# PKI & Windows CA IIS 7.x

Jan Žák

Microsoft CERTIFIED Trainer

Systems Administration
Systems Engineering

# PKI & Windows CA

# Co je to PKI?

- **PKI** (Public Key Infrastructure) je soustavou technických a především organizačních opatření spojených s vydáváním, správou, používáním a odvoláváním platností kryptografických klíčů a certifikátů ☺
- Obvykle pod termínem „PKI“ rozumíme instalaci CA a vydávání certifikátů ☹

# Kryptografické algoritmy

- Otisk (hash)
  - Otisk je jednocestná funkce, nevyužívají se klíče
  - MD-5, SHA-1, SHA-224/256/384/256..
- Symetrické šifry (Symmetric key algorithms)
  - Tajný klíč
  - DES, 3DES, IDEA, RC2/4, AES, Twofish…
- Asymmetric key algorithms
  - Veřejný a privátní (soukromý) klíč
  - RSA,
    - Diffie-Hellman (pro výměnu klíčů)
    - ECC – Elliptic Curve Cryptography

Public-key cryptography refers to a cryptographic system requiring two separate keys, one to lock or encrypt the plaintext, and one to unlock or decrypt the cyphertext. Neither key will do both functions. One of these keys is published or public and the other is kept private. If the lock/encryption key is the one published then the system enables private communication from the public to the unlocking key's owner. If the unlock/decryption key is the one published then the system serves as a signature verifier of documents locked by the owner of the private key.

- **MD5: 216a41e1db96e6f973dd92beba5d180f**
- **SHA1: 73e38d9ae1e6defe5e09c869542d6b2f455c3077**

Test

- **MD5: 0cbc6611f5540bd0809a388dc95a615b**

- **SHA1: 640ab2bae07bedc4c163f679a746f7ab7fb5d1fa**
- **SHA1: A94a8fe5ccb19ba61c4c0873d391e987982fbbd3** (test)

# Hash....

| Strength | Symetric | RSA | ECDSA | SHA |
|---|---|---|---|---|
| 80 bit | 2TDEA | RSA 1024 | ECDSA 160 | SHA-1 |
| 112 bit | 3TDEA | RSA 2048 | ECDSA 224 | SHA-224 |
| 128 bit | AES-128 | RSA 3072 | ECDSA 256 | SHA-256 |
| 192 bit | AES-192 | RSA 7680 | ECDSA 384 | SHA-384 |
| 256 bit | AES-256 | RSA 15360 | ECDSA 512 | SHA-512 |

# Comparable Algorithm Strengths (SP800-57)

http://www.sevecek.com

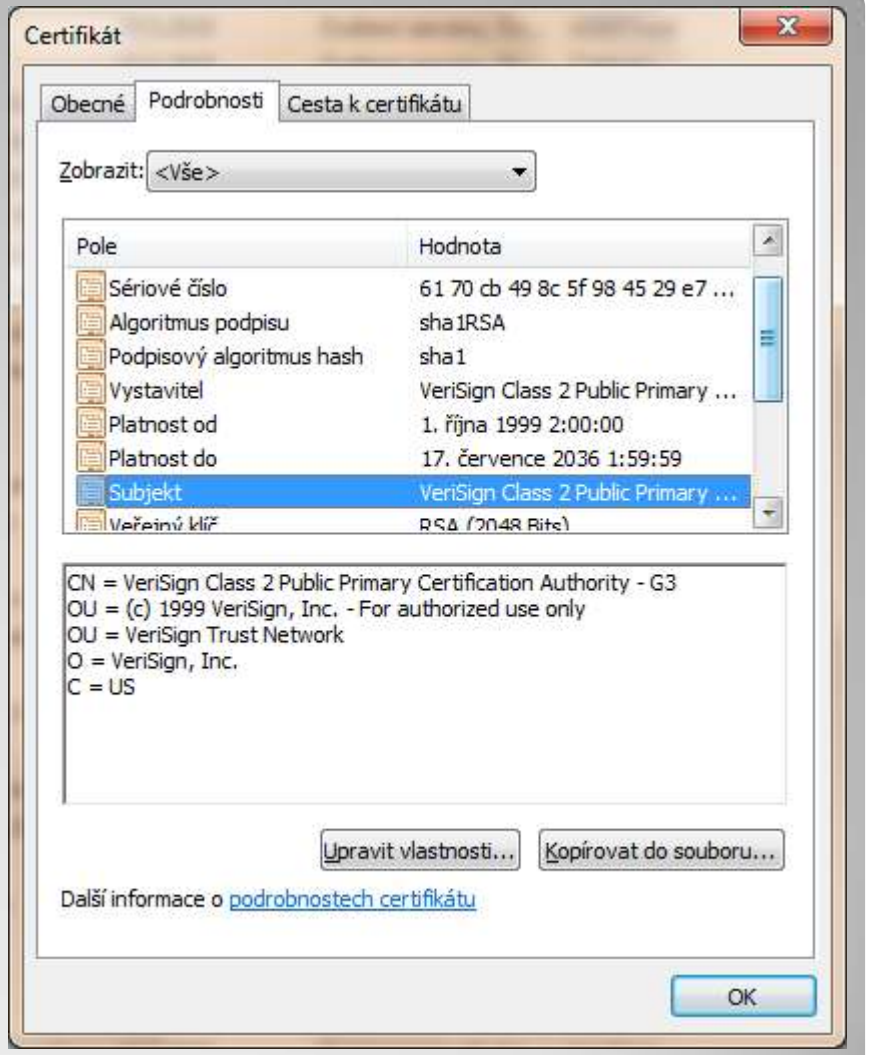
# Prostředky pro bezpečné ukládání aktiv

- Uložení na disk (roamingový profil, instalece dalšího OS…)
- Autentizační kalkulátory (pro autentizaci klienta, autorizaci dat…)
- Hardwarové klíče (USB, PCMCIA, SCSII…)
- Čipové karty (kontaktní, bezkontaktní)
- USB tokeny
- HSM (Host Security Modul) – „černá skříňka s výbušninou“)

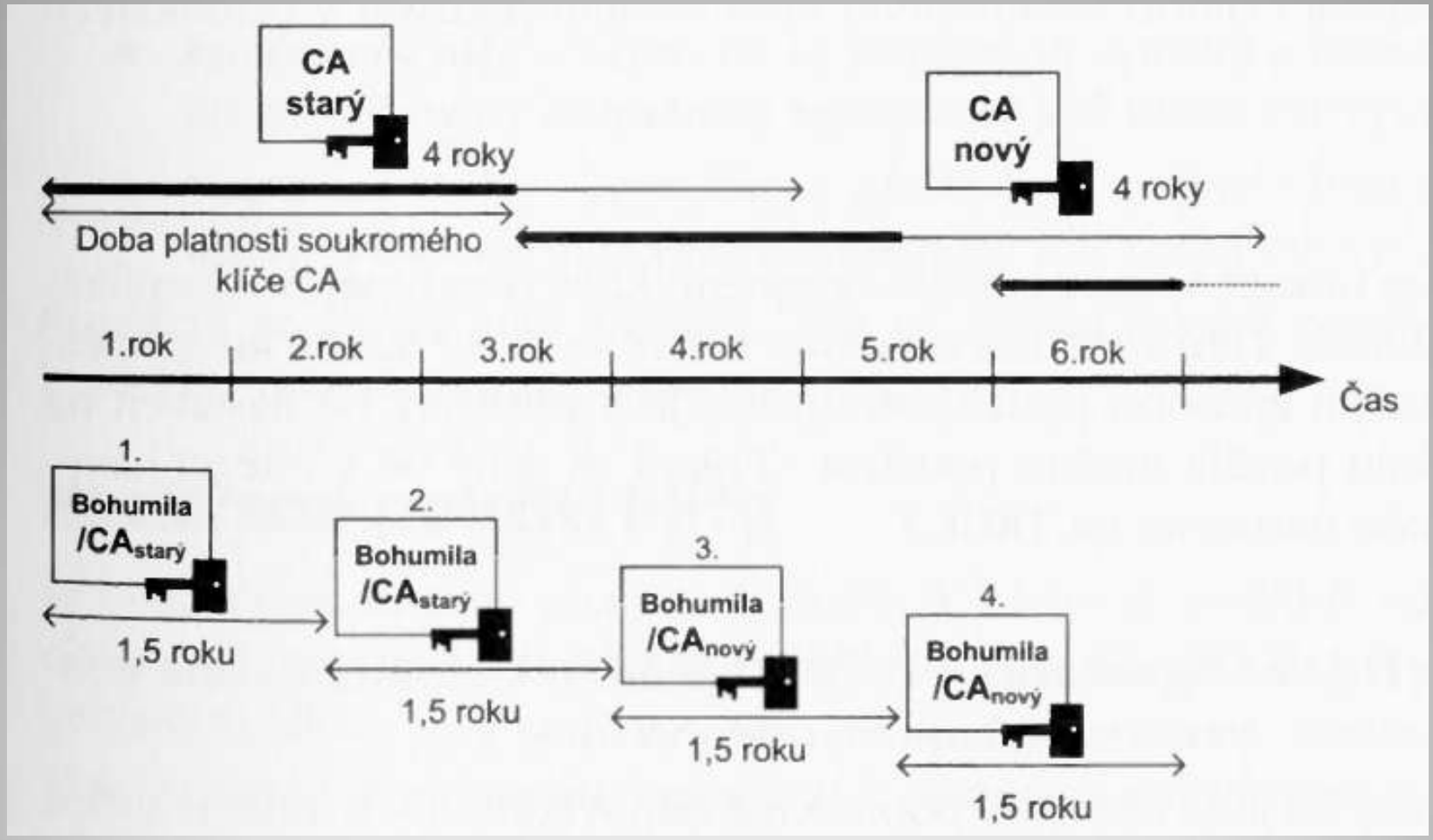
# Certifikáty a certifikační autority

- Soukromý klíč, veřejný klíč, certifikace veřejného klíče
- Certifikát je veřejná listina, podobná např. občanskému průkazu
- Strukturu certifikátu definuje několik norem (X.509, EDI, WAP…)
- Na Internetu se vychází ze standardu X.509 verze 3 (např. RFC-5280)

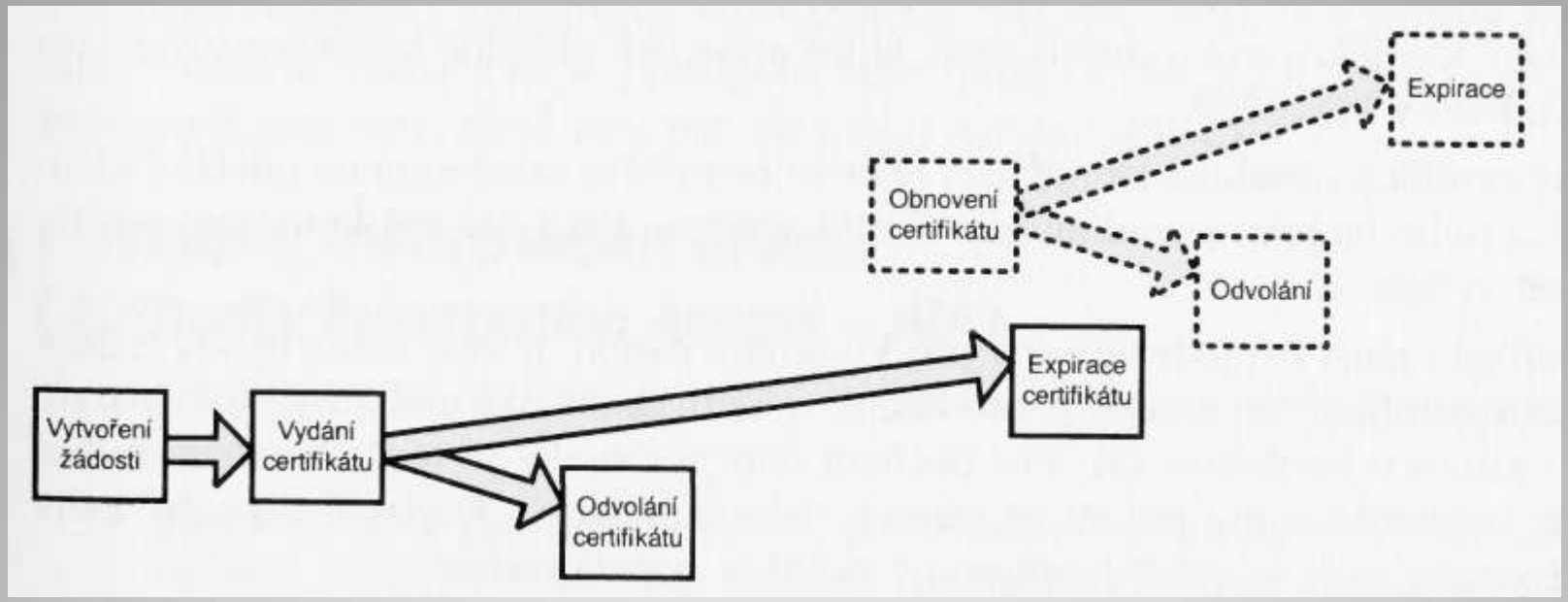
- **Verze** (Version)
- „Pořadové" číslo (Serial number)
- **Algoritmus podpisu** (Signature Algorithm)
- **Vydavatel** (Issuer)
- **Platnost** (Validity)
- **Předmět** (Subject): jméno, adresa, URL, email..
- **Veřejný klíč** (Subject Publice Key)
- **Rozšíření certifikátu** (Extension): SAN, Cert. Template name, AIA, Biometric Information…
- **Elektronický podpis** (Digital Signature)
- **Kryptografický otisk** (Thumbprint)




