Postup získání komerčního serverového certifikátu I.CA pro Internet Information Server (Windows Server 2008 / Vista a vyšší)

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=test2k8r2.hrkica.local,O=ICA,OU=testing,C=CZ,L=Hradec Kralove,St=Kralovahradecky kraj"
; Subject opravit podle udaju serveru, pro ktery je generovana zadost
; v CN musi byt FQDN serveru jinak bude pristupujicim klimentum hlasen nesouhlas mezi jmenem SRV a udaji v certifikatu
; vyplneny musi byt alespon polozky C a CN, dalsi v souladu s certifikacni politikou
; pole: CN =Common Name (jmeno, FQDN jmeno 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 ;opravit na pozadovanou delku klice
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=1.3.6.1.5.5.7.3.1 ;pro Server Authentication
```

Položky Subject a KeyLength upravte v souladu s 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 ***název.req***, který je možné zobrazit a kopírovat jako text (jedná se o base64 zakódovaná binární data).

3. Obsah žádosti vložte do online formuláře pro tvorbu žádosti o komerční serverový certifikát (více na https://www.ica.cz/Ziskat-komercni-serverovy-certifikat), doplňte zbývající povinné údaje (např. heslo pro zneplatnění…), a vytvořte žádost o certifikát.

   S takto vytvořenou žádostí a dokumenty pro vydání certifikátu se dostavte na Registrační autoritu I.CA, kde Vám obratem certifikát vydají.

4. Instalaci certifikátu na IIS serveru (na kterém jste tvořili žádost) proveďte (ve formátu DER) prostřednictvím příkazu:

   IISsrv>
   certreq -accept <nnnnn.der>

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

   Poznámka: Kořenový certifikát pro oblast komerčních certifikátů I.CA musí být v trusted root v úložišti počítače, jinak příkaz *cetreq -accept* ohlásí chybu. Certifikát by se nenainstaloval – nedojde k párování se 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:

- Použitím uvedené šablony je vygenerována žádost o certifikát bez položek sMIMECapabilities a subjectKeyIdentifier.
- Uvedený vzor šablony předpokládá: uložení klíčů v operačním systému, standalone Web server
- Výše uvedený postup nelze použít pro Windows Server 2003.