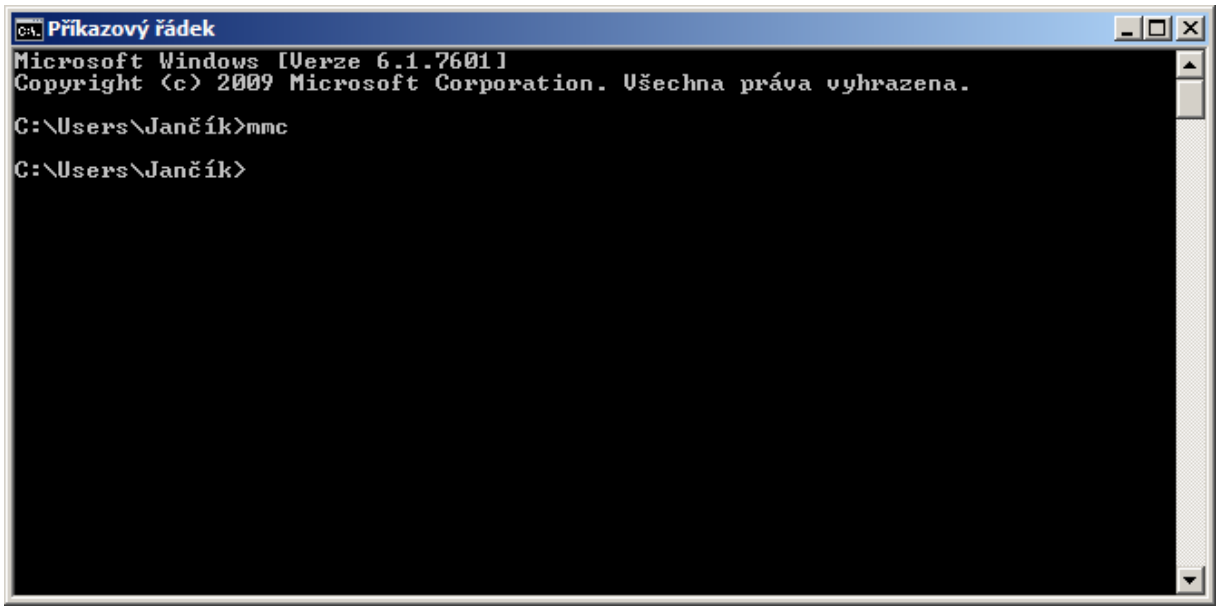
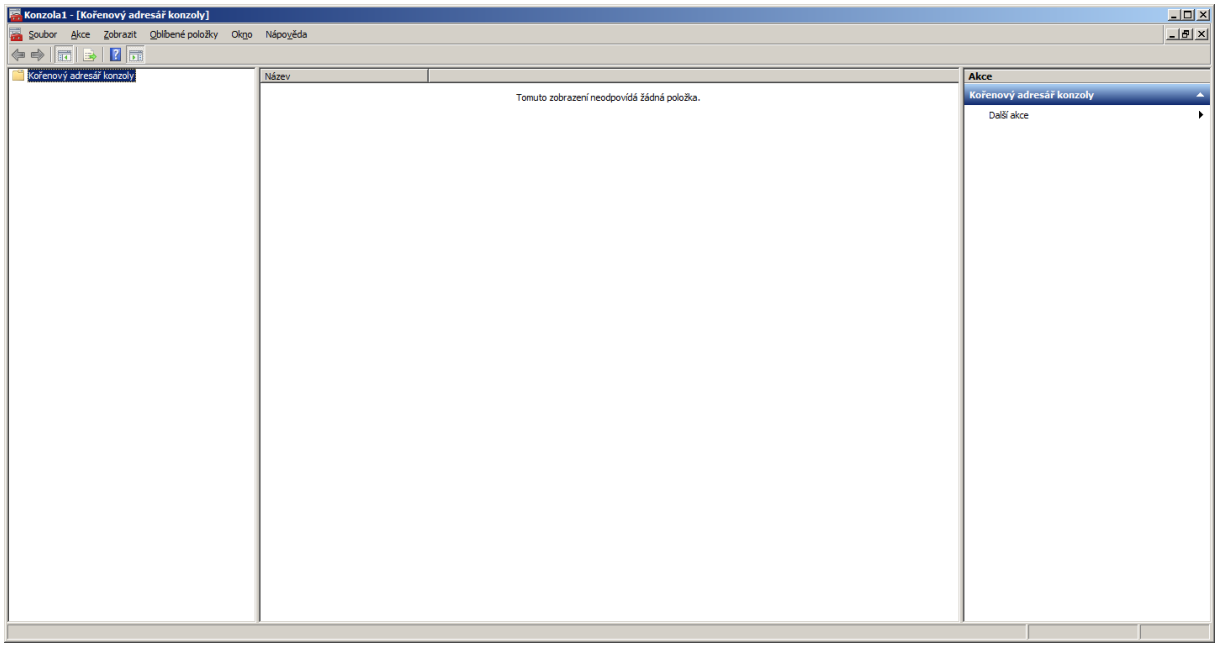
Vytvoření žádosti o certifikát
na Windows Serveru 2008/Vista a vyšší
a zobrazení MMC konzole pro zálohu privátního klíče