# Certifikát a jeho atributy




# Platnost soukromého klíče




# Životní cyklus certifikátu

# Použití klíče

- **Digitální podpis** (Digital Signature) pro autentizaci uživatelů nebo ověření integrity dat. NEOPRAVŇUJE k ověření pravosti!
- **Neodvolatelnost** (Non Repudiation) pro ověření pravosti – nepopiratelné odpovědnosti
- **Zakódování klíče** (Key Enciphement)
- **Zakódování dat** (Data Encipherment)
- **Key Agreement**
  - **Encipher Only**
  - **Decipher Only**
- **Podepisování certifikátu** (Key Certificate Sign)
- **Podepisování CRL** (CRL Sign)

# Certifikační autorita

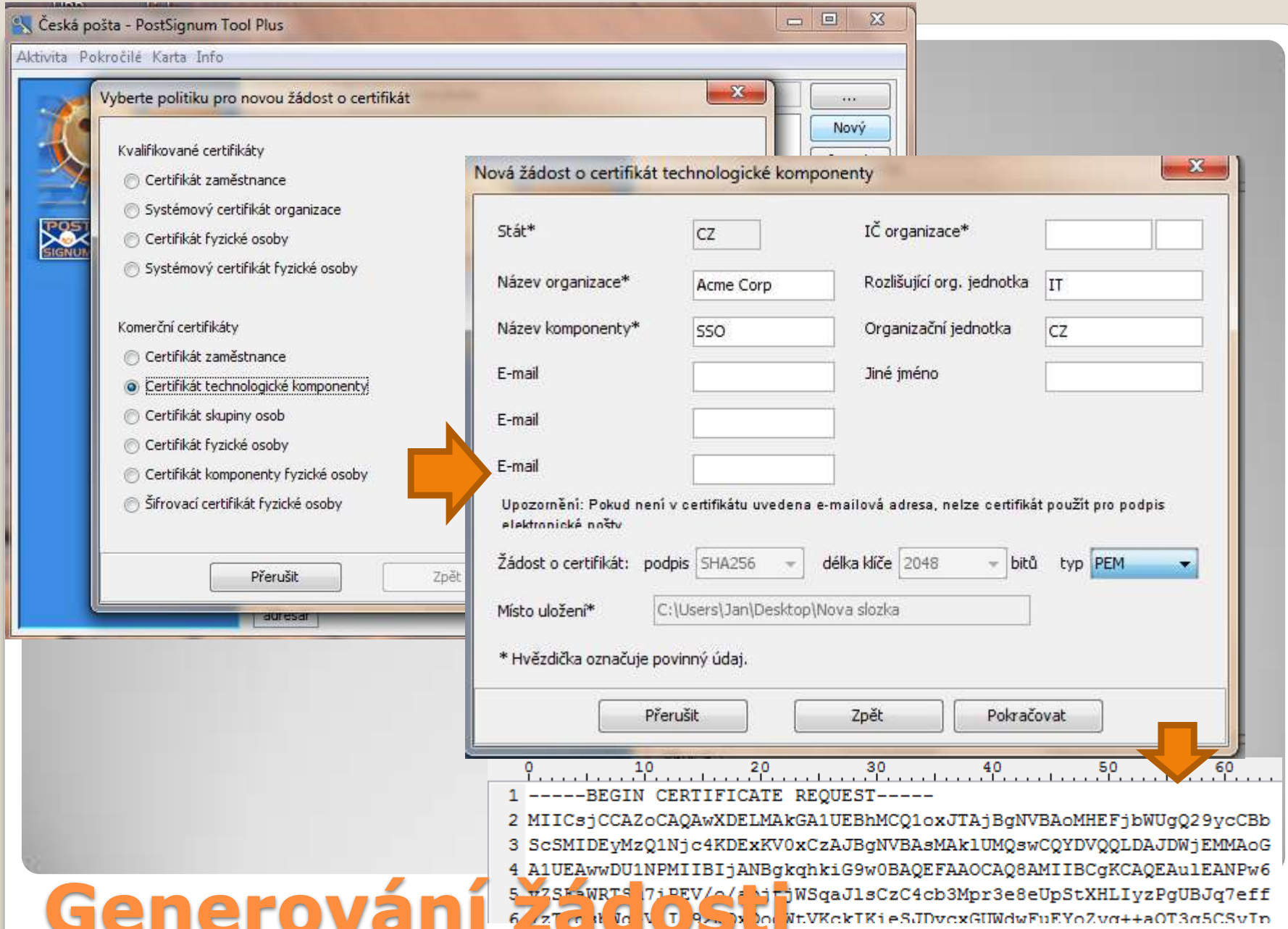
- Certifikační politiky
- Mapování zásad
- Omezení využívání certifikátu (Constrains)
- Základní omezení (Basic Constrains)
- Omezení jmen
- Distribuční místa CRL
- AIA
- …

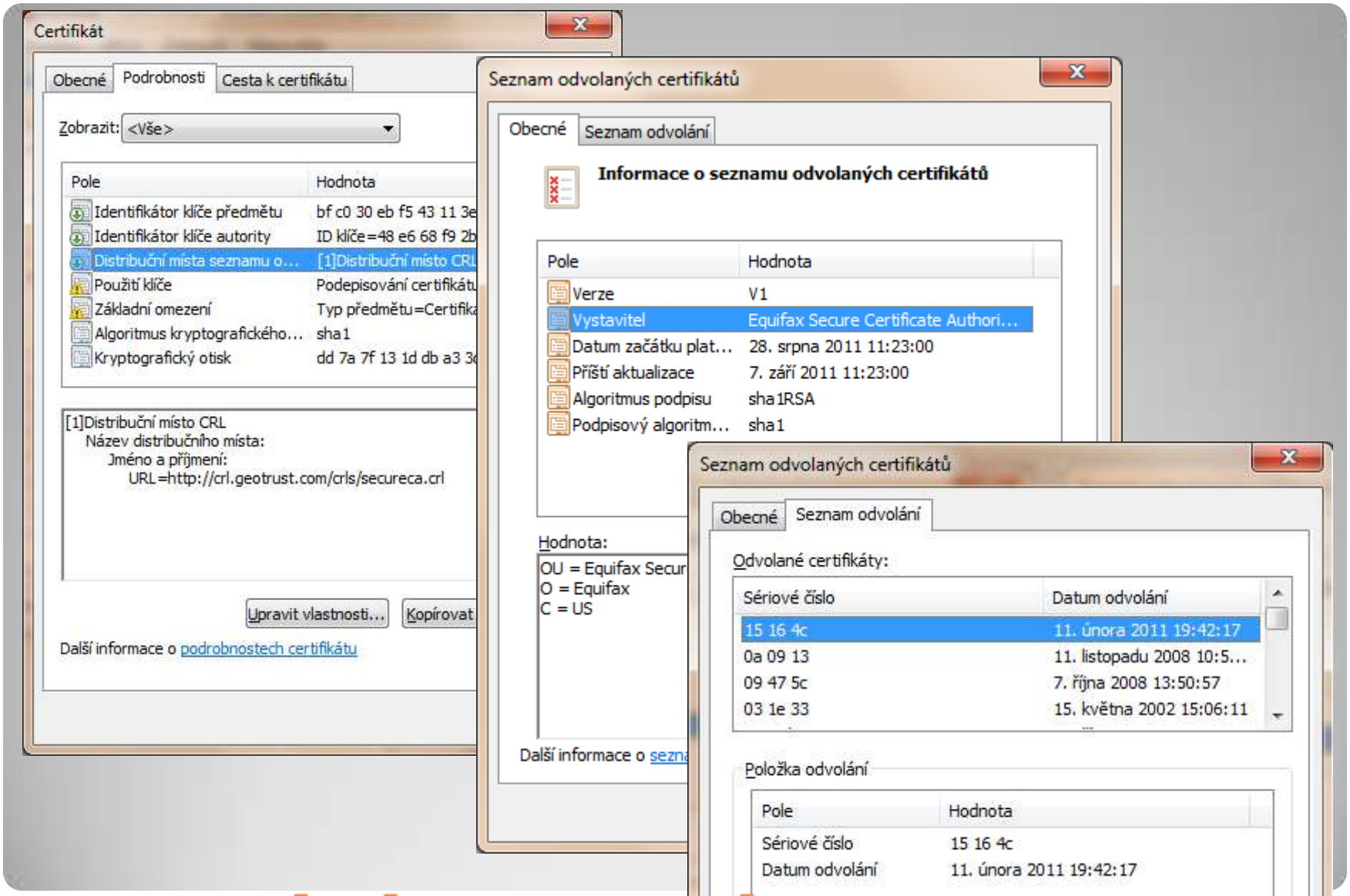
- CA vydává certifikáty
- RA vyřizuje žádosti o certifikáty (např. Service Desk) a zprostředkovávají vydání certifikátu.

# Registrační autorita

# Žádost o certifikát

- Kořenový (self-signed) certifikát (pozor- kořenový certifikát CA je něco zcela jiného) – s jeho pomocí se vygeneruje také žádost pro podpis na CA
  - PEM – orientován na el. poštu, častý v Linuxu, dnes se používá Base64
  - PKCS#10 – podniková norma RSA
  - CRMF – obsahuje mnoho rozšíření
  - SPK – nestandardní od Netscape
  - Web enrollment – ActiveX, Java applet
  - CMC – využíván i v AD CS např. pro více podpisů na certifikátu

