SPRÁVA ZÁKLADNÍCH REGISTRŮ

Postup pro vytvoření žádosti o digitální certifikát pro produkční prostředí Základních registrů

Verze dokumentu:	1.6
Datum vydání:	19. září 2012
Klasifikace:	Veřejný dokument

SPRÁVA ZÁKLADNÍCH REGISTRŮ

Obsah

1. Žádost o certifikát

Certifikáty vydávané Certifikační autoritou SZR slouží k identifikaci a autentizaci AIS vůči Informačnímu systému základních registrů. Používá se ve dvou situacích:

- AIS navazuje spojení s ISZR.
- ISZR navazuje spojení s AIS při odpovědi na asynchronní dotaz v aktivním režimu.

V obou případech je možné použít stejný certifikát.

Vydávání certifikátů Certifikační autoritou SZR se řídí Certifikační politikou SZR. Žádost o certifikát podává OVM pro konkrétní AIS. Podáním žádosti o certifikát se OVM zavazuje dodržovat podmínky Certifikační politiky SZR a Bezpečnostní požadavky na AIS pro připojení k produkčnímu prostředí Základních registrů. Oba dokumenty jsou dostupné na webu SZR.

Pro generování dvojice klíčů a žádosti o certifikát doporučujeme používat freeware OpenSSL. Tento software je dostupný pro více operačních systémů, mj. pro MS Windows a Linux.

Žádost o certifikát musí být ve formátu PKCS#10. Typ klíče musí být RSA a minimální délka klíče je 2048 bitů.

2. Postup s OpenSSL v OS Windows

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

http://www.szrcr.cz/vyvojari/spravci

- 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 spusťte příkazem **cmd.exe**. Pro práci s programem se přepněte do adresáře, kam jste nakopírovali výše stažený soubor, a jeho podadresáře bin příkazem **cd \adresar\bin**

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

Základní postup:

- Připravíte si konfigurační soubor certreq.config, který použijete při generování asymetrického klíčového páru (pro váš server).
- Vygenerujete klíčový pár, jehož veřejnou část připojíte jako přílohu k formuláři „Žádost o umožnění přístupu orgánu veřejné moci ke službám vnějšího rozhraní ISZR“.
- Žádost s přílohou zašlete do datové schránky Správy základních registrů (ID **jjqjqih**),
- Certifikační autorita SZR vaši žádost zkontroluje. Pokud je vše v žádosti i ve formuláři správně, vygeneruje certifikát. Pokud je tam chyba, vrátí vám SZR žádost zpět.
- SZR 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.

