Vytvoření žádosti o certifikát na Windows Serveru 2008/Vista a vyšší a zobrazení MMC konzole pro zálohu privátního klíče

Nejprve je potřeba přidat modul snap-in do konzole mmc

V příkazové řádce napište "mmc" a stiskněte Enter



Níže vidíte prázdnou konzoli mmc

🚟 Konzola1 - [Kořenový adresář konzoly]				<u>- 🗆 ×</u>
Soubor Akce Zobrazit Oblibené položky Ok <u>n</u> o	Nápo <u>v</u> ěda			_ & ×
(= =) 📅 🛃 🖬				
🧮 Kořenový adresář konzoly	Název		Akce	
		Tomuto zobrazení neodpovídá žádná položka.	Kořenový adresář konzoly	~
			Další akce	•
1	1			_



👼 Konzola 1 - [Kořenový adresář konzoly]		×
Soubor Akce Zobrazit Oblíbené položky Ok	no Nápověda	_ 8 ×
A Nový Ctrl+N		
Otevřít Ctrl+O	Tax (
Uložit Ctrl+S	Název	Akce
Uložit jako	Tomuto zobrazení neodpovídá žádná položka.	Kořenový adresář konzoly
Přidat nebo odebrat modul snap-in Ctrl+M		Další akce
Možnosti		
1 C:\Users\\Konzola1.msc		
2 certmgr.msc		
3 compmgmt.msc		
Ukončit		
	·	
1		
1		
the weather the state of the st		

Zvolte "Soubor" a "Přidat nebo odebrat modul snap-in"

Přidejte modul "Certifikáty"

Přidat nebo odebrat modul	y snap-in			×
Pro tuto konzolu můžete vybr také vybrat povolená rozšířen	at moduly snap-in z ıí.	toha	to počítače a tyto moduly poté nakonfigurovat. Pro rozšířitelné moduly	v snap-in můžete
Moduly snap-in k dispozici:			Vybrané modu <u>l</u> y snap-in:	
Modul snap-in	Dodavatel		Cořenový 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		<u>P</u> ridat >	
📹 Ovládací prvek ActiveX	Microsoft Corp			
🕑 Plánovač úloh	Microsoft Corp			
🛃 Prohlížeč událostí	Microsoft Corp			
🚔 Řízení služby WMI	Microsoft Corp			
🔞 Sdílené složky	Microsoft Corp			
Nedování výkonu 🔊	Microsoft Corp			Llořespit
🗟 🕄 Sledování zabezpečen	Microsoft Corp	_		opresnit
Popis:				
Modul snan-in Certifikáty um	ožňuje procházet ob	sah	úložišť certifikátů pro vás, pro službu pebo pro počítač.	
1				
				OK Storno



Vyberte "Účet počítače"

	-1
Tento modul snap-in bude vždy spravovat certifikáty pro:	
○ <u>M</u> ůj uživatelský účet	
O Účet <u>s</u> lužby	
<u>Účet počítače</u>	
< ∠pet <u>D</u> alši > Stomo	

Zvolte "Místní počítač"

Vybrat počítač	×
Vyberte počítač, který chcete spravovat tímto modulem sn	ap-in.
Tento modul snap-in bude vzdy spravovat:	
Místní počítač (počítač, ve kterém je spuštěna tato)	konzola)
O Jiný počítač:	<u>P</u> rocházet
Povolit změn <u>u</u> vybraného počítače při spuštění z při konzolu uložíte)	íkazového řádku (platí, pouze pokud
	< Zpět Dokončit Storno



Níže už vidíte úspěšně přidaný modul snap-in

Editor objektů zásad s… Microsoft Corp… Konfigurace a analýza… Microsoft Corp… Konfigurace klienta NAP Microsoft Corp… Mistní uživatelé a sku… Microsoft Corp… Odkaz na webovou a… Microsoft Corp… Ovládací prvek ActiveX Microsoft Corp… Plánovač úloh Microsoft Corp… Plánovač úloh Microsoft Corp… Piánovač úloh Microsoft Corp… Šdilené složky Microsoft Corp… Sledování výkonu Microsoft Corp… Sledování výkonu Microsoft Corp… Sledování zabezpečen… Microsoft Corp…	odul snap-in Brána Windows Firew Certifikáty	Dodavatel Microsoft Corp	•		Certifikáty (místni)	Upravit rozšíření Odebrat
Plánovač úloh Microsoft Corp Prohlížeč událostí Microsoft Corp Rízení služby WMI Microsoft Corp Sdilené složky Microsoft Corp Sledování výkonu Microsoft Corp Sledování zabezbečen Microsoft Corp	Editor objektů zásad s Konfigurace a analýza Konfigurace klienta NAP Místní uživatelé a sku Odkaz na webovou a Ovládací prvek ActiveX	Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp		Přidat >		Na <u>h</u> oru Dgjů
Siedování zabezpečen… Microsoft Corp…	Plánovač úloh Prohlížeč událostí Řízení služby WMI Sdílené složky Sledování výkonu	Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp	-			Upřesnit
	i Siedovani zabezpečen	Microsoft Corp			1	

Poté Vám v levém menu přibude modul "Certifikáty (místní), kde po otevření složky "Požadavek na zápis certifikátu" uvidíte vygenerované privátní klíče – poté proveďte jeho export (tím provedete zálohu privátního klíče. Vygenerovaný PK se Vám zobrazí po vytvoření žádosti pomocí příkazu certreq, který je popsán níže)

