SPRÁVA ZÁKLADNÍCH REGISTRŮ

Postup pro vytvoření žádosti o digitální certifikát pro přístup k Základním registrům

Verze dokumentu:	2.0
Datum vydání:	20. června 2017
Klasifikace:	Veřejný dokument

Obsah

1. Žádost o certifikát

Certifikáty vydávané Certifikační autoritou Správy základních registrů (SZR) slouží k identifikaci a autentizaci AIS. Používají se ve dvou situacích:

1. AIS navazuje spojení s ISZR.
2. 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 **pro produkční prostředí** základních registrů se řídí Certifikační politikou SZR pro vydávání certifikátů pro AIS. Tato politika je dostupná na webu SZR. **Pro testovací prostředí** základních registrů certifikační politika neexistuje, ale SZR postupuje při vydávání certifikátů pro testovací prostředí obdobně jako pro produkční prostředí.

Technický postup pro generování klíčů a žádosti o certifikát je pro produkční a testovací prostředí základních registrů stejný. Žádosti pro jednotlivá prostředí se liší v položce CisloAIS - viz dále. Správce AIS vyznačuje ve formuláři žádosti o vydání certifikátu, zda žádá certifikát pro produkční nebo testovací prostředí.

Žádost o certifikát podává správce AIS pro konkrétní AIS.

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 délka klíče 2048 bitů.

2. Postup s OpenSSL v OS Windows

Program je součástí softwarového balíčku, který si můžete stáhnout ze stránek SZR http://www.szrcr.cz/vyvojari/spravci

Pracovat s OpenSSL budete v příkazové řádce.

Příkazovou řádku spusťte příkazem **cmd.exe**. Pro práci s programem se přepněte do adresáře, kam jste nakopírovali OpenSSL, a jeho podadresáře bin příkazem **cd \adresar\bin**

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

Základní postup:

- Připravíte si konfigurační soubor certreq.config, který použijete při generování asymetrického klíčového páru (pro váš AIS).
- Vygenerujete dvojici klíčů (klíčový pár), vytvoříte žádost (soubor) obsahující veřejný klíč a tuto žádost připojíte jako přílohu k formuláři „zadost_registrace_AIS.zfo“.
- Vyplněný formulář s přílohou zašlete do datové schránky SZR (jjqjqih).
- Certifikační autorita SZR formulář i 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 a soukromý klíč nainstalujete na svůj server.

2.1 Příprava konfiguračního souboru pro vygenerování klíčového páru

Konfigurační soubor vytvoříte pomocí editoru, např. Notepad.
Na webu SZR je připravený soubor **certreq.txt**, který upravíte pro vaši potřebu a pojmenujete ho **certreq.config.**

Při vyplňování změňte obsah těch položek, které jsou na následujícím výpisu červeně.

```
distinguished_name      = req_distinguished_name
string_mask             = nombstr
```

```
prompt                  = no

[req_distinguished_name]
0.commonName            = JmenoServeru
0.organizationName      = ICO
organizationalUnitName  = CisloAIS
countryName             = Zeme
localityName            = Obec=Obec,Ulice=Ulice,PSC=PSC
stateOrProvinceName     = NazevOVM
```

Požadovaný obsah jednotlivých položek je definován Certifikační politikou SZR pro vydávání certifikátů pro AIS.