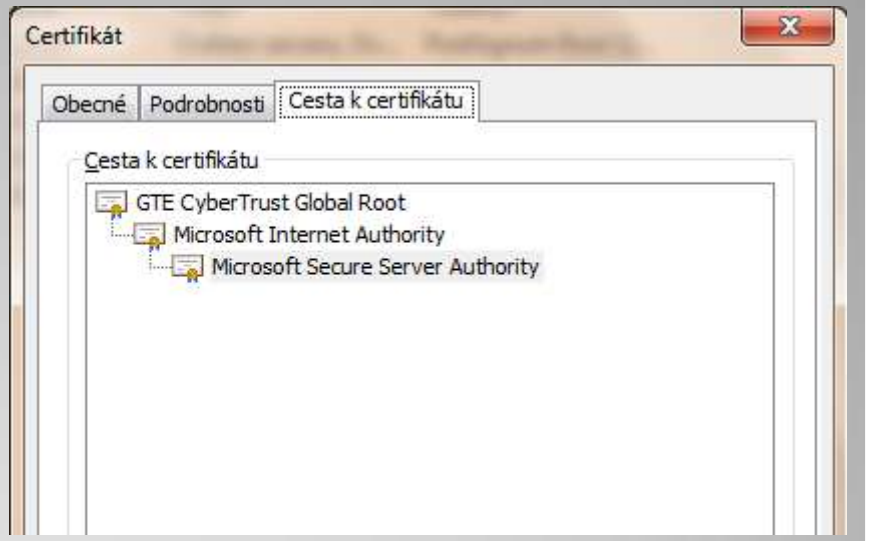

Česká pošta - PostSignum Tool Plus
Aktivita Pokročilé Karta Info
Vyberte politiku pro novou žádost o certifikát
Kvalifikované certifikáty
Certifikát zaměstnance
Systémový certifikát organizace
Certifikát fyzické osoby
Systémový certifikát fyzické osoby
Komerční certifikáty
Certifikát zaměstnance
Certifikát technologické komponenty
Certifikát skupiny osob
Certifikát fyzické osoby
Certifikát komponenty fyzické osoby
Šifrovací certifikát fyzické osoby
Přerušit
Zpět
Nový
Nová žádost o certifikát technologické komponenty
Stát* CZ
IČ organizace*
Název organizace* Acme Corp
Rozlišující org. jednotka IT
Název komponenty* SSO
Organizační jednotka CZ
E-mail
Jiné jméno
E-mail
E-mail
Upozornění: Pokud není v certifikátu uvedena e-mailová adresa, nelze certifikát použít pro podpis
Žádost o certifikát: podpis SHA256 délka klíče 2048 bitů typ PEM
Místo uložení* C:\Users\Jan\Desktop\Nova slozka
* Hvězdička označuje povinný údaj.
Přerušit
Zpět
Pokračovat
0 10 20 30 40 50 60
1 -----BEGIN CERTIFICATE REQUEST-----
2 MIICsjCCAZoCAQAwXDELMAkGA1UEBhMCQ1oxJTAjBgNVBAoMHEFjbWUgQ29ycCBb
3 ScSMIDEyMzQ1Njc4KDExKV0xCzAJBgNVBAsMAklUMQswCQYDVQQLDAJDWjEMMAoG
4 A1UEAwwDU1NPMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAulEANPw6
Generování žádosti




# Odvolání certifikátu

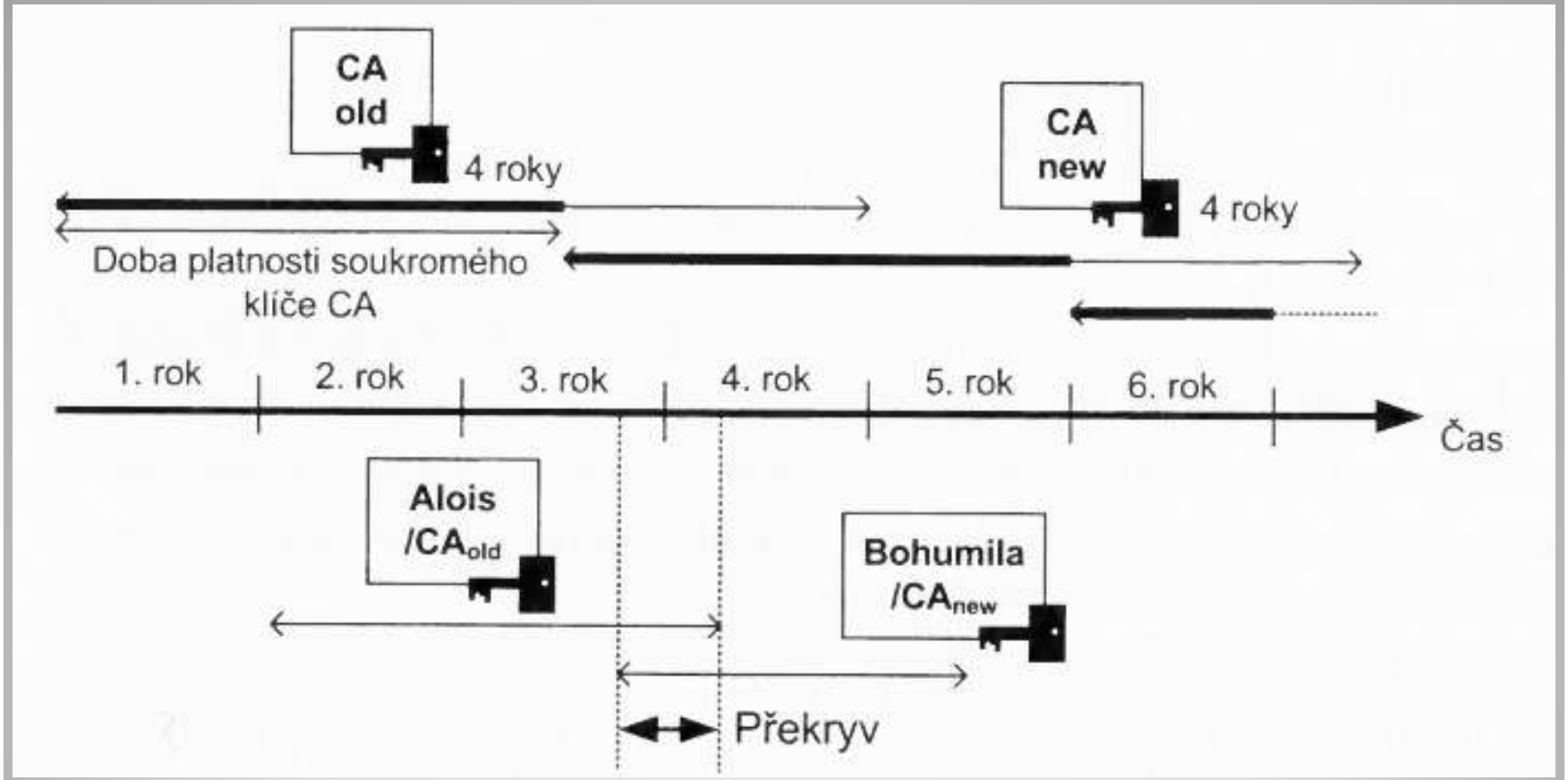
# Certifikační cesta a důvěryhodné kotvy

- CA si mohou podepisovat certifikáty vzájemně (křížové certifikace, mosty…)
- https://www.ebca.de (a další)
- WebTrust (využívá Microsoft) www.webtrust.org

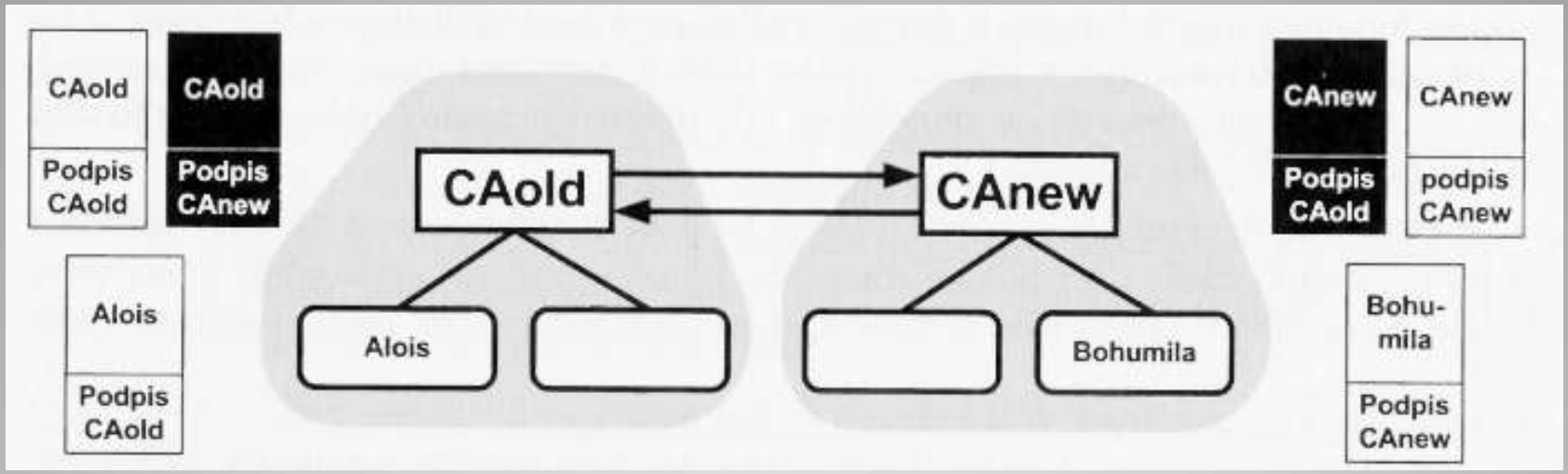


# Obnovování certifikátů

- **Obnovené** certifikáty vs. další (**následné**) certifikáty
- **Renew** (obnovení certifikátu téhož veř. klíče) vs. **Rekey** (obnovení certifikátu s vygenerováním nových párových dat




# Obnovování certifikátů CA




Pozn.: CRL bude vydáváno pro oba platné certifikáty

# Obnovování certifikátů CA – křížová certifikace

| Komponenta / Funkce | Windows Server 2008 R2 Standard | Windows Server 2008 R2 Enterprise |
|---|---|---|
| NDES | | ANO |
| OCSP | | ANO |
| Šablony cert. v. 1-3 | ANO | ANO |
| Archivace priv. klíčů | | ANO |
| Oddělení admin. rolí | | ANO |
| Omezení pro enrollment agenta | | ANO |

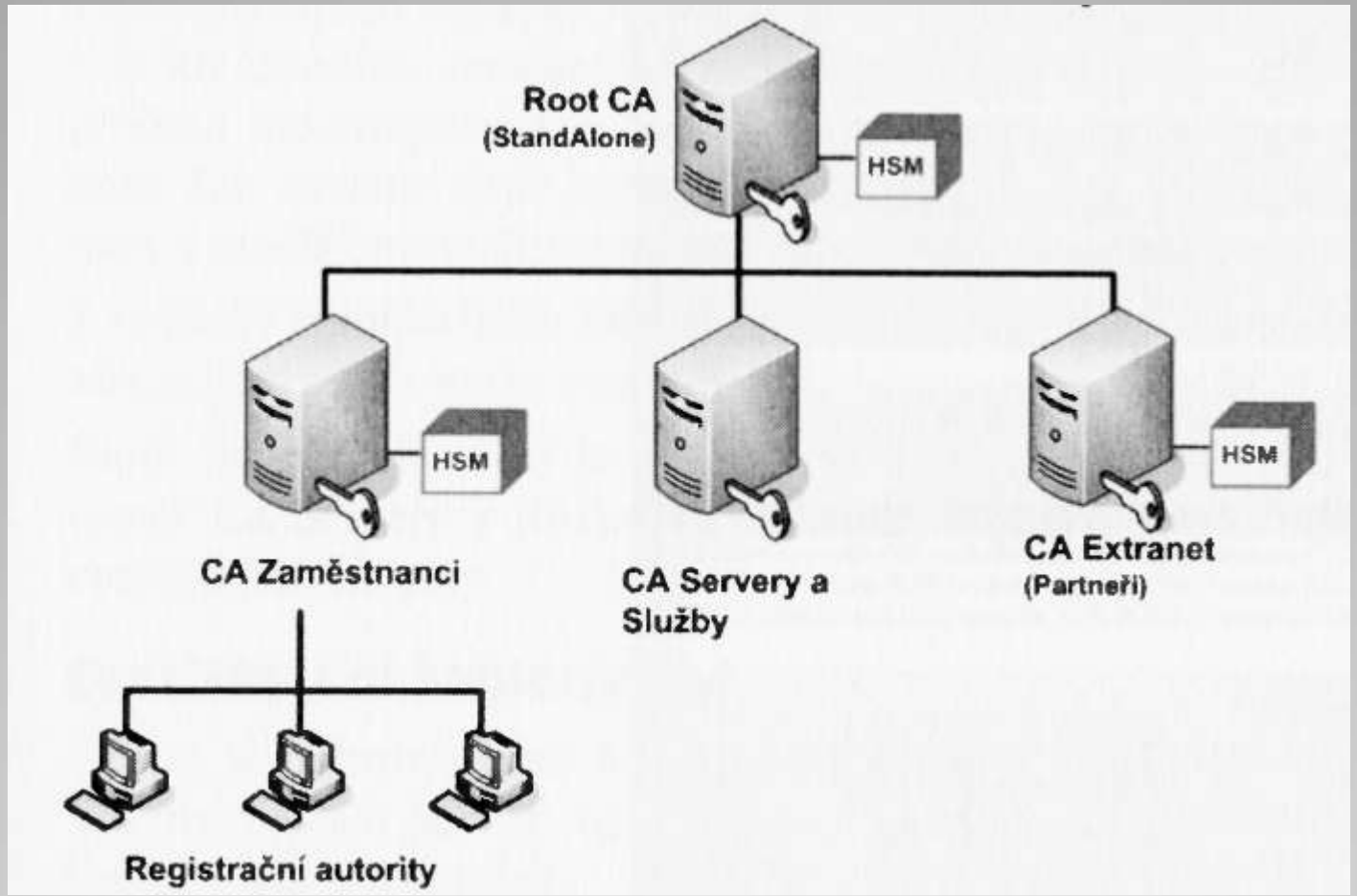
# Microsoft CA (AD CS)

| Stand-alone CA | Enerprise CA |
| --- | --- |
| Konfigurace může být ručně publikována v AD | Konfigurace CA je vždy publikována v AD |
| CRL, Delta CRL a certifikát ca může být do AD publikován ručně | CRL, Delta CRL, CA certifikát a křížové certifikáty se do AD publikují automaticky |
| Vydávání certifikátů je možné provádět pomocí webového rozhraní nebo ručně | Vydávání certifikátů je možné provádět pomocí webového rozhraní, MMC, autoenrollment |
| Šablony certifikátů se nepoužívají | Používají se šablony certifikátů |
| Certifikáty jsou vydávány automaticky nebo po schválení – ale vždy na úrovni CA | Pro každou šablonu je možné nastavit způsob vydávání |
| Server nemusí být v doméně | Vždy na serveru v rámci AD |

