DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

Postup pro vytvoření žádosti o digitální certifikát pro přístup k ISZR a ISSS

Verze dokumentu:	3.3
Datum vydání:	22.4.2024
Klasifikace:	Veřejný dokument

Obsah

1. Žádost o certifikát

Certifikáty vydávané Certifikační autoritou (CA) Digitální a informační agentury (DIA) slouží k identifikaci a autentizaci agendových informačních systémů (AIS) vůči ISZR (Informační systém základních registrů), ISSS (Informační systém sdílené služby, dříve eGSB) a vůči jiným AIS.

Vydávání certifikátů Certifikační autoritou DIA **pro produkční prostředí** základních registrů a ISSS se řídí Certifikační politikou DIA pro vydávání certifikátů pro AIS. Certifikační politika je dostupná na webu DIA. **Pro testovací prostředí** základních registrů a ISSS certifikační politika neexistuje, ale DIA postupuje při vydávání certifikátů pro testovací prostředí základních registrů a ISSS obdobně jako pro produkční prostředí.

Technický postup pro generování klíčů a žádosti o certifikát je pro produkční a testovací prostředí ISZR/ ISSS 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 žádosti o certifikát a následné spojení certifikátu a privátního klíče ve většině případů doporučujeme používat aplikaci GeneratorCertRAZR, která nabízí grafické uživatelské rozhraní. Aplikace je k nalezení na webu DIA.

V případě, kdy např. používáte platformu, kde není možné aplikaci GeneratorCertRAZR použít, pokračujte v následujícím postupu.

V tomto případě je možné používat freeware OpenSSL. Tento software je dostupný pro více operačních systémů (MS Windows, Linux a další). Je však možné použít jakýkoli software, který vytváří žádosti o digitální certifikát podle příslušných standardů.

Žádost o certifikát musí být ve formátu PKCS#10. Typ klíče musí být RSA a délka klíče 3072 bitů.

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.
- V aplikaci RAZR požádejte o vydání certifikátu pro vámi spravovaný AIS a soubor s žádostí připojte jako přílohu.
- Certifikační autorita DIA formulář i žádost zkontroluje. Pokud je vše v žádosti i ve formuláři správně, vygeneruje certifikát. Pokud je tam chyba, vrátí vám DIA žádost zpět.
- DIA vám zašle zpět do aplikace RAZR a současně do vaší datové stránky certifikát.
- Certifikát a soukromý klíč nainstalujete na server s AIS.

2. Postup s OpenSSL v OS Microsoft Windows

Program je součástí softwarového balíčku, který si můžete stáhnout z webu DIA nebo z internetu .

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.**

2.1 Příprava konfiguračního souboru pro vygenerování klíčového páru

Konfigurační soubor vytvoříte pomocí editoru, např. Notepad.
Na webu DIA 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]
commonName              = JmenoServeru
organizationName        = ICO
organizationalUnitName  = CisloAIS
countryName             = Zeme
localityName            = Obec=Obec,Ulice=Ulice,PSC=PSC
stateOrProvinceName     = NazevSpravceAIS
```

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

Do jednotlivých (červeně zvýrazněných) položek uvedete:

JmenoServeru Do položky vyplňte jméno, ze kterého bude poznat, o jaký AIS se jedná.
Příklady:
Spisova sluzba
spis.subjekt.cz
Maximální délka 64 znaků.
Upozornění:
V případě, že chcete, aby AIS vystupoval vůči ISSS jako publikační, uveďte DNS jméno, které je součástí URL, na kterém ISSS s AIS komunikuje. A toto jméno musí být z domény cms2.cz.
Příklady: aisXXXX.egsb.cms2.cz
aisXXXX-test.egsb.cms2.cz
Kde XXXX znamená identifikátor (číslo) AIS.

Poznámka.
Uvádějte DNS jméno, které odpovídá IP adrese, ze které bude AIS komunikovat s ISZR, respektive ISSS. Pokud bude spojení navazováno v KIVS, musí být vyplněno jméno, pod kterým je počítač dosažitelný v síti KIVS. Pokud bude spojení navazováno v Internetu, pak by mělo jít o DNS jméno z veřejné domény.
Příklady:
server.vaseovm.cz
server.vaseovm.cms2.cz

ICO IČO správce AIS nebo identifikátor OVM v RPP, pokud správce AIS nemá IČO, (**číslo bez mezer**), délka maximálně 8 číslic, lze včetně nul na začátku i bez nich, např.
00345678 nebo 345678.

CisloAIS Identifikace (**číslo**) AIS v RPP, nebo identifikátor přidělený DIA v případě, že AIS není v RPP. Dále je potřeba doplnit informaci, zda jde o publikační (-P) nebo čtenářský (-E) AIS a zda jde o produkční (/PROD) nebo testovací (/TEST) prostředí ISZR/ISSS, maximální délka je 64 znaků.
Příklady:
123-E/PROD
123-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

NazevSpravceAIS Název správce AIS (**bez diakritiky**), maximální délka 128 znaků, např. Digitalni a informacni agentura

Povinné položky jsou:

- organizationName: musí přesně odpovídat IČO správce AIS nebo identifikátoru OVM v RPP, pokud OVM nemá IČO.
- organizationalUnitName: musí přesně odpovídat číslu AIS

2.2 Subject Alternative Name

Rozšíření SAN (Subject Alternative Name) je potřebné v následujících situacích:

- Potřebujete vydat certifikát pro více DNS jmen.
- Potřebujete použít certifikát pro komunikaci s nějakým AIS, který vyžaduje mít vyplněný atribut SAN.
  Poznámka: ISZR ani ISSS nevyžadují vyplněný atritbut SAN.

V obou případech použijte rozšíření SAN (Subject Alternative Name). Do souboru certreq.config přidejte řádek `req_extensions` a sekce `[req_ext]` a `[alt_names]`.

V případě více jmen například takto:

```
distinguished_name      = req_distinguished_name
string_mask             = nombstr
prompt                  = no
req_extensions          = req_ext

[req_distinguished_name]
commonName              = JmenoServeru
organizationName        = ICO
organizationalUnitName  = CisloAIS
countryName             = Zeme
localityName            = Obec=Obec,Ulice=Ulice,PSC=PSC
stateOrProvinceName     = NazevSpravceAIS

[req_ext]
subjectAltName = @alt_names

[alt_names]
DNS.1 = JmenoServeru2
DNS.2 = JmenoServeru3
```

V případě potřeby vyplněného SAN například takto:

```
distinguished_name      = req_distinguished_name
string_mask             = nombstr
prompt                  = no
req_extensions          = req_ext

[req_distinguished_name]
commonName              = JmenoServeru
organizationName        = ICO
organizationalUnitName  = CisloAIS
countryName             = Zeme
localityName            = Obec=Obec,Ulice=Ulice,PSC=PSC
stateOrProvinceName     = NazevSpravceAIS

[req_ext]
subjectAltName = @alt_names

[alt_names]
DNS.1 = JmenoServeru2
```

Dobře si vše překontrolujte!

Příklad 1:

```
distinguished_name      = req_distinguished_name
string_mask             = nombstr
prompt                  = no

[req_distinguished_name]
0.commonName            = server.ovm.cz
0.organizationName      = 12345678
organizationalUnitName  = 123-E/TEST
countryName             = CZ
localityName            = Obec=Praha,Ulice=Vaclavske namesti,PSC=10100
stateOrProvinceName     = Ministerstvo
```

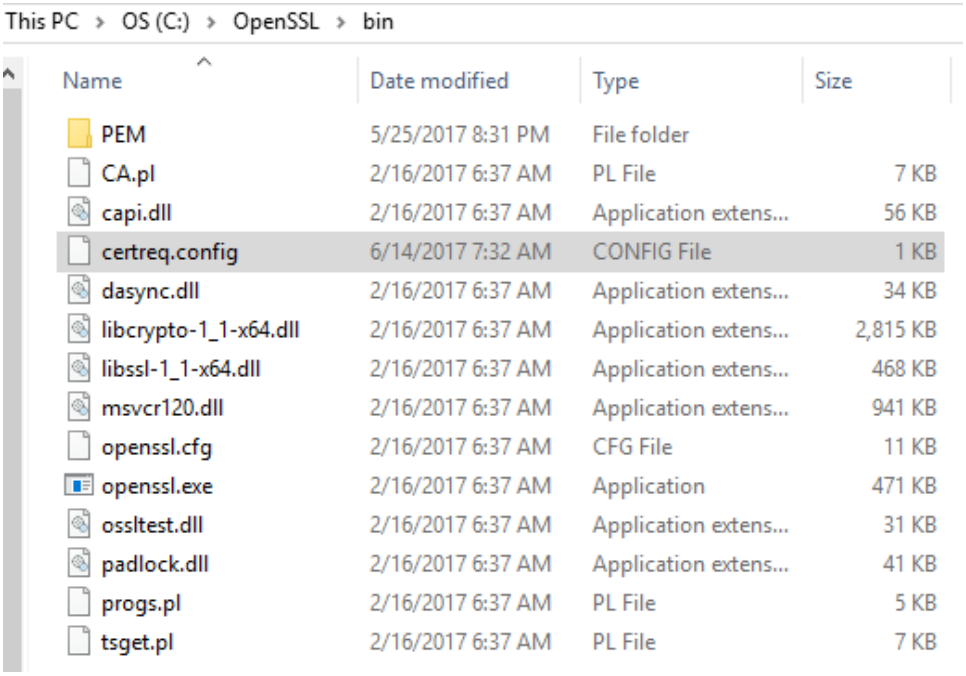
Poznámka organizationalUnitName: 123-E/TEST – znamená čtenářský AIS pro testovací prostředí.

Příklad 2:

```
distinguished_name      = req_distinguished_name
string_mask             = nombstr
prompt                  = no
req_extensions          = req_ext
[req_distinguished_name]
0.commonName            = server.ovm.cz
0.organizationName      = 12345678
organizationalUnitName  = 123-E/PROD
countryName             = CZ
localityName            = Obec=Praha,Ulice=Vaclavske namesti,PSC=10100
stateOrProvinceName     = Ministerstvo
[req_ext]
subjectAltName = @alt_names
[alt_names]
DNS.1 = aplikace.ovm.cz
DNS.2 = agenda.ovm.cz
```

Poznámka u organizationalUnitName: 123-E/PROD – znamená čtenářský AIS pro produkční prostředí.

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

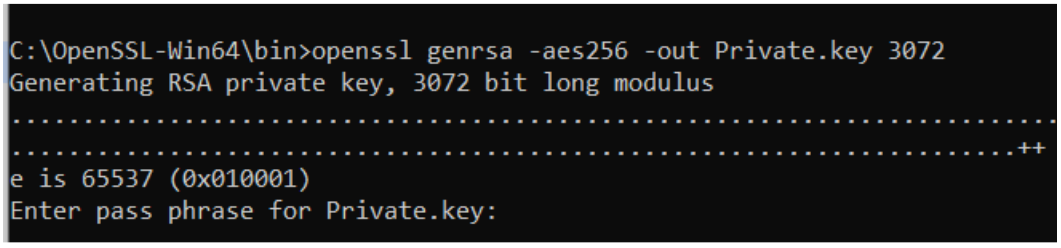


2.3 Generování klíčového páru

V adresáři bin programu OpenSSL zadejte příkaz:

openssl genrsa –aes256 -out Private.key 3072

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

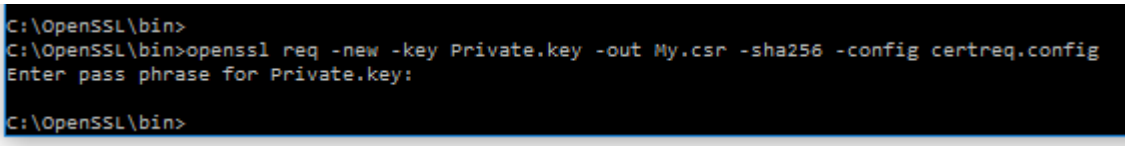


Během provedení příkazu vytvoří OpenSSL soubor **Private.key**, který obsahuje zašifrované klíče chráněné heslem, které jste zadali.

2.4 Vytvoření žádosti o certifikát

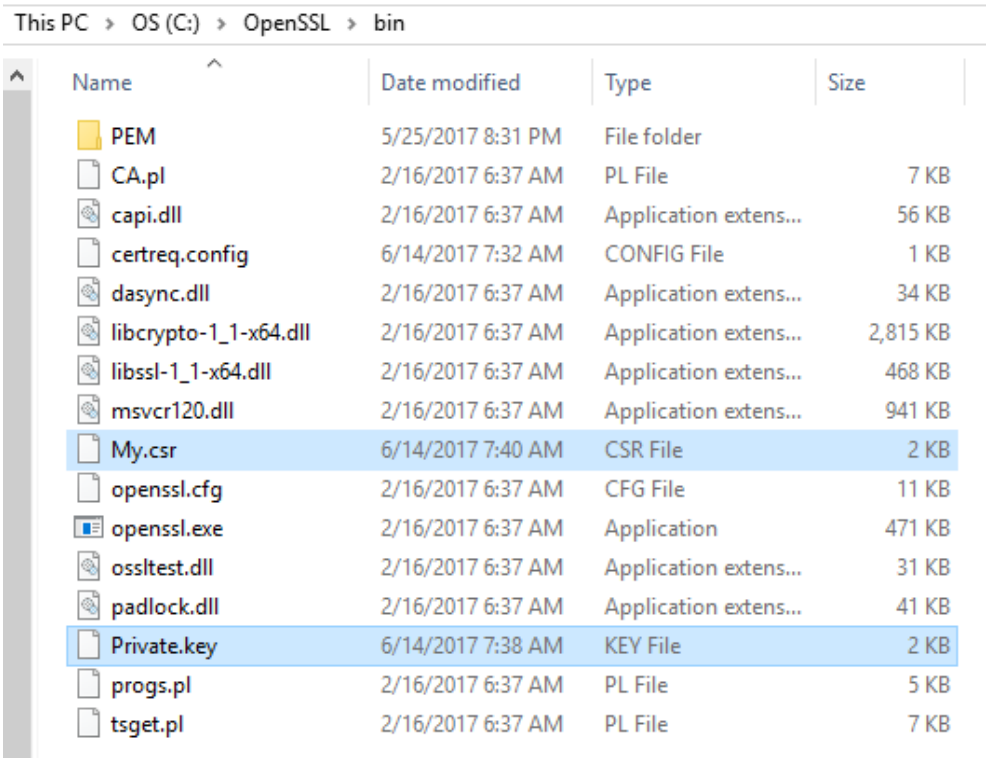
V adresáři bin programu OpenSSL zadejte příkaz:

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.



Obsah žádosti si můžete zobrazit příkazem:

openssl req -in My.csr -noout -text

Doporučujeme přejmenovat soubor **My.csr** na **Mycsr_XXXXXXXX_AAAA.csr/.txt** (XXXXXXXX je IČO a AAAA je číslo AIS).

Následně je nutné odeslat tento soubor v příloze formuláře vyplněného v aplikaci RAZR k certifikaci vašeho veřejného klíče.

Soubor Private.key se soukromým klíčem si schovejte.
Pokud připravujete více žádostí o certifikát, před generováním každého dalšího klíčového páru si předcházející soubor Private.key schovejte, budete ho ještě potřebovat, a to až do chvíle než dokončíte celý proces popsaný v tomto dokumentu (včetně kapitoly 2.4). Např. ho přejmenujte na Private_AAAA.key.

Pokud bude certifikace úspěšná, obdržíte od DIA do aplikace RAZR a do datové schránky certifikát se stejným názvem jako měla žádost. Přejmenujte ho na **Cert.cer** (nebo na jiné jméno podle vašich potřeb nebo konvencí).

Zkontrolujte obsah certifikátu, že skutečně odpovídá vaší žádosti!

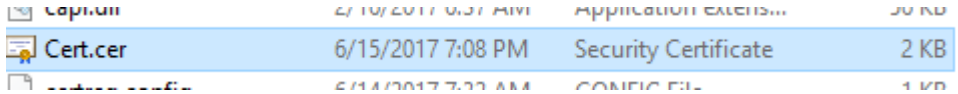
Například v adresáři bin programu OpenSSL zadejte příkaz:

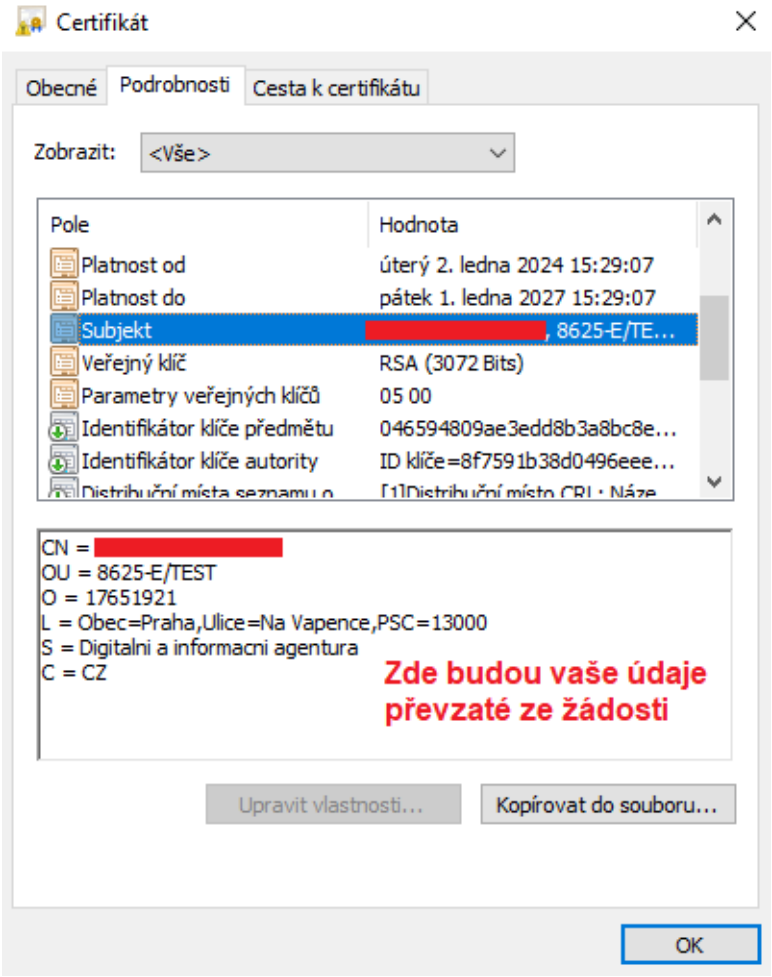
openssl x509 -in Cert.cer -text

```
C:\OpenSSL-Win64\bin>openssl x509 -in Cert.cer -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            1a:97:4a:6a:00:01:00:00:00:24
    Signature Algorithm: sha384WithRSAEncryption
        Issuer: C = CZ, L = Praha, O = DIA, CN = ISZR CA
        Validity
            Not Before: Jan  2 13:29:07 2024 GMT
            Not After : Jan  1 13:29:07 2027 GMT
        Subject: C = CZ, ST = Digitalni a informacni agentura, L = "Obec=Praha,Ulice=Na Vapence,PSC=130
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (3072 bit)
                Modulus:
                    00:c3:a6:c0:0e:a4:77:4e:6d:41:9e:24:62:36:51:
                    6c:e0:96:f8:9d:80:86:b2:98:78:a2:b2:8d:0a:fb:
                    f2:da:d8:6f:6b:78:a3:76:99:bd:3f:2e:ea:72:8f:
                    00:9c:63:cc:02:8c:71:3b:55:ed:da:1d:fc:d0:ea:
                    b1:5a:c4:47:6c:32:c0:2c:5e:d3:b2:95:4f:1e:68:
                    25:fb:9d:4b:a6:bf:ac:13:48:a1:c9:d7:ac:13:1f:
                    08:10:e1:a4:ea:d7:9e:88:79:14:e9:e0:aa:2d:2d:
                    9b:34:09:51:c6:e7:66:7f:25:9a:80:bc:46:61:20:
                    80:2c:20:7a:5a:94:a5:d1:29:01:89:22:0f:92:af:
                    9f:f9:4f:e6:d3:5c:bc:10:c3:13:1a:b8:09:1d:18:
                    95:13:b7:e2:80:8e:45:6e:14:39:e6:0b:8a:9f:07:
                    a5:7e:a4:01:d7:0d:07:59:71:88:d9:ec:4e:4f:d1:
                    cb:bf:1b:ab:51:88:58:6b:d7:09:08:bb:db:b4:9e:
                    ae:c6:80:de:95:8a:61:47:25:6e:12:9c:97:bf:72:
                    a8:25:c5:15:92:b3:37:fb:c3:22:84:df:c6:83:9f:
                    1f:28:92:28:a7:87:d8:6c:a0:d6:c7:9c:51:98:4e:
                    87:45:94:3a:21:08:53:24:0e:fa:3a:e3:4d:a8:13:
                    e7:85:e8:82:42:1c:8d:6d:8c:02:6d:7d:35:f4:45:
                    37:b8:6d:6f:04:8f:18:9d:3a:ae:ce:f9:ce:0e:cb:
                    a9:3f:67:6d:23:1b:e4:33:85:fb:f0:67:cb:45:e8:
                    69:8f:cc:38:af:3e:84:ea:b6:75:d8:ac:ec:d3:63:
                    11:35:e3:87:5c:a1:f2:bb:8b:78:82:a2:1b:6e:ba:
                    0b:6f:b5:9a:a4:4d:24:a8:3a:4a:06:5f:eb:bb:b3:
                    ec:b9:79:75:dd:da:32:f9:45:09:6a:7f:09:60:e0:
                    e9:0a:57:6f:bc:2a:41:b9:b8:89:d2:73:81:be:09:
                    4b:e9:30:9b:03:bc:02:02:a7:ed
                Exponent: 65537 (0x10001)
        X509v3 extensions:
```

Zde budou vaše údaje převzaté ze žádosti

nebo použijte standardní prohlížeč certifikátů MS Windows:





Poznámka: CN = Common name, tj. jméno serveru.

2.5 Spojení certifikátu se soukromým klíčem

Proces musíte dokončit spojením certifikátu se soukromým klíčem.

Soubor Cert.cer s certifikátem z certifikační autority uložte do adresáře bin programu OpenSSL, ujistěte se, že tam je také správný soubor Private.key a zadejte v adresáři bin následující příkaz:

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

```
F:\OpenSSL\bin>openssl pkcs12 -export -in Cert.cer -inkey Private.key -out Cert.pfx
Enter pass phrase for Private.key:
Enter Export Password:
Verifying - Enter Export Password:
```

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 jsou serverové, tj. vydávají se pro počítače, ne pro osoby.

Certifikát a soukromý klíč (Cert.pfx) nainstalujte na všechna zařízení (servery, komunikační sběrnice, SSL koncentrátory, firewally atd.), která zajišťují šifrovanou komunikaci s ISZR, ISSS nebo jinými AIS.

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

Certifikáty a odpovídající soukromé klíče nainstalujte pouze na nezbytný počet zařízení.

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 DIA pro vydávání certifikátů pro AIS - k nalezení zde.