# Vytvorenie žiadosti o certifikát na Windows Serveru 2008/Vista a vyššie a zobrazenie MMC konzoly pre zálohu privátneho kľúča

Najprv je potreba pridať modul snap-in do konzoly mmc

V príkazovom riadku napíšte **"mmc**" a stlačte Enter



Nižšie vidíte prázdnu konzolu mmc



🔚 Konzola1 - [Kořenový adresář konzoly]		_ D ×
Soubor Akce Zobrazit Oblibené položky Okno	Nápo <u>v</u> ěda	
	Nému	Akca
	Tom ito zobrazení neodnovídá žádná položka	Kořenový adresář konzoly
	Laurana Kanuaran urandha una Kanua bananimi	Další akce
1	7	,



# Zvoľte "Súbor" a "Pridať alebo odobrať modul snap-in"

🛱 Konzola 1 - [Kořenový adresář konzoly]	
Soubor Akce Zobrazit Oblíbené položky Okno Nápověda	_ 8 ×
Nový Ctri+N	
Ctri+C Ct	Alue
Uoàt Ctri+S Marey	ARCE
Ulozit jako Tomuto zobrazení neodpovídá žádná položka.	Korenovy adresar konzoly
Přidat nebo odebrat modul snap-in Ctrl+M	Další akce 🕨
Možnost	
1 C:Users\Konzola1.msc	
2 certmgr.msc	
3 compright msc	
Ukonöt	
možňuje přídávat a odebírat moduly snap-in z konzoly.	

## Pridajte modul "Certifikáty"

odul snap-in	Dodavatel	•	Kořenový adresář konzoly	Upravit rozšíření
Brána Windows Firew	Microsoft Corp			
Certifikáty	Microsoft Corp			Odebrat
Editor objektů zásad s…	Microsoft Corp			
Konfigurace a analýza	Microsoft Corp			Nahoru
Konfigurace klienta NAP	Microsoft Corp			
Místní uživatelé a sku…	Microsoft Corp			Dglů
Odkaz na webovou a	Microsoft Corp		Přidat >	
Ovládací prvek ActiveX	Microsoft Corp			
Plánovač úloh	Microsoft Corp			
Prohlížeč událostí	Microsoft Corp			
Řízení služby WMI	Microsoft Corp			
Sdílené složky	Microsoft Corp			
) Sledování výkonu	Microsoft Corp			Llořespit
Sledování zabezpečen	Microsoft Corp	•		opresilition



## Vyberte "Účet počítača"

Modul snap-in Certifikáty	×
Tento modul snap-in bude vždy spravovat certifikáty pro:	
◯ <u>M</u> ůj uživatelský účet	
O Účet <u>s</u> lužby	
	_
< Znět Další > Stomo	

#### Zvoľte "Miestny počítač"

Vybrat počítač		×
Vyberte počítač, který ch	cete spravovat tímto modulem snap-in.	
<ul> <li>Místní počítač (po</li> </ul>	je vzdy spravovat: čítač, ve kterém je spuštěna tato konzola)	
O <u>J</u> iný počítač:	Procházet	
Povolit změn <u>u</u> vybr konzolu uložíte)	aného počítače při spuštění z příkazového řádku (platí, pouze pokud	
		_
	< <u>∠</u> pět Dokončit Stomo	



#### Nižšie už vidíte úspešne pridaný modul snap-in

odul snap-in	Dodavatel	•	Kořenový adresář konzoly	Upra <u>v</u> it rozšíření
Brana Windows Firew	Microsoft Corp		🛱 Certifikäty (mistni)	Odebrat
Editor objektů zásad s	Microsoft Corp			
Konfigurace a analýza	Microsoft Corp			5 februari
Konfigurace klienta NAP	Microsoft Corp			Ivanoru
Místní uživatelé a sku	Microsoft Corp			Dolů
Odkaz na webovou a	Microsoft Corp		Přidat >	
Ovládací prvek ActiveX	Microsoft Corp			
Plánovač úloh	Microsoft Corp			
Prohlížeč událostí	Microsoft Corp			
Řízení služby WMI	Microsoft Corp			
Sdílené složky	Microsoft Corp			
Sledování výkonu	Microsoft Corp			Unčernit
Sledování zabezpečen	Microsoft Corp	_		Opreshit
s:				
		_		
Sledování výkonu Sledování zabezpečen is:	Microsoft Corp Microsoft Corp Microsoft Corp	•		Upřesn

