DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

Návod na vytvoření žádosti o digitální certifikát s OpenSSL

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

Obsah

1. Vydávání certifikátů

Certifikáty vydávané Certifikační autoritou (CA) Digitální a informační agentury (DIA) jsou určené 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.

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 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 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
```

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

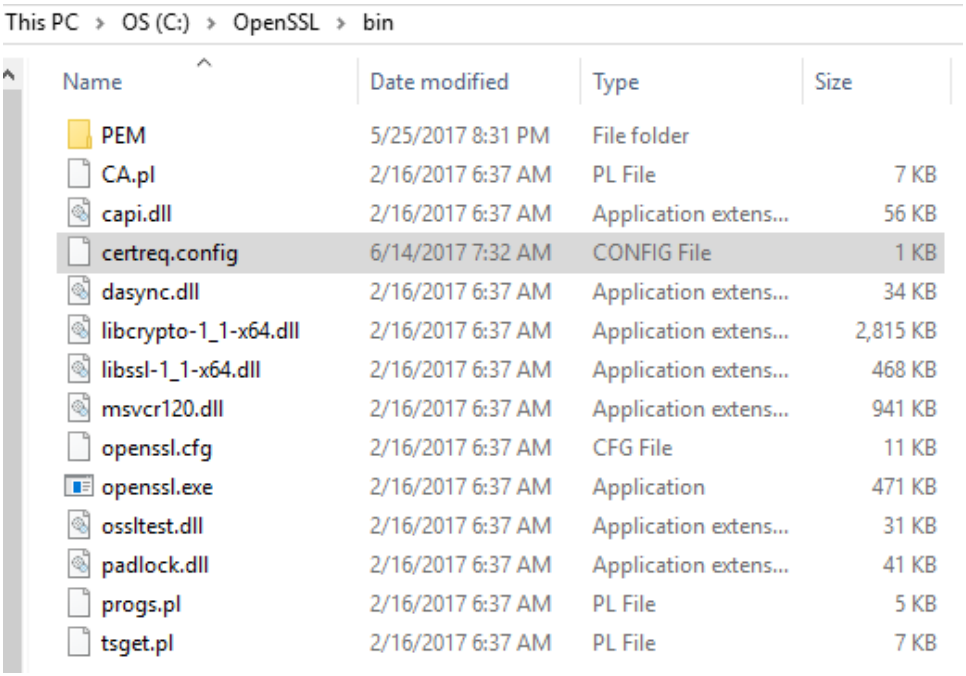
Příklad 1 – čtenářský AIS v testovacím prostředí bez alternativního DNS jména:

```
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 dvěmi 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.



2.3 Generování klíčového páru

V adresáři bin programu OpenSSL zadejte příkaz:

openssl genrsa –aes256 -out Private.key 3072

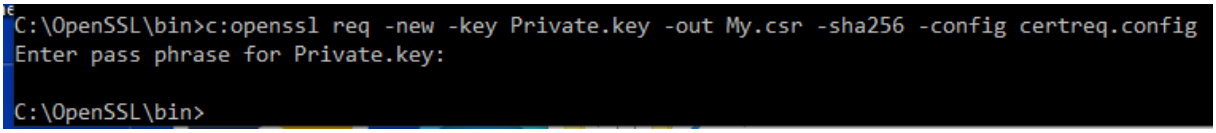
Po spuštění příkazu budete vyzváni k definici hesla a k jeho následnému ověření.

