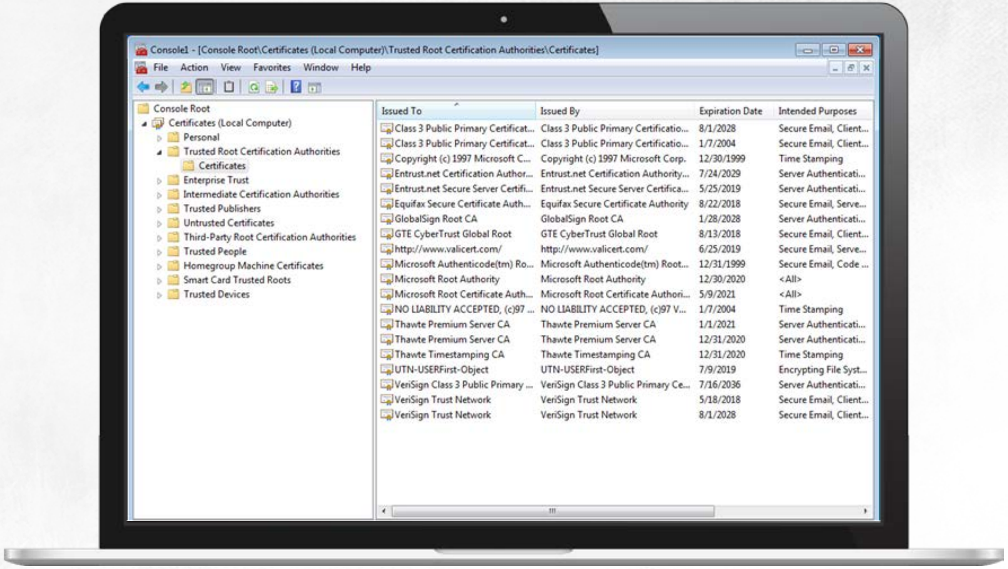
- Must comply with X.509
- Must have a correct thumbprint
- Must be valid (not pertaining to root CA certificates)
- Must not be revoked (its number is not included in CRLs issued by an appropriate CA)
- Is used as intended

Certificate authorities

System users get their identity verified against certificates, and this means that also certification authorities must have their certificates

This is applicable to root CAs as well (CAs at the very top of a trust hierarchy)

The root CA certificate is self-signed as the CA cannot request another CA to issue the certificate


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Homegroup Machine Certificates
Smart Card Trusted Roots
Trusted Devices

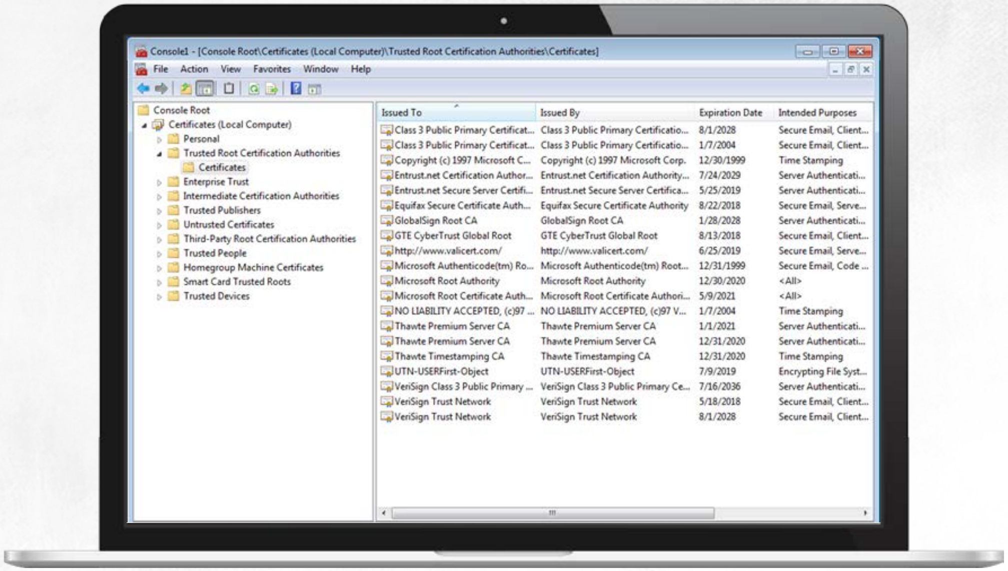
Issued To	Issued By	Expiration Date	Intended Purposes
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Secure Email, Client...
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	1/7/2004	Secure Email, Client...
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping
Entrust.net Certification Author...	Entrust.net Certification Authority...	7/24/2029	Server Authenticati...
Entrust.net Secure Server Certifi...	Entrust.net Secure Server Certifica...	5/25/2019	Server Authenticati...
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Server Authenticati...
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Secure Email, Client...
http://www.valicert.com/	http://www.valicert.com/	6/25/2019	Secure Email, Serve...
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...
Microsoft Root Authority	Microsoft Root Authority	12/30/2020	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	1/7/2004	Time Stamping
Thawte Premium Server CA	Thawte Premium Server CA	1/1/2021	Server Authenticati...
Thawte Premium Server CA	Thawte Premium Server CA	12/31/2020	Server Authenticati...
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping
UTN-USERFirst-Object	UTN-USERFirst-Object	7/9/2019	Encrypting File Syst...
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	7/16/2036	Server Authenticati...
VeriSign Trust Network	VeriSign Trust Network	5/18/2018	Secure Email, Client...
VeriSign Trust Network	VeriSign Trust Network	8/1/2028	Secure Email, Client...

