

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

Verze dokumentu:	2.5
Datum vydání:	28. července 2020
Klasifikace:	Veřejný dokument

Obsah

1.	Žádost o certifikát	3
2.	Postup s OpenSSL v OS Microsoft Windows	3
2.1	Příprava konfiguračního souboru pro vygenerování klíčového páru	3
2.2	Generování klíčového páru.....	6
2.3	Vytvoření žádosti o certifikát.....	7
2.4	Spojení certifikátu se soukromým klíčem	10
3.	Použití certifikátu a soukromého klíče	11

1. Žádost o certifikát

Certifikáty vydávané Certifikační autoritou (CA) Správy základních registrů (SZR) slouží k identifikaci a autentizaci agendových informačních systémů (AIS). Je možné je použít v následujících situacích:

1. AIS navazuje spojení s ISZR (informační systém základních registrů).
2. ISZR navazuje spojení s AIS při odpovědi na asynchronní dotaz v aktivním režimu.
3. AIS navazuje spojení s eGSB (eGon Service Bus) / ISSS (informační systém sdílených služeb), tj. AIS čerpá data prostřednictvím eGSB / ISSS.
4. eGSB / ISSS navazuje spojení s AIS, tj. AIS publikuje data prostřednictvím eGSB / ISSS.
5. Při vzájemné komunikaci dvou AIS

Ve všech případech je možné použít stejný certifikát a příslušný soukromý klíč.

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 (<https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu-2>). **Pro testovací prostředí** základních registrů certifikační politika neexistuje, ale SZR postupuje při vydávání certifikátů pro testovací prostředí základních registrů 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 CiskoAIS - 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. 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 2048 bitů.

2. Postup s OpenSSL v OS Microsoft Windows

Program je součástí softwarového balíčku, který si můžete stáhnout ze stránek SZR <https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu-2>

Pracovat s OpenSSL budete v příkazové řádce.

Příkazovou řádku spustíte 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.
- V aplikaci RAZR požádejte o vydání certifikátu pro vámi spravovaný AIS a soubor s žádostí připojte jako přílohu.
- 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 aplikace RAZR a současně 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]
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 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.
V případě, že chcete, aby AIS vystupoval vůči eGSB / ISSS jako publikační, uveďte Jméno, které je součástí URL, na kterém eGSB / ISSS s AIS komunikuje.
Maximální délka 64 znaků.
Příklady:
server.vaseovm.cz
server.vaseovm.cms2.cz
- ICO** IČO správce AIS nebo identifikátor OVM v RPP, pokud OVM 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 SZR v případě, že AIS není v RPP,
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,
Příklady:
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
- NazevSpravceAIS** Název správce AIS (**bez diakritiky**), maximální délka 128 znaků, např. Sprava zakladnich registru

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

Pokud potřebujete více vydat certifikát pro více DNS jmen, použijte rozšíření SAN (Subject Alternative Name). Do souboru certreq.config přidejte řádek `req_extensions` a sekce `[req_ext]` a `[alt_names]`, 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
```

Dobře si vše překontrolujte!

Příklady:



*certreq.config - Notepad

File Edit Format View Help

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

[req_distinguished_name]
commonName              = server01.vaseovm.cz
organizationName        = 12345678
organizationalUnitName = 123-P/TEST
countryName             = CZ
localityName            = Obec=Praha,Ulice=Na Vapence,PSC=13000
stateOrProvinceName    = Sprava zakladnich registru
```

|

```
*certreq.config - Notepad
File Edit Format View Help
distinguished_name      = req_distinguished_name
string_mask             = nombstr
prompt                 = no
req_extensions         = req_ext

[req_distinguished_name]
commonName              = server01.vaseovm.cz
organizationName       = 12345678
organizationalUnitName = 123-P/TEST
countryName            = CZ
localityName           = Obec=Praha,Ulice=Na Vapence,PSC=13000
stateOrProvinceName    = Sprava zakladnich registru

[req_ext]
subjectAltName = @alt_names

[alt_names]
DNS.1 = server01.vaseovm.cms2.cz
DNS.2 = server01.vaseovm.gov.cz
```

