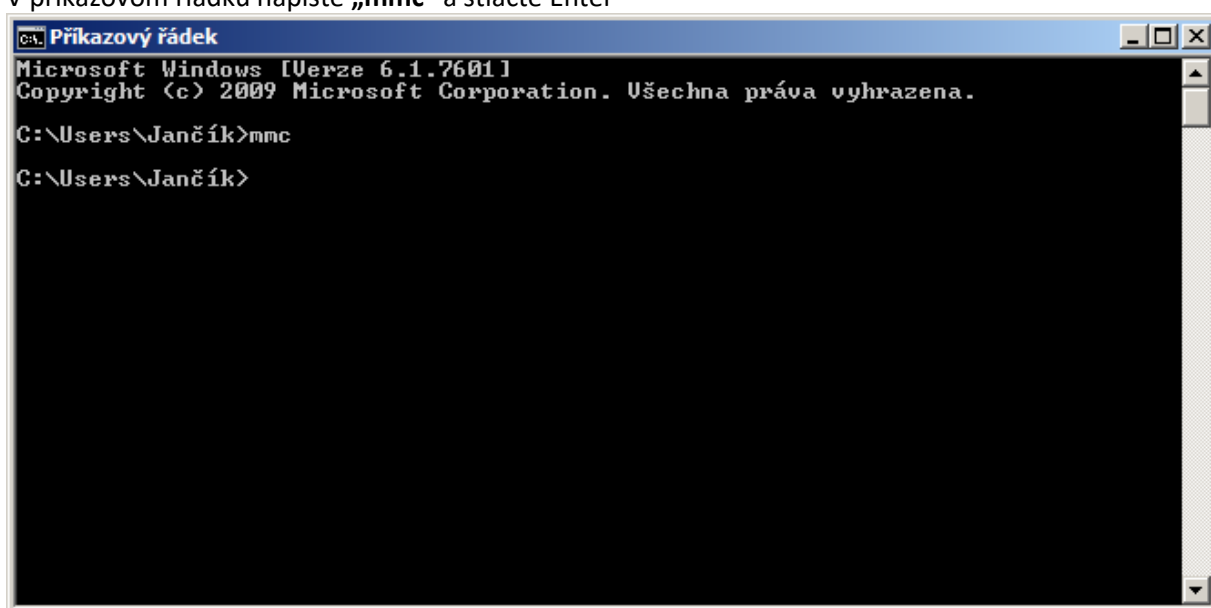


Vytvorenie žiadosti o certifikát na Windows Serveru 2008/Vista a vyššie a zobrazenie MMC konzoly pre zálohu privátneho kľúča

