Public Key Infrastrukture (PKI), díl 1.

Základním stavebním prvkem každého PKI je certifikační autorita, která má za úkol vystavovat a případně také zneplatňovat digitální certifikáty. Při návrhu celého řešení si musíme umět odpovědět na celou řadu důležitých otázek: Kolik úrovní bude celá hierarchie PKI mít? Je výhodné integrovat certifikační autoritu do Active Directory? Jakou délku klíče zvolit? Certifikát kořenové certifikační autority by měl mít platnost 1 rok nebo 20 let? Na tyto a mnohé další otázky naleznete odpověď v úvodním prvním díle seriálu o PKI.

1. Vlastní certifikační autorita nebo komerční?

Na tuto otázku samozřejmě neexistuje vždy stejná odpověď. Pokud potřebuji například vystavit jeden digitální certifikát pro webový server, bude výhodnější ho pořídit nákupem od komerční CA. Naopak pokud budu řešit požadavek na automatické vystavení certifikátů pro EFS v prostředí AD s několika tisíci uživateli, je určitě efektivnějším řešením vlastní CA. Pro správné rozhodnutí pojďme shrnout výhody a nevýhody obou možností.

Výhody vlastní CA:

- **Cena**: s rostoucím počtem certifikátů klesá cena za 1 certifikát
- **Flexibilita**: parametry certifikátů, certifikační politiky atd. si mohu stanovit dle potřeby
- **Rozšiřitelnost**: přidání uživatelů či nových typů certifikátů je velmi snadné a málo nákladné
- **Integrace do AD**: přináší celou řadu výhod. Např. autoenrollment, který dramaticky zjednodušuje proces vystavení certifikátů a snižuje tak náklady na implementaci i následnou správu.

Výhody komerční CA:

- **Důvěryhodnost**: při správně zvolené CA budou vydané certifikáty důvěryhodné i externě
- **Rychlost**: nemusím navrhovat ani implementovat vlastní PKI a certifikát mohu získat prakticky ihned
- **Právní aspekt**: kvalifikované certifikáty od státem akreditované CA mohu potřebovat např. pro podání daňového přiznání, komunikaci se státní správou apod.

2. Kolik úrovní bude mít hierarchie certifikačních autorit?

Důvodů proč nemít jednu jedinou CA, ale budovat hierarchii o několika úrovních je hned několik:

- **Distribuce rizika: p**okud dojde ke kompromitaci 1 z 10 podřízených online autorit je dopad mnohem nižší než když je napadena CA v jednoúrovňovém systému PKI, která vystavuje 100% certifikátů.

Flexibilita: není problém přidání nového AD forestu, zapojení jiné než Microsoft CA do hierarchie atd.

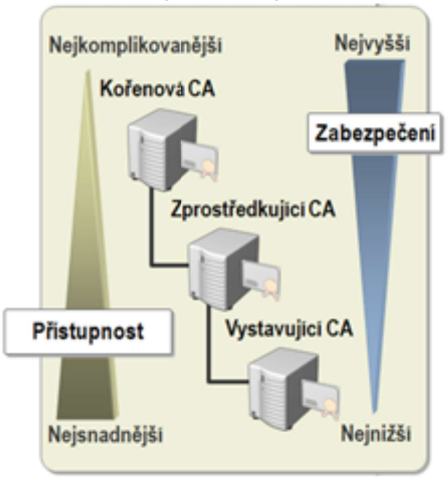
- **Bezpečnost:** zatímco vystavující CA bývá kvůli dostupnosti zpravidla online, naopak kořenová CA může být offline a tak je při dobrém fyzickém zabezpečení prakticky nenapadnutelná.

V zásadě je možné vybrat ze tří modelů:

1 úroveň – vhodné pro menší řešení a nízký počet vystavovaných certifikátů. Je to jednoduché a levné řešení, které je ale zároveň nejméně flexibilní a bezpečné.