# Stand-alone vs. Enterprise

# Certifikační šablony certifikátů

- Verze 1
  - Nelze editovat, kompatibilní s W2000
  - Nepodporují autoenrollment
- Verze 2
  - Od verze W2003/XP
  - Podporují autoenrollment i editaci
  - Možnost vytvářet vlastní šablony (duplikací)
- Verze 3
  - Od Vista/W2008
  - Podporují silnější kryptografii (CNG, Suite B, SHA-2)




Pozn.: někdy poslouží jediná Enterprise CA lépe než zbytečně složitá struktura.

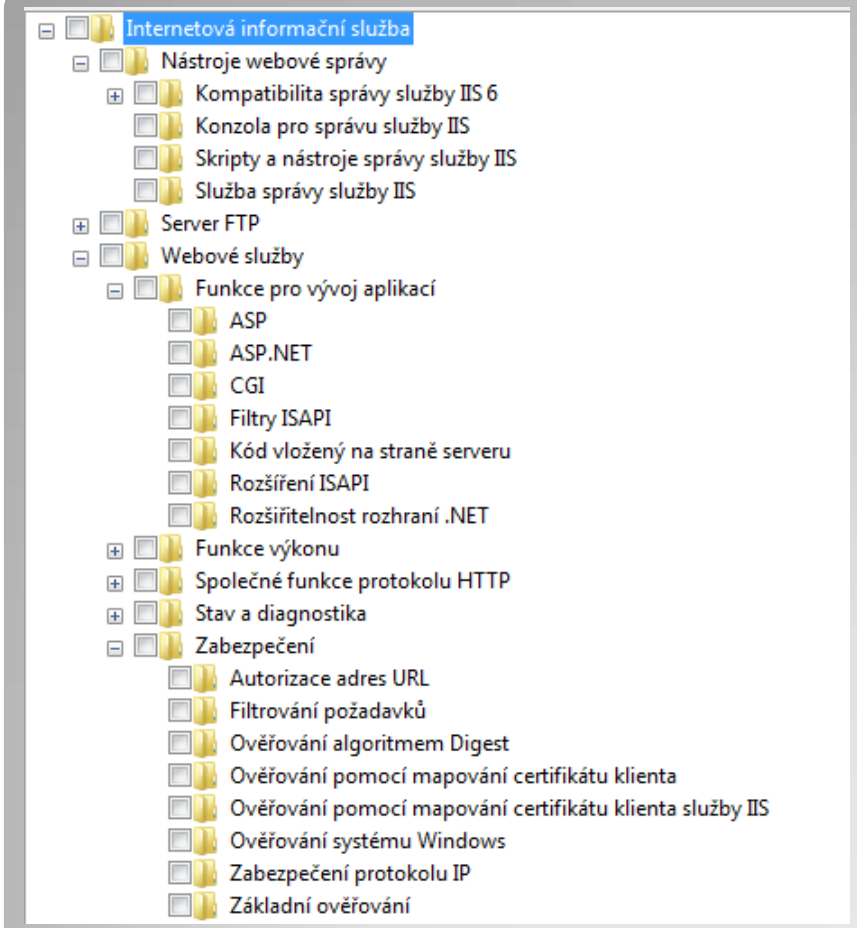
# Design hierarchie CA

# Zdroje a odkazy - PKI

- Implementing and Administering Certificate Templates in Windows Server 2008: http://www.microsoft.com/downloads/en/details.aspx?FamilyID=3c670732-c971-4c65-be9c-c0ebc3749e24
- Suite B PKI in Windows Server 2008: http://www.microsoft.com/downloads/en/details.aspx?FamilyID=6f319ffa-739e-4fe8-bac3-92547baef7a9
- Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003: http://www.microsoft.com/downloads/en/details.aspx?FamilyID=64e63a75-3206-4036-b836-40f2e721add0
- TechNet Webcast: Deploying a PKI Solution with Active Directory Certificate Services: https://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?culture=en-US&EventID=1032445999&CountryCode=US
- Onřej Ševeček blog: http://www.sevecek.com/Lists/Categories/Category.aspx?CategoryId=8&Name=PKI
- Libor Dostálek, Marta Vohnoutová: Velký průvodce infrastrukturou PKI a technologií telektronického podpisu (http://www.alza.cz/velky-pruvodce-infrastrukturou-pki-d78078.htm)
- Brian Komar: Windows Server 2008 PKI and Certificate Security (http://www.microsoft.com/learning/en/us/book.aspx?ID=9549&locale=en-us)

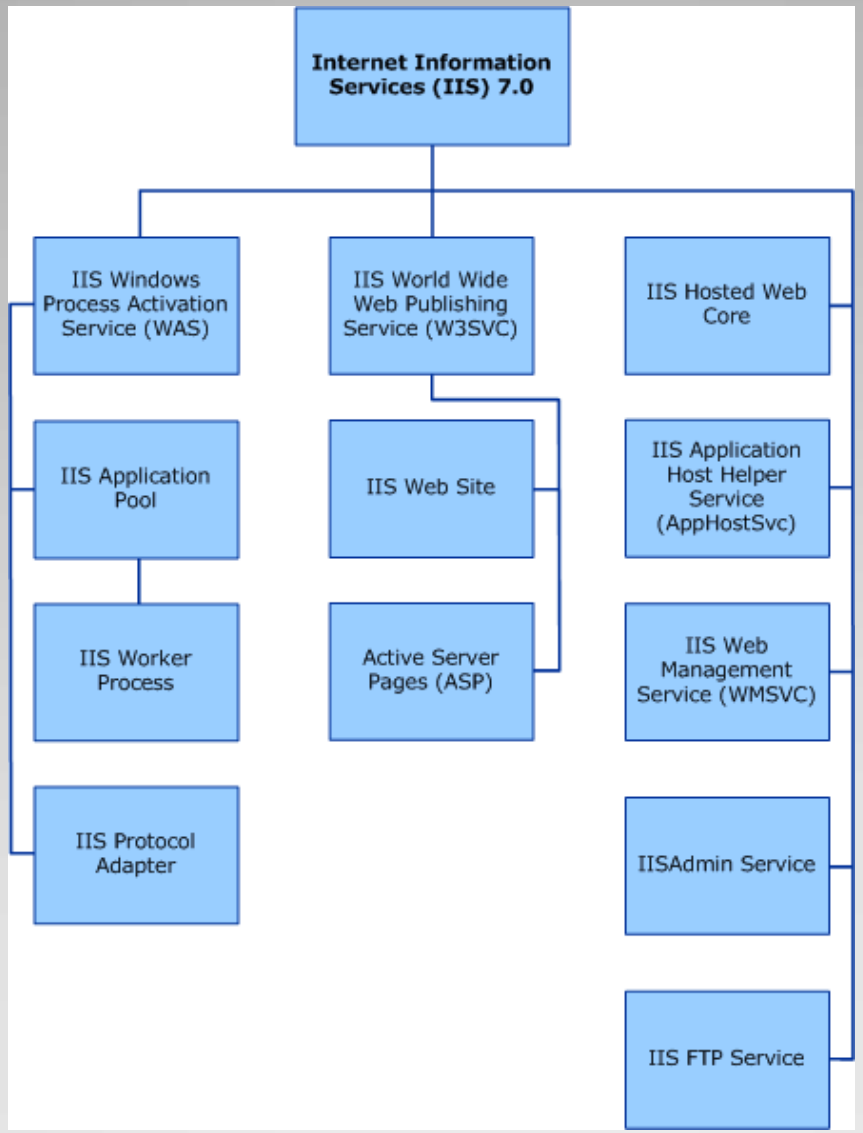
- **RFC 3029:** Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols (http://www.faqs.org/rfcs/rfc3029.html)
- Public key infrastructure on Wikipedia: http://en.wikipedia.org/wiki/Public_key_infrastructure
- http://csrc.nist.gov/publications/drafts/800-57/Draft_SP800-57-Part1-Rev3_May2011.pdf

# IIS 7.0/7.5




- ISS je modulární systém )cca 40 modulů) → vyšší zabezpečení i výkon
- Nové API pro rozšíření funkčnosti – lze např. modifikovat možnosti ověřování
- …