Najprv je potreba pridať modul snap-in do konzoly mmc

V príkazovom riadku napíšete „mmc“ a stlačíte Enter

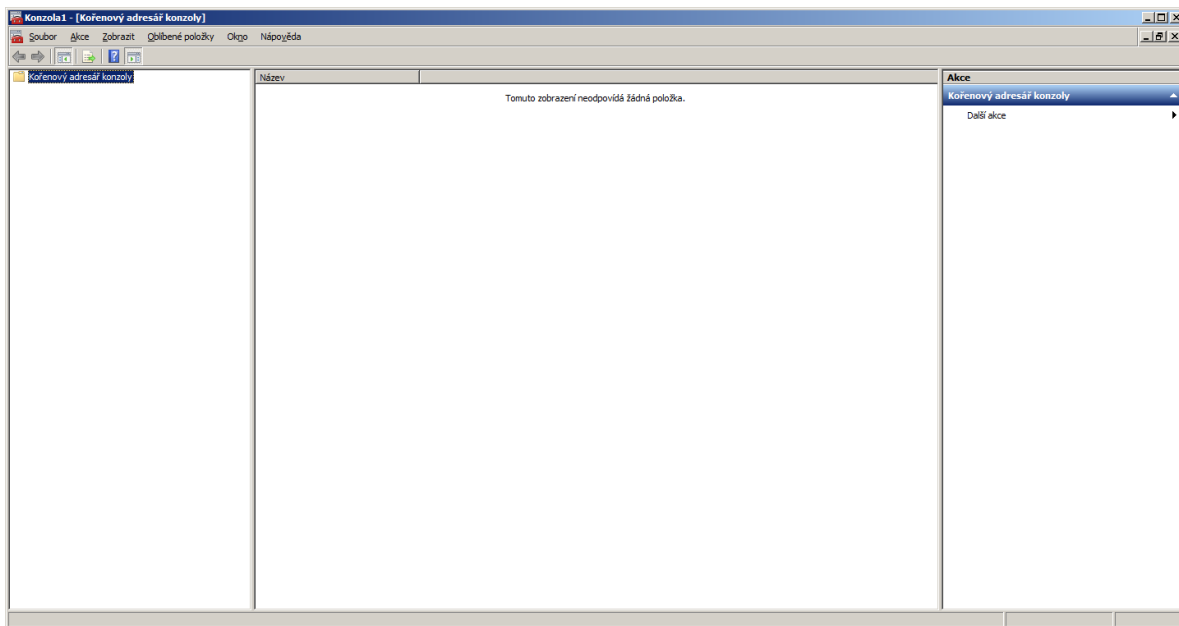


```

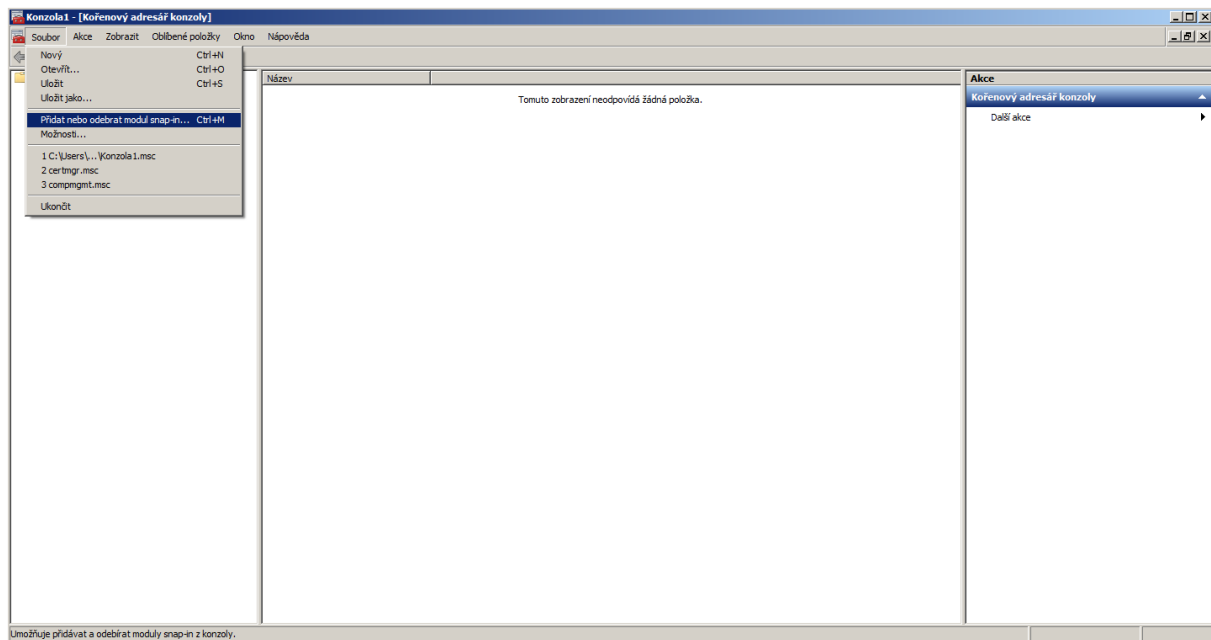
C:\> Příkladový řádek
Microsoft Windows [Verze 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Všechna práva vyhrazena.

C:\Users\Jančík>mmc
C:\Users\Jančík>
  