2 úrovně – toto řešení nejčastěji odpovídá potřebám společnosti. První úrovní je offline kořenová CA, na druhé úrovni jsou online vystavující CA. Řešení je bezpečné, flexibilní, ale přesto stále přehledné a snadno spravovatelné.

3 úrovně – řešení pro velké organizace s maximální úrovní bezpečnosti. První úrovní je offline kořenová CA, na druhé úrovni jsou offline CA oddělující části PKI s různou bezpečnostní politikou, na třetí jsou pak vystavující online CA.



Obrázek 1 Hierarchie PKI s 3 úrovněmi

3. Integrovat certifikační autoritu do AD či nikoliv (Enterprise/Standalone)?

Intergace CA do Active Directory (režim Enterprise) má celou řadu přínosů oproti režimu bez AD (režim Standalone). Mezi nejdůležitější patří:

- Žádost o certifikát je potvrzena/zamítnuta automaticky na základě informací v AD
- Certifikáty i seznamy zneplatněných certifikátů mohou být publikovány přímo do AD

Subjekt žádá o certifikát prostřednictvím šablon certifikátů. Přístup k šablonám je řízen oprávněními v rámci Active Directory

- Enterprise režim je podmínkou pro řadu funkcí jako je archivace privátního klíče, autoenrollment apod.

Enterprise režim je tak typicky vyžíván pro vystavující online CA, standalone je zase naopak vhodný pro kořenovou offline CA nebo do prostředí bez Active Directory.

4. Musím řešit vysokou dostupnost? Jaké jsou možnosti zajištění vysoké dostupnosti CA?

V zásadě se dá říci, že krátkodobý výpadek nemá obvykle u toho typu služby žádný závažnější dopad. Jakmile mám k dispozici vystavený a platný digitální certifikát, certifikační autoritu do doby obnovování platnosti vlastně vůbec nepotřebuji.

Pozor. Výjimkou jsou ale scénáře, kde se používají certifikáty s krátkou dobou platnosti. Například 4hodinový výpadek CA při požití technologie Network Access Protection (NAP) znamená odpojení všech počítačů od sítě! Abychom takovouto nezáviděníhodnou situaci nezažily, řešením je:

- Redundance – danou šablonu certifikátu vypublikujeme na více různých CA
- Clustering – od verze Windows Server 2008 je podporován také failover clustering této role

5. Jakou platnost certifikátů CA zvolit?

Zde existuje jednoznačné doporučení:

- Kořenová Standalone CA – 20 let
- Zprostředkující Standalone CA – 10 let
- Vystavující Enterprise CA – 5 let

Kromě stanovení platnosti je také třeba určit, kdy se bude provádět obnova certifikátu. CA nikdy nesmí vystavit certifikát s delší platností než je platnost jejího vlastního certifikátu. Prakticky to tedy znamená, že kořenová CA po 18 letech již nemůže vystavit certifikát pro zprostředkující CA s platností 10 let, neboť sama má certifikát, který bude platný již jen 2 roky. Řešením je každých 10 let provádět obnovu certifikátu kořenové CA. Tímto způsobem musíme stanovit pravidla pro obnovování certifikátu každé CA.

6. Jakou délku klíče zvolit?

Doporučení jsou následující:

- Kořenová Standalone CA – 4096 bitů
- Zprostředkující Standalone CA – 2048 bitů
- Vystavující Enterprise CA – 2048 bitů

V roce 2008 byl prolomen klíč RSA o délce 663 bitů a nyní se dokončuje prolomení klíče o délce 768 bitů. Je tedy více než zřejmé, že častou používaná délka 1024 bitů to bude mít dříve či později také již spočítané a pro certifikáty s delší dobou platnosti bychom ji již proto neměli využívat.

Závěr

V tomto článku jsme vysvětlili základní parametry certifikační autority, které musíme mít rozhodnuty a určeny ještě před vlastní implementací. Příští díl bude zaměřen více prakticky a podíváme se společně na úskalí a doporučení pro nejběžnější variantu dvouúrovňového PKI – kořenová Standalone CA a pod ní zapojená vystavující Enterprise CA.