# Instalace IIS



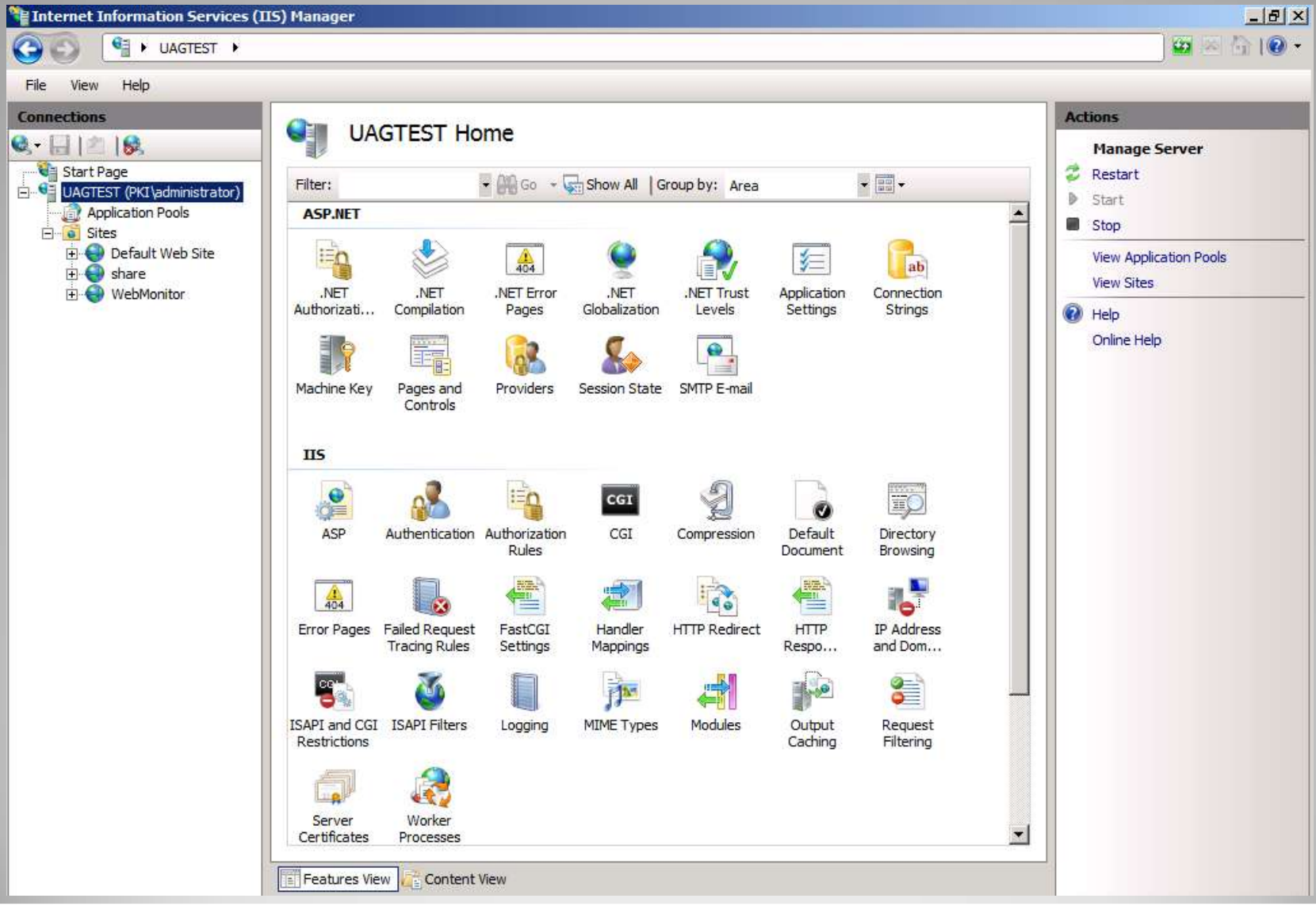

# Hierarchie „Managed Entities“

- IIS Windows Process Activation Service (WAS) Windows Process Activation Service (WAS) manages application pool configuration and the creation and lifetime of worker processes for HTTP and other protocols. The World Wide Web Publishing Service (W3SVC) and other services depend on WAS.
- IIS Application Pool An Internet Information Services (IIS) application pool is a grouping of URLs that is routed to one or more worker processes. Because application pools define a set of Web applications that share one or more worker processes, they provide a convenient way to administer a set of Web sites and applications and their corresponding worker processes. Process boundaries separate each worker process; therefore, a Web site or application in one application pool will not be affected by application problems in other application pools. Application pools significantly increase both the reliability and manageability of a Web infrastructure.
- IIS Worker Process An Internet Information Services (IIS) worker process is a windows process (w3wp.exe) which runs Web applications, and is responsible for handling requests sent to a Web Server for a specific application pool.
- IIS Protocol Adapter An Internet Information Services (IIS) protocol adapter is a Windows service that receives messages on a specific network protocol and communicates with The Windows Process Activation Service (WAS) to route incoming messages to the correct worker process.
- IIS FTP Service  The Internet Information Services (IIS) FTP Service enables the Web server to be a File Transfer Protocol (FTP) server. If this service is stopped, the server cannot function as an FTP server.

# Managed Entities

- IIS Web Management Service (WMSvc) The Internet Information Services (IIS) Web Management Service (WMSvc) enables remote and delegated management of a Web server and its Web sites and applications.
- IIS Application Host Helper Service (AppHostSvc) The Internet Information Services (IIS) ApplicationHost Helper Service (AppHostSvc) enables IIS configuration history and application pool SID (security identifier) mapping. It enables the configuration history functionality by saving the ApplicationHost.config file to separate configuration history subdirectories at set intervals.
- IISADMIN Service The Internet Information Services (IIS) IISAdmin service hosts the IIS 6.0 configuration compatibility component (metabase). The metabase is required to run IIS 6.0 administrative scripts, SMTP, and FTP.
- IIS Hosted Web Core The Internet Information Services (IIS) Hosted Web Core (HWC) is a low-level component that is used to run Web applications without the Windows Process Activation Service (WAS) or the built-in IIS configuration store (ApplicationHost.config).
- IIS World Wide Web Publishing Service (W3SVC) The Internet Information Services (IIS) World Wide Web Publishing Service (W3SVC), sometimes referred to as the WWW Service, manages the HTTP protocol and HTTP performance counters.
- IIS Web Site An Internet Information Services (IIS) Web site is a unique collection of Web pages and Web applications that is hosted on an IIS Web server. Web sites have bindings that consist of a port number, an IP address, and an optional host name or names.
- Active Server Pages (ASP) Active Server Pages (ASP) enables Web servers to dynamically generate Web pages and create interactive Web applications by using server-side scripting technology.
- Logging and Tracing

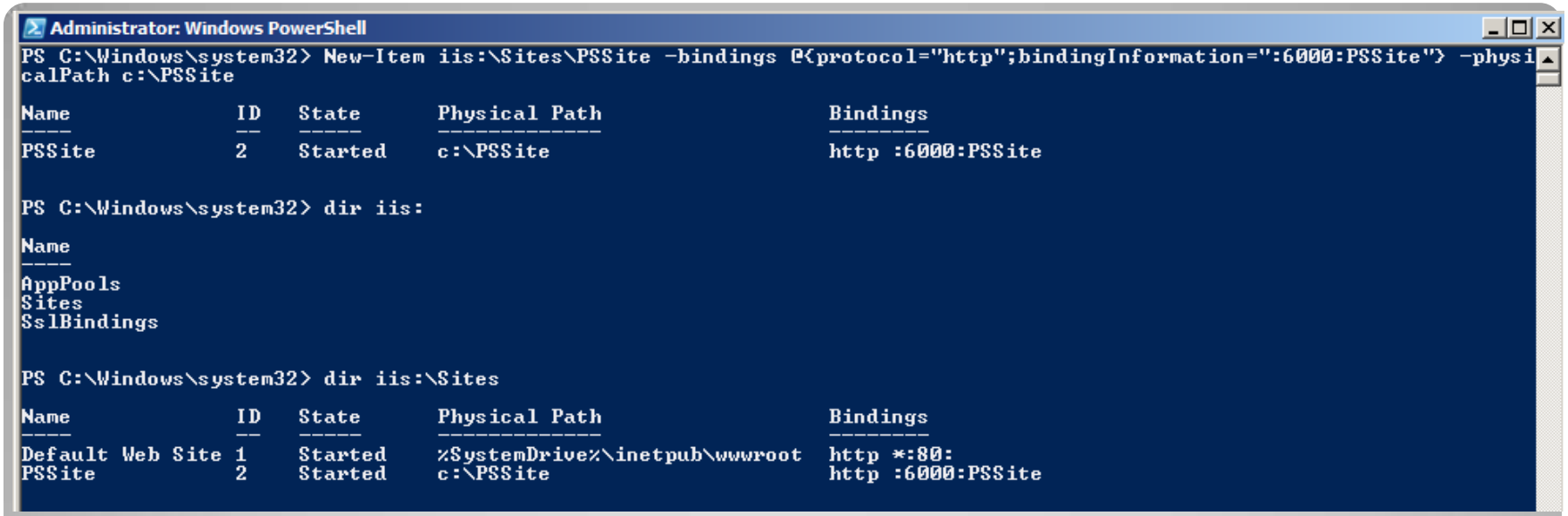
# Managed Entities (pokračování)

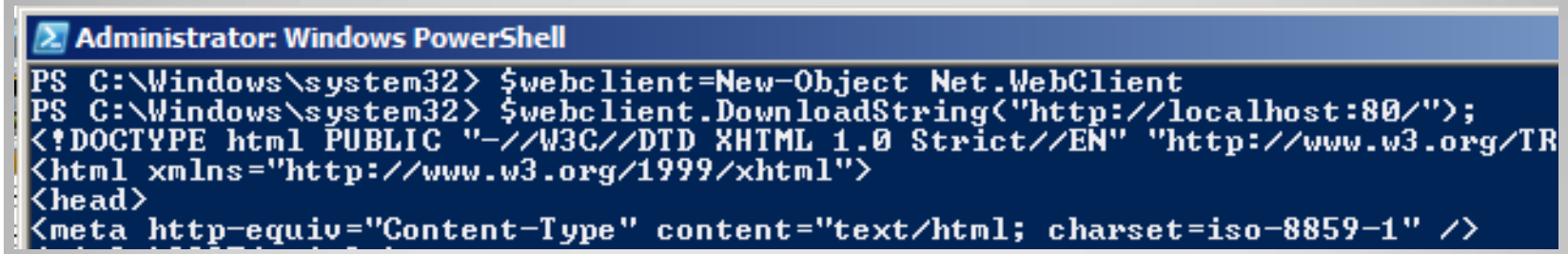

Internet Information Services (IIS) Manager
UAGTEST
File View Help
Connections
Start Page
UAGTEST (PKI\administrator)
Application Pools
Sites
Default Web Site
share
WebMonitor
UAGTEST Home
Filter:
Go
Show All
Group by: Area
ASP.NET
.NET Authorizati...
.NET Compilation
.NET Error Pages
.NET Globalization
.NET Trust Levels
Application Settings
Connection Strings
Machine Key
Pages and Controls
Providers
Session State
SMTP E-mail
IIS
ASP
Authentication
Authorization Rules
CGI
Compression
Default Document
Directory Browsing
Error Pages
Failed Request Tracing Rules
FastCGI Settings
Handler Mappings
HTTP Redirect
HTTP Respo...
IP Address and Dom...
ISAPI and CGI Restrictions
ISAPI Filters
Logging
MIME Types
Modules
Output Caching
Request Filtering
Server Certificates
Worker Processes
Features View
Content View
Actions
Manage Server
Restart
Start
Stop
View Application Pools
View Sites
Help
Online Help

# IIS Manager

```
C:\> appcmd list sites
SITE "Default Web Site"
  (id:1,bindings:HTTP/*:80:,state:Started)
SITE "Site1"
  (id:2,bindings:http/*:81:,state:Started)
SITE "Site2"
  (id:3,bindings:http/*:82:,state:Stopped)
```