```

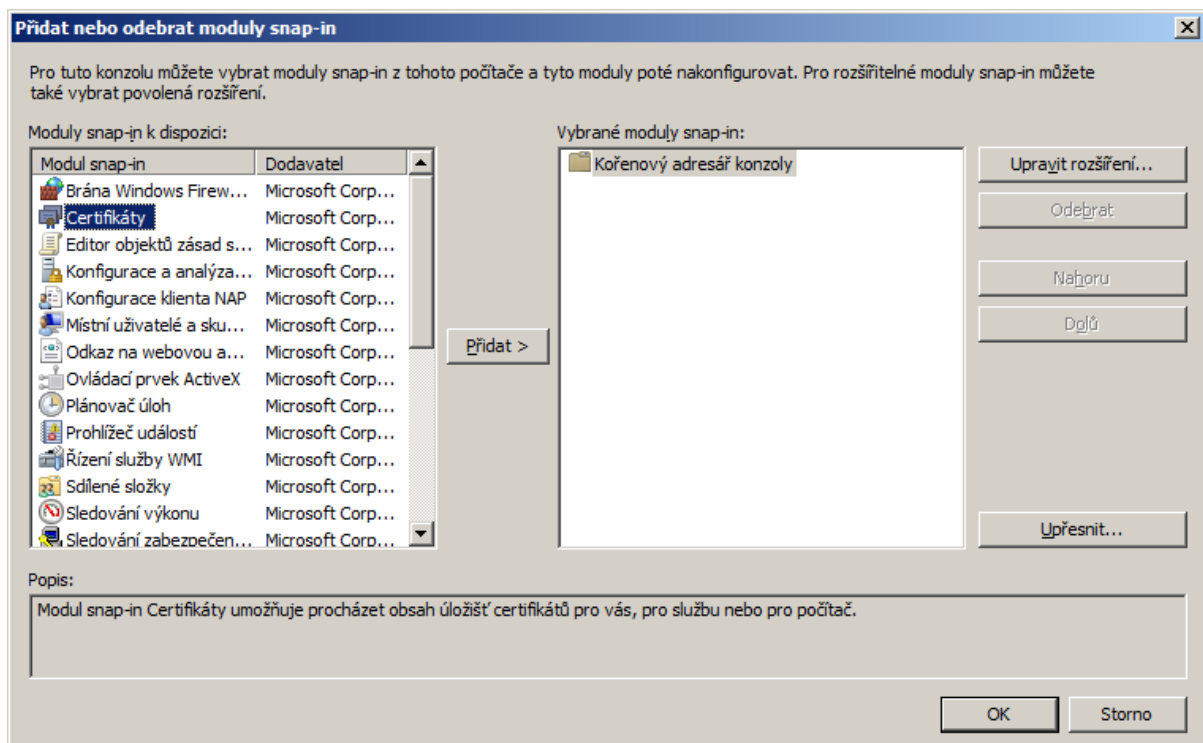
Nižšie vidíte prázdnu konzolu mmc



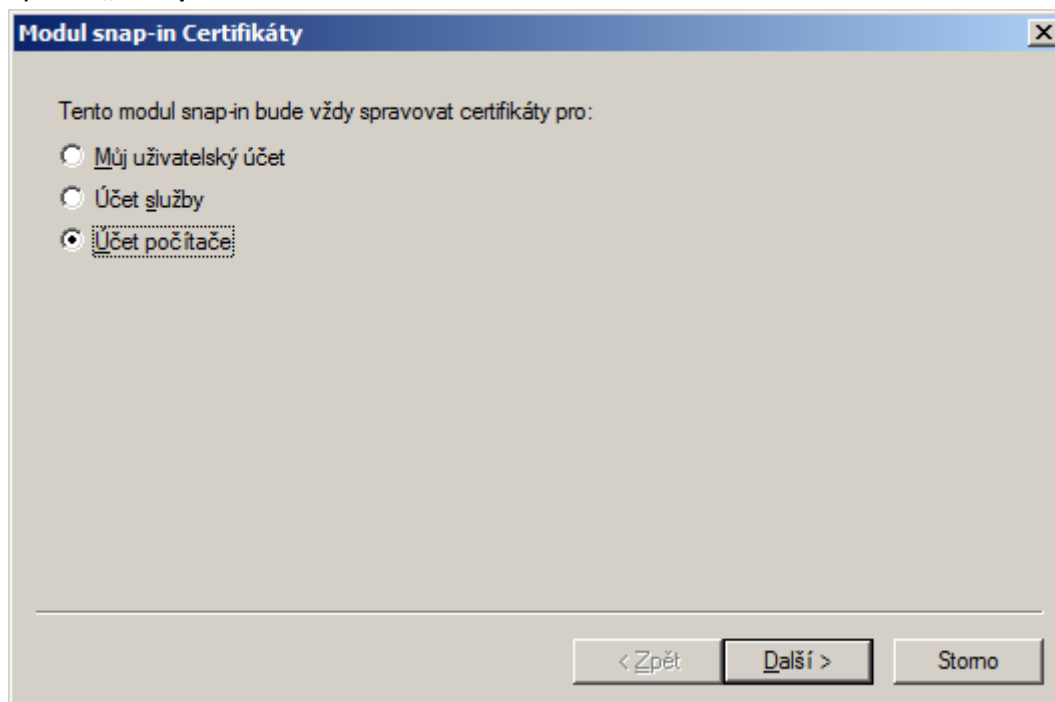
Zvolte „Súbor“ a „Pridať alebo odebrať modul snap-in“