Certificate authorities

Building trust starts with adding this certificate to your list of trusted certification authorities

The global (Internet) trust model involves automatically placing several root CA certificates on lists of trusted certification authorities for all computers

If you trust a CA, you trust all the valid certificates it signs, including certificates issued for other CAs

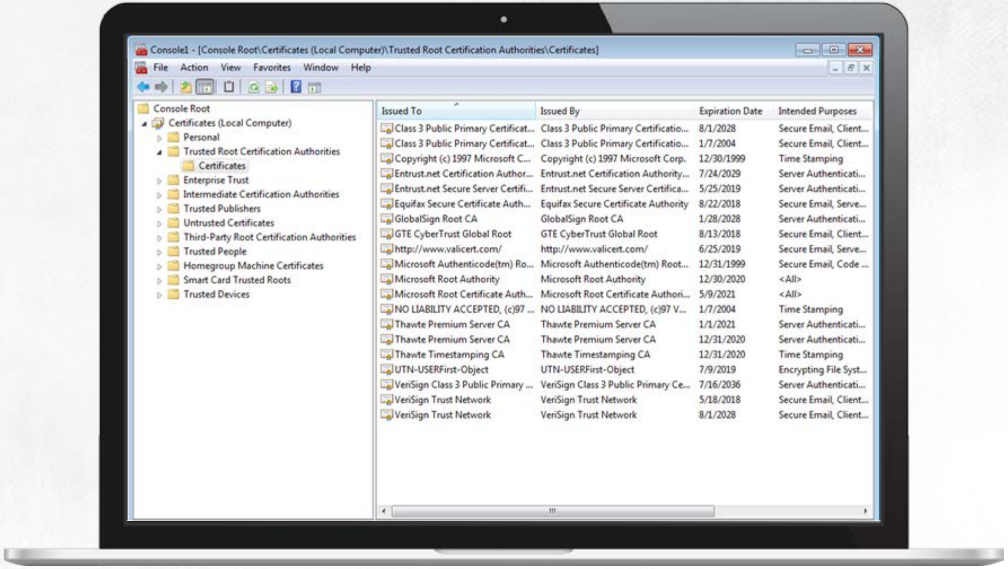

File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Homegroup Machine Certificates
Smart Card Trusted Roots
Trusted Devices

Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Secure Email, Client...
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	1/7/2004	Secure Email, Client...
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping
Entrust.net Certification Author...	Entrust.net Certification Authority...	7/24/2029	Server Authenticati...
Entrust.net Secure Server Certifi...	Entrust.net Secure Server Certifica...	5/25/2019	Server Authenticati...
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Server Authenticati...
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Secure Email, Client...
http://www.valicert.com/	http://www.valicert.com/	6/25/2019	Secure Email, Serve...
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...
Microsoft Root Authority	Microsoft Root Authority	12/30/2020	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	1/7/2004	Time Stamping
Thawte Premium Server CA	Thawte Premium Server CA	1/1/2021	Server Authenticati...
Thawte Premium Server CA	Thawte Premium Server CA	12/31/2020	Server Authenticati...
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping
UTN-USERFirst-Object	UTN-USERFirst-Object	7/9/2019	Encrypting File Syst...
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	7/16/2036	Server Authenticati...
VeriSign Trust Network	VeriSign Trust Network	5/18/2018	Secure Email, Client...
VeriSign Trust Network	VeriSign Trust Network	8/1/2028	Secure Email, Client...

