

## Návod na vytvoření žádosti o digitální certifikát s OpenSSL

Verze dokumentu:	3.5
Datum vydání:	9. září 2024
Klasifikace:	Veřejný dokument

## Obsah

<b>1.</b>	<b>Vydávání certifikátů .....</b>	<b>3</b>
<b>2.</b>	<b>Postup pro získání certifikátu .....</b>	<b>3</b>
2.1	Příprava konfiguračního souboru pro vygenerování klíčového páru .....	3
2.2	Subject Alternative Name .....	5
2.3	Generování klíčového páru .....	7
2.4	Vytvoření žádosti o certifikát .....	7
2.5	Odeslání žádosti o certifikát .....	8
2.6	Převzetí certifikátu .....	8
2.7	Spojení certifikátu se soukromým klíčem .....	9
<b>3.</b>	<b>Použití certifikátu a soukromého klíče .....</b>	<b>10</b>

## 1. Vydávání certifikátů

Certifikáty vydávané Certifikační autoritou (CA) Digitální a informační agentury (DIA) jsou určeny 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. Tato 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 základních registrů a ISSS stejný. Správce AIS určuje v žádosti, 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 doporučujeme používat aplikaci GeneratorCertRAZR, která nabízí grafické uživatelské rozhraní. Aplikace je na [webu DIA](#).**

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

Pro vytvoření žádosti je možné použít jakýkoli software, který vytváří žádosti o digitální certifikát podle příslušných standardů.

**Tento dokument popisuje vytvoření žádosti o certifikát s použitím freeware OpenSSL** pod operačním systémem MS Windows.

## 2. Postup pro získání certifikátu

Program OpenSSL 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.

### 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 (webová aplikace pro správu přístupů do základních registrů) požádejte o vydání certifikátu pro vámi spravovaný AIS a soubor s žádostí připojte jako přílohu.
- RAZR předá žádost o certifikát CA DIA.
- CA DIA vydá certifikát a předá ho aplikaci RAZR.
- RAZR zařídí odeslání certifikátu do vaší datové schránky a umožní vám stažení certifikátu přímo z aplikace RAZR.
- Certifikát a soukromý klíč nainstalujete na všechna zařízení (servery, firewally, komunikační sběrnice, SSL koncentrátory, HSM apod.) tak, aby AIS mohl komunikovat s ISZR anebo s ISSS anebo s jinými AIS.

### 2.1 Příprava konfiguračního souboru pro vygenerování klíčového páru

Konfigurační soubor vytvoříte pomocí editoru, např. Notepad.

## DIGITÁLNÍ A INFORMAČNÍ AGENTURA\_

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** FQDN, ze kterého AIS komunikuje. Maximální délka 64 znaků. Např. spis.subjekt.cz. V případě, že chcete, aby AIS vystupoval vůči ISSS jako publikační, uveďte DNS jméno, které je součástí URL, na kterém ISSS s AIS komunikuje. Toto jméno musí být z domény cms2.cz s uvedeným číslem vašeho AIS, tj.

- aisXXXX.egsb.cms2.cz – produkční prostředí
- aisXXXX-test.egsb.cms2.cz – testovací prostředí.

Příklady:

- ais1234.egsb.cms2.cz
- ais1234-test.egsb.cms2.cz

Pokud zde publikační AIS nebude mít jednu z výše uvedených možností, je potřeba toto jméno uvést do alternativního DNS jména (Subject Alternative Name), viz dále.

**ICO** IČO správce AIS nebo identifikátor správce AIS 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 (nebo dříve SZR) v případě, že AIS není v RPP doplněný o informaci, zda jde o žádost o přístup do produkčního (/PROD) nebo testovacího (/TEST) prostředí základních registrů anebo ISSS.

Příklady:

```
123/PROD
567/TEST
```

Může být doplněné o informaci, že jde o certifikát pro publikaci na ISSS.