Potom vám v ľavom menu pribudne modul **"Certifikáty (miestne)"**, kde po otvorení zložky **"Požiadavka na zápis certifikátu"** uvidíte vygenerované privátne kľúče – potom vykonajte jeho export (tým vykonáte zálohu privátneho kľúča. Vygenerovaný PK sa vám zobrazí po vytvorení žiadosti pomocou príkazu certreq, ktorý je popísaný nižšie)

🐺 Konzola 1 - [Kořenový adresář konzoly/Certifikáty (mistní)/Požadavek na zápis certifikátu/Certifikáty]								
Soubor Akce Zobrazit Obilbené položky. Oknjo Nápověda								
	[	far an and	Tex 1 Tr	-		1 au	18.00	
Certificaty (mistro)	Vystaveno pro A	CEDITIES Tart	Datum ukonceni	2 Zamysiene ucely	Popisny nazev	Stav	Sabic	AKCE
E Contracty (model)	CENTREQ - Test	CERTREQ - Test	26.4.2013	Overeni serveru	<zdurty></zdurty>			Certifikáty 🔺
🗐 🦰 Důvěrvhodné kořenové certifikační autority	Calcontrac Test	CERTREQ - Test	20.4.2013	Overeni serveru	<2duriy >			Další akce
🖲 🧧 Důvěrvhodnost v rámci rozlehlé sítě	CENTREQ - Test	CERTREQ - Test	3.5.2013	Overeni serveru	<2duriy >			
E Zprostředkující certifikační autority	Partice of the second s	CERTREQ - Test	3.3.2013	Overeni serveru	<zduriy></zduriy>			
Důvěryhodní vydavatelé	Participation of the second se	tesedar igwr u digt2kar 2.11 kica.iocai	15.4.2015	Overeni serveru	<2duriy >			
E Produčený statu na produkte n produkte na produkte na produk	California des formats the track of the second seco	tesedar igwir u digtzkar 2.11 kica.iocal	26.4.2013	Overeni serveru	<2duriy >			
표 🚞 Kořenové certifikační autority třetích stran	tesedarfgwrtrthgtzkar2.nrkica.iocai	tesedartgwrtrthgt2kar2.hrkica.iocal	26.4.2013	Overeni serveru	<zadny></zadny>			
Důvěryhodné osoby	tesedartgwrtrthgtzkarz.nrkica.iocai	tesedartgwrtrthgt2kar2.nrkica.iocal	13.4.2013	Overeni serveru	<zadny></zadny>			
🕑 🧮 Ostatní uživatelé	tesedartgwrtrthgtzkarz.nrkica.iocal	tesedarigwrtrthgt2kor2.nrkica.iocai	26.4.2013	Overeni serveru	<zaony></zaony>			
Požadavek na zápis certifikátu	Laltest2k8r2.hrkica.local	test2k8r2.hrkica.local	28.3.2013	Overeni serveru	<zadny></zadny>			
Certifikáty:	Lal test2kdr2.hrkica.local	test2k8r2.hrkica.local	16.4.2013	Overeni serveru	<zadny></zadny>			
Důvěryhodné kořeny čipových karet	test2k8r2.hrkica.local	test2k8r2.hrkica.local	28.3.2013	Overeni serveru	<zádný></zádný>			
Důvěryhodná zařízení	test2k8r2.hrkica.local	test2k8r2.hrkica.local	16.4.2013	Overeni serveru	<zádný></zádný>			
	test2k8r2.hrkica.local	test2k8r2.hrkica.local	28.3.2013	Ověření serveru	<zádný></zádný>			
	test2k8r2.hrkica.local	test2k8r2.hrkica.local	28.3.2013	Ověření serveru	<Žádný>			
	test2k8r2.hrkica.local	test2k8r2.hrkica.local	16.4.2013	Ověření serveru	<Žádný>			
	1							
	1							
	1							
	1							
	1							
	1							
	1							
	1							
	1							
	1							
	1							
	1							
	1							
	1							
	1							
	1							
	1							
	1							
	1							
	1							
	41					-	in the second	
1	1.21						_	
Uložiště Požadavek na zápis certifikátu obsahuje 16 certifikátí	Ĵ.							