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

This PC > OS (C:) > OpenSSL > bin

Name	Date modified	Type	Size
PEM	5/25/2017 8:31 PM	File folder	
CA.pl	2/16/2017 6:37 AM	PL File	7 KB
capi.dll	2/16/2017 6:37 AM	Application extens...	56 KB
certreq.config	6/14/2017 7:32 AM	CONFIG File	1 KB
dasync.dll	2/16/2017 6:37 AM	Application extens...	34 KB
libcrypto-1_1-x64.dll	2/16/2017 6:37 AM	Application extens...	2,815 KB
libssl-1_1-x64.dll	2/16/2017 6:37 AM	Application extens...	468 KB
msvcr120.dll	2/16/2017 6:37 AM	Application extens...	941 KB
openssl.cfg	2/16/2017 6:37 AM	CFG File	11 KB
openssl.exe	2/16/2017 6:37 AM	Application	471 KB
ossltest.dll	2/16/2017 6:37 AM	Application extens...	31 KB
padlock.dll	2/16/2017 6:37 AM	Application extens...	41 KB
progs.pl	2/16/2017 6:37 AM	PL File	5 KB
tsget.pl	2/16/2017 6:37 AM	PL File	7 KB

2.2 Generování klíčového páru

V adresáři bin programu OpenSSL zadejte příkaz:

openssl genrsa -aes256 -out Private.key 2048

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

```
C:\OpenSSL\bin>
C:\OpenSSL\bin>openssl genrsa -aes256 -out Private.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x010001)
Enter pass phrase for Private.key:
Verifying - Enter pass phrase for Private.key:

C:\OpenSSL\bin>
```

Během provedení příkazu vytvoří OpenSSL soubor **Private.key**, který obsahuje zašifované klíče 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

```
C:\OpenSSL\bin>
C:\OpenSSL\bin>openssl req -new -key Private.key -out My.csr -sha256 -config certreq.config
Enter pass phrase for Private.key:

C:\OpenSSL\bin>
```

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.

This PC > OS (C:) > OpenSSL > bin

Name	Date modified	Type	Size
PEM	5/25/2017 8:31 PM	File folder	
CA.pl	2/16/2017 6:37 AM	PL File	7 KB
capi.dll	2/16/2017 6:37 AM	Application extens...	56 KB
certreq.config	6/14/2017 7:32 AM	CONFIG File	1 KB
dasync.dll	2/16/2017 6:37 AM	Application extens...	34 KB
libcrypto-1_1-x64.dll	2/16/2017 6:37 AM	Application extens...	2,815 KB
libssl-1_1-x64.dll	2/16/2017 6:37 AM	Application extens...	468 KB
msvcr120.dll	2/16/2017 6:37 AM	Application extens...	941 KB
My.csr	6/14/2017 7:40 AM	CSR File	2 KB
openssl.cfg	2/16/2017 6:37 AM	CFG File	11 KB
openssl.exe	2/16/2017 6:37 AM	Application	471 KB
ossltest.dll	2/16/2017 6:37 AM	Application extens...	31 KB
padlock.dll	2/16/2017 6:37 AM	Application extens...	41 KB
Private.key	6/14/2017 7:38 AM	KEY File	2 KB
progs.pl	2/16/2017 6:37 AM	PL File	5 KB
tsget.pl	2/16/2017 6:37 AM	PL File	7 KB

Obsah žádosti si můžete zobrazit příkazem:

openssl req -in My.csr -noout -text

Přejmenujte soubor **My.csr** na **Mycsr_XXXXXXXX_AAAA.txt** (XXXXXXXX je IČO a AAAA je číslo AIS) a pošlete ho 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 popsany v tomto dokumentu (včetně kapitoly 2.4). Např. ho přejmenujte na Private_AAAA.key.

Pokud bude certifikace úspěšná, obdržíte od SZR do aplikace RAZR a 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).