Public Key Infrastructure (PKI), díl 2.

…díl druhý, **jak správně na dvouúrovňové PKI**

V minulém díle jsme popsali základní parametry PKI, které by měly být součástí každého návrhu. Pro většinu organizací je optimální architektura s dvěma úrovněmi CA: jedna standalone offline kořenová CA a pod ní libovolné množství podřízených online enterprise vystavujících CA. Tento článek si neklade za cíl vytvořit detailní „step by step" příručky, ale spíše jen upozornit na úskalí, která na nás při implementaci této architektury čekají. Veškeré kroky jsou vyzkoušeny v prostředí Windows Server 2008 R2, ale jsou obecně platné i pro předchozí verze.

1. Krok: instalace kořenové standalone CA

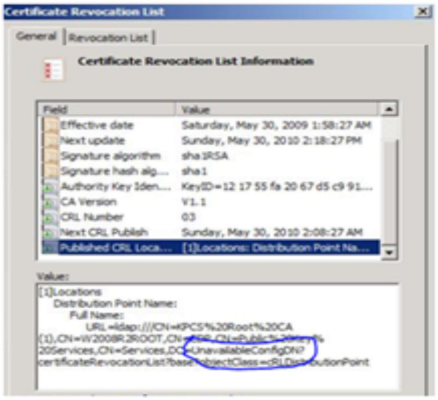
Vlastní instalaci provedeme jednoduše pomocí průvodce přidáváním a odebíraním rolí v rámci správci serveru. V předchozím článku jsme popsali doporučené parametry:

- Délka klíče: 4096 bitů
- Délka platnosti certifikátu CA: 10 let

2. Krok: konfigurace kořenové standalone CA

- **Nastavení DN konfiguračního oddílu AD**

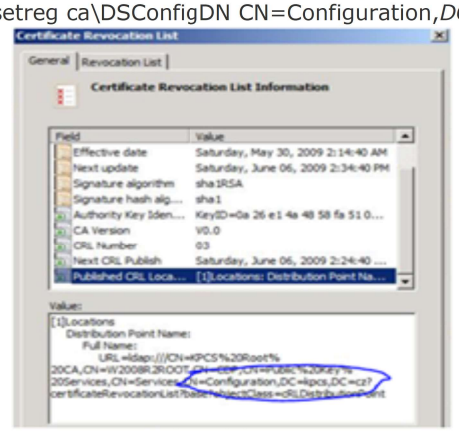
CRL, které publikuje kořenová CA, obsahuje informaci o tom, v jaké LDAP cestě má být CRL umístěno. Protože ale tento server stojí mimo AD, je třeba službu CA tuto lokaci „naučit".



Obrázek 1 CRL standalone offline CA před nastavením DN konfiguračního oddílu CA

Nastavení provedeme pomocí nástroje příkazové řádky

certutil.exe –setreg ca\DSConfigDN CN=Configuration,*DC=kpcs,DC=cz*



Obrázek 2 CRL standalone offline CA po nastavení DN konfiguračního oddílu CA

- **Nastavení maximální délky platnosti vystavovaných certifikátů**

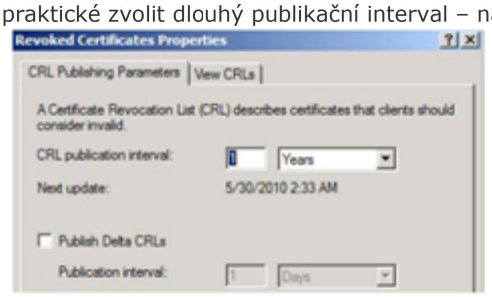
Standalone CA umožňuje ve výchozím nastavení vystavovat certifikáty s maximální délkou platnosti 1 rok. Naše

podřízená CA má mít délku platnosti 5 let, a proto musíme tedy provést zvýšení hodnoty tohoto parametru z příkazové řádky.