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

2.4 Vytvoření žádosti o certifikát

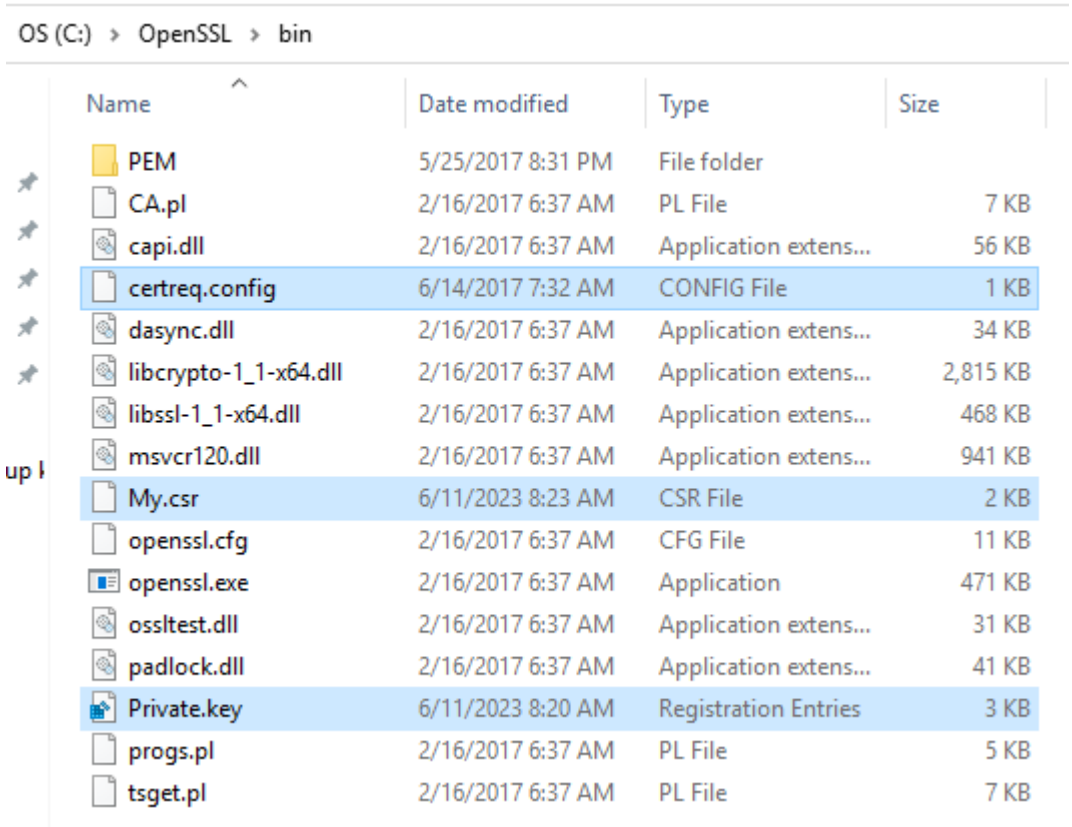
V adresáři bin programu OpenSSL zadejte příkaz:

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



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

2.5 Odeslání žádosti o certifikát

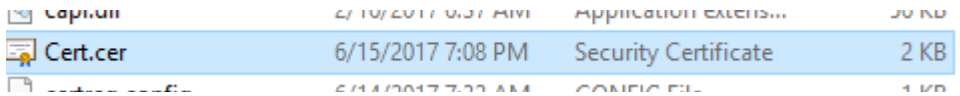
Přejmenujte soubor **My.csr** na **Mycsr_XXXXXXXX_AAAA.txt** (XXXXXXXX je IČO a AAAA je číslo AIS) a pošlete ho v příloze formuláře vyplněného v aplikaci RAZR k certifikaci vašeho veřejného klíče.

- 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 popsaný v tomto dokumentu. Např. ho přejmenujte na Private_AAAA.key.

2.6 Převzetí certifikátu

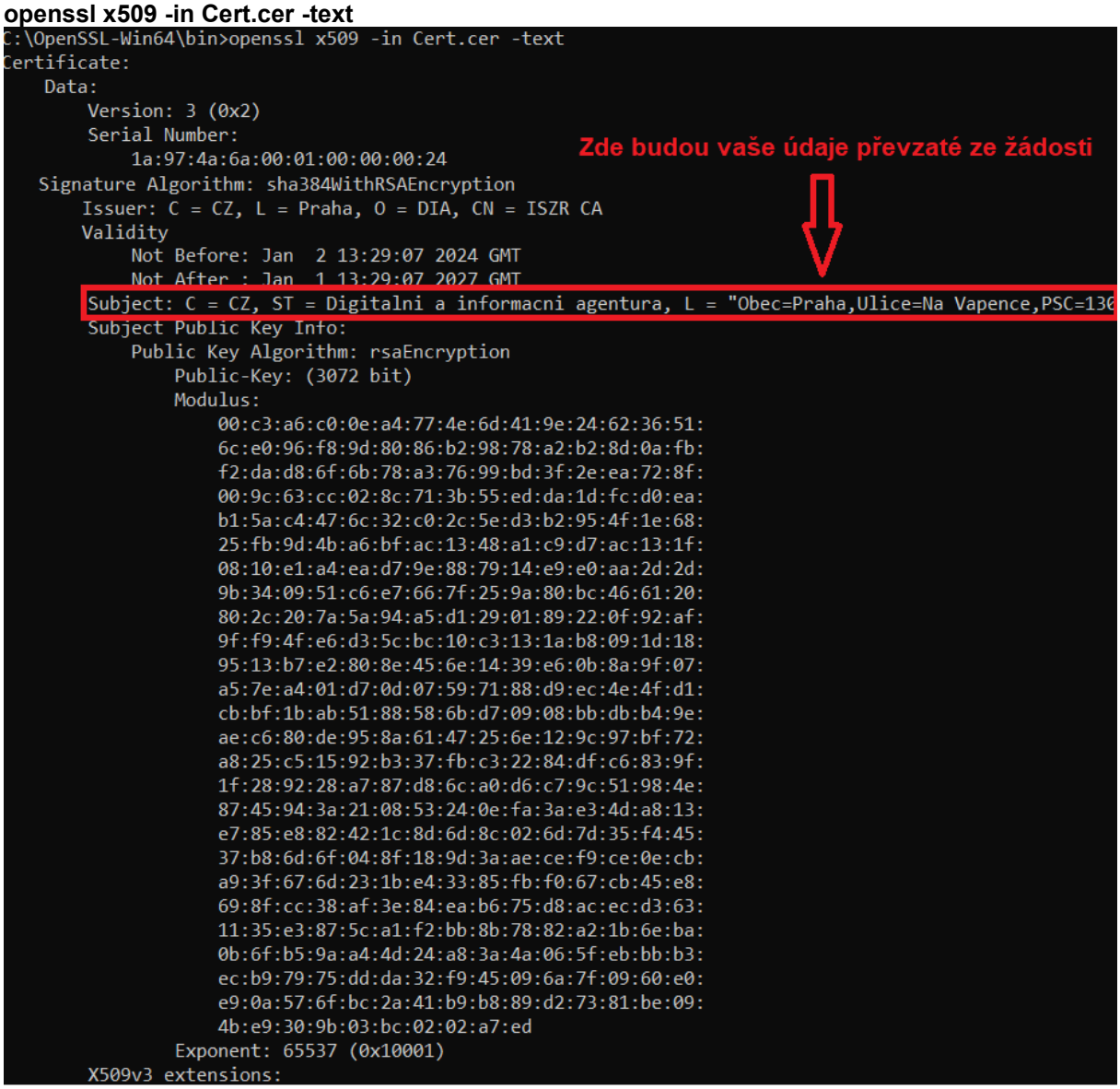
Pokud bude certifikace úspěšná, obdržíte do aplikace RAZR a do datové schránky certifikát v souboru **YYYYYMycsr_XXXXXXXX_AAA.txt** (YYYYY je číslo, které přidělil RAZR). Přejmenujte ho na **Cert.cer** (nebo na jiné jméno podle vašich potřeb nebo konvencí).



Zkontrolujte obsah certifikátu, že skutečně odpovídá vaší žádosti!

Například v adresáři bin programu OpenSSL zadejte příkaz:

openssl x509 -in Cert.cer -text



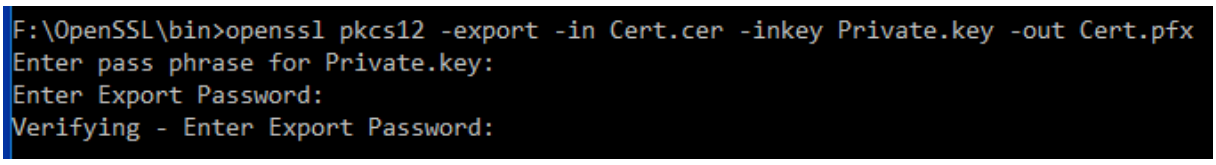
nebo použijte standardní prohlížeč certifikátů MS Windows.

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



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.