Nejprve je potřeba přidat modul snap-in do konzole mmc

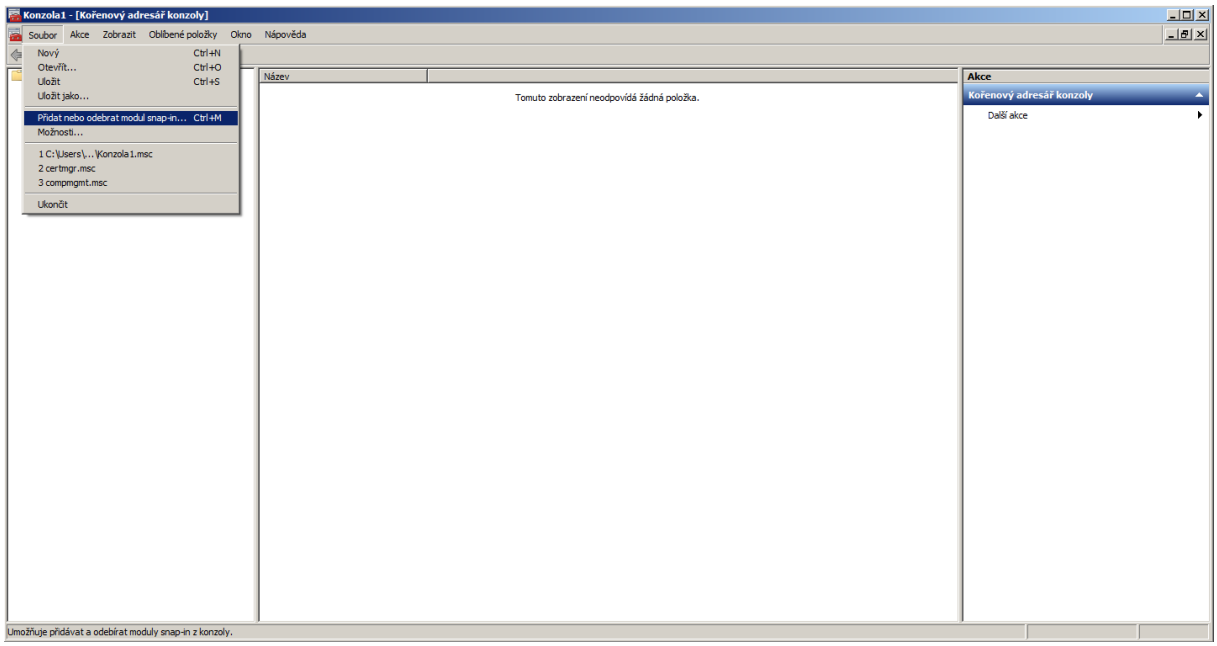
V příkazové řádce napište „**mmc**“ a stiskněte Enter