certutil -setreg ca\ValidityPeriodUnits 5
certutil -setreg ca\ValidityPeriod "Years"
net stop certsvc & net start certsvc

- **Konfigurace CRL a Delta CRL**

Protože offline CA je vypnutá a vždy před uplynutím platnosti CRL je vždy nutné ji zapnout a vypublikovat nové CRL do všech definovaných umístění, je praktické zvolit dlouhý publikační interval – nastavíme 1 rok. Delta CRL zcela vypneme.



Obrázek 3 Konfigurace intervalu publikace CRL offline kořenové CA

- **Konfigurace CDP**

Ve výchozím nastavení CDP ponecháme umístění LDAP a lokání soubor, všechna ostatní odebereme. Pokud potřebujeme umožnit ověřování platnosti certifikátů i pro počítače mimo AD, přidáme HTTP lokaci ve formátu:

http://*www.kpcs.cz/pki*/%3%8%9.crl

Dále provedeme nastavení dalších parametrů viz následující tabulka:

Nastavení CDP	Soubor	HTTP	LDAP
Publish CRLs to this location	Nastavit	N/A	Zrušit
Include in all CRLs	N/A	N/A	Nastavit
Include in CRLs	N/A	Zrušit	Zrušit
Include in the CDP extension of issued certificates	N/A	Nastavit	Nastavit
Publish delta CRLs to this location check box	Zrušit	N/A	Zrušit

Tabulka 1 Konfigurace CDP standalone offline CA

- **Konfigurace AIA**

Ve výchozím nastavení AIA ponecháme umístění LDAP a lokání soubor, všechna ostatní odebereme. Pokud potřebujeme umožnit ověřování důvěryhodnosti certifikátů i pro počítače mimo AD, přidáme HTTP lokaci ve formátu:

http://*www.kpcs.cz/pki*/%1_%3%4.crt

Dále provedeme nastavení dalších parametrů viz následující tabulka:

Nastavení AIA	FILE	HTTP	LDAP
Include in the AIA extension of issued certificates check box	N/A	Nastavit	Nastavit
Include in the online certificate status protocol (OCSP) extension check box	N/A	Zrušit	Zrušit

Tabulka 2 Konfigurace AIA standalone offline CA

- **Krok: publikování CRL a certifikátu CA do AD**

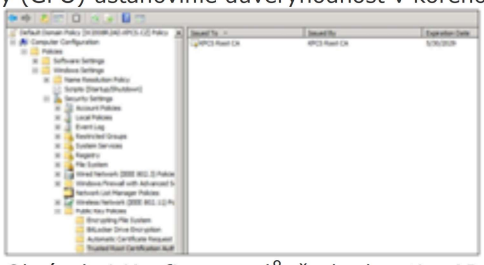
Vynutíme vystavení nového CRL a soubory s crl a certifikátem kořenové CA si vykopíruje na počítač, který je členem AD. Vlastní vypublikování provedeme s administrátorskými právy příkazy:

certutil -dspublish -f c:\KPCSRootCert.crt RootCA
certutil -dspublish -f c:\KPCSRootCRL.crl *W2008R2ROOT*

W2008R2ROOT je v našem příkladu jméno serveru kořenové CA. V případě použití http lokace v AIA a CDP je nutné tyto soubory také umístit na určený webový server.

- **Krok: ustanovení důvěryhodnosti kořenové CA v Active Directory**

V rámci doménové politiky (GPO) ustanovíme důvěryhodnost v kořenovou CA, kterou jsme nainstalovali.