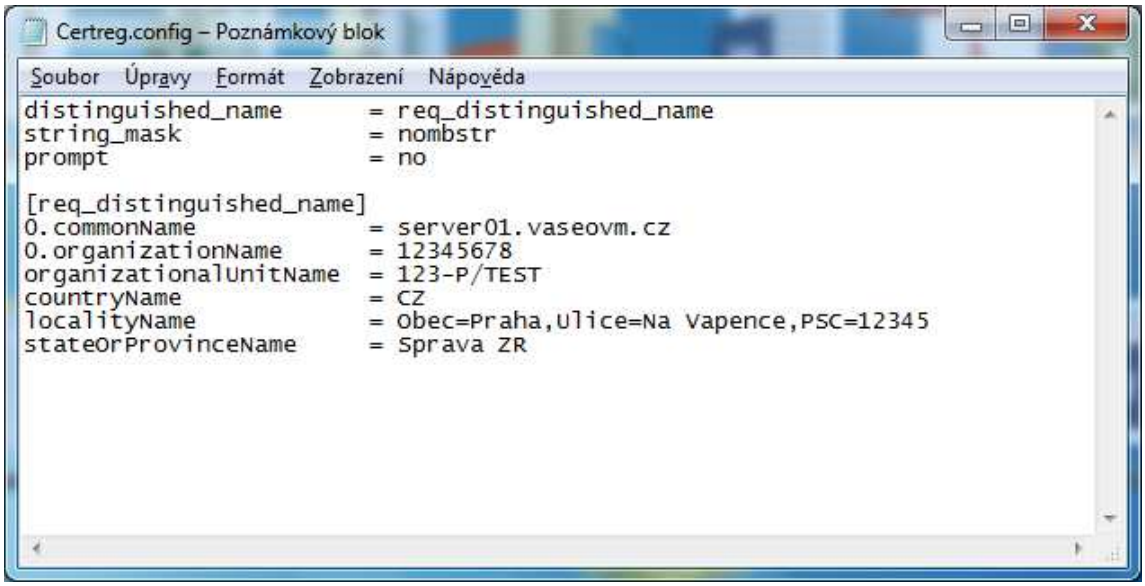
Do jednotlivých (červeně zvýrazněných) položek uvedete:

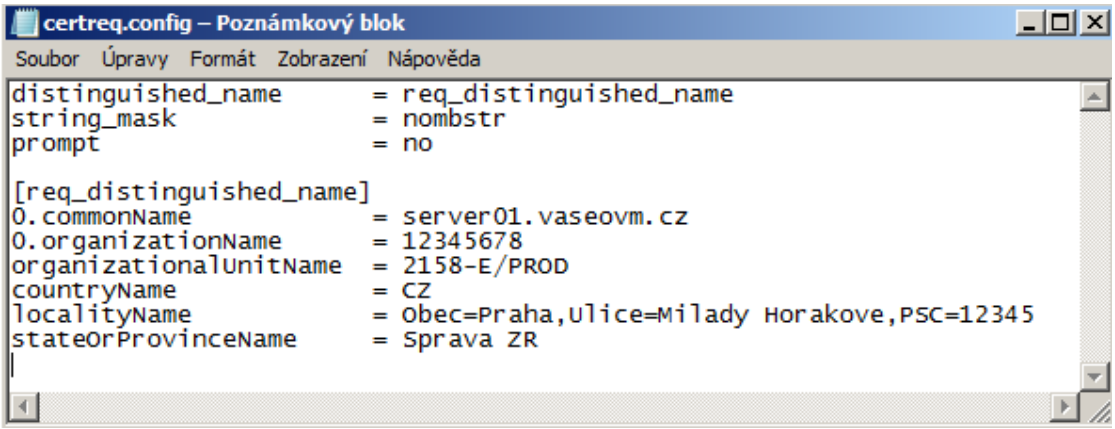
JmenoServeru	Doporučujeme uvádět DNS **jméno** počítače, který bude přijímat zpětná volání v případě, kdy ISZR vrací odpověď na asynchronní dotaz v aktivním režimu. Pokud bude spojení navazováno v KIVS, mělo by jít o jméno, pod kterým je počítač dosažitelný v síti KIVS. Pokud bude spojení navazováno 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.cms2.cz
ICO	IČO OVM (**číslo bez mezer**), délka maximálně 8 číslic, lze včetně nul na začátku i bez nich, např. 00345678 nebo 345678.
CisloAIS	identifikace (**číslo**) AIS v ISoISVS (nebo identifikátor přidělený SZR v případě, že na AIS se nevztahuje zákon č. 365/2000 Sb.), doporučujeme doplnit o informaci, zda jde o publikační (-P) nebo editační (-E) AIS a že jde o produkční (/PROD) nebo testovací (/TEST) prostředí základních registrů, maximální délka 64 znaků, např.: 123-E/PROD 567-P/TEST
Zeme	Kód státu (**dvě velká písmena**), např. CZ, musí jít o členský stát EU
Obec	Jméno obce (**bez diakritiky**), např. Hradec Kralove
Ulice	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=PSČ“ je 128 znaků
NazevOVM	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