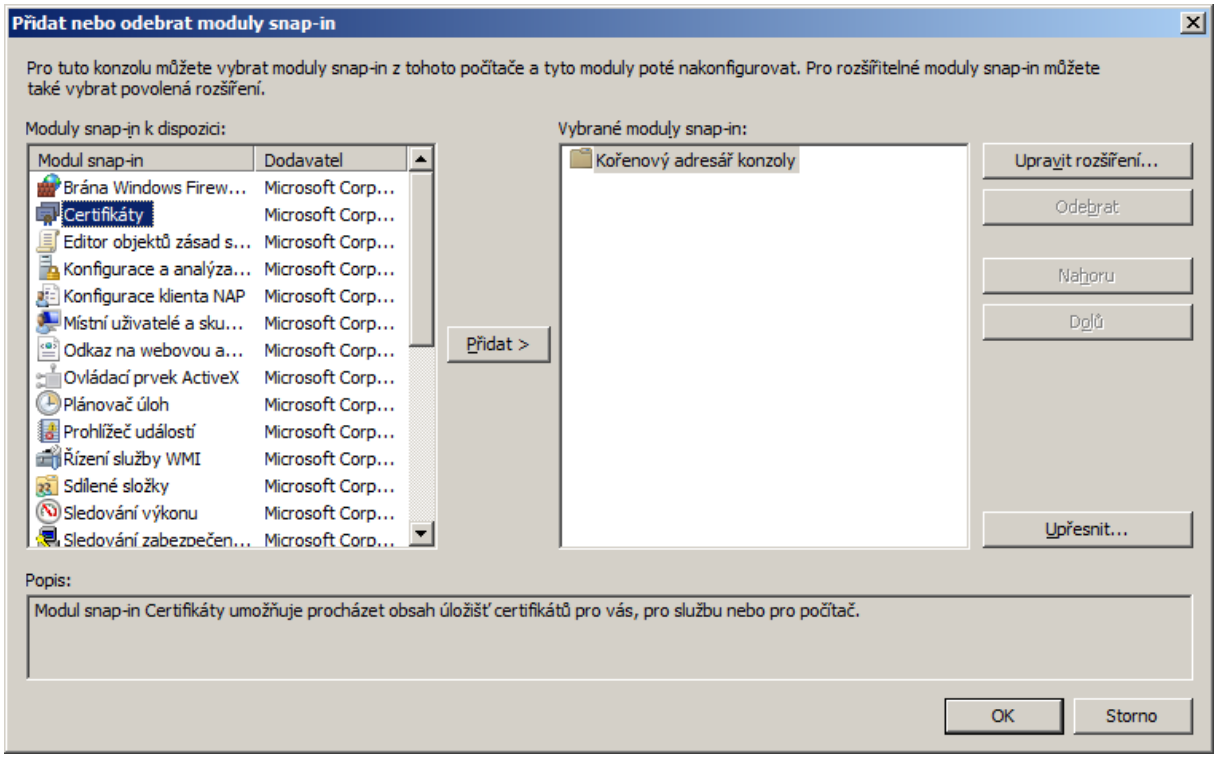
Níže vidíte prázdnou konzoli mmc



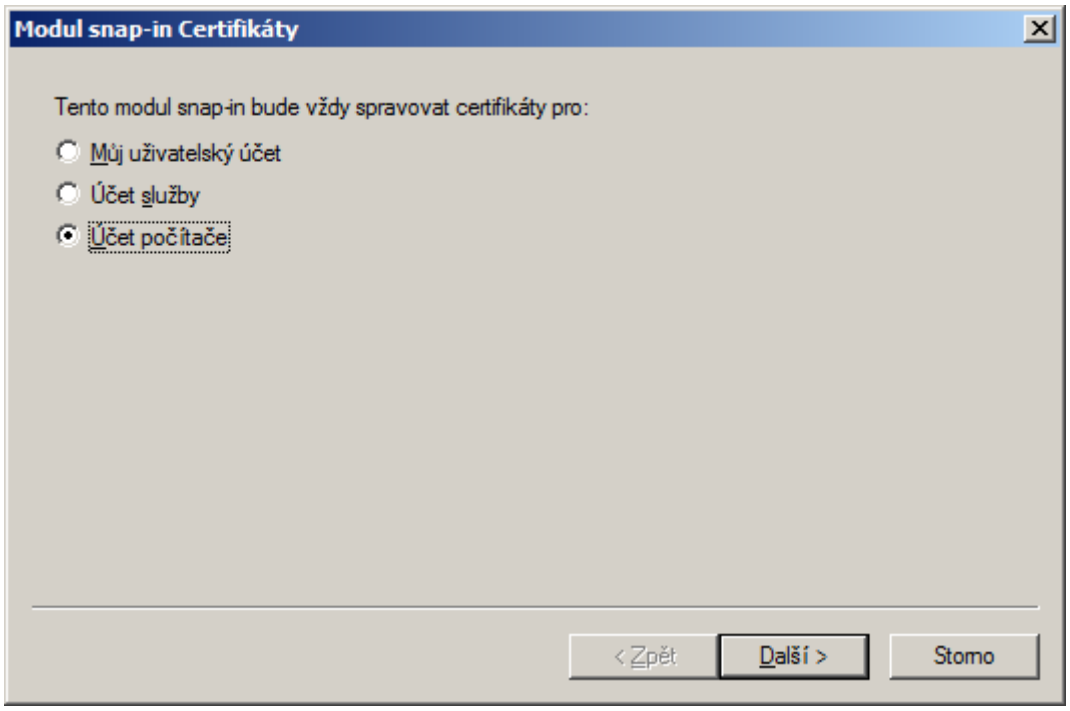
Zvolte „Soubor“ a „Přidat nebo odebrat modul snap-in“