Obrázek 4 Konfigurace důvěryhodnosti v AD

- **Krok: instalace vystavující enterprise CA**

Nyní je vše již připraveno k instalaci podřízené enterprise CA, kterou zpovozíme opět pomocí průvodce přidáváním a odebíraním rolí v rámci správci serveru, a to s následujícími parametry:

- Délka klíče: 2048 bitů
- Délka platnosti certifikátu CA: 5 let

V případě potřeby ještě upravíme CDP a AIA informace a provedeme pomocí nástroje Enterprise PKI závěrečnou kontrolu viz obrázek.

Tabulka 3 Kontrola pomocí Enterprise PKI

Závěr

Implementace PKI s dvěma úrovněmi CA je spojena s nutností provést celou řadu důležitých kroků. Provedení těchto konfigurací je nutnou podmínkou pro korektní fungování PKI. Věřím ale, že se v tomto článku podařilo je stručně a výstižně popsat a tak implementace PKI bude nyní pro každého již snadnou záležitostí.

Public Key Infrastructure (PKI), díl 3.

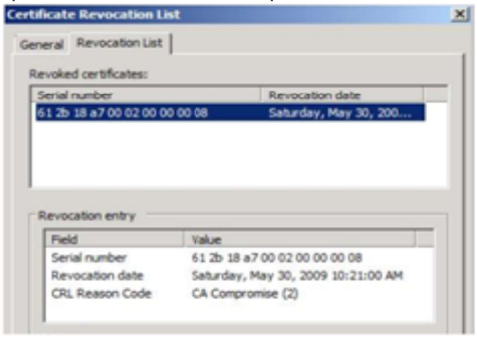
…díl třetí, **kontrola zneplatněných certifikátů**

Platnost certifikátů končí buď přirozeně uplynutím doby, na kterou byly vystaveny, nebo jejich zneplatněním. Důvody pro zneplatnění mohou být různé: kompromitace privátního klíče, odchod zaměstnance z firmy apod.

PKI musí nabídnout způsob jak umožnit ověřování toho, zda je certifikát zneplatněný či ne. O tom, jaké metody se nabízí v rámci MS Windows a jaká jsou doporučení pro jejich implementaci, si povíme právě v tomto třetím díle našeho seriálu.

1. Seznamy zneplatněných certifikátů – CRL (Certificate Revocation List)

Základní metodou je pravidelné publikování seznamu zneplatněných certifikátů, u kterých ještě nevypršela jejich časová platnost. Tento seznam je uložen do souboru a publikován do umístění zvaných CDP (CRL Distribution Point). Informace o CDP je pak přidávána do každého vystaveného certifikátu.



Obrázek 1 Zamítnutý certifikát v CRL

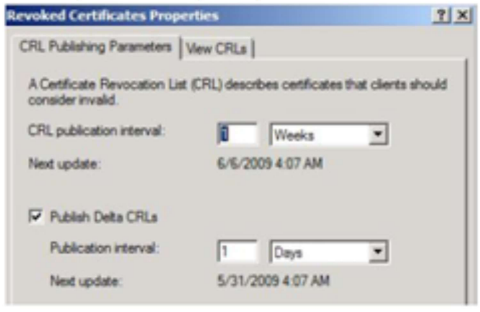
Z hlediska plánování jsou důležité primárně dva faktory:

- **Jak často?** Pokud publikuji CRL příliš často, vytvářím zátěž díky častému stahování CRL a zkracuji si reakční dobu pro případnou havárii CA. Naopak zásadní nevýhodou málo frekventovaného publikování CRL je neaktuálnost dat. Např. CRL s měsíční publikační frekvencí je analogicky stejné, jako kdyby po zablokování Vaší kreditní karty s ní mohl ještě měsíc po nahlášení zloděj nakupovat. Frekvenci publikování také ovlivňuje, zda je CA online či offline. U offline CA se doporučuje dlouhá platnost CRL – bez problémů i 1 rok. U vystavujících online CA je výchozím nastavením 1 týden.
- **Kam?** CDP může být nasměrováno do Active Directory (LDAP), na FTP server, HTTP server nebo do souborového systému. CDP může být použito několik současně. Dále uvedeme klíčová doporučení pro CDP:
  - Pokud je PKI využíváno převážně v prostředí jednotné AD, je ideálním CDP LDAP umístění. Replikace AD zajišťuje automaticky vysokou dostupnost CRL.
  - Výjimkou je AD s dlouho dobou konvergence. V určitých situacích může být například platnost CRL kratší než je doba nutná k zreplikování CRL v rámci AD. V takovémto případě bychom se měli LDAP umístění naopak vyhnout.
  - Pokud je PKI vyžíváno převážně v prostředí mimo AD, doporučeným CDP je HTTP umístění. Pro vysokou dostupnost je třeba použít více HTTP CDP nebo zajistit vysokou dostupnost web serveru technologiemi typu DNS Round Robin, NLB apod.
  - Pokud používáme HTTP i LDAP lokaci, LDAP by měl být vždy na prvním místě.
  - Offline CA nesmí mít CDP pouze sama na sebe (výchozí nastavení), neboť je z principu offline, a tak je tím pádem nedostupné i CRL.

2. Rozdílové seznamy zneplatněných certifikátů – Delta CRL

Pro zajištění aktuálnějších dat o zneplatněných certifikátech při zachování nízké zátěže je možné od verze Windows Serveru 2003 publikovat rozdílové seznamy zneplatněných certifikátů od posledního CRL – tzv. Delta CRL. Nasazení Delta CRL podléhá následujícím pravidlům a doporučením:

- Delta CRL je podporován ve verzi Windows Server 2003, Windows XP a novější
- Offline CA by neměla publikovat Delta CRL
- Vystavující online CA by měla 1x týdně publikovat základní CRL a 1x denně Delta CRL



Obrázek 2 Publikační interval CRL a Delta CRL

3. OCSP (Online Certificate Status Protocol)

OCSP je protokol založený na přenosu pomocí http, který umožňuje dotazovat se online na aktuální platnost ověřovaného certifikátu. Klient tak nestahuje celé CRL, ale dotazuje se pouze na certifikát, který aktuálně zpracovává. Protože nedochází ke stahování CRL, je tak možné CRL publikovat mnohem častěji bez rizika vysoké zátěže CDP. Základním stavebním kamenem je komponenta Windows Serveru 2008, která se nazývá Online Responder. Online Responder si z certifikační autority stahuje platné CRL či Delta CRL. Na základě zde uvedených informací pak komunikuje pomocí http protokolu s klienty Windows Vista a novějšími a posílá jim digitálně podepsanou zprávu o tom, zda ověřovaný certifikát byl zneplatněn či nikoli.
Jeden Online Responder může fungovat pro více certifikačních autorit. Naopak platí., že pro jednu certifikační autoritu může existovat více Online Repsonderů, které se dají spojit do jednoho pole pomocí NLB, a tak zajistit vysokou dostupnost OCSP.

Obrázek 3 OCSP s nebo bez vysoké dostupnosti
Detailní demo s postupem pro konfiguraci OCSP můžete shlédnout na MS TV WS2008 R2 – PKI (4) – Online Certificate Status Protocol

Závěr

Kontrola zneplatněných certifikátů je jedním ze základních stavebních prvků celého PKI. Vysoká dostupnost a implementace dle doporučení je pak nutno podmínkou spolehlivé a bezpečné infrastruktury veřejného klíče. V příštím díle se můžete těšit na popis novinek Windows Serveru 2008 R2 v oblasti PKI.

Public Key Infrastructure (PKI), díl 4.