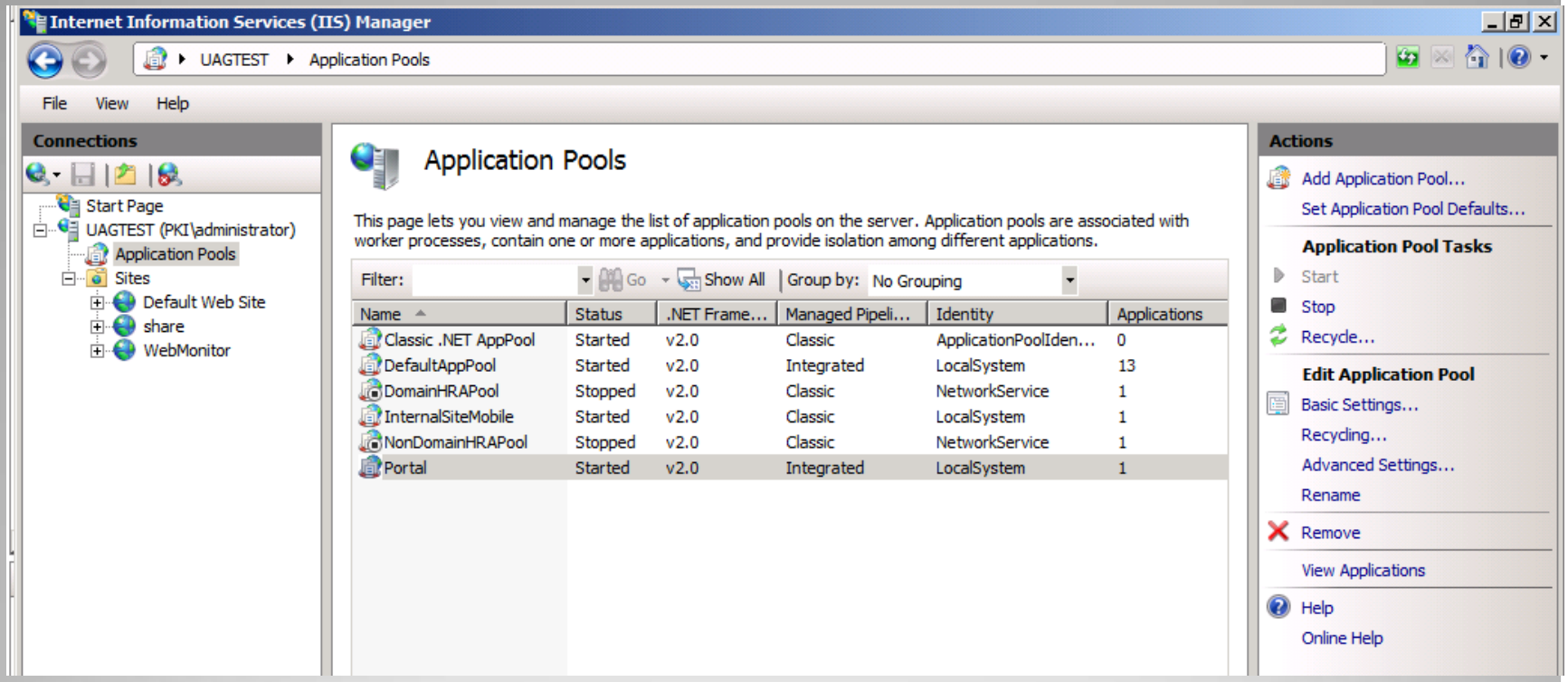
# appcmd.exe



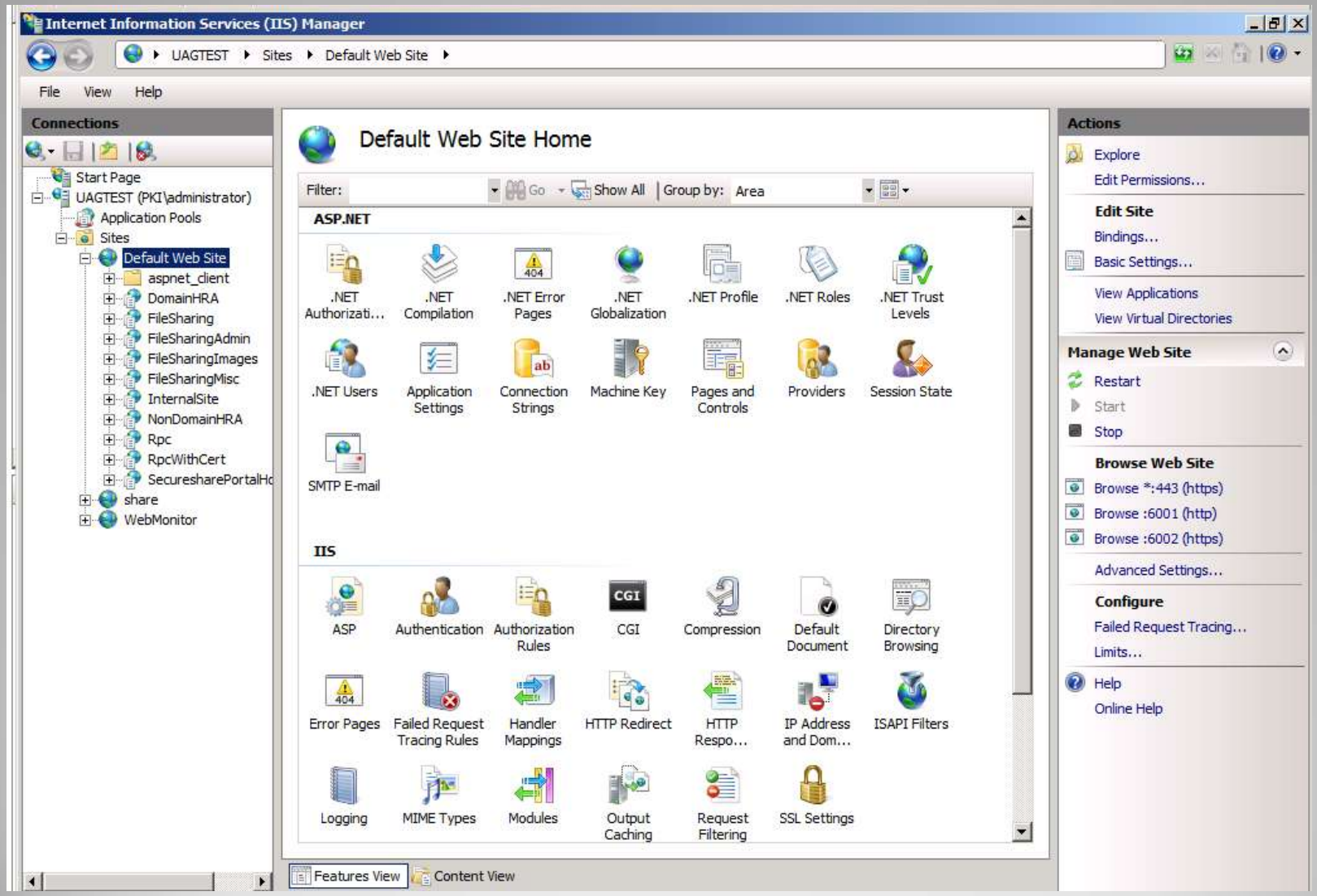




http://learn.iis.net/page.aspx/433/powershell-snap-in-creating-web-sites-web-applications-virtual-directories-and-application-pools/