Příklad: 123-P/PROD

Maximální délka 64 znaků,

**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
- rozlišení produkce / test

## 2.2 Subject Alternative Name

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

- Potřebujete vydat certifikát pro více DNS jmen.
- Pokud se jedná o publikační AIS a potřebujete vyplnit DNS jméno, které je součástí URL, na kterém ISSS s AIS komunikuje (a nebylo možné toto jméno uvést v rámci položky JmenoServeru). Uveďte jej ve formátu:
  - aisXXXX.egsb.cms2.cz – produkční prostředí
  - aisXXXX-test.egsb.cms2.cz – testovací prostředí

Příklady:

- ais1234.egsb.cms2.cz
- ais1234-test.egsb.cms2.cz
- Potřebujete použít certifikát pro komunikaci s nějakým AIS, který vyžaduje mít vyplněný atribut SAN.

*Poznámka: ISZR ani ISSS nevyžadují vyplněný atribut 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 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 = JmenoServeru
```

**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
```

## DIGITÁLNÍ A INFORMAČNÍ AGENTURA\_

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

### Příklad 1 – čtenářský AIS v testovacím prostředí bez alternativního DNS jména:

```
distinguished_name = req_distinguished_name  
string_mask        = nombstr  
prompt             = no  
[req_distinguished_name]  
0.commonName      = razr-test.egon.gov.cz  
0.organizationName = 17651921  
organizationalUnitName = 8625/TEST  
countryName       = CZ  
localityName      = Obec=Praha,Ulice=Na Vapence,PSC=13000  
stateOrProvinceName = Digitalni a informacni agentura
```

### Příklad 2 – čtenářský AIS v produkčním prostředí se dvěma alternativními DNS jmény:

```
distinguished_name = req_distinguished_name  
string_mask        = nombstr  
prompt             = no  
req_extensions     = req_ext  
[req_distinguished_name]  
0.commonName      = razr-test.egon.gov.cz  
0.organizationName = 17651921  
organizationalUnitName = 8625/PROD  
countryName       = CZ  
localityName      = Obec=Praha,Ulice=Na Vapence,PSC=13000  
stateOrProvinceName = Digitalni a informacni agentura  
[req_ext]  
subjectAltName     = @alt_names  
[alt_names]  
DNS.1 = razr-test.dia.gov.cz  
DNS.2 = razr-test.szrcr.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

### 2.3 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.

```
C:\OpenSSL\bin>openssl genrsa -aes256 -out Private.key 3072
Generating RSA private key, 3072 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 zašifrované klíče (soukromý a veřejný) 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**

```
C:\OpenSSL\bin>c: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.

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	6/11/2023 8:23 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
osstest.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	6/11/2023 8:20 AM	Registration Entries	3 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**

## 2.5 Odeslání žádosti o certifikát

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.

- RAZR z Internetu: <https://razr.egon.gov.cz/>
- RAZR z KIVS: <https://razr.egon.cms2.cz/>

**Soubor Private.key 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. Např. ho přejmenujte na Private\_AAAA.key.

## 2.6 Převzetí certifikátu

Pokud bude certifikace úspěšná, obdržíte do aplikace RAZR a do datové schránky certifikát v souboru **YYYYMycsr\_XXXXXXXX\_AAA.txt** (YYYYY je číslo, které přidělil RAZR). Přejmenujte ho na **Cert.cer** (nebo na jiné jméno podle vašich potřeb nebo konvencí).

Capi.dll	2/16/2017 6:37 AM	Application extens...	56 KB
Cert.cer	6/15/2017 7:08 PM	Security Certificate	2 KB
certreq.config	6/14/2017 7:32 AM	CONFIG File	1 KB

**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=136
    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.

## 2.7 Spojení certifikátu se soukromým klíčem

Pokud váš AIS vyžaduje certifikát a privátní klíč v jednom souboru ve formátu PKCS12, můžete použít OpenSSL k vytvoření souboru v uvedeném formátu.

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 zašifrovaný a chráněný 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, HSM 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.

**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.**