..díl čtvrtý, **Windows Server 2008 R2: Novinky v oblasti PKI**

PKI se samozřejmě s každou novou verzí operačního systému Windows rovněž vyvíjí a objevují se nové funkce vylepšující bezpečnost, zjednodušující nasazení a správu apod. V posledním díle seriálu se podíváme na novinky, na které se můžeme těšit v blížícím se Windows Serveru 2008 R2

1. Podpora Server Core

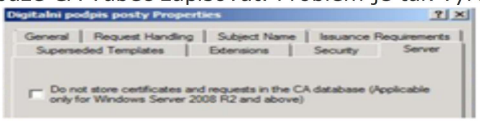
Role certifikační autority je nově podporována i v rámci instalace typu Server Core

2. Podpora pokročilých funkcí i ve verzi Windows Server 2008 R2 Standard Edition

Asi každý z nás, kdo někdy implementoval PKI na platformě Windows, zjistil, že funkce certifikační autority se zásadně liší podle toho, zda se jedná o edici Standard či vyšší. Ve Windows Serveru 2008 R2 jsou tato omezení již minulostí a tak i s instalovanou edicí Standard se můžeme těšit z podpory šablon certifikátů V2 a V3, autoenrollmentu, archivace privátního klíče atd.

3. Řešení problému s certifikáty s krátkou dobou platnosti

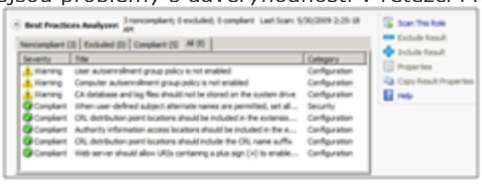
Představte si situaci, kdy máte v síti 1000 počítačů a implementovaný NAP s IPSec vynucením. Protože v rámci této technologie je zdravým počítačům vystavován certifikát s platností pouze na 4h, za 1 den tu máme 6 000 vystavených certifikátů, za 1 rok dokonce 2 190 000 vystavených certifikátů. Takto dojde velmi rychle k zahlcení databáze certifikátů na certifikační autoritě, navíc typem certifikátu, který vůbec nepotřebuji tímto způsobem zaznamenávat.
Windows Server 2008 R2 nově umožňuje v konkrétní šabloně certifikátů nastavit, že se vystavované certifikáty nebudou do databáze CA vůbec zapisovat. Problém je tak vyřešen.



Obrázek 1 Možnost neukládat certifikáty v CA databázi

4. BPA pro PKI

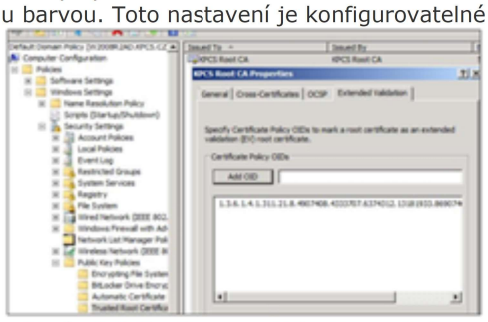
Microsoft již delší dobu uvolňuje pro různé produkty a technologie velmi populární kategorii nástrojů tzv. Best Practices Analyzery, které umí zkontrolovat, zda je Vaše prostředí nakonfigurováno dle doporučených praktik.
Nově nalezneme ve Windows Serveru 2008 R2 Best Practices Analyzer přímo pro roli certifikační autority. Zkontroluje nám například, zda máme správně nastavené AIA a CDP, jestli je funkční OCSP, není-li již čas na obnovu certifikátu CA nebo zda nejsou problémy s důvěryhodností v řetězci PKI.



Obrázek 2 Best Practices Analyzer pro CA

5. Enterprise SSL EV certifikát

Novinkou Windows Serveru 2008 R2 je také možnost označit kořenovou Enterprise CA jako extended validation (EV) root a tak certifikáty vystavené v rámci této hierarchie budou v internetovém prohlížeči vyznačený důvěryhodnou zelenou barvou. Toto nastavení je konfigurovatelné pomocí Group Policy.

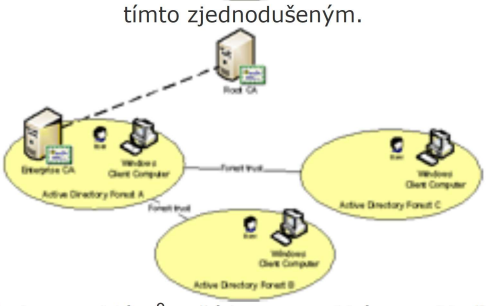


Obrázek 3 Konfigurace EV v Group Policy

6. Konsolidace certifikačních autorit v prostředí s více Active Directory foresty, mezi kterými je navázán forest-trust vztah

Obrazněřečeno je možné nahradit stávající schéma

tímto zjednodušeným.



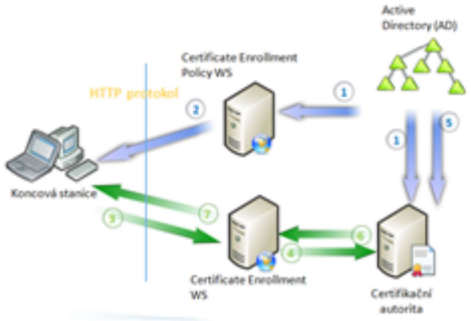
Subjekt z jednoho AD forestu si může bez problémů zažádat o certifikát certifikační autoritu z jiného AD forestu, a to i prostřednictvím autoenrollmentu. Toto je umožněno díky dvěma klíčovým změnám:

- Systém obsahuje powershell příkaz pro synchronizaci šablon certifikátů mezi AD foresty. Protože uživateli se načítá seznam šablon z jeho domovského AD forestu a CA zase naopak požívá šablony ze svého AD, konfigurace šablon musí být udržována konzistentní.

CA má nově schopnost používat tzv. LDAP referrals, což znamená, že může přistupovat k informacím o uživateli či počítači v jiném AD forestu.

7. Vystavování certifikátů pomocí http protokolu

Http enrollment plně nahrazuje stávající RPC/DCOM protocol, který se dosud používal například pro autoenrollment. Důvodem změny není zdaleka jen změna samotného protokolu, ale především umožnění nových scénářů pro automatické vystavování certifikátů i pro počítače z jiného AD forestu bez vztahu důvěry nebo pro počítače stojící zcela mimo AD.



Obrázek 4 Vystavování certifikátů pomocí WS

Celý proces vypadá následovně:

1. Šablony certifikátů jsou vypublikovány z AD pomocí Web Service Certificate Enrollment Policy, což je nová služba role ve Windows Serveru 2008 R2
2. Klient kontaktuje Certificate Enrollment Policy server, který mu posílá seznam šablon
3. Klient si vybírá šablonu a žádá o certifikát jinou webovou službu – Certificate Enrollment WS
4. Certificate Enrollment WS přeposílá žádost na certifikační autoritu
5. CA ověřuje data o žadateli v Active Directory
6. Vystavený certifikát je předán Certificate Enrollment WS serveru
7. Vystavený certifikát je předán koncové stanici

Tento systém je zcela otevřený a předpokládá se rostoucí podpora ze strany komerčních CA. Takže se možná v budoucnu dočkáme scénářů typu:

- Zřídím si elektronické bankovnictví a ve svém počítači si zkonfiguruji cestu k webové službě pro vystavení certifikátu od CA mojí banky. Nejenom že mi bude vystaven certifikát, ale už se nikdy nebudu muset starat o obnovu certifikátu, tu si bude řídit systém sám na pozadí.
- Koupím si od komerční CA certifikát pro můj webový server, ale už nikdy nebudu nucen hlídat pravidelné obnovování. To za mě bude řešit právě tato nová služba.

Závěr

Nové funkce a možnosti PKI na Windows Server 2008 R2 nejsou zdaleka jen kosmetické, ale zásadním způsobem umožňují PKI značně zjednodušit, implementovat zcela nové scénáře využití a správu činí mnohem jednodušší. Věřím, že se teď na novou verzi Windows Serveru těšíte stejně jako já :).