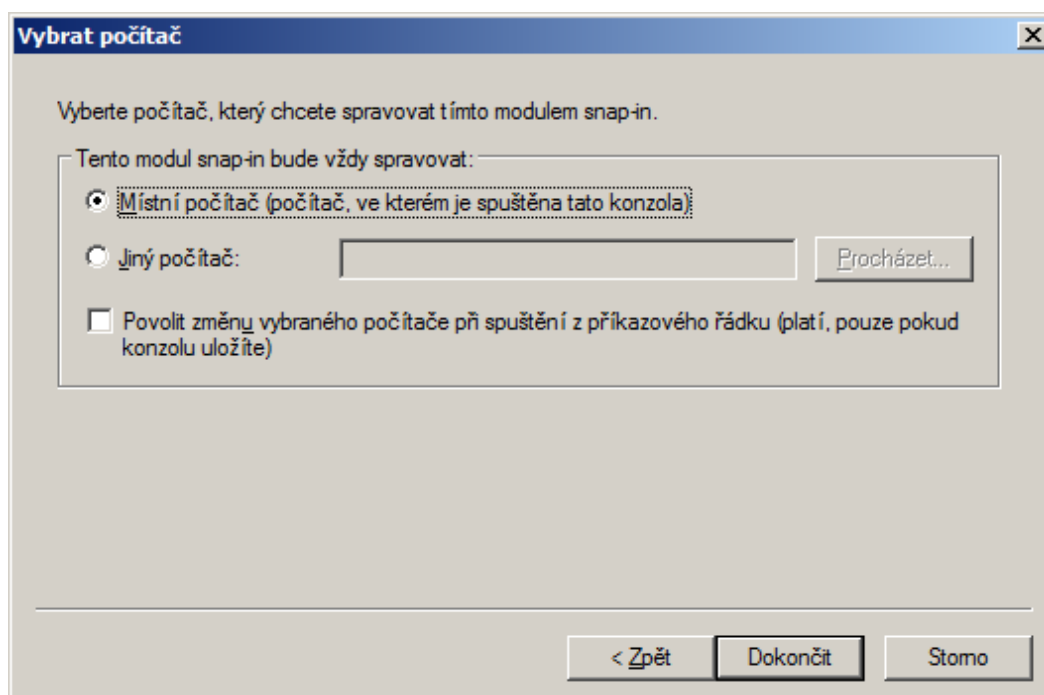
Pridajte modul „Certifikáty“



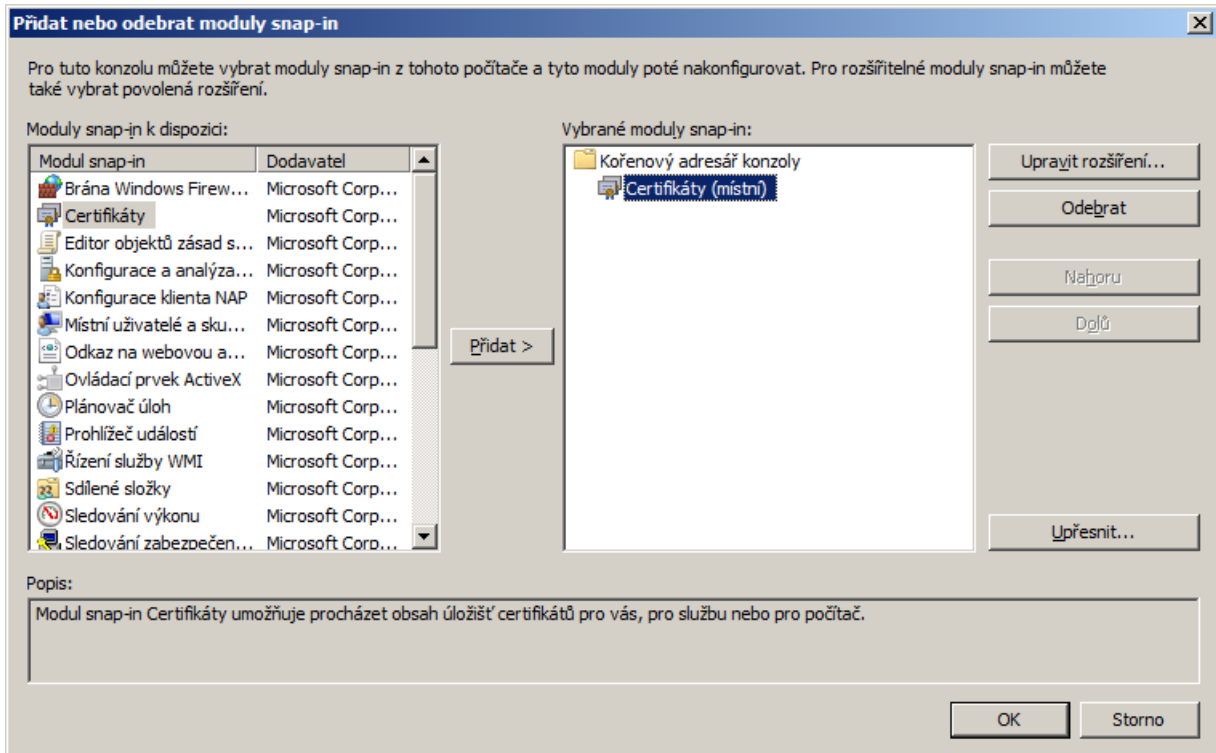
Vyberte „Účet počítača“



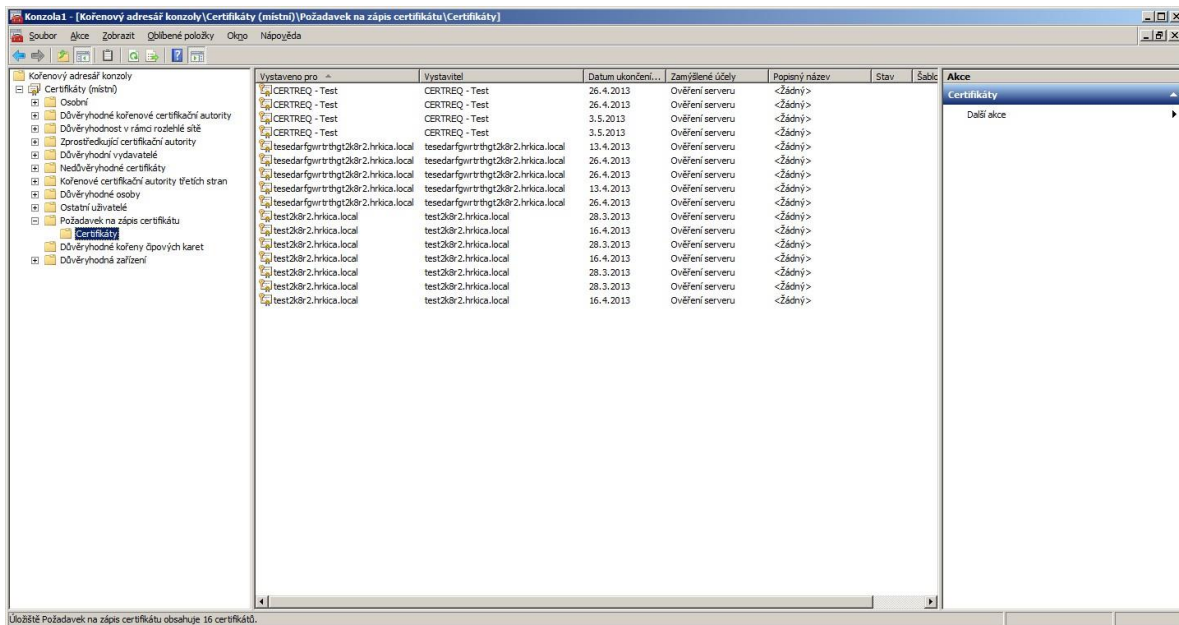
Zvolte „Miestny počítač“



Nižšie už vidíte úspešne pridaný modul snap-in



Potom vám v ľavom menu pribudne modul „**Certifikáty (místne)**“, 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)



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 podľa údajov Vášho serveru, položka CN nesmie obsahovať doménové meno, FQDN, (napr. www.ica.cz) a IP adresu (napr. 193.86.0.248)

; vyplnený musí byť aspoň položky C a CN, ostatní v súlade s certifikacnými politikami

; pole: CN =Common Name (názov serveru)

; O =Organization (organizácia, firma)

; OU =Organization Unit (organizácia jednotka)

; L =Locality (lokality, mesto)

; C =Country (zeme, štát)

; 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 Client Authentication
```

Položky Subject a KeyLength 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.**

```
IISrv>
```

```
certreq -new IISreq.inf IISreq.txt
```

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

3. Obsah žiadosti predložte obvyklým spôsobom na I.CA. Na www.ica.cz 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::

```
IISrv>
```

certreq -accept <nnnnn.der>

kde **<nnnnn.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 použiť pro WS2003.