Certificate authorities

Trust means that if you trust a root CA, you also trust the certificates signed by subordinate CA it authorises



Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Homegroup Machine Certificates
Smart Card Trusted Roots
Trusted Devices

Issued To	Issued By	Expiration Date	Intended Purposes
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Secure Email, Client...
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	1/7/2004	Secure Email, Client...
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping
Entrust.net Certification Author...	Entrust.net Certification Authority...	7/24/2029	Server Authenticati...
Entrust.net Secure Server Certifi...	Entrust.net Secure Server Certifica...	5/25/2019	Server Authenticati...
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Server Authenticati...
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Secure Email, Client...
http://www.valicert.com/	http://www.valicert.com/	6/25/2019	Secure Email, Serve...
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...
Microsoft Root Authority	Microsoft Root Authority	12/30/2020	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	1/7/2004	Time Stamping
Thawte Premium Server CA	Thawte Premium Server CA	1/1/2021	Server Authenticati...
Thawte Premium Server CA	Thawte Premium Server CA	12/31/2020	Server Authenticati...
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping
UTN-USERFirst-Object	UTN-USERFirst-Object	7/9/2019	Encrypting File Syst...
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	7/16/2036	Server Authenticati...
VeriSign Trust Network	VeriSign Trust Network	5/18/2018	Secure Email, Client...
VeriSign Trust Network	VeriSign Trust Network	8/1/2028	Secure Email, Client...

Planning the PKI

Because one CA sign should not issue all certificates in a system, the first thing to consider is to plan a certification authority hierarchy

Designing your CA hierarchy, here's several factors you should take into account:

- Certificate usage (secure email, authenticating users via smart cards, encrypting files, using IPSec to secure communications)
- The existing security policy (for instance, the different privileges of permanent and contingent workers)
- The (probable) necessity to exchange data with business partners
- Administrative requirements (who will manage certification authorities and certificates)
- Availability and reliability requirements (how a potential CA failure will affect the operation of a computer system and when this disaster must be dealt with)
- Legal requirements (for instance whether your system must comply with international security standards to get for example the FIPS 140-1 level 2 certificate)

Planning the PKI

If your system is running multiple certification authorities, this minimises the risks connected to compromising the root CA

Because the loss of trust between all users is a consequence of losing control over the root certification authority, the root CA must be offline and stored in a safe place

Deploying the PKI

Windows servers may have the role of a stand-alone certification authority or enterprise certification authority (which are CAs integrated with Active Directory)

Stand-alone	Enterprise certification authority
Doesn’t need Active Directory	May only be run on a member server in Active Directory (including domain controllers).
Enrolment must be requested manually	Autoenrollment possible, based on certificate templates.
Certificate requests must be evaluated manually	Certificate requests may be evaluated automatically, based on a certificate’s access control list

Root ca

The CAPolicy.inf configuration file should contain the following:

- Existing security policies. Each policy must have a unique name and identifier, a short description and the URL to it (this data will be put in all certificates issued by a CA)
- Publication intervals for CRLs
- Validity period for CA certificates and settings for renewal after expiry
- CA key length
- CRL distribution point URLs as well as AIA URLs. For root certification authorities, both pieces of information should be deleted. Thanks to this, only the presence of the root CA certificate will be checked