👼 Konzola 1 - [Kořenový adresář konzoly\Certifikáty (místmi)\Požadavek na zápis certifikáty] 📃 📃								
Soubor Akce Zobrazit Oblibené položky Okno	Nápověda							_ 8 ×
Kořepový adrecíř konzoly	Vueteuree ere	Vueter del	Datum dan Janí	Zamóžiané óžak	Design's a fam.	Chau	Čabla	Alven
E Certifikáty (místní)	CEPTREO - Test	CEPTREO - Test	26.4.2012	Quěření cerveru	<zidovia< td=""><td>Juan</td><td>Jabic</td><td>ARCE</td></zidovia<>	Juan	Jabic	ARCE
🗑 🧮 Osobní	CEPTREO - Test	CERTREQ - Test	26.4.2013	Ověření serveru	<Žádný>			Certifikāty 🔺
Důvěryhodné kořenové certifikační autority	CEPTREO - Test	CERTREO - Test	3 5 2013	Ověření serveru	<Žádný >			Další akce
Důvěryhodnost v rámci rozlehlé sítě	CEPTREO - Test	CERTREQ - Test	3 5 2013	Ověření serveru	<Žádný >			
E Zprostředkující certifikační autority	tesedarfriwrtrthnt2k8r2.hrkica.local	tesedarfowrtrthot2k8r2.hrkica.local	13.4.2013	Ověření serveru	<Žádný>			
Důvěryhodní vydavatelé	tesedarfowrtrthot2k8r2 brkica local	tesedarfowrtrthot2k8r2 brkica local	26.4.2013	Ověření serveru	<Žádný >			
E Medůvěryhodné certifikáty	tesedarfgwrtrthot2k8r2.hrkica.local	tesedar fgwrtr thot 2k8r2, hrkica, local	26.4.2013	Ověření serveru	<Žádný>			
E Kořenové certifikační autority třetích stran	tesedarfgwrtrthgt2k8r2.hrkica.local	tesedarfowrtrthot2k8r2.hrkica.local	13.4.2013	Ověření serveru	<Žádný>			
Düveryhodne osoby	tesedarfgwrtrthot2k8r2.hrkica.local	tesedarfgwrtrthot2k8r2.hrkica.local	26.4.2013	Ověření serveru	<Žádný>			
Ostatni uzivatele	test2k8r2.hrkica.local	test2k8r2.hrkica.local	28.3.2013	Ověření serveru	<Žádný>			
	test2k8r2.hrkica.local	test2k8r2.hrkica.local	16.4.2013	Ověření serveru	<Žádný>			
Důvěrvhodné kořeny čipových karet	test2k8r2.hrkica.local	test2k8r2.hrkica.local	28.3.2013	Ověření serveru	<Žádný>			
Důvěryhodná zařízení	test2k8r2.hrkica.local	test2k8r2.hrkica.local	16.4.2013	Ověření serveru	<Žádný>			
	test2k8r2.hrkica.local	test2k8r2.hrkica.local	28.3.2013	Ověření serveru	<Žádný>			
	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							<u> </u>	1
Uložiště Požadavek na zápis certifikátu obsahuje 16 certifikátů	h.							J J



Postup získání komerčního serverového certifikátu I.CA pro IIS

(WS2008/Vista a výše)

Pro vytvoření žádosti o certifikát je možné použít nástroj *certreq* (který je přítomen na každé instanci Windows Server) podle následujícího

postupu:

1. Vytvořte textový soubor se šablonou pro vygenerování žádosti o certifikát - např. *IISreq.inf* - podle následujícího 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 KeyLength upravte v souladu komentářem na identifikaci Vašeho serveru a na potřebnou délku klíče. (Středníkem jsou uvozené komentáře.)

2. Vytvořte žádost o certifikát na cílovém serveru. POZOR! musí být provedeno přímo na IIS serveru, protože při vytváření žádosti je

generován nový pár klíčů.

IISsrv>

certreq -new IISreq.inf IISreq.txt

Vytvořená žádost bude uložena v souboru *IISreq.txt*, který je možné zobrazit a kopírovat jako text (jde o base64 zakódovaná binární

data).

3. Obsah žádosti předložte obvyklým způsobem na I.CA. Na <u>www.ica.cz</u> proveďte vložení obsahu žádosti do formuláře pro komerční

serverový certifikát I.CA, doplnění hesla pro zneplatnění atd., vytvoření žádosti o serverový certifikát. Dále proveďte předání žádosti na

RA.

4. Po získání certifikátu na IIS serveru (na kterém jste vytvářeli žádost) proveďte instalaci certifikátu (ve formátu DER) pomocí příkazu:

IISsrv>



certreq -accept <nnnnn.der>

kde *<nnnn.der>* je název souboru se získaným certifikátem ve formátu der.

Poznámka:

Kořenový certifikát vydávající komerční I.CA musí být v trusted root v úložišti počítače, jinak příkaz *cetreq -accept* ohlásí chybu a

certifikát nenainstaluje (a nespojí jej s vygenerovaným soukromým klíčem).

5. Nyní v IIS nakonfigurujte/zvolte pro SSL zabezpečení zvoleného website nově instalovaný certifikát, a ověřte správnost funkce při

přístupu klienta na webový server.

Závěrečné poznámky:

1. Použitím uvedené šablony je vygenerována žádost o certifikát bez položek sMIMECapabilities a subjectKeyIdentifier.

- 2. Uvedený vzor šablony předpokládá:
- uložení klíčů v operačním systému,
- standalone Web server,
- nelze ji použít pro WS2003.