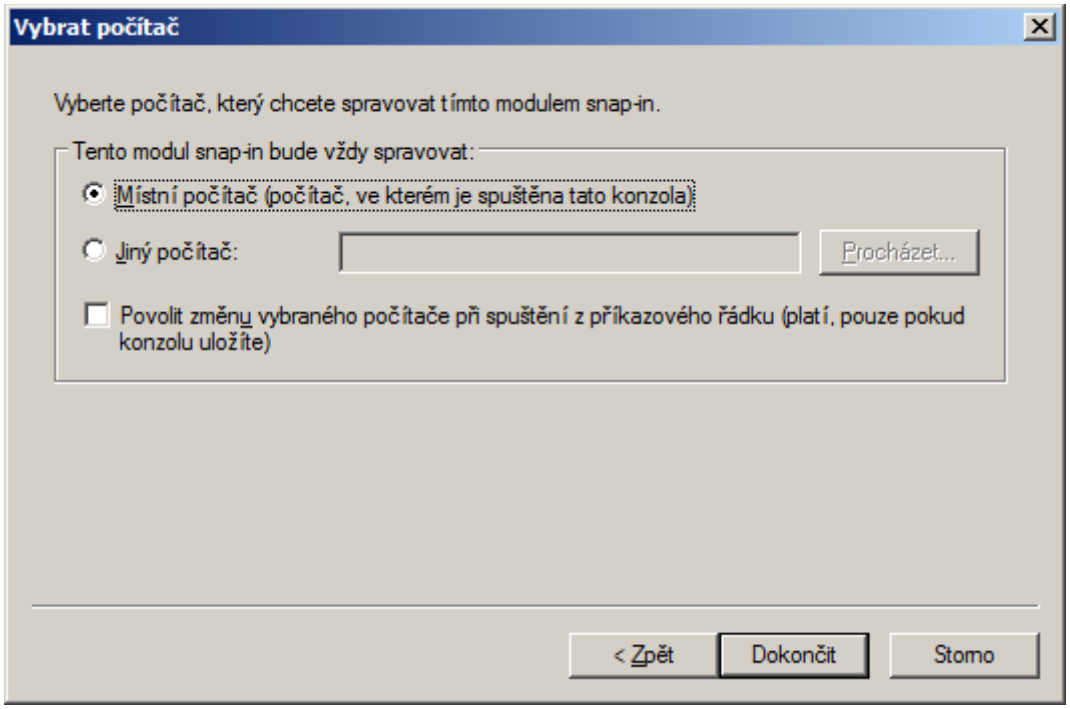
Přidejte modul „Certifikáty“



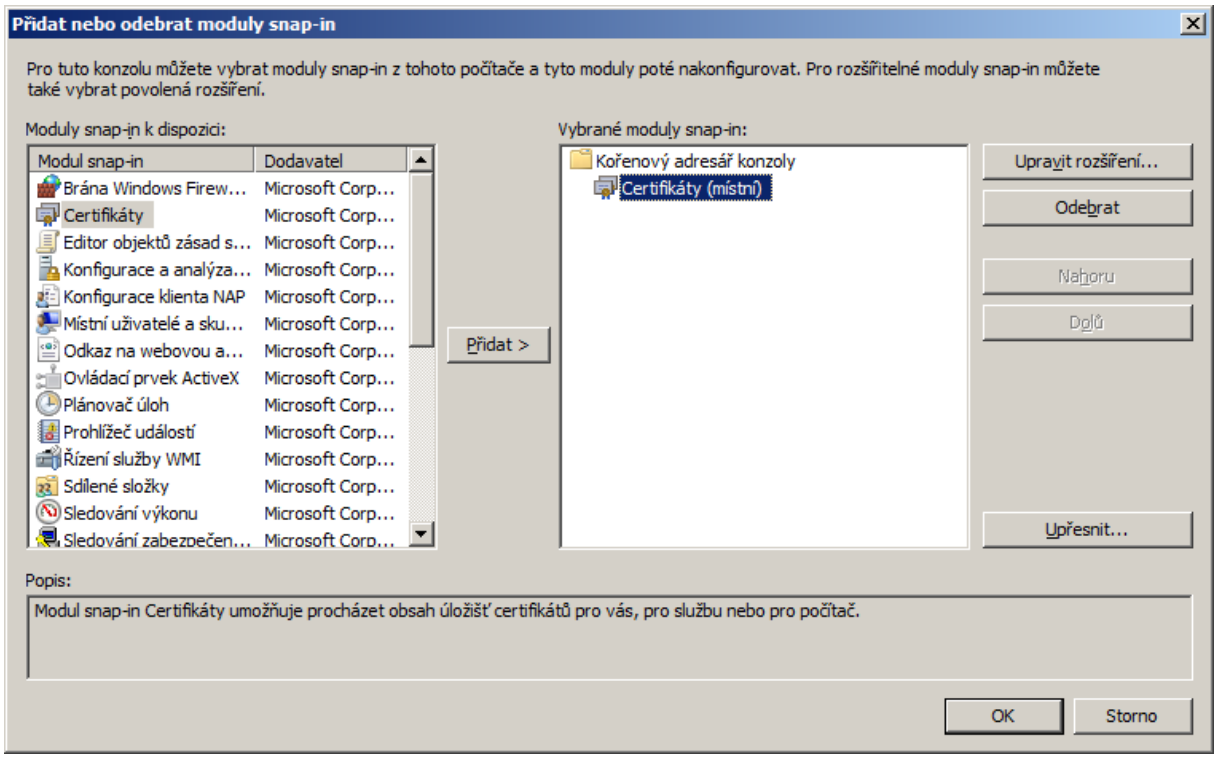
Vyberte „Účet počítače“



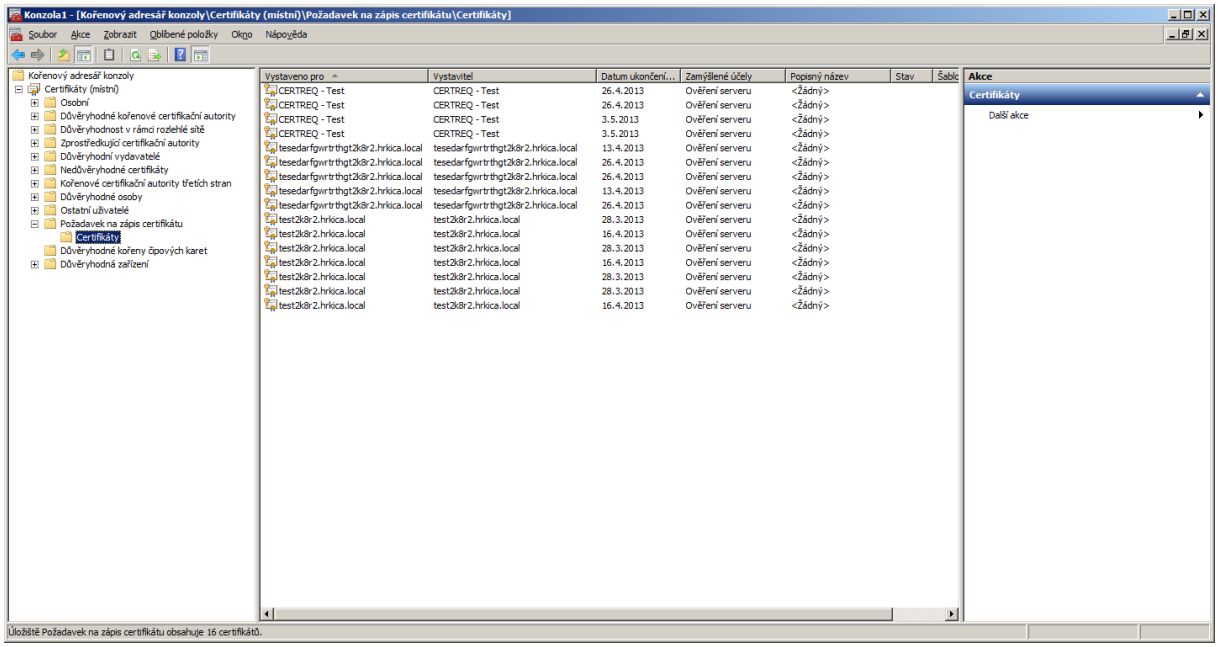
Zvolte „Místní počítač“



Níže už vidíte úspěšně přidaný modul snap-in



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)



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. www.ica.cz) 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 www.ica.cz 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 <*nnnnn.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.