A finished CAPolicy.inf file should be saved to the Windows system folder

The Add Roles wizard will guide you through the remaining steps in root CA installation

```
[Version]
Signature = "$Windows NT$"

[CAPolicy]
Policies = InternalPolicy

[InternalPolicy]
OID = 1.2.3.4.5.6.7.8.9.10
NOTICE = "Root CA security policy …"
URL = "http://subca.ms.pl/RootCA.htm"

[certsrv_server]
RenewalKeyLength = 4096
RenewalValidityPeriodUnits = 16
RenewalValidityPeriod = years
CRLPeriodUnits = 12
CRLPeriod = weeks
CRLDeltaPeriodUnits = 0
CRLDeltaPeriod = days

[AuthorityInformationAccess]
Empty = True

[CRLDistributionPoint]
Empty = True
```

Root ca

Since root CA will not be online at all times, you need to change the default paths to its CRL distribution points and authority information access (AIA) as well as prolong the validity period of certificates issued by this CA

Additionally, you need to prolong the validity period of certificates issued by root CA to for example 10 years: this value will simultaneously specify the maximum possible validity period for certificates signed by subordinate certification authorities

- certutil -setreg ca\ValidityPeriodUnits 10
- certutil -setreg ca\ValidityPeriod "Years"

Root ca

Next, you need to generate a CRL and publish it along with a root CA certificate on a web server and in Active Directory

- certutil -addstore -f Root RootCA_ROOTCA.crt
- certutil -addstore -f Root RootCA.crl
- certutil -dspublish -f RootCA_ROOTCA.crt
- certutil -dspublish -f RootCA.crl

Root ca

Installing and setting up subordinate certification authorities follows the same blueprint and is independent from their position in the hierarchy

Because these certification authorities are usually enterprise CAs, they don’t require having a CAPolicy.inf file or self-publication of their certificates

What is required is having them signed by the root CA

PKI administration

Administering a public key infrastructure is managing certification authorities and certificates

The two functions should be delegated to two different administrators. The CC standards specify that no user of a public key infrastructure may have more than one administrative role in it

In Windows servers you can assign one of these four roles to users (members of any of these cannot be simultaneously system administrators)

- Certification authority administrator
- Certificate manager
- Certification authority backup operator with rights to create and restore backups of certification authorities
- Certification authority auditor with rights to monitor all other system users

The two latter roles are configured using Group Policy

When you assign a user to a role, enable role separation. When role separation is enabled, users who are members of more than one role will lose access to the certification authority

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

PKI administration

Administering a public key infrastructure is managing certification authorities and certificates

The two functions should be delegated to two different administrators. The CC standards specify that no user of a public key infrastructure may have more than one administrative role in it

In Windows servers you can assign one of these four roles to users (members of any of these cannot be simultaneously system administrators)

- Certification authority administrator
- Certificate manager
- Certification authority backup operator with rights to create and restore backups of certification authorities
- Certification authority auditor with rights to monitor all other system users

The two latter roles are configured using Group Policy

When you assign a user to a role, enable role separation. When role separation is enabled, users who are members of more than one role will lose access to the certification authority

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

PKI administration

Administering a public key infrastructure is managing certification authorities and certificates

The two functions should be delegated to two different administrators. The CC standards specify that no user of a public key infrastructure may have more than one administrative role in it

In Windows servers you can assign one of these four roles to users (members of any of these cannot be simultaneously system administrators)

- Certification authority administrator
- Certificate manager
- Certification authority backup operator with rights to create and restore backups of certification authorities
- Certification authority auditor with rights to monitor all other system users

The two latter roles are configured using Group Policy

When you assign a user to a role, enable role separation. When role separation is enabled, users who are members of more than one role will lose access to the certification authority

certutil -setreg CA\RoleSeparationEnabled 1

PKI administration

Managing certification authorities task list:

- Installing and setting up certification authorities
- CA certificate renewal
- Monitoring operations run by users and administrators in the system
- Identifying key recovery agents
- Creating and restoring CA backups

Managing certificates task list:

- Creating and modifying certificate templates
- Evaluating certificate requests
- Revoking certificates and deleting revoked certificates
- Publishing CRLs
- Creating and restoring users’ private key backups

Certificate templates

Stored in the Active Directory folder, certificate templates define the contents and format of certificates: key length, validity period and usage

Some of these certificates can allow you to create a general-purpose certificate, while others are used to generate specific-purpose certificates

Depending on the recipient type, templates are split into user certificate templates and computer certificate templates

Certificate templates

Three versions:

- Version 1 templates are Windows 2000-based (can also be used in newer systems) and are not customisable apart from permissions. By default, there are more than 20 version 1 certificate templates installed, including administrator, computer, domain controller and user templates
- Version 2 certificate templates comply with Windows 2003 and newer systems and are fully customisable but may only be issued by Windows Enterprise or Datacenter servers. At CA installation, eight version 2 certificate templates are created, including key recovery agent templates, RAS and IAS server templates and Kerberos authentication templates
- Version 3 certificate templates comply with Windows 2008 and newer systems and are fully customisable, enabling among others the use of the most modern cryptography algorithms. Like version 2 certificate templates, they can only be issued by Windows Enterprise or Datacenter servers. At CA installation, one version 3 certificate template is created automatically: it’s the certificate template that allows computers that have the online responder role to digitally sign CRLs

Certificate revocation

Three versions:

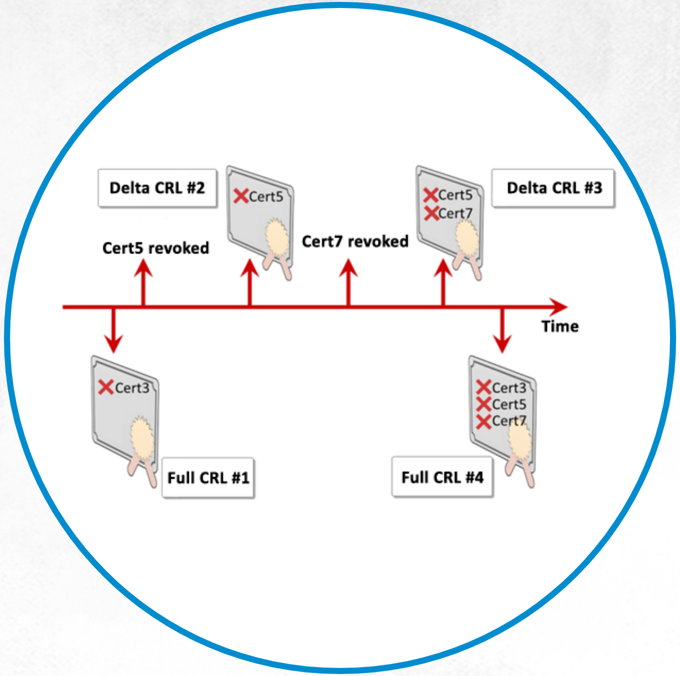
- Version 1 templates are Windows 2000-based (can also be used in newer systems) and are not customisable apart from permissions. By default, there are more than 20 version 1 certificate templates installed, including administrator, computer, domain controller and user templates
- Version 2 certificate templates comply with Windows 2003 and newer systems and are fully customisable but may only be issued by Windows Enterprise or Datacenter servers. At CA installation, eight version 2 certificate templates are created, including key recovery agent templates, RAS and IAS server templates and Kerberos authentication templates
- Version 3 certificate templates comply with Windows 2008 and newer systems and are fully customisable, enabling among others the use of the most modern cryptography algorithms. Like version 2 certificate templates, they can only be issued by Windows Enterprise or Datacenter servers. At CA installation, one version 3 certificate template is created automatically: it's the certificate template that allows computers that have the online responder role to digitally sign CRLs

Certificate revocation

A certificate manager can revoke a certificate even prior to its expiry

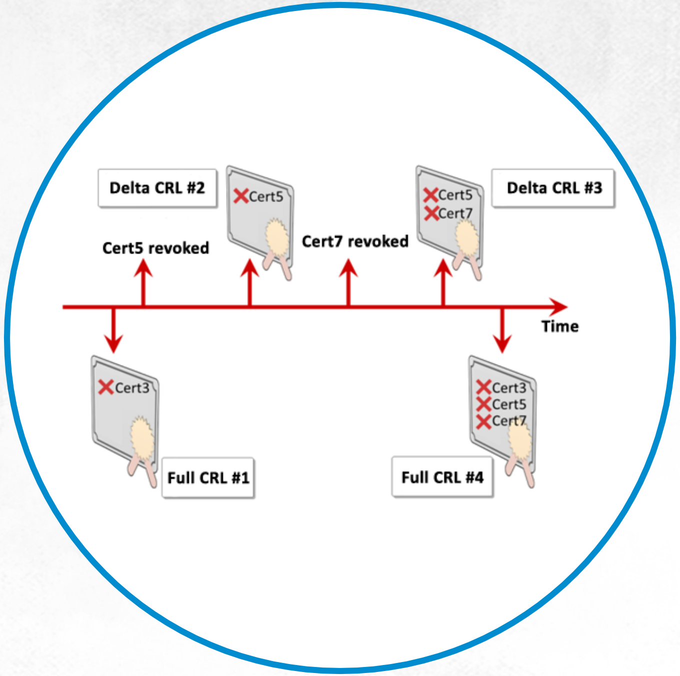
The serial numbers of revoked certificates are automatically put on the CRL lists of a certification authority and once they are published, it’s no longer possible to use the certificate