2.1 Příprava konfiguračního souboru pro vygenerování klíčového páru

Konfigurační soubor vytvoříte pomocí editoru, např. Notepad.
Na webu SZR je připravený soubor **CertServer.txt**, 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=PSČ
stateOrProvinceName = NAZEV3
countryName = CZ
```

Požadovaný obsah jednotlivých položek je definován Certifikační politikou SZR.

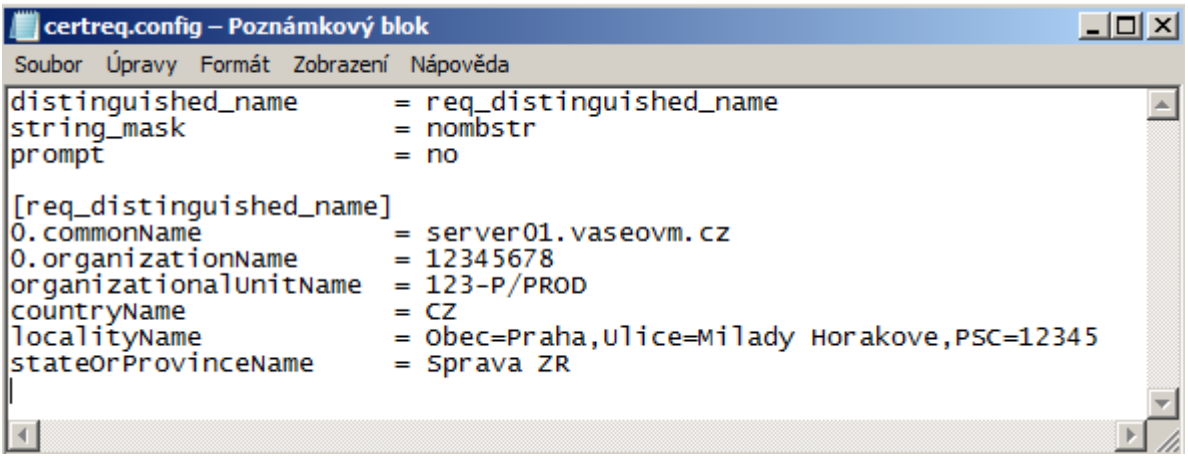
Do jednotlivých (červeně zvýrazněných) položek uvedete:

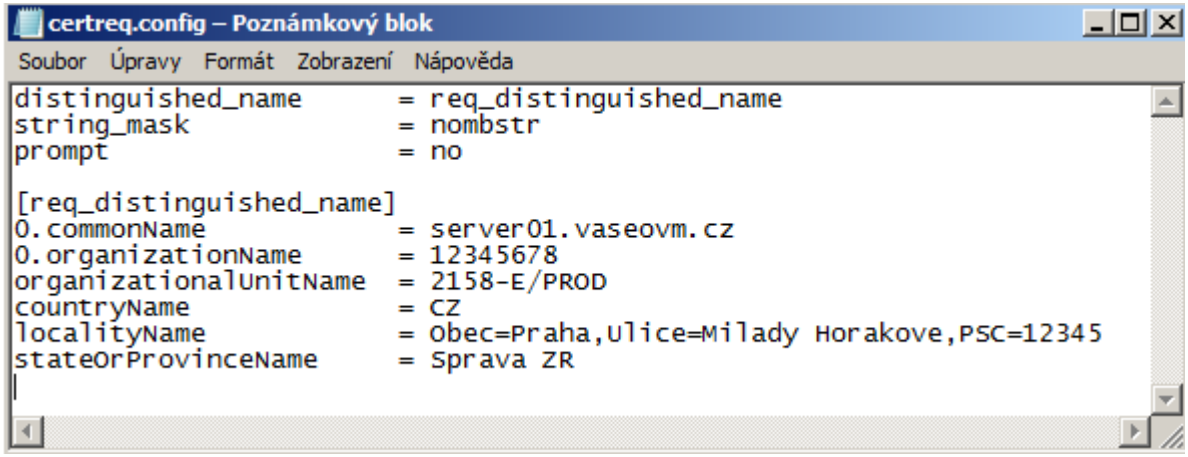
ServerName	Doporučujeme uvádět DNS jméno počítače, který bude přijímat zpětná volání v případě, kdy ISZR vrací odpověď na asynchronní dotaz v aktivním režimu. Pokud bude spojení navazováno v KIVS, mělo by jít o jméno, pod kterým je počítač dosažitelný v síti KIVS. Pokud bude spojení navazováno v Internetu, pak by mělo jít o veřejné DNS jméno. Pokud AIS asynchronní volání v aktivním režimu nebude používat, doporučujeme uvádět DNS jméno AISu v KIVS, respektive v Internetu. Maximální délka 64 znaků, např. server.vaseovm.cz nebo server.vaseovm.cms
IČO	IČO OVM (**bez mezer**), délka maximálně 8 číslic, lze včetně nul na začátku i bez nich, např. 00345678 nebo 345678.
AIS	identifikace (číslo) AIS v ISoISVS, doporučujeme doplnit o informaci, zda jde o publikační (-P) nebo editační (-E) AIS a že jde o produkční (/PROD) prostředí, maximální délka 64 znaků, např.: 123-E/PROD 567-P/PROD
NAZEV1	Jméno obce (**bez diakritiky**), např. Hradec Kralove
NAZEV2	Jméno ulice (**bez diakritiky**), např. Milady Horakove