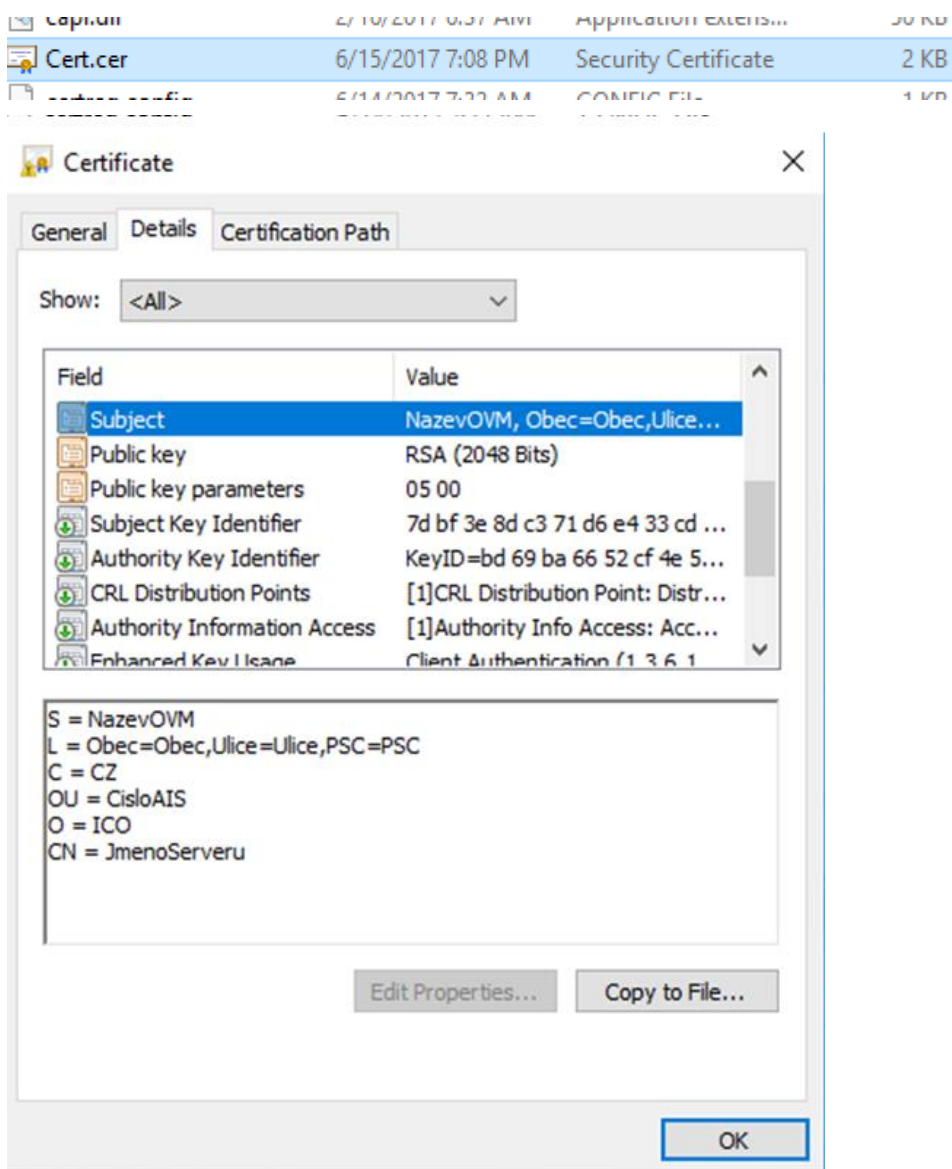
Zkontrolujte obsah certifikátu, že skutečně odpovídá vaší žádosti!

