



Postup pro generování asymetrického klíčového páru

Historie verzí

Datum	Verze	Popis	Zpracoval
30.10.2011	1.0	Vytvořen dokument	AC/SZR
30.1.2012	2.0	Upraveno pro testovací provoz	SZR



Obsah:

1.1	OpenSSL	3
1.2	Postup v OS Windows.....	3
1.3	Příprava konfiguračního souboru pro vygenerování klíčového páru.....	3
1.4	Generování klíčového páru	5
1.5	Vytvoření souboru k žádosti o připojení.....	5
1.6	Instalace certifikátu	6



1.1 OpenSSL

Program OpenSSL je freeware a je možné jej použít ve více druzích operačních systémů, například:

OPENSSL pro Windows

OPENSSL pro Linux

1.2 Postup v OS Windows

Program je součástí balíčku, který si můžete stáhnout ze stránek SZR

<http://www.szrcr.cz/vyvojari>

- pro 32 bitové Windows: **openssl-0.9.8e_WIN32.zip**
- pro 64 bitové Windows: **openssl-0.9.8e_X64.zip**

Pracovat s OpenSSL budete v příkazové řádce.

Příkazovou řádku spustíte příkazem **cmd.exe**. Pro práci s programem se přepněte do adresáře, ve kterém jste umístili stažený soubor a jeho podadresáře bin. (**Příkazem cd \adresar\bin**).

Základní postup

- Připravíte si konfigurační soubor **certreq.config**, který použijete při generování asymetrického klíčového páru (pro váš server).
- Vygenerujete klíčový pár, z něhož veřejnou část připojíte jako přílohu k tiskopisu „Žádost o umožnění přístupu orgánu veřejné moci ke službám vnějšího rozhraní ISZR“.
- Žádost s přílohou zašlete do datové schránky certifikační autority - Správy základních registrů (ID **jjqjqi**),
- Certifikační autorita vám zašle zpět do vaší datové stránky certifikát.
- Certifikát nainstalujete na svůj server. Na serveru musí být společně certifikát (v něm je veřejný klíč) i váš privátní klíč.

1.3 Příprava konfiguračního souboru pro vygenerování klíčového páru

Konfigurační soubor vytvoříte pomocí editoru, např. Notepad.

Na webu SZR je připravený soubor **CertServer.txt pro server**, který upravíte pro vaši potřebu a pojmenujete ho **certreq.config**.

Obsah většiny položek konfiguračního souboru je přednastaven a při jeho vyplňování změníte obsah jenom těch položek, které jsou zde zvýrazněny červeně.

distinguished_name	= req_distinguished_name
string_mask	= nombstr
prompt	= no
[req_distinguished_name]	
0.commonName	= ServerName
0.organizationName	= ICO
organizationalUnitName	= AIS
localityName	= Obec= NAZEV1 , Ulice= NAZEV2 , PSC= PSC
stateOrProvinceName	= NAZEV3
countryName	= CZ

Do jednotlivých (červeně zvýrazněných) položek OVM uvede:



ServerName	Plně kvalifikované DNS jméno serveru, maximální délka 64 znaků, např. server01.vaseovm.cz
IČO	IČO OVM (bez mezer), délka maximálně 8 číslic, lze včetně nul na začátku i bez nich, např. 00345678 nebo 345678.
AIS	zkrácený název AISu (bez diakritiky) doplněný o informaci, zda jde o publikační (-P) nebo editační (-E) AIS a zda jde o testovací (/TEST) nebo produkční (/PROD) prostředí, maximální délka 64 znaků, např.: AIS123-E/TEST AIS123-P/TEST AIS123-E/PROD AIS123-P/PROD
NAZEV1	Jméno obce (bez diakritiky), např. Hradec Kralove
NAZEV2	Jméno ulice (bez diakritiky), např. Milady Horakove
PSC	PSČ (bez mezer), např. 11025 Celková maximální délka adresy, tj. znakového řetězce „Obec= NAZEV1 ,Ulice= NAZEV2 ,PSC= PSC “ je 128 znaků
NAZEV3	Název OVM (bez diakritiky), maximální délka 128 znaků, např. Sprava zakladnich registru

Nejdůležitější položky jsou:

- 0.organizationName: musí přesně odpovídat IČO organizace, kterou jste uvedli na žádosti
- 0.CommonName: plně kvalifikované DNS jméno serveru, na které bude certifikát vystaven.

Dobře si vše překontrolujte!

Pokud uděláte překlep, certifikát nebude funkční a budete muset o něj žádat znovu.

Příklady:

```
certreq.config - Poznámkový blok
Soubor Úpravy Formát Zobrazení Nápověda
distinguished_name = req_distinguished_name
string_mask = nombstr
prompt = no

[req_distinguished_name]
0.commonName = server01.vaseovm.cz
0.organizationName = 12345678
organizationalUnitName = AIS123-P/TEST
countryName = CZ
localityName = Obec=Praha,Ulice=Milady Horakove,PSC=12345
stateOrProvinceName = Sprava ZR
```



```
certreq.config - Poznámkový blok
Soubor Úpravy Formát Zobrazení Nápověda
distinguished_name = req_distinguished_name
string_mask = nombstr
prompt = no

[req_distinguished_name]
0.commonName = server01.vaseovm.cz
0.organizationName = 12345678
organizationalUnitName = AIS123-E/PROD
countryName = CZ
localityName = Obec=Praha,Ulice=Milady Horakove,PSC=12345
stateOrProvinceName = Sprava ZR
```

Konfigurační soubor uložte v adresáři programu OpenSSL do adresáře \bin pod názvem certreq.config.

Název	Velikost	Typ
libeay32.dll	1 004 kB	Rozšíření aplikace
openssl	288 kB	Aplikace
ssleay32.dll	196 kB	Rozšíření aplikace
CertServer	1 kB	Textový dokument
certreq.config	1 kB	Soubor CONFIG

1.4 Generování klíčového páru

V adresáři programu OpenSSL \bin provedeme příkaz:

openssl genrsa -des3 -out Privatekey.key 1024

```
Správce: Příkazový řádek
D:\OpenSSL\bin>openssl genrsa -des3 -out Privatekey.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)
Enter pass phrase for Privatekey.key:
Verifying - Enter pass phrase for Privatekey.key:
D:\OpenSSL\bin>
```

Po spuštění příkazu budete vyzváni k vytvoření hesla a k jeho následnému ověření. Po příkazu dojde ke generování souboru **Privatekey.key**, který obsahuje privátní klíč chráněný heslem, který jste si při generování zadali.

1.5 Vytvoření souboru k žádosti o připojení

Zadejte následující příkaz pro vygenerování vašeho certifikátu:

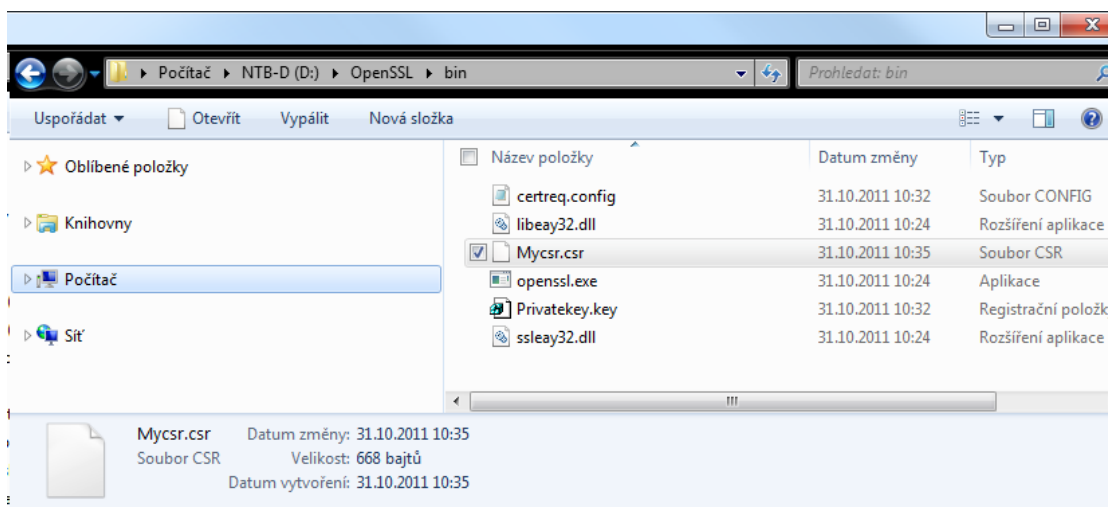
openssl req -new -key Privatekey.key -out Mycsr.csr -config certreq.config



```
Správce: Příkazový řádek
D:\OpenSSL\bin>openssl req -new -key Privatekey.key -out Mycsr.csr -config certreq.conf
Enter pass phrase for Privatekey.key:
Loading 'screen' into random state - done
D:\OpenSSL\bin>
```

Po zadání příkazu budete dotázáni na vaše heslo.

Výsledkem je soubor Mycsr.csr obsahující váš certifikát (veřejná část klíčového páru).



Zkopírujte soubor **Mycsr.csr** do souboru **Mycsr_XXXXXXXX.txt** (XXXXXXXX je IČO) a pošlete ho v příloze „Žádosti o umožnění přístupu orgánu veřejné moci ke službám vnějšího rozhraní ISZR“ na certifikační autoritu (SZR) k podpisu a ke schválení vašeho certifikátu.

Pokud bude schválení úspěšné, obdržíte od certifikační autority do datové schránky podepsaný certifikát v souboru **Mycsr_XXXXXXXX.cer.txt**. Zkopírujte ho (tj. přejmenujte) do souboru **certnew.cer**.

1.6 Instalace certifikátu

Proces musíte dokončit spojením certifikátu s privátním klíčem.

Schválený soubor s certifikátem z certifikační autority vložíte do podadresáře \bin v OpenSSL adresáři a spojíte privátní klíč s certifikovaným veřejným klíčem. Toto provedete spuštěním příkazu v podadresáři \bin:

openssl pkcs12 -export -in certnew.cer -inkey privatekey.key -out mykey.pfx

```
D:\OpenSSL\bin>openssl pkcs12 -export -in certnew.cer -inkey privatekey.key -out mykey.pfx
Loading 'screen' into random state - done
Enter pass phrase for privatekey.key:
Enter Export Password:
Verifying - Enter Export Password:
D:\OpenSSL\bin>
```



Po spuštění příkazu budete dotázáni na heslo, které jste zadali při generování žádosti (certifikátu) a na jeho ověření. Pak zadáte heslo k privátní části klíče a heslo pro exportovaný klíč.

Tím bude proces generování certifikátu dokončen.

Výsledkem je certifikát v souboru **mykey.pfx**.

Upozornění: Příkazy v tomto dokumentu nekopírujte, ale přepisujte do příkazové řádky. Některé typy Windows nemusí být schopny toto překopírování správně interpretovat a program OpenSSL pak hlásí chybu příkazu.

Svůj certifikát uchovávejte na zvlášť bezpečném místě, které zajistí jeho maximální ochranu před zneužitím.