#### Postup získania komerčného serverového certifikátu I.CA pre IIS (WS2008/Vista a vyššie)

Po vytvorení žiadosti o certifikát je možné použiť nástroj certreq (ktorý je prítomný na každej instancii Windows Server) podľa nasledujúceho postupu:

1. Vytvorte textový súbor so šablónou pre vygenerovanie žiadosti o certifikát – napr- **IISreq.inf** – podľa nasledujúceho vzoru:

#### [NewRequest]

Subject = "CN=mailServer,O=ICA,OU=testing,C=CZ,St=Kralovahradecky kraj"

; Subject opravte podle udaju Vaseho serveru, položka CN nesmi obsahovat domenove jmeno, FQDN, (např. <u>www.ica.cz</u>) a IP adresu (např. 193.86.0.248)

- ; vyplneny musi byt alespon polozky C a CN, ostatni v souladu s certifikacni politikou
- ; pole: CN =Common Name (nazev serveru)
- ; O =Organization (organizace, firma)
- ; OU =Organization Unit (organizacni jednotka)
- ; L =Locality (lokalita, mesto)
- ; C =Country (zeme, stat)
- ; St =stateOrProvince (kraj) KeySpec = 1
- HashAlgorithm = sha256 KeyLength = 2048

UseExistingKeySet = FALSE Exportable =

TRUE UserProtected = FALSE

MachineKeySet = TRUE



ProviderName = "Microsoft RSA SChannel Cryptographic Provider" ProviderType = 12

RequestType = PKCS10

KeyUsage = 0xa0 SMIME =

False

SuppressDefaults = true [EnhancedKeyUsageExtension]

OID=1.3.6.1.5.5.7.3.2 ;pro Clietn Authentication

Položky Subject a KeyLenght upravte v súlade s komentárom na identifikáciu vášho servera a na potrebnú dĺžku kľúča. (Stredníkom sú uvedené komentáre.)

2. Vytvorte žiadosť o certifikát na cieľovom servery. **POZOR! Musí byť uskutočnené priamo na IIS** servery, pretože pri vytváraní žiadosti je generovaný nový pár kľúčov.

IISsrv>

#### certreq -new IISreq.inf IISreq.txt

Vytvorená žiadosť bude uložená v súbore **IISreq.txt**, ktorý je možné zobraziť a kopírovať ako text (ide o base 64 zakódované binárne dáta).

3. Obsah žiadosti predložte obvyklým spôsobom na I.CA. Na <u>www.ica.cz</u> vykonajte vloženie obsahu žiadosti do formulára pre komerčný serverový certifikát I.CA, doplnenie hesla pre zneplatnenie atd., vytvorenie žiadosti o serverový certifikát. Ďalej vykonajte predanie žiadosti na RA.

4. Po získaní certifikátu na ISS servery (na ktorom ste vytvárali žiadosť) uskutočnite inštaláciu certifikátu (vo formáte DER) pomocou príkazu::

IISsrv>



#### certreq -accept <nnnnn.der>

kde **<nnnn.der>** je názov súboru so získaným certifikátom vo formáte der.

Koreňový certifikát vydávajúci komerčný I.CA musí byť v trusted root v úložisku počítača, inak príkaz certreq –accept ohlási chybu a certifikát nenainštalujete (a nespojí ho s vygenerovaným súkromným kľúčom).

5. Teraz v IIS nakonfigurujte/zvoľte pre SSL zabezpečenie zvolenej website novo inštalovaný certifikát, a overte správnosť funkcie pri prístupu klienta na webový server.

Záverečné poznámky:

- 1. Použitím uvedenej šablóny je vygenerovaná žiadosť o certifikát bez položiek sMIMECapabilities a subjectKeyIdentifier.
- 2. Uvedený vzor šablóny predpokladá:
  - uloženie kľúčov v operačnom systéme,
  - standalone Web server,
  - nelze ji použít pro WS2003.