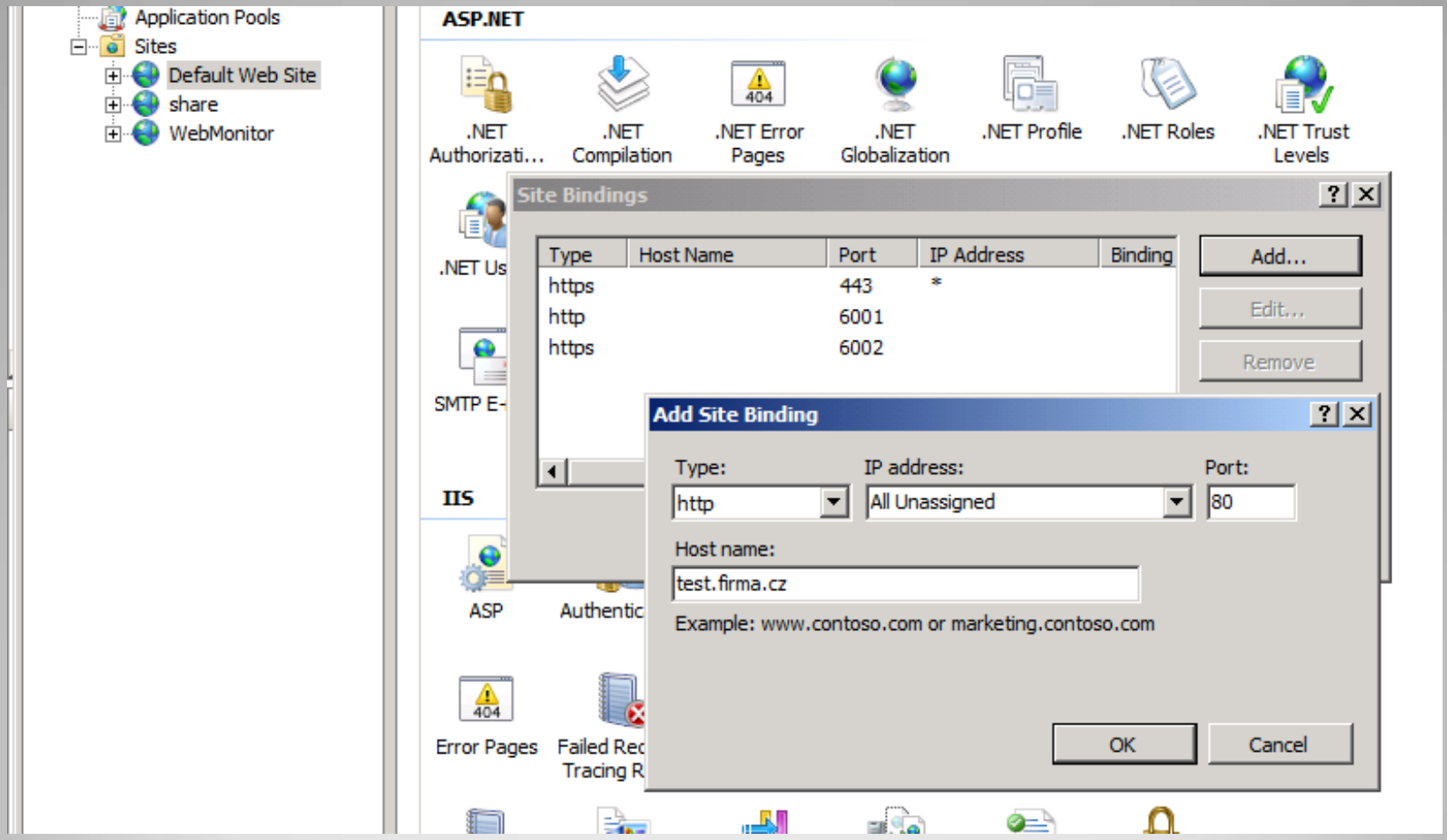
# PowerShell



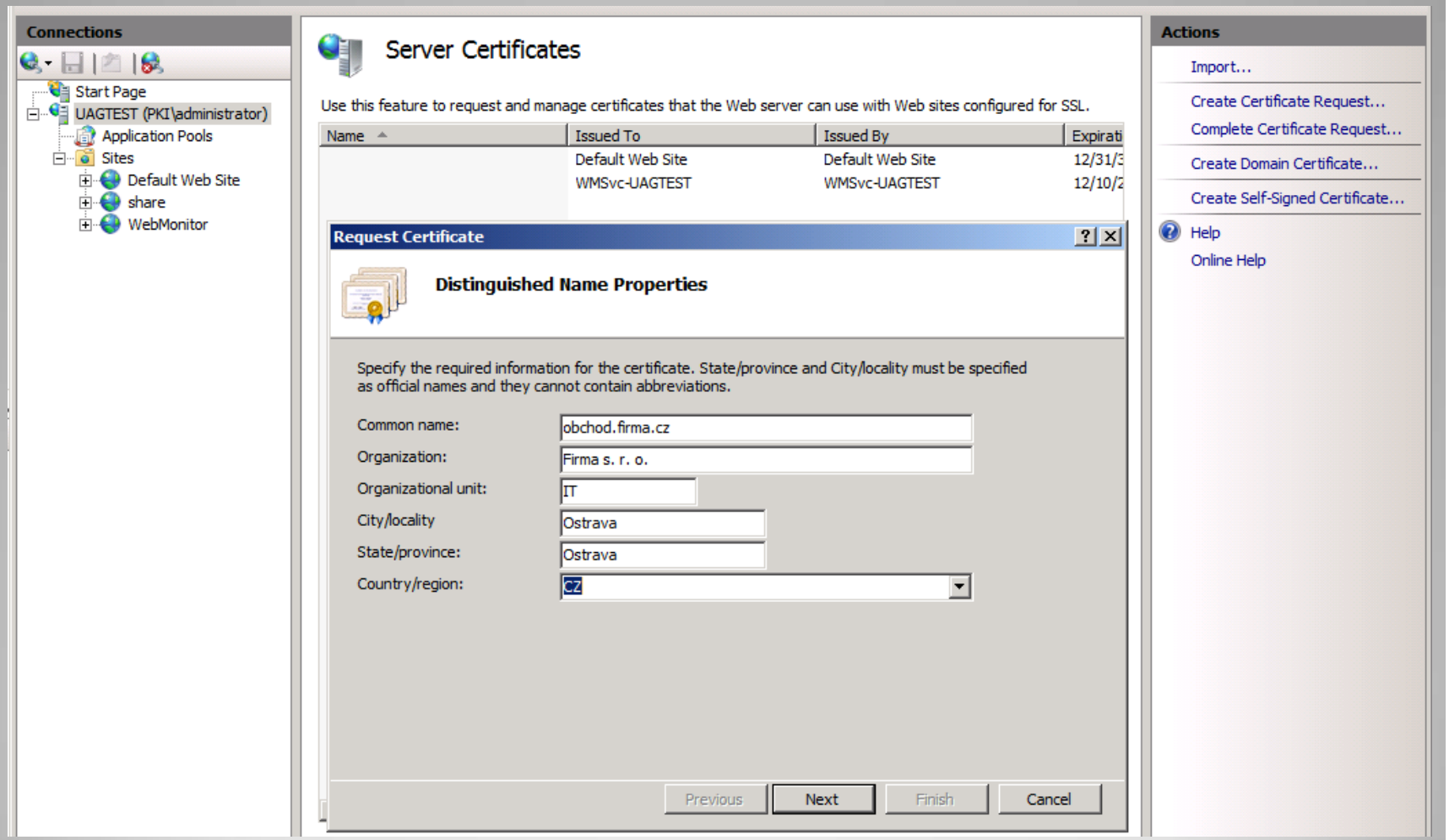

# Application Pools



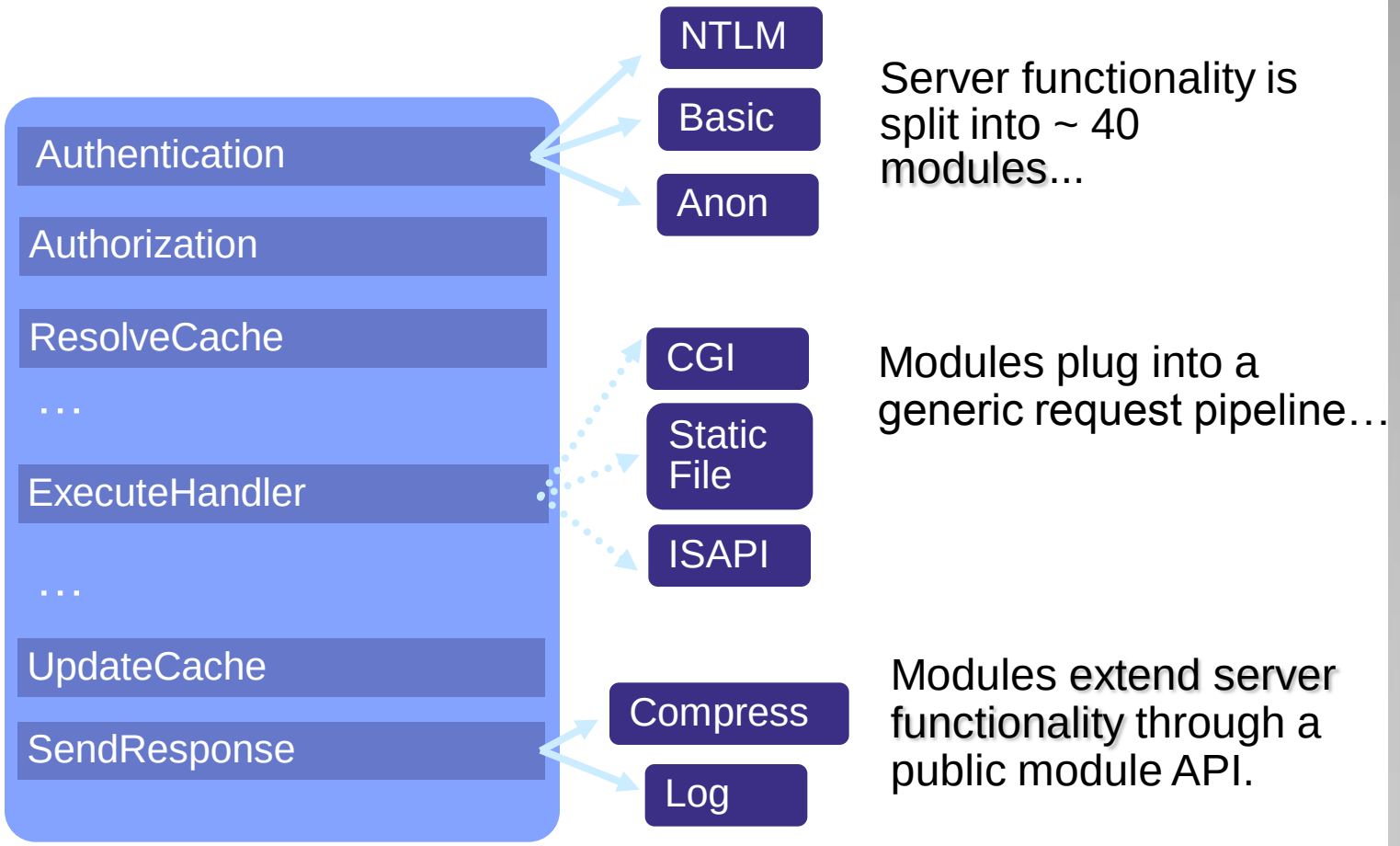

# Sites; virtuální adresáře; aplikace



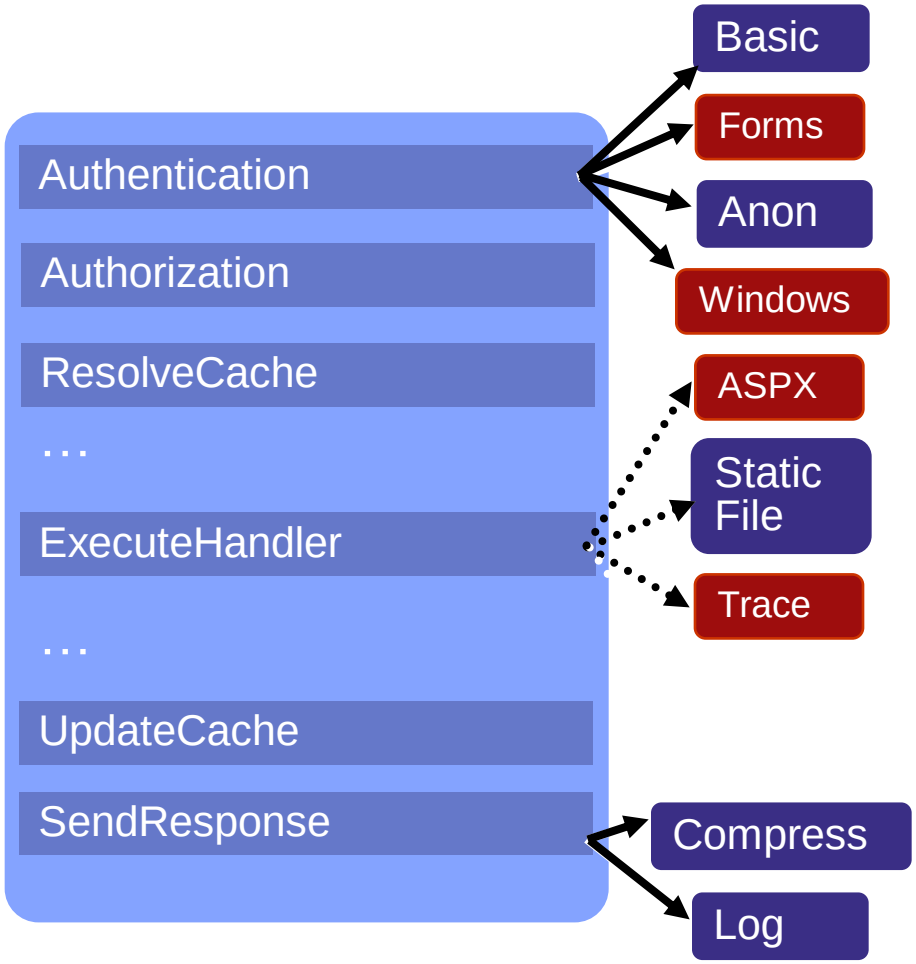

# Site Bindings




# Vystavování SSL certifikátu

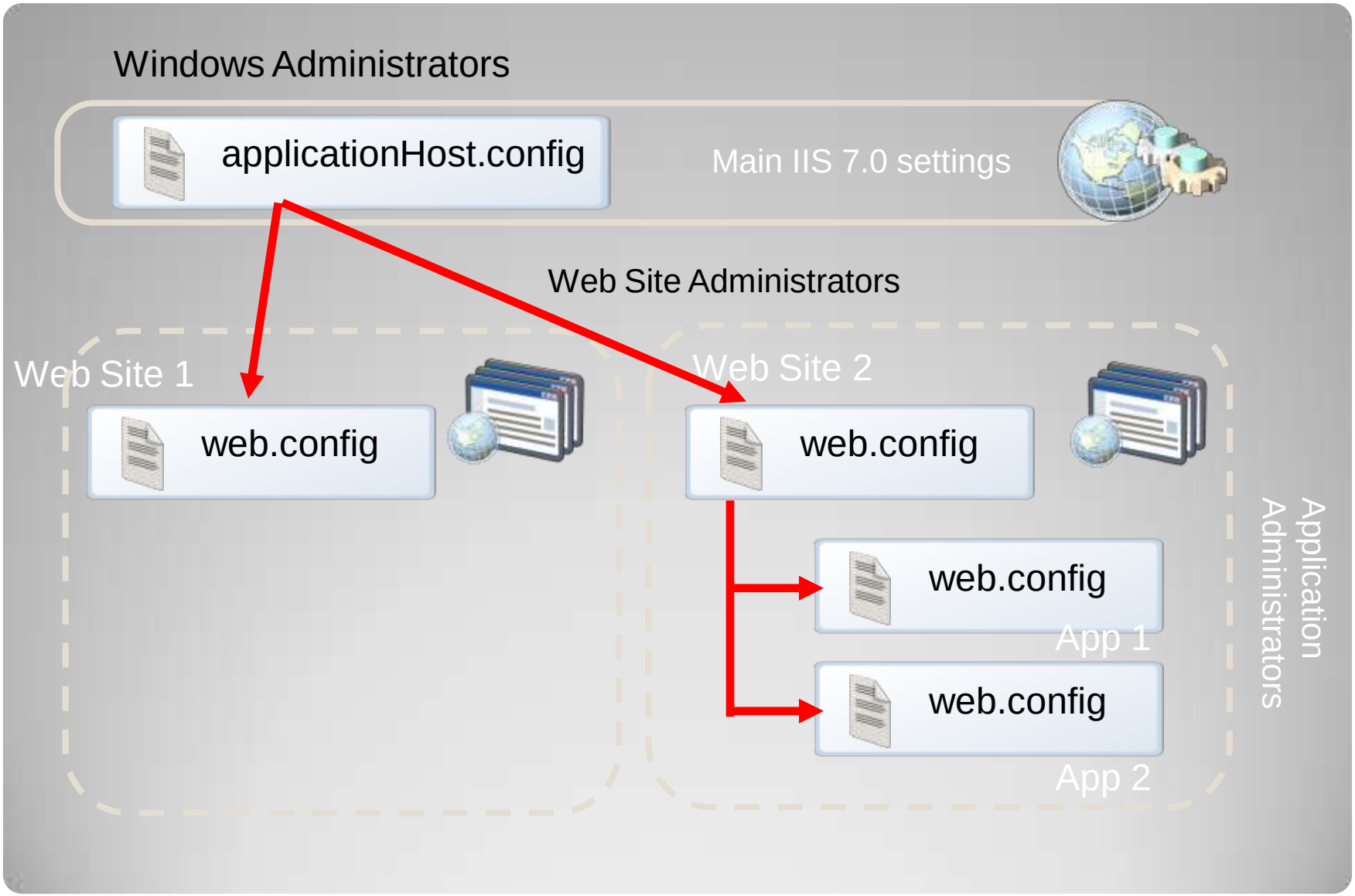



# Zpracování požadavků v IIS

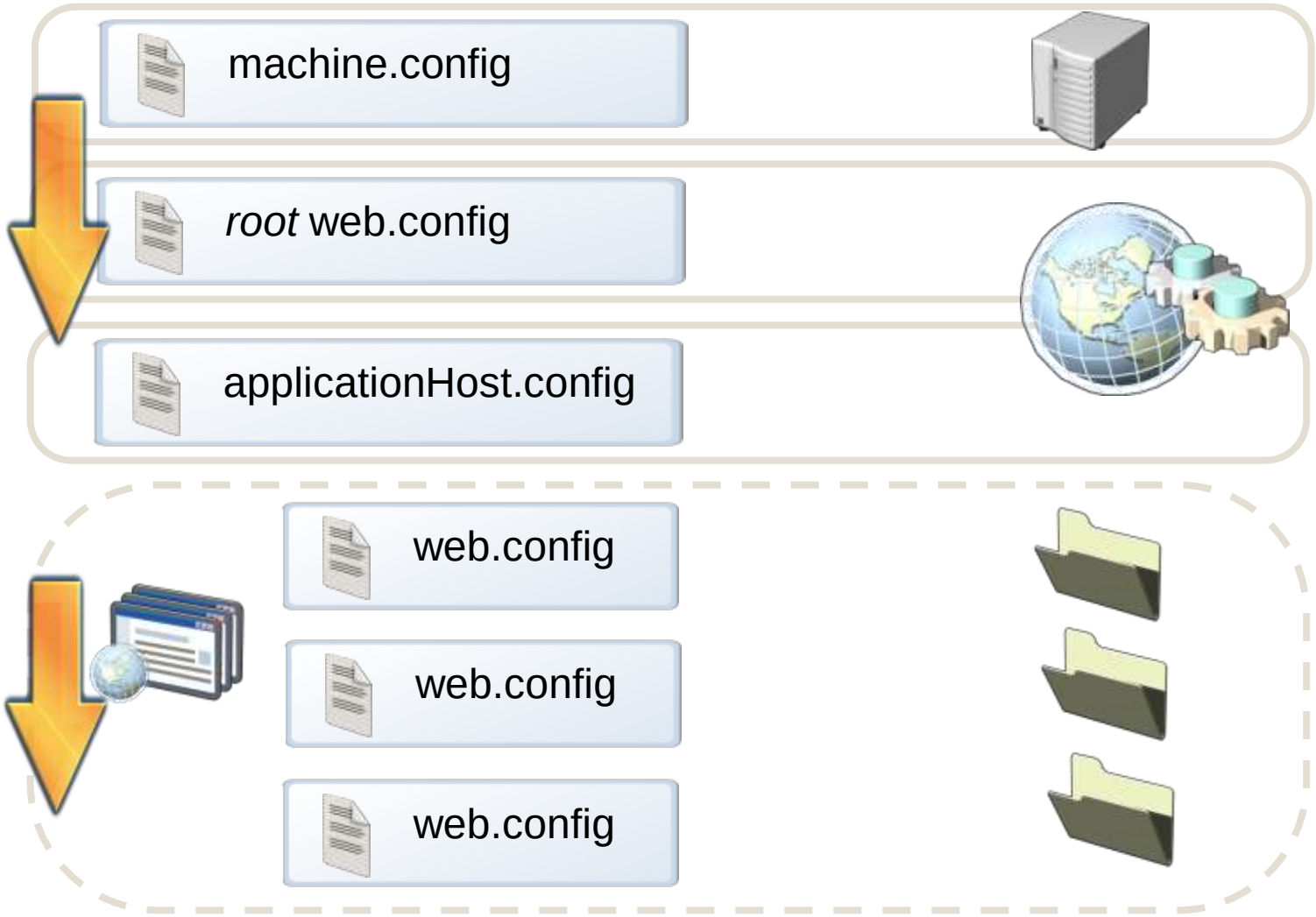



- **Classic Mode**
  - Runs as ISAPI
- **Integrated Mode**
  - .NET modules / handlers plug directly into pipeline
  - Process all requests
  - Full runtime fidelity

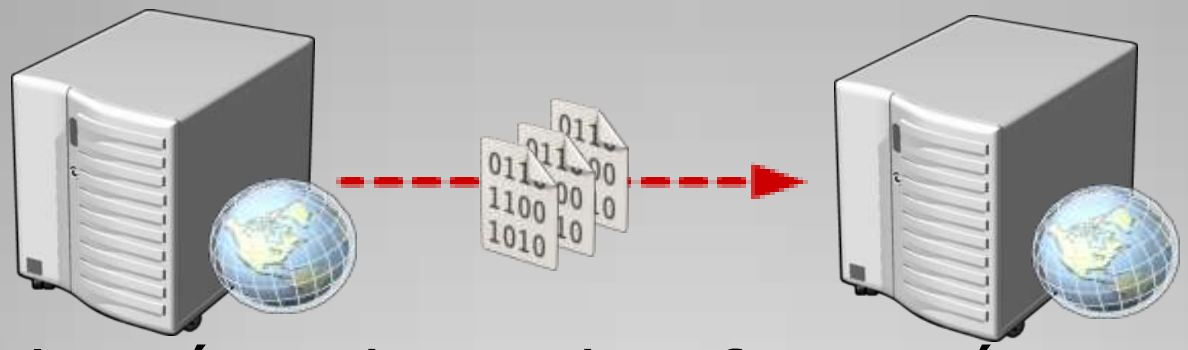
# Integrace ASP.NET



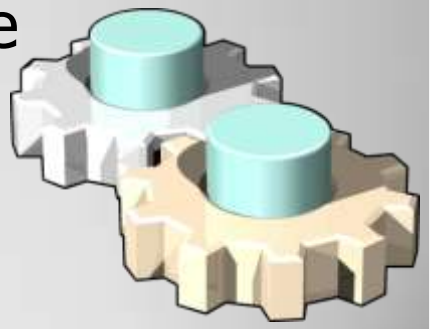

# Hierarchie konfiguračních souborů



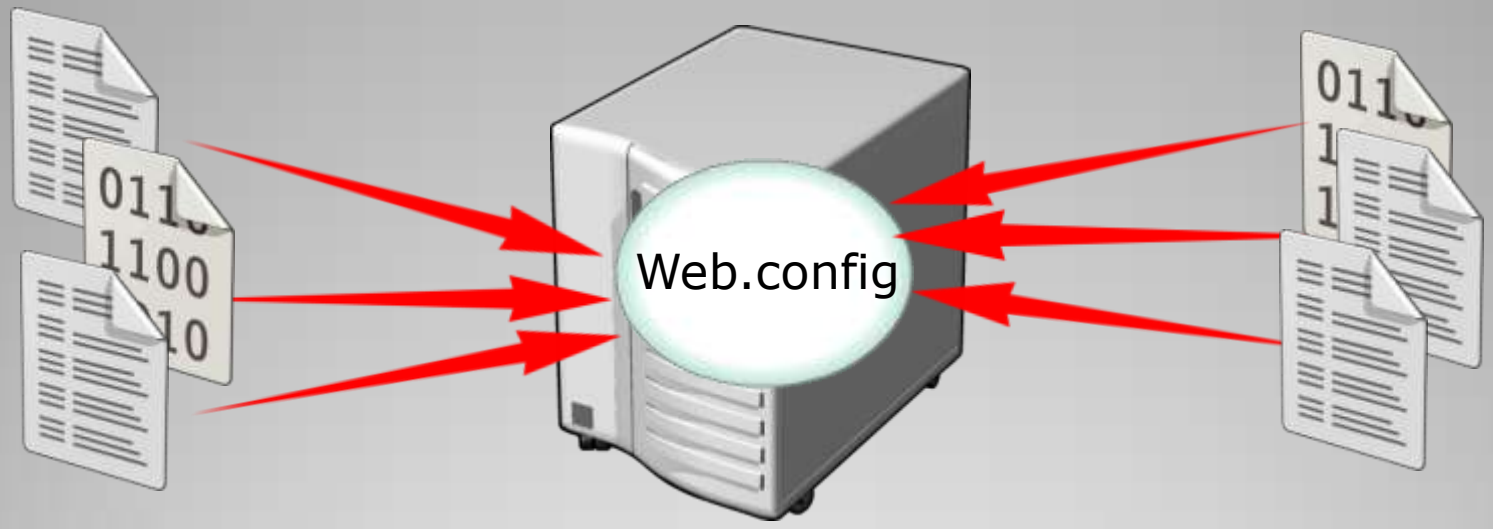

# Hierarchy of Configuration Files




- Hlavní soubor s konfigurací IIS
  - Vestavěný účet “Internet User”
  - Stačí zkopírovat soubory
- Konfigurace IIS ve Web.config
  - XCopy pro kopírování dat aplikace



# Replikace obsahu a konfigurace




- Konfigurace IIS
  - Centrální soubor na file serveru – soubory Web.config
- File System:
  - Používají se „offline soubory“ - Client Side Caching (CSC)
  - Je možné použít také „Distributed File System Replication (DFSR)“

# Centralizace obsahu a nastavení

# Nový systém konfigurace IIS 7.0

- Již se nepoužívá „Metabase „
- Názvy vlastností ale zůstávají stejné jako v původní metabázi
- Hlavní centrální soubor:
  **ApplicationHost.config**
  - Definováno schéma
  - Používá se „ASP.NET semantics“
- Distribuovaná konfigurace
  - Výchozí hodnoty v **ApplicationHost.config**
  - Nastavení mohou být delegována

- Main configuration in applicationHost.config
- Consistent with ASP.NET web.config
- Two main groupings of settings:
  - system.applicationHost
  - system.webServer

# IIS 7.0 Configuration Concepts

```
<system.webServer>
    <defaultDocument enabled="true">
        <files>
            <add value="Default.htm" />
            <add value="Default.asp" />
            <add value="index.htm" />
            <add value="index.html" />
            <add value="iisstart.htm" />
            <add value="default.aspx" />
        </files>
    </defaultDocument>
</system.webServer>
```

# Section Groups

```
<system.webServer>
    <defaultDocument enabled="true">
        <files>
            <add value="Default.htm" />
            <add value="Default.asp" />
            <add value="index.htm" />
            <add value="index.html" />
            <add value="iisstart.htm" />
            <add value="default.aspx" />
        </files>
    </defaultDocument>
</system.webServer>
```

# Sections

```
<system.webServer>
    <defaultDocument enabled="true">
        <files>
            <add value="Default.htm" />
            <add value="Default.asp" />
            <add value="index.htm" />
            <add value="index.html" />
            <add value="iisstart.htm" />
            <add value="default.aspx" />
        </files>
    </defaultDocument>
</system.webServer>
```

# Elements

```
<system.webServer>
    <defaultDocument enabled="true">
        <files>
            <add value="Default.htm" />
            <add value="Default.asp" />
            <add value="index.htm" />
            <add value="index.html" />
            <add value="iisstart.htm" />
            <add value="default.aspx" />
        </files>
    </defaultDocument>
</system.webServer>