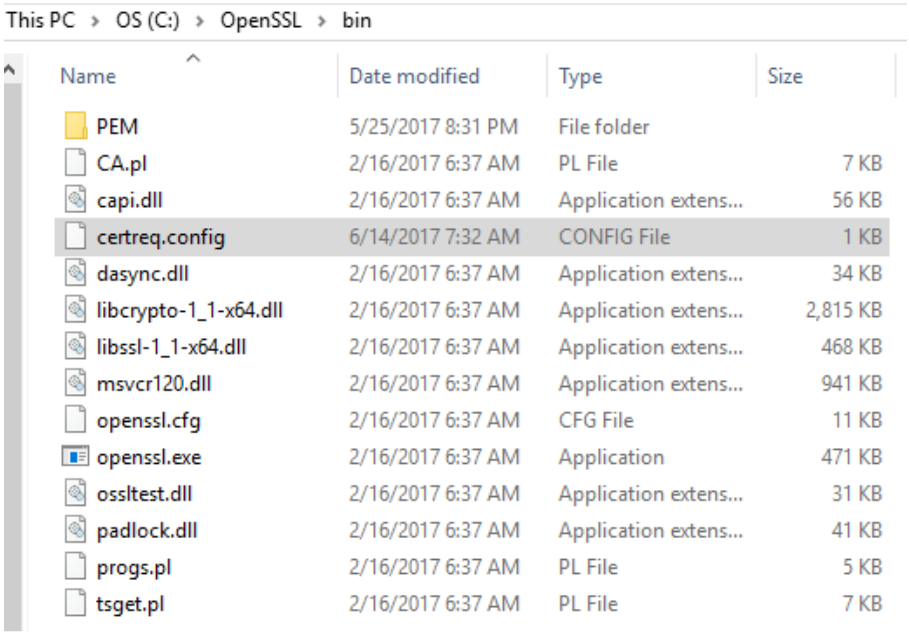
Dobře si vše překontrolujte!

Příklady:





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

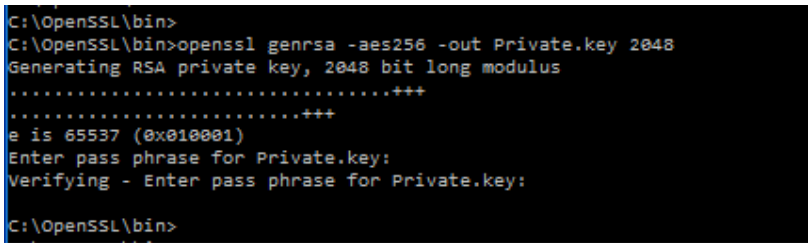


2.2 Generování klíčového páru

V adresáři in programu OpenSSL zadejte příkaz:

openssl genrsa –aes256 -out Private.key 2048

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

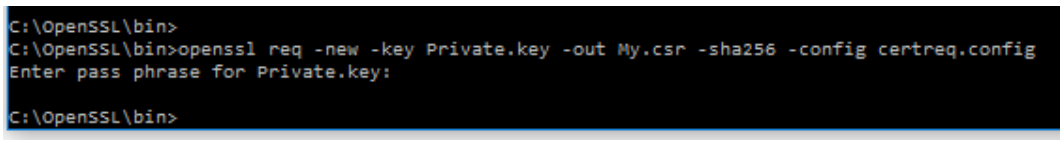


Během provedení příkazu vytvoří OpenSSL soubor **Private.key**, který obsahuje zašifrovaný soukromý i veřejný klíč chráněné heslem, které jste zadali.

2.3 Vytvoření žádosti o certifikát

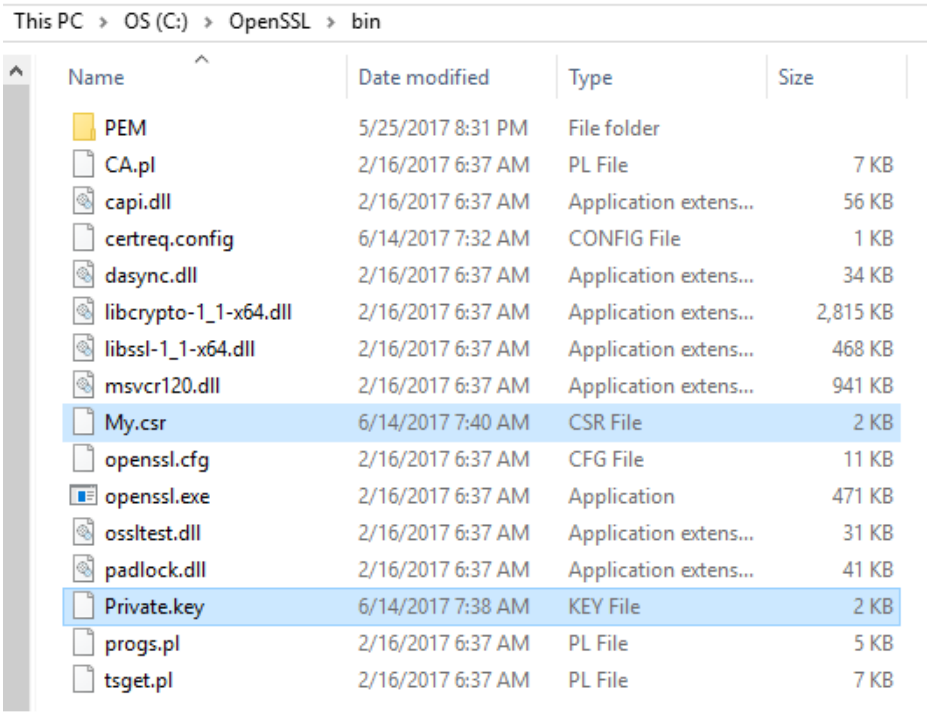
V adresáři bin programu OpenSSL zadejte příkaz:

openssl req -new -key Private.key -out My.csr -sha256 -config certreq.config



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

Výsledkem provedení příkazu je soubor My.csr obsahující žádost o certifikát (obsahuje mj. veřejný klíč) ve formátu PKCS#10.



Přejmenujte soubor **My.csr** na **Mycsr_XXXXXXXX_AAAA.txt** (XXXXXXXX je IČO a AAAA je číslo AIS) a pošlete ho v příloze formuláře „Registrace a Správa AIS v JIP Czech POINT a základních registrech“ (zadost_registrace_AIS.zfo) do datové schránky SZR k certifikaci vašeho veřejného klíče. Ve formuláři označte, zda žádáte o certifikát pro produkční nebo testovací prostředí základních registrů.

Pokud bude certifikace úspěšná, obdržíte od SZR do datové schránky certifikát v souboru **produkce_XXXXXXXX_AAA.txt**, respektive **test_XXXXXXXX_AAA.txt**. Přejmenujte ho na **Cert.cer** (nebo na jiné jméno podle vašich potřeb nebo konvencí).

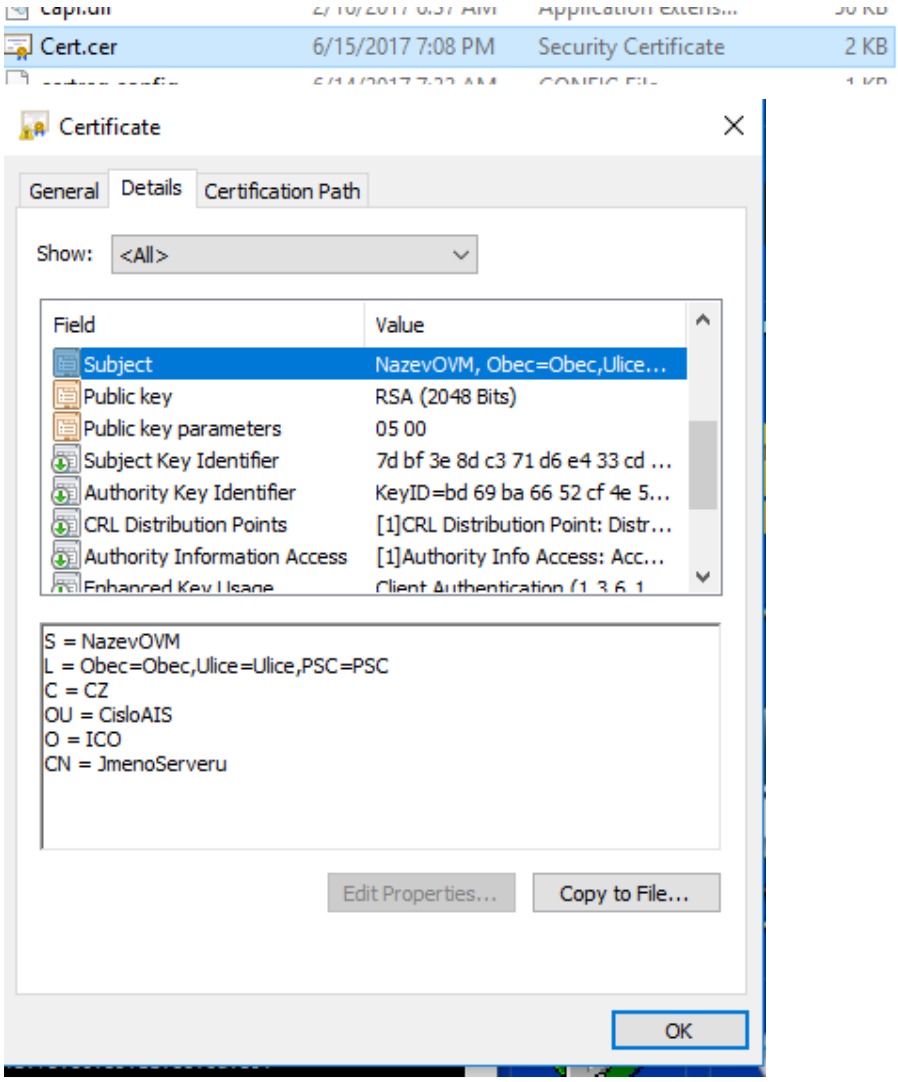
Zkontrolujte obsah certifikátu, že skutečně odpovídá vaší žádosti!

Například v adresáři bin programu OpenSSL zadejte příkaz:

openssl x509 -in Cert.cer -text

```
C:\OpenSSL\bin>openssl x509 -in Cert.cer -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            63:5e:c0:af:00:01:00:00:04:04
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = Informacni system zakladnich registru SubCA1
        Validity
            Not Before: Jun 15 17:08:48 2017 GMT
            Not After : Jun 14 17:08:48 2020 GMT
        Subject: CN = JmenoServeru, O = ICO, OU = CisloAIS, C = CZ, L = "Obec=Ob
ec,Ulice=Ulice,PSC=PSC", ST = NazevOVM
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b7:82:53:dd:e5:3c:fd:56:94:36:1c:5f:ca:a6:
                    41:37:2b:a7:c2:e6:21:7a:b1:70:b8:af:46:67:a9:
                    d1:55:29:5e:1d:88:97:c5:d3:9f:df:cd:b4:34:bb:
                    b8:78:cb:b7:0c:d5:96:50:2d:52:4c:c4:8f:90:ff:
                    74:94:e8:7f:0d:79:6b:ce:f4:a5:49:ee:c1:1a:3e:
                    5d:95:77:2f:58:8b:3c:4f:20:3e:fc:c1:a6:09:75:
                    f8:05:c8:8f:5f:1b:30:dc:10:8a:b7:9f:a4:78:e6:
                    2a:5f:91:87:94:5a:77:94:89:52:93:9e:95:a9:51:
                    77:eb:b5:6d:76:72:5b:03:00:bf:59:d0:b9:d4:78:
                    44:5f:7d:09:bf:f6:a0:49:be:8f:ac:8b:6b:4a:08:
                    5b:16:76:55:43:7c:fb:71:67:03:54:f6:6a:2e:32:
                    19:d8:86:99:e0:79:b3:86:d0:fb:3f:19:91:e9:e0:
                    dc:fb:7c:05:df:54:da:b9:98:ad:d9:c1:8e:7f:5a:
                    8a:b9:e2:6d:10:0f:e4:54:d0:cb:eb:e0:aa:9c:09:
                    e9:90:b9:da:02:f2:47:1f:d1:67:39:51:74:6e:47:
                    1d:53:1d:87:99:c3:90:a3:66:a8:cf:75:83:dc:0b:
                    4e:7e:4b:68:22:71:92:d1:52:35:8d:67:9f:e9:6a:
                    b6:51
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                7D:BF:3E:8D:C3:71:D6:E4:33:CD:4E:DC:4B:9E:A3:9A:6A:54:28:68
            X509v3 Authority Key Identifier:
                keyid:BD:69:BA:66:52:CF:4E:5A:AA:D4:0F:83:E3:27:AF:B5:25:0B:BC:8
8

            X509v3 CRL Distribution Points:

                Full Name:
        URI:http://crliszr1.egon.gov.cz/ISZRRootCA.crltCA.crl

            Authority Information Access:
                CA Issuers - URI:http://crliszr1.egon.cms/ISZRRootCA.crt
                CA Issuers - URI:http://crliszr1.egon.gov.cz/ISZRRootCA.crt

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, TLS Web Server Authentication
    Signature Algorithm: sha256WithRSAEncryption
         70:4b:8c:9c:64:a3:5f:1f:01:fc:40:92:70:78:24:f9:6c:54:
         30:61:04:a1:06:4a:90:29:32:09:a2:ff:16:d9:4e:c1:88:b5:
         c4:e0:79:5c:13:4a:c4:4a:41:3f:0d:75:8f:63:e9:d6:9f:f5:
         da:65:2d:50:5a:09:9c:53:54:87:b4:6e:4d:88:d1:60:d1:03:
         be:9f:4c:c5:ca:21:e3:aa:e6:71:f5:a4:3a:97:a7:d5:67:40:
         a6:e9:fc:9d:cc:fb:b6:dd:16:a5:9a:7c:49:ec:ca:91:40:e4:
         10:14:92:5e:20:23:bb:c4:e5:ae:12:1c:16:ae:33:7e:df:16:
         a7:88:a8:a1:50:e1:e7:2d:71:4f:a7:8d:dd:61:88:48:7c:13:
         57:7d:49:4b:f5:d5:f0:36:f1:60:41:fb:6c:85:1a:e6:6d:89:
         15:cf:06:fb:52:66:c2:fa:4e:63:a2:56:08:f5:64:47:d2:b8:
         c8:ad:12:18:0c:c0:67:64:48:01:ab:87:b7:70:ce:d1:54:d5:
         49:90:2b:e7:3f:1d:9e:fb:09:10:8d:6b:c8:4a:e7:12:e6:34:
         72:8f:98:dd:f5:56:1f:a5:78:35:40:91:5c:18:17:31:b4:55:
         f7:3b:e1:d8:24:e5:07:3e:f0:e5:bd:76:78:c7:e1:e3:57:50:
         26:a5:4a:a4
-----BEGIN CERTIFICATE-----
MIIEmDCCA4CgAwIBAgIKY17ArwABAAAEBDANBgkqhkiG9w0BAQsFADA3MTUwMwYD
VQQDDCxJbmZvcm1hY25pIHN5c3RlbSB6YWtsYWRuaWNoIHJlZ2lzdHJ1IFN1YkNB
MTAeFw0xNzA2MTUxNzA4NDhaFw0yMDA2MTQxNzA4NDhaMIGAMRUwEwYDVQQDEwxK
bWVub1NlcnZlcnUxDDAKBgNVBAoTA0lDTzERMA8GA1UECxMIQ2lzbG9BSVMxCzAJ
BgNVBAYTAkNaMSYwJAYDVQQHEx1PYmVjPU9iZWMsVWxpY2U9VWxpY2UsUFNDPVBT
QzERMA8GA1UECBMITmF6ZXZPVk0wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC3glPd5Tz9VpQ2HF/KpkE3K6fC5iF6sXC4r0ZnqdFVKV4diJfF05/fzbQ0
u7h4y7cM1ZZQLVJMxI+Q/3SU6H8NeWvO9KVJ7sEaPl2Vdy9YizxPID78waYJdfgF
yI9fGzDcEIq3n6R45ipfkYeUWneUiVKTnpWpUXfrtW12clsDAL9Z0LnUeERffQm/
9qBJvo+si2tKCFsWdlVDfPtxZwNU9mouMhnYhpngebOG0Ps/GZHp4Nz7fAXfVNq5
```

nebo použijte standardní prohlížeč certifikátů MS Windows:

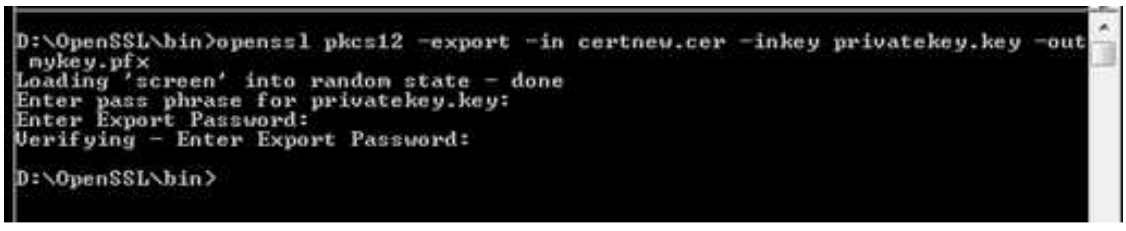


2.4 Spojení certifikátu se soukromým klíčem

Proces musíte dokončit spojením certifikátu se soukromým klíčem.

Soubor s certifikátem z certifikační autority uložte do adresáře bin programu OpenSSL a zadejte v adresáři bin následující příkaz:

openssl pkcs12 -export -in Cert.cer -inkey Private.key -out Cert.pfx



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

Potom budete vyzváni k zadání (definici) hesla, kterým bude chráněn soukromý klíč a certifikát v souboru Cert.pfx, a k jeho následnému ověření.

Výsledkem je soukromý klíč a certifikát v souboru **Cert.pfx**. Soukromý klíč je v souboru zašifrován a chráněn heslem.

3. Použití certifikátu a soukromého klíče

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

Certifikát a soukromý klíč (Cert.pfx) 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. Pokud váš AIS požaduje soukromý klíč a certifikát v oddělených souborech, použijte Private.key a Cert.cer.

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).

Soukromý klíč chraňte před zneužitím.

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

Povolené použití certifikátů vydaných pro produkční prostředí základních registrů je vymezeno Certifikační politikou SZR pro vydávání certifikátů pro AIS.