CRL are the go-to way for publishing information about revoked certificates: the more often CRLs are published, the shorter the certificates that have been revoked in the meantime will be used



Certificate revocation

Regular publications of all CRLs will produce an increase in the amount of data sent across networks. A good solution to this problem is publishing full and Delta CRLs. While full CRLs contain the numbers and reasons for revoking all certificates of a given CA (frequently over several megabytes of data), Delta CRLs only contain information about certificates that have not been included in the previously-published full CRL

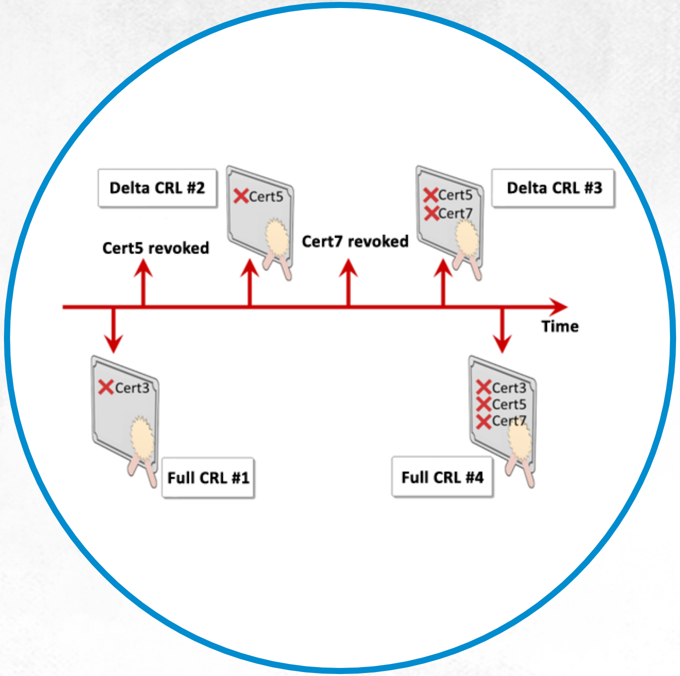


Certificate revocation

Most symmetric ciphers are block ciphers

Block cipher mode defines the transformation method of variable-length messages (streams of data) into fixed-length blocks

Most block ciphers use Feistel's network, which may be used with any encryption function and doesn't require the function to be reversible



Key archival

Enterprise certification authorities running in the Windows Enterprise or Datacenter systems can be tasked with archiving private keys

This allows you to restore certificates and related private keys that are lost when a profile is deleted, a smart card is damaged, when the host is corrupted or lost or when the system is reinstalled

Key archival

Key archival and recovery:

- A user requests a certificate based on a template with the enabled option Archive subject’s encryption private key
- The private key, generated in a user’s computer, is encrypted using the certification authority public key and is added to a certificate request sent to this authority
- The CA decrypts the private key of the certificate subject, and then encrypts it using a key recovery agent’s key and saves it to its database
- The user reports the loss of a private key to a certificate manager
- The certificate manager retrieves the serial number of the certificate to which the lost key was related
- The certificate manage retrieves the encrypted private key and exports it along with the user certificate to the PKCS #7 file
- The encrypted file is forwarded to the key recovery agent, which decrypts it using its private key
- The key recovery agent exports the user certificate and the related private key to the PKCS #12 file
- PKCS #12 along with the password that protects it is released to the user, who imports the certificate contained in it and the lost private key

THANKS