```

# Collections

```
<system.webServer>
    <defaultDocument enabled="true" >
        <files>
            <add value="Default.htm" />
            <add value="Default.asp" />
            <add value="index.htm" />
            <add value="index.html" />
            <add value="iisstart.htm" />
            <add value="default.aspx" />
        </files>
    </defaultDocument>
</system.webServer>
```

# Attributes

```
<location path="MyWebSite"
    overrideMode="Allow">
<system.webServer>
    <defaultDocument enabled="true">
        <files>
            <add value="index.htm" />
            <add value="iisstart.htm" />
            <add value="default.aspx" />
        </files>
    </defaultDocument>
</system.webServer>
</location>
```

# Locations

# Locking Configuration Settings

- You can allow non administrators to:
  - Modify configuration properties
  - Override configuration properties
- overrideMode: Defines the lockdown state of a configuration section

# Default Locking of Sections

- Defined in <configSections>
  - Use overrideModeDefault

```
<configSections>
...
<section name="defaultDocument"
    overrideModeDefault="Allow" />
...
</configSections>
```

```
<location path="MySite"
    overrideMode="Deny">
      <system.webServer>
        <defaultDocument/>
      </system.webServer>
    </location>

<location path="YourSite"
    overrideMode="Deny">
      <system.webServer>
        <defaultDocument enabled="true">
          <files>
            <clear/>
            <add value="default.aspx"/>
          </files>
        </defaultDocument>
      </system.webServer>
    </location>
```

# Locking <location> Sections

# Granular Locking

- Unlocking a section allows any part of it to be changed by application or site owners
- With granular locking you can restrict changes to specific elements or attribute settings
- You can also restrict the *type* of change to add, remove, or modify

- Specifies attributes that are locked

```
<location path="MyWebSite"
    allowOverride="Allow">
<system.webServer>
  <defaultDocument enabled="true"
    lockAttributes="enabled">
    <files>
      <add value="index.htm" />
      <add value="iisstart.htm" />
    </files>
  </defaultDocument>
</system.webServer>
</location>
```

Locked

# lockAttributes & lockAllAttributesExcept

- Limits what can be done to an element

```
<location path="MyWebSite"
    allowOverride="Allow">
<system.webServer>
  <defaultDocument enabled="true"
      <files lockElements="add">
    <add value="index.htm" />
      <add value="iisstart.htm" />
    </files>
  </defaultDocument>
</system.webServer>
</location>
```

Elements cannot be added

# lockElements add remove clear

- Locks a single item

```
<location path="MyWebSite"
    allowOverride="Allow">
<system.webServer>
  <defaultDocument enabled="true">
    <files>
      <add value="index.htm" lockItem="true"
      />
      <add value="iisstart.htm" />
    </files>
  </defaultDocument>
</system.webServer>
</location>
```

Locked

# lockItem

# Zdroje a odkazy - IIS

- Domovská stránka IIS, nejlepší zdroj informací a nástrojů
  http://iis.net
- Krátký úvod do IIS, videonávody
  http://learn.iis.net/
- Informace o IIS 7 na Microsoft Technetu
  http://technet.microsoft.com/en-us/library/dd364124%28WS.10%29.aspx
- IIS a PowerShell
  http://learn.iis.net/page.aspx/447/managing-iis-with-the-iis-powershell-snap-in/