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=Obec,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:e0:7f: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:c8:0f: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:d8:06:99: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:00:aa:9c:09:
        e9:90:b9:da:02:f2:47:1f:d1:67:39:51:74:6e:47:
        1d:53:1d:87:90: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:03:E3:27:AF:85:25:0B:BC:8
    X509v3 CRL Distribution Points:
      Full Name:
      URI:http://crliszr1.egon.gov.cz/ISZRRootCA.crlCA.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:d5:07:40:
      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:09:
      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:b7:79:ce:d1:54:d5:
      49:90:2b:e7:3f:1d:9e:fb:09:10:8d:6b:c8:4a:e7:12:e6:34:
      72:8f:90:dd:f5:56:1f:a5:78:35:40:91:5c:10:17:31: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-----
  MIIEmDCA4CgAIBAgIKY17A7wAABAAAEBDANBgkqhkiG9w0BAQsFADA3MTUwMwYD
  VQDDCxIbmZvcmlhY25pIHNSc3R1b5S6YwtsYWRuaWNoIHJ1Z21zdHJ1IFN1YkN
  MTAEF0xNzA2MjUxNzA4NDhAF0YMDA2MTQxNzA4NDhAMIGAMRUwEYDQQDEWxk
  bWVub1N1cnZlcmludDAkBgNVBAQTA010TERMA8GA1UECxiIQ21zbG9BSVhxCzA1
  BgNVBAYTAkNAc2V5IjYVDQYwYDQDEWxkYjYxNjY3YDQDEWxkYjYxNjY3YDQDE
  QZERMA8GA1UECmI1MTMfZ6XZPVk6kwgEiMA0GCSCqGS1b3DQEBAQUAA4IDWAwggE
  KAAQBAQCg1P45Tz9VpQ2HF/KpkE3K6FC5:F6sXC4n0ZnqDFVW4di3ff05/fzB09
  U7hdy7cM1Z2ZQLVjMxi+Q/3SU6H8NemV09KvJ7SeAp12vdy9yizxPID78wayJdGf
  YI9fGzDcEIq3n6R451pFkYeUWneU1VKTnpwUXFrTW12c1SDAL9Z0LnUErFFQm/
  9qBjvo+s12tKCFsWdlVDFptXzWu9mouMhnyHpngeb0G0P9/GZHp4Nz7FAFXVnq5
  mk3ZwV5/Woq54m0QD+RU0MvR4KqcCemQudoc8kcF0wC5UXRUrX:1THyEzW5Cj2qjP
  dYpCC05+52gicZLRUjWnZ5/parZRAgMBAAGJggFahiIBVjadBgNVHQ4EFQwUfb8+
  jcnX:1uQzU7c5S6jmmPUKgwHnyDVR0jBBggFoAUwVm6Z1LPT1qq1A+D4yevtSUL
  VIGwaYDVR0fBGEGXzBdoFugMvYZahR0cDovL2Nybg1ZenIxLmVnb24y21zL01T
  W1J5b290Q9EUY33sMH5GCCsGAQuFBWBBG8wBTazBggrrBggEFBQCwA0YnaHR0cDov
  L2Nybg1ZenIxLmVnb24y21zL01TW1J5b290Q9EUY33sMH5GCCsGAQuFBzAChiPo
  dHRwOi8yY3ZsXN6c3JlZUzdWdvi5nb3Yy0vSvNVnaul3yb3RDQ553cnQwDgV0DVR0
  AQH/BAQDAgMB0GA1UdJQQMBQGCCsGAQuFBWCBggrrBggEFBQCwDATANBgkqhkiG
  9w0BAQsFAAQCAQEAeUhmG5jXx8B/ECSChGk+WxUMGEE0QZkKcKyCaL/Ft10WYi1
  X0BSXNkXep8Pw1j2Pp1p/12mUtUfo3fNuh7RuTyjRYNEDvp9Hxcoh48mCfwk
  Open1wdApun8ncz7tWpZp85eZkKudKEBSSXIAjU8T1rhiCfQ4zft8Wp4iooVdh
  5y1xT6eN3WGISHwT31J5/XV8DbxYEH7bIua5mZ3Fc8G+1JmvvP0Y6JwCPVkr9K4
  YK0SGAZAZ2RIAaHuH3D00VTVSZA528dnvsJEI1ryErnEuYco+Y3FVW6V4NUCR
  XBgXhBRV9zvH2CT1Bz7w5b12eHfh41dQJqVKpA==
  -----END CERTIFICATE-----
c:\Openssl\bin>
```

nebo použijte standardní prohlížeč certifikátů MS Windows:



2.4 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 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, ISSS nebo jinými AIS. 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

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.