PSČ	PSČ (bez mezer), např. 11025 Celková maximální délka adresy, tj. znakového řetězce „Obec=NAZEV1,Ulice=NAZEV2,PSC=PSČ“ 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 OVM, které jste uvedli na formuláři
organizationalUnitName: musí přesně odpovídat číslu AIS, které jste uvedli na formuláři

Dobře si vše překontrolujte!

Příklady:





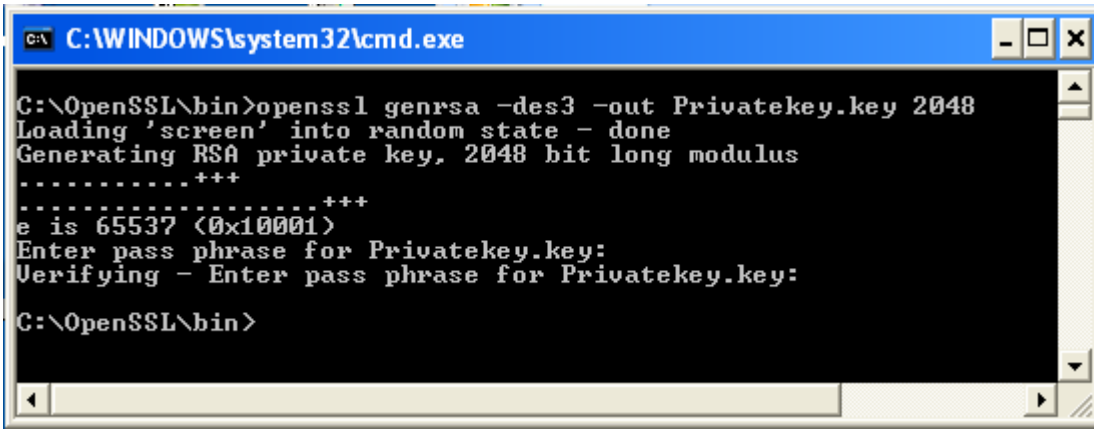
Konfigurační soubor uložte v adresáři programu OpenSSL do adresáře \bin pod názvem certreq.config.

2.2 Generování klíčového páru

V adresáři \bin programu OpenSSL zadejte příkaz:

openssl genrsa -des3 -out Privatekey.key 2048

Po spuštění příkazu budete vyzváni k vytvoření hesla a k jeho následnému ověření.

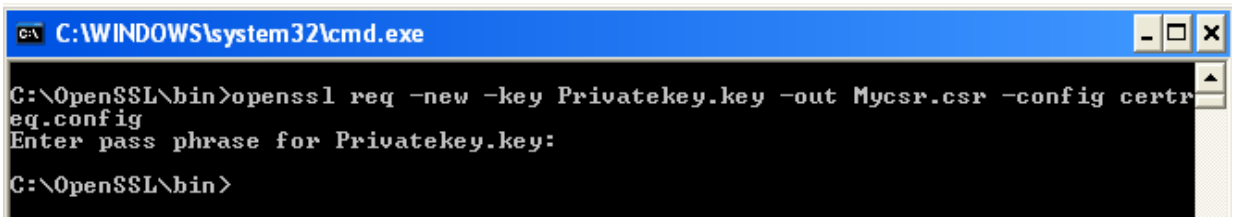


Během provedení příkazu dojde k vygenerování souboru **Privatekey.key**, který obsahuje privátní klíč chráněný heslem, které jste zadali.

2.3 Vytvoření souboru s žádostí o certifikát

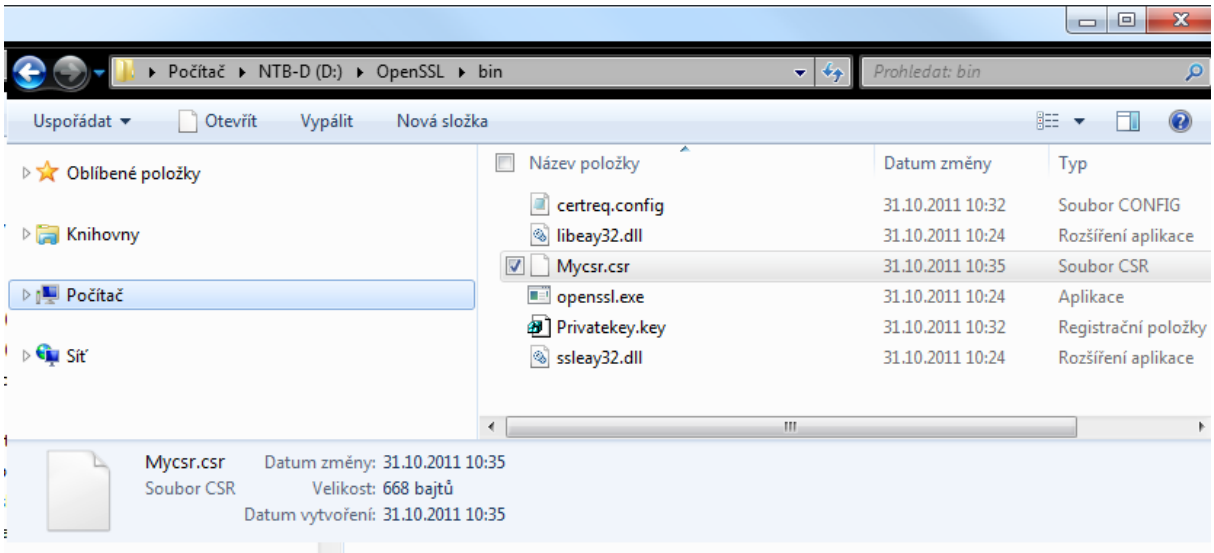
V adresáři \bin programu OpenSSL zadejte příkaz:

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



Po zadání příkazu budete dotázáni na vaše heslo, které jste vytvořili při generování klíčového páru.

Výsledkem provedení příkazu je soubor Mycsr.csr obsahující žádost o certifikát (obsahuje mj. veřejnou část klíčového páru) ve formátu PKCS#10.



Zkopírujte soubor **Mycsr.csr** do souboru **Mycsr_XXXXXXXX_AAAA.txt** (XXXXXXXX je IČO a AAAA je číslo AIS v ISoISVS) a pošlete ho v příloze formuláře „Registrace a Správa AIS v JIP Czech POINT a základních registrech“ do datové schránky SZR k certifikaci vašeho veřejného klíče.

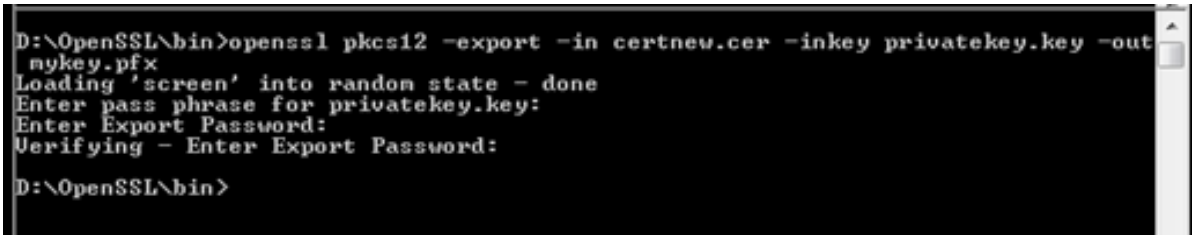
Pokud bude certifikace úspěšná, obdržíte od SZR do datové schránky certifikát v souboru **Mycsr_XXXXXXXX_AAA.cer.txt**. Zkopírujte ho do souboru **certnew.cer.**

2.4 Spojení certifikátu s privátním klíčem

Proces musíte dokončit spojením certifikátu s privátním klíčem.

Soubor s certifikátem z certifikační autority vložte do podadresáře \bin v OpenSSL adresáři a zadejte v podadresáři \bin následující příkaz:

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



Po spuštění příkazu budete nejprve dotázáni na heslo, které jste vytvořili při generování klíčového páru.

Potom budete vyzváni k vytvoření hesla, kterým bude chráněn privátní klíč a certifikát v souboru mykey.pfx, a k jeho následnému ověření.

Výsledkem je privátní klíč a certifikát v souboru **mykey.pfx**. Privátní klíč je v souboru zašifrován a chráněn heslem.

3. Použití certifikátu

Certifikáty vydávané SZR jsou serverové, tj. vydávají se pro počítače, ne pro osoby.

Certifikát a privátní klíč nainstalujte na všechny počítače, které budou komunikovat s ISZR. Musí to být počítače, které jsou součástí AIS a splňují všechny bezpečnostní požadavky pro provoz AIS. SZR doporučuje instalovat certifikáty a odpovídající soukromé klíče na pouze nezbytný počet serverů

Při navazování spojení mezi ISZR a AIS se certifikát může použít jednak jako klientský (spojení navazuje AIS) a za druhé jako serverový (spojení navazuje ISZR při odpovědi na asynchronní dotaz v aktivním režimu).

Privátní část klíče chraňte před zneužitím.

Certifikát používejte pouze pro ty účely, pro které byl vydán. Je zakázáno ho používat pro jiné AIS.

Povolené použití certifikátu je vymezeno